Regolamento della Funzione Compliance

Regolamento emesso il 22/12/2023
Owner del processo: Funzione Compliance

INDICE

1. PREMESSA

Il presente documento richiama gli obiettivi, i processi e la mission della Funzione Compliance di Flowe S.p.A. (di seguito anche "Flowe"), nell'ambito del Gruppo Bancario Mediolanum (di seguito anche ""Gruppo Bancario" o Gruppo").

La Funzione *Compliance* (di seguito anche "Funzione") di Flowe è responsabile del processo di verifica e presidio del rischio di non conformità alle norme, nel novero del proprio perimetro di attività identificato a partire dall'attività aziendale secondo un approccio *risk based.*

Nell'ambito del presidio del rischio assumono rilevanza i controlli di linea (c.d. "controlli di primo livello"), "*diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse strutture operative (ad esempio, controlli di tipo gerarchico, sistematici e a campione). Le strutture operative sono le prime responsabili del processo di gestione dei rischi: nel corso dell'operatività giornaliera 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*[1]*".*

Il presente Regolamento illustra quindi l'architettura organizzativa ed i processi adottati dalla Funzione Compliance per il soddisfacimento della propria mission e le responsabilità/compiti.

[1] Circolare n. 285 della Banca d'Italia del 17 dicembre 2013 (Parte I, Titolo IV, Capitolo III, Sezione I, Paragrafo 6 "Principi generali") e successivi aggiornamenti.

1.1 OBIETTIVI DEL DOCUMENTO

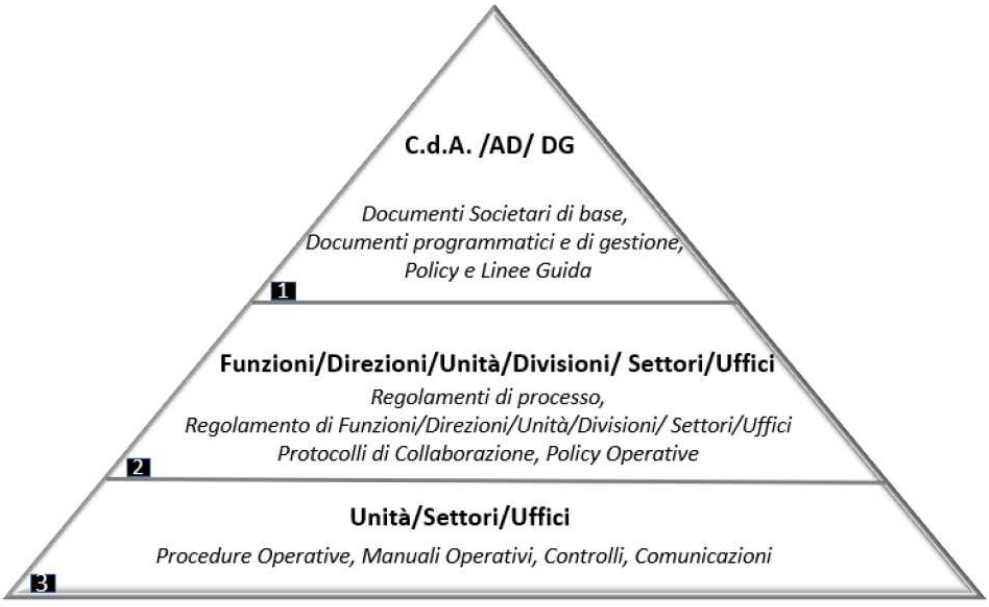
Il presente documento ha l'obiettivo di:

- dare attuazione ai principi guida contenuti nel documento "Compliance Policy[2]";
- definire l'ambito di attività e responsabilità della Funzione Compliance, in relazione agli adempimenti volti ad assicurare la piena conformità *(compliance)* con i requisiti definiti dalle Autorità di Vigilanza;
- dettagliare quanto già delineato nell'Ordinamento dei Servizi della Capogruppo, in relazione all'assetto organizzativo, ai compiti e alle responsabilità;
- descrivere gli obiettivi gestionali interni e i principali processi riconducibili alla Funzione;
- descrivere le principali interrelazioni con la Funzione Compliance della Capogruppo e con le altre Unità Organizzative ed i relativi Flussi informativi, ove presenti.

* * *

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

Modello della normativa interna di riferimento



[2] Compliance Policy approvata dal Consiglio di Amministrazione di Flowe in data 12/12/2023.

1.2 STRUTTURA DEL DOCUMENTO

Il Regolamento si compone complessivamente di n. 5 capitoli incluso il presente. Di seguito, sono descritte sinteticamente le principali tematiche trattate in ogni capitolo.

Capitolo 2: Gli attori coinvolti

Il Capitolo illustra la mission, la struttura organizzativa e le principali responsabilità della Funzione *Compliance*, nell'ambito del contesto organizzativo di Flowe S.p.A e della Capogruppo Banca Mediolanum S.p.A..

Capitolo 3: I processi

Il Capitolo descrive il quadro di riferimento dei processi operativi della Funzione, delle fasi ed attività che li compongono, dei principali output e presidi di controllo in essere. Nello specifico vengono descritte le attività di planning, di svolgimento delle attività "ex-ante" ed "ex-post" della Funzione, nonché le attività di Reporting.

Capitolo 4: Interrelazioni con Organi, altre Società del Gruppo ed altre Unità Organizzative

Il Capitolo illustra le modalità di coordinamento della Funzione Compliance con le altre Funzioni di Compliance "locali", nonché le principali interazioni con altri Organi ed unità organizzative del Gruppo.

Capitolo 5: Il quadro normativo di riferimento

Il Capitolo sintetizza il quadro normativo di riferimento delle attività svolte dalla Funzione, considerando le disposizioni normative "esterne" (normativa di primo e secondo livello) e quelle interne connesse allo svolgimento dell'attività di Compliance.

2. La Funzione Compliance

La Funzione Compliance di Flowe riporta al Compliance Officer della Società, nominato dal Consiglio di Amministrazione.

2.1 RUOLO E RESPONSABILITÀ

La Funzione Compliance di 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 presidiati direttamente dalla Funzione.

In particolare, per gli ambiti normativi applicabili a Flowe, coerentemente alle linee guida di indirizzo e coordinamento della Capogruppo, svolge le seguenti attività:

- presidia l'evoluzione della normativa e della regolamentazione internazionale e nazionale applicabili a Flowe;
- raccoglie, indirizza e coordina le fasi di consultazione attivate dai *Regulator* o dalle Associazioni di categoria;
- identifica gli impatti rivenienti dallo sviluppo della normativa, redigendo, ove necessario un documento di Gap Analysis normativa, gli adeguamenti necessari per garantire il presidio del rischio di non conformità alle norme, avvalendosi delle funzioni aziendali interessate per l'attivazione delle iniziative necessarie alla definizione, programmazione e realizzazione degli specifici interventi rivenienti dagli adeguamenti identificati;
- fornisce il supporto alle funzioni aziendali interessate per l'attivazione delle iniziative necessarie alla definizione, programmazione e realizzazione degli adeguamenti necessari per colmare i gap normativi identificati e garantire il presidio del rischio di non conformità, monitorando la 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;
- valuta *ex ante* proposte di modifiche, anche organizzative e procedurali, derivanti 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, monitorandone il successivo follow up prima dell'entrata in vigore della norma o dell'avvio della nuova attività/business;
- fornisce consulenza specialistica ed assistenza agli Organi Aziendali e alle altre funzioni di Flowe sugli ambiti di pertinenza;

- valuta *ex ante* la conformità alla regolamentazione applicabile di tutti i progetti innovativi che Flowe intenda intraprendere con riferimento, in particolare, agli obblighi di *product governance* per la commercializzazione di nuovi prodotti e servizi (o alle modifiche sostanziali apportate ai prodotti, processi e sistemi esistenti) e alla modifica del sistema premiante aziendale;
- valuta le procedure organizzative per le tematiche in cui assumono rilevanza significativa gli aspetti di compliance;
- predispone/aggiorna le policy di Flowe relative agli ambiti normativi presidiati direttamente dalla Funzione Compliance;
- valida le policy e gli altri documenti di normativa interna (linee guida, regolamenti di processo, policy e procedure operative ad esclusione dei manuali, documenti societari di base e documenti programmatici e di gestione) in funzione delle normative dalla stessa presidiate come individuate dal modello di Compliance di volta in volta vigente, in linea con quanto previsto dalla "Policy di Conglomerato sulle modalità di redazione, aggiornamento, approvazione e diffusione della Normativa Interna";
- supporta le strutture preposte nell'attività di definizione/pianificazione dell'attività di formazione alle diverse unità organizzative sulle materie di pertinenza in cui assume rilievo il rischio di non conformità;
- produce le informazioni relative alle fasi del processo di compliance di competenza ai fini dell'informativa periodica verso gli Organi Aziendali e le Autorità di Vigilanza;
- partecipa ai gruppi di lavoro associativi per tematiche specialistiche di competenza;
- supporta, con l'ausilio dell'Unità Framework, Reporting & Coordinamento di Gruppo, il Compliance Officer nella predisposizione del piano delle verifiche sui processi afferenti alle aree normative presidiate direttamente dalla Funzione, in coerenza con il framework di compliance;
- esegue le verifiche pianificate e procede alla loro formalizzazione, successivamente alla condivisione tramite "exit meeting" con le Unità Aziendali di riferimento, mediante i seguenti documenti:
    - Report di Compliance: contenente le valutazioni dello stato di conformità alle norme del processo analizzato, il riepilogo dell'attività svolta, le eventuali azioni di mitigazione rilevate e le date fornite dal management per la loro risoluzione;
    - Allegato al Report: contenente il dettaglio delle analisi effettuate e i relativi esiti, in termini di adeguatezza ed efficacia per la valutazione dei presidi adottati da Flowe al fine di mitigare i rischi di non conformità;

- definisce e svolge opportune verifiche, anche analizzando appositi indicatori di sintesi e di dettaglio, avvalendosi del supporto dell'Unità Framework, Reporting & Coordinamento di Gruppo per la realizzazione degli stessi;
- produce le informazioni relative alle fasi del processo di compliance di competenza, ai fini dell'informativa periodica verso gli Organi Aziendali e le Autorità di Vigilanza.

2.2 PRINCIPALI STRUMENTI UTILIZZATI

A supporto delle diverse attività di compliance, la Funzione Compliance della Capogruppo si è dotata di un applicativo GRC (Governance-Risk Management-Compliance), denominato Sphera, il cui perimetro di adozione ricomprende anche le società italiane del Gruppo Bancario.

La Funzione Compliance utilizza inoltre nel continuo servizi di «informativa regolamentare» forniti da un Provider specializzato leader di mercato, attraverso sia l'accesso ad un Portale dedicato sia la ricezione giornaliera via posta elettronica degli aggiornamenti relativi ai singoli servizi (alert specialistici su novità normative e regulatory news, inventario strutturato degli obblighi normativi, sanzioni comminate dalla vigilanza organizzate per area tematica, ecc.).

3. I PROCESSI

Il processo di *compliance* di cui si è dotata Flowe prevede l'adozione del *framework* definito dalla Capogruppo Banca Mediolanum, in grado di garantire un adeguato presidio degli ambiti normativi individuati. Spetta infatti alla Funzione Compliance l'identificazione, con periodicità almeno annuale, del quadro normativo applicabile e rilevante, 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 a Flowe (c.d. *Rule Map*) e valutare l'adeguatezza dei presidi in essere.

La Funzione Compliance presidia il rischio di non conformità con riferimento alle normative rientranti nel perimetro identificato, quali, a titolo di esempio, quelle connesse alla gestione dei conflitti di interesse, alla trasparenza nei confronti della clientela, agli ambiti ICT e di sicurezza e, più in generale, alla disciplina a tutela del consumatore.

Nell'ambito delle normative rientranti nel perimetro di competenza, la Funzione Compliance presidia inoltre i rischi di non conformità correlati ad ambiti che impattano trasversalmente i

processi aziendali, quali 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.

Al fine di garantire uniformità nella gestione del rischio di non conformità da parte delle differenti unità organizzative coinvolte, Flowe, in linea con il modello definito dalla Capogruppo, 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.

3.1 FRAMEWORK

L'attività consiste nella definizione delle metodologie per la valutazione del rischio di non conformità, 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.

La responsabilità del presidio del *framework* compete all'Unità Framework Reporting & Coordinamento di Gruppo, che si avvale del supporto della Funzione, per quanto di propria competenza, al fine di proporre al Responsabile eventuali aggiornamenti o interventi che si rendono necessari.

3.2 PLANNING

Di seguito si descrivono le fasi dell'attività di gestione e controllo del rischio di non conformità relative alla definizione dello "*scoping*" normativo e alla pianificazione delle attività di Compliance.

3.2.1 SCOPING NORMATIVO

L'attività di *scoping* normativo consiste nella definizione e nel successivo monitoraggio del quadro normativo rilevante per Flowe. La finalità è quella di confermare/aggiornare su base annuale l'elenco delle normative in perimetro di interesse per Flowe, in base agli ambiti di rilevanza per la Funzione e per il business aziendale. Tale elenco prende il nome di "*Rule Map*", che tiene conto, anche tramite l'attività di *alert* normativo, degli aggiornamenti che intervengono di volta in volta.

Qualora una norma abbia i requisiti per impattare sul *business* della società in termini di rischio di non conformità (considerato in relazione, ad esempio, alla dimensione, complessità e trasversalità dei processi rilevanti ed ai prodotti offerti), essa viene inclusa nel perimetro normativo di riferimento.

La *Rule Map* viene formalizzata nell'ambito della relazione annuale presentata dalla Funzione al Consiglio di Amministrazione, specificando gli ambiti normativi in perimetro diretto: normative rilevanti per Flowe e/o quelle fatte ricadere espressamente in tale perimetro dalle normative vigenti.

3.2.2 PIANIFICAZIONE DELLE ATTIVITA' DI COMPLIANCE

L'attività di pianificazione delle attività di controllo della Funzione Compliance viene svolta considerando un orizzonte temporale triennale, con un maggiore dettaglio su base annuale relativo al nuovo esercizio in apertura.

La pianificazione prevede un aggiornamento ed una validazione annuale dei processi aziendali in perimetro, da svolgersi di norma entro il primo trimestre dell'esercizio. Tale attività genera la predisposizione di un programma di attività di controllo da sottoporre agli Organi aziendali, in cui sono identificati i processi aziendali che espongono maggiormente Flowe ai rischi di non conformità, sui quali vengono programmati i relativi interventi di verifica.

L'adozione di una metodologia di valutazione del rischio di non conformità "per processo" permette di efficientare le attività di controllo, supportando l'identificazione di ruoli, compiti e responsabilità delle unità organizzative aziendali a cui è demandato lo svolgimento delle diverse fasi del processo, la valutazione di rischi, presidi e controlli sottesi ed eventualmente, se del caso, la proposta di azioni di mitigazione per ridurre il rischio di non conformità rilevato.

La metodologia adottata per l'individuazione della rischiosità dei processi tiene conto non solo del profilo sanzionatorio espresso dalla normativa, ma anche di taluni elementi

aggiuntivi, internamente alla Funzione definiti *driver*, quali l'analisi dei rilievi emessi dalla Funzione Internal Audit e l'esistenza di eventuali azioni di mitigazioni in essere, qualora riferiti ai processi in esame.

Di seguito si dettagliano gli step operativi metodologicamente previsti dal processo di pianificazione:

a) A fronte dei processi aziendali in perimetro, verifica dell'associazione dei Compliance Risk (in breve anche "CR") ai processi stessi e associazione degli eventuali nuovi CR ai processi di competenza. Il CR esprime uno specifico adempimento richiesto da una determinata normativa, per non incorrere in sanzioni di natura giudiziaria o amministrativa, perdite finanziarie rilevanti o danni reputazionali. I CR vengono forniti e aggiornati su base mensile da una società terza, che presta servizi di informativa regolamentare alla Funzione. Ogni CR è caratterizzato da un grado di rischio a 4 livelli, in funzione della severità dell'impatto sanzionatorio (Serious, High, Medium, Low).
b) Determinazione del Rischio Inerente di processo (di partenza), in base alla media dei risk impact associati ai singoli CR agganciati al processo in esame. Il grado di rischio è declinato in 4 livelli, utilizzando la scala adottata da tutte le Funzioni Aziendali di Controllo in ottica di uniformità di reportistica (Alto, Medio Alto, Medio Basso, Basso).
c) Applicazione di specifici elementi di personalizzazione/normalizzazione (c.d. *driver*) riferiti alla Società in esame, al fine di determinare il Rischio Inerente di processo (finale), sempre declinato in 4 livelli (Alto, Medio Alto, Medio Basso, Basso):
    - Esiti degli audit impattanti aspetti attinenti alla Compliance e riferiti al processo specifico (es. il mancato aggiornamento di una procedura operativa o di una Policy), sulla base delle informazioni fornite dalla Funzione Internal Audit (relazione al 30/09);
    - Azioni di mitigazione emesse dalla Funzione Compliance e ancora in corso, con riferimento al processo specifico;
    - Eventi di perdita registrati dalla Funzione Risk Management – Operational Risk, caratterizzati da esborso superiore all'importo di 10.000 Euro, se occorsi negli ultimi 5 anni, con riferimento al processo specifico (fonte: Operational Risk – Applicativo Op-Risk);
    - Presenza di punto di controllo registrato dalla Funzione Risk Management – Operational Risk associato al processo specifico (RFCA – Risk Factor Control Assessment), se con rating inferiore ad «Efficace» (fonte: Operational Risk – Applicativo Op-Risk);
    - Rischio residuo verifiche precedenti: esito di eventuali verifiche svolte nei tre anni precedenti dalla Funzione Compliance sul medesimo processo.

Con riferimento agli ambiti ICT e sicurezza, presidiati dall'Unità ICT Compliance e Advisory & Controls Flowe della Capogruppo, si applicano specifici elementi di personalizzazione/normalizzazione (c.d. *driver*) relativi agli aspetti ICT:

- Azioni di mitigazione emesse dall'Unità ICT Compliance e Advisory & Controls Flowe della Capogruppo, in ambito ICT e ancora in corso, con riferimento al processo specifico;
- Presenza di rilievi degli audit impattanti aspetti attinenti alla ICT Compliance e riferiti al processo specifico sulla base delle informazioni fornite dalla Funzione Internal Audit (relazione al 30/09);
- Eventi di perdita in ambito ICT registrati dalla Funzione Risk Management, caratterizzati da esborso superiore all'importo di 10.000 Euro, se occorsi negli ultimi 5 anni, con riferimento a specifiche tipologie di evento (fonte: Operational Risk – Applicativo Op-Risk);
- Rischio residuo verifiche precedenti in ambito ICT: esito di eventuali verifiche svolte nei tre anni precedenti dalla Funzione Compliance sul medesimo processo;
- Presenza di gravi incidenti operativi e di sicurezza, in ragione del perimetro normativo presidiato, se occorsi negli ultimi 3 anni.

A fronte del rischio inerente finale associato a ciascun processo in perimetro, il Responsabile dei Controlli ha comunque facoltà di modificare in incremento o decremento la severità del relativo grado di rischio, motivandone le ragioni. Successivamente vengono identificati i processi da assoggettare a verifica per il nuovo anno e per i due anni successivi, in ottica di pianificazione triennale, tenendo altresì conto dei seguenti aspetti:

- Obbligatorietà della norma nel richiedere verifiche su base annuale, ovvero un flusso informativo periodico verso gli Organi;
- Evoluzione della normativa esterna;
- Evoluzione del business della società;
- Copertura dei processi caratterizzati da maggiore rischiosità nell'arco di una pianificazione triennale complessiva.

Anche le c.d. Gap Analysis normative svolte dalla Funzione, qualora ritenute rilevanti, possono essere utilizzate come elemento di attenzione per una pianificazione delle attività di controllo di Compliance.

Ulteriori valutazioni potranno in ogni caso essere effettuate a fronte delle attività rivenienti dall'analisi dei reclami ricevuti dalla clientela, da istanze provenienti dalle Autorità di Vigilanza e da evidenze rilevate dagli indicatori a distanza (Key Compliance Indicators) monitorati dalla Funzione Compliance.

Il piano delle verifiche costituisce parte integrante della Relazione Annuale della Funzione e, come tale, viene sottoposto per approvazione al Consiglio di Amministrazione di Flowe.

Il Compliance Officer condivide, preliminarmente alla finalizzazione e presentazione al Consiglio di Amministrazione, i singoli piani di lavoro con il Compliance Officer di Gruppo.

Nella periodica relazione di Flowe viene fornito un puntuale aggiornamento sullo stato di avanzamento delle verifiche pianificate e sui relativi esiti, che viene presentato agli Organi Sociali.

3.3 ADVISORY & CONTROLS

Di seguito si descrivono le attività di gestione e controllo del rischio di non conformità relative alla consulenza e formazione, monitoraggio delle evoluzioni normative, analisi di impatto e valutazioni di adeguatezza ex ante.

3.3.1 CONSULENZA E FORMAZIONE

L'attività, prestata dalla Funzione Compliance, consiste nel fornire:

- Consulenza: finalizzata a prestare assistenza agli Organi Aziendali, all'Alta Direzione ed alle funzioni interessate di Flowe, in tutte le materie per le quali il rischio di conformità assume particolare rilievo, un parere specialistico tramite l'analisi e valutazione del rischio di non conformità riguardante l'adempimento degli obblighi posti dalla normativa.

  L'attività di consulenza può avvenire nell'ambito di progettualità specifiche o gruppi di lavoro nei quali la Funzione di Compliance è coinvolta ovvero può essere avviata a seguito dell'ingaggio da parte delle unità richiedenti. In quest'ultimo caso l'ingaggio può tradursi in una richiesta di valutazione di conformità oppure di parere.

  Le richieste di consulenza vengono inserite dagli Advisor della Funzione competenti per materia sull'applicativo GRC, dal quale vengono generate le e-mail di risposta indirizzate alle unità richiedenti. Il parere, rispetto alla valutazione di conformità, è caratterizzato da una maggiore complessità e prevede la formalizzazione e l'emissione di un documento in forma scritta (Nota di parere), può essere sottoposto anche all'attenzione degli Organi Aziendali. Nel fornire tale parere, la Funzione Compliance è chiamata ad individuare gli

eventuali gap normativi e valutarne il relativo rischio di non conformità ovvero il livello di rischio residuo. Nello specifico, all'interno della Nota di parere, con profondità proporzionata alla natura ed urgenza della richiesta, vengono descritti e commentati i risultati dell'analisi, le possibili soluzioni atte a colmare i *gap* identificati ed eventuali opinioni che la Funzione ritiene necessario segnalare agli interessati.

- Formazione: per quanto riguarda la formazione su tematiche normative, il modello adottato prevede l'attivazione del Settore Formazione Risorse Umane su indicazione della Funzione Compliance, che per quanto di loro competenza, identificano i contenuti ed il perimetro di assegnazione, in funzione del ruolo ricoperto dai discenti, nonché i tempi a disposizione per la fruizione.

La Funzione Compliance può essere chiamata anche a contribuire direttamente alla predisposizione di corsi di formazione relativi alle normative primarie e secondarie di natura bancaria, assicurativa e dei servizi di investimento, provvedendo alla rappresentazione di tali attività nell'ambito della reportistica periodica.

3.3.2 MONITORAGGIO EVOLUZIONI NORMATIVE E ALERT

La Funzione Compliance monitora costantemente l'evoluzione del contesto normativo allo scopo di rappresentare alle strutture interessate di Flowe le novità normative e regolamentari rilevanti (*alert normativo/informativo*) presidiate dalla stessa Funzione e di analizzare i possibili impatti sull'operatività dell'azienda.

L'attività di monitoraggio si basa sulla consultazione diretta di fonti specializzate (es. siti internet e specializzati, siti delle Autorità di Vigilanza), tramite una società terza che fornisce nel continuo servizi di informativa regolamentare e tramite il supporto di ulteriori attori esterni che forniscono un dedicato sistema di *alerting* strutturato e periodico in caso di intervenuta modifica al contesto normativo (es. ABI, Assoreti, Assogestioni, studi legali, ecc.).

In questo ambito, è altresì prevista la partecipazione ad eventuali gruppi di lavoro organizzati dalle associazioni di categoria per le tematiche di competenza.

Nel caso siano intervenute modifiche al contesto normativo di riferimento, gli Advisor della Funzione inviano una comunicazione via e-mail alle Unità organizzative coinvolte (*alert* normativo), avvalendosi dell'applicativo GRC in uso. Vengono allegati una copia della normativa in oggetto e, di norma, un commento relativo ai principali contenuti, alla modalità ed alle tempistiche di eventuale entrata in vigore. Le comunicazioni di *alert* presentano, ove necessario, le eventuali integrazioni evidenziate da gruppi di lavoro presso le Associazioni di Categoria, Autorità di Vigilanza, convegni e seminari.

3.3.3 ANALISI DI IMPATTO E VALUTAZIONI 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:

- identifica gli adempimenti normativi richiesti, rispetto al modello operativo specifico di Flowe;
- identifica i gap normativi e i rischi di non conformità derivanti dall'introduzione dei nuovi adempimenti normativi e trasmette la gap analysis (secondo un format prestabilito) alle strutture organizzative impattate, coinvolgendo, se opportuno, la Direzione Portafoglio Progetti e Sviluppo Organizzativo 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 e per assicurare un adeguato presidio dei rischi di non conformità individuati, richiedendo agli owner di allineare la Funzione rispetto allo stato di implementazione delle soluzioni predefinite, con particolare riferimento ad eventuali necessità di revisione delle stesse, in termini sia 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 o la modifica di quelli esistenti) di Flowe. È pertanto previsto il coinvolgimento della Funzione Compliance nella valutazione ex ante della conformità alla regolamentazione applicabile dalla stessa presidiata di tutti i progetti innovativi che Flowe intenda intraprendere. A tal fine, la Funzione Compliance fornisce consulenza specialistica sui progetti innovativi in cui può rilevare il rischio di non conformità e ne valuta ex ante, su richiesta della funzione proponente ai Comitati interni, la conformità alla regolamentazione applicabile, con riferimento, in particolare, alla commercializzazione di nuovi prodotti e servizi (o di prodotti e servizi già esistenti ma modificati in modo sostanziale o comunque offerti in un nuovo mercato di riferimento) 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 monitora nel continuo che, a seguito dei gap rilevati, le strutture owner provvedano all'implementazione delle azioni condivise secondo la pianificazione definita, avvalendosi dell'attività della Divisione Organizzazione e Project Management laddove coinvolta.

In particolare, la Funzione Compliance è coinvolta dalla struttura aziendale proponente sin dalle fasi di avvio delle iniziative progettuali che presentano le seguenti caratteristiche, al fine di valutarne l'impatto sul rischio di non conformità:

- la realizzazione del progetto prevede una modifica sostanziale del sistema informativo coinvolto;
- la realizzazione del progetto ha notevole rilevanza economica;
- la realizzazione del progetto coinvolge iniziative strategiche;
- la realizzazione del progetto prevede esternalizzazioni;
- la realizzazione del progetto impatta il livello di rischio ICT potenziale con valore pari o superiore ad alto;
- la realizzazione del progetto è finalizzata ad attività di adeguamento su input interno o esterno (rilievi da parte dell'Autorità di Vigilanza).

Nell'ambito delle predette verifiche di adeguatezza "ex ante", rientra la validazione delle policy e dei documenti di normativa interna rilevanti, relativi alle aree normative rientranti nel perimetro normativo identificato (Rule Map) e con riferimento agli aspetti di rischio di non conformità, nel rispetto di quanto previsto dalla "Policy di Conglomerato sulle modalità di redazione, aggiornamento, approvazione e diffusione della Normativa Interna".

Con specifico riferimento alle valutazioni in ambito POG, la Funzione compila la sezione di competenza della specifica Scheda di Notifica di Avvenuta Approvazione (N.A.A), emettendo la propria valutazione in merito ai nuovi prodotti e servizi o modifiche sostanziali degli stessi.

3.4 CONTROLS

Di seguito si descrivono le attività di gestione e controllo del rischio di non conformità relative alle verifiche di adeguatezza e di funzionamento, alle analisi degli indicatori (KCI) e delle azioni di mitigazione. La formalizzazione delle verifiche e l'emissione e monitoraggio delle azioni di mitigazione sono effettuate con il supporto dell'applicativo GRC ed i relativi risultati sono opportunamente documentati e formalizzati.

3.4.1 CONTROLLI EX POST: VERIFICHE DI ADEGUATEZZA E DI FUNZIONAMENTO

Il modello di controllo per processo consente 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, o di una fase del processo, alla normativa vigente. Qualora si rilevi un giudizio di non piena conformità, vengono indicati piani di intervento atti a mitigare o rimuovere gli eventuali gap riscontrati (azioni di mitigazione).

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 degli applicativi informatici in termini di adeguatezza di controlli e attendibilità dei dati elaborati o prodotti, relativamente alle verifiche in esame e, nell'ambito delle verifiche svolte dalla Funzione, anche la verifica della aderenza agli standard tecnici e alle best practice per le materie ICT, oltre che della adeguatezza delle misure di sicurezza previste e del loro efficace funzionamento (ad es. presenza e adeguata approvazione delle policy, corretto svolgimento dei processi di monitoraggio e controllo, previsione di iniziative di formazione, ecc.).

A seguito delle valutazioni sopra descritte possono essere proposte azioni di mitigazione atte 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 ICT a supporto di specifiche fasi del processo;
- iniziative di formazione del personale;
- il rafforzamento dei controlli di linea (c.d. di I livello).

Nell'ambito delle attività di verifica viene effettuata inoltre l'opportuna attività di follow up rispetto ad azioni di mitigazione, aperte o chiuse, emerse nell'ambito del medesimo processo in interventi precedenti.

Lo svolgimento delle singole verifiche prevede le seguenti tre fasi:

1) Predisposizione del Piano di Lavoro
2) Esecuzione della verifica
3) Valutazione della verifica

3.4.1.1. Predisposizione del Piano di Lavoro

Per la definizione del Piano di Lavoro, che descrive l'obiettivo, il perimetro e le attività di verifica dell'intervento, vengono analizzati preliminarmente (fase di assessment) per i processi aziendali indagati, i seguenti aspetti:

- la normativa esterna e interna della materia di riferimento (ambito normativo) ed eventuali aggiornamenti impattanti il business aziendale;
- il complessivo disegno del processo o dei processi esistenti sui quali insiste la verifica;
- l'esistenza di eventuali variazioni significative avvenute nel processo (normative, organizzative, di controllo, ispettive), anche rispetto a precedenti verifiche svolte nel passato;
- eventuali pareri e valutazioni di conformità significativi emessi dalla Funzione, nonché eventuali progettualità in essere riferite all'ambito oggetto di verifica;
- l'identificazione delle unità Organizzative che attuano il processo;
- gli applicativi informatici in uso e le relative modalità di interazione con l'operatività;
- i Compliance Risk che ricadono nel perimetro della verifica e che formeranno oggetto di valutazione;
- i Compliance Risk esclusi dal perimetro della verifica con le relative motivazioni a supporto dell'esclusione;
- gli eventuali KCI rilevati dalla Funzione Compliance e relativi al processo oggetto della verifica.

Nella fase di pianificazione dell'intervento, vengono identificate e formalizzate anche le modalità di svolgimento della verifica (verifiche di impianto e/o di funzionamento), le tempistiche previste per lo svolgimento delle attività ed il team incaricato dell'attività.

Il Piano di lavoro viene condiviso con le Unità Aziendali coinvolte nella verifica di Compliance. Nello specifico, attraverso l'invio di una **Comunicazione formale** (c.d. lettera di avvio verifica) vengono informate le Unità coinvolte nel processo di controllo (principalmente le funzioni responsabili dei processi sottoposti ad esame) e, se in specifici casi, anche i vertici aziendali delle Società interessate dalla verifica. Nella lettera di avvio della verifica, inviata via e-mail, vengono rappresentati gli obiettivi dell'intervento, il team incaricato delle attività ed eventuali osservazioni utili alla comprensione del perimetro dell'iniziativa.

Alla comunicazione segue un ***Entry meeting***, ossia un incontro di avvio operativo della verifica, finalizzato ad approfondire con le Unità Aziendali gli obiettivi dell'intervento di controllo e a raccogliere ulteriori informazioni utili circa il/i processi oggetto di analisi.

3.4.1.2. Esecuzione della verifica

Lo svolgimento della verifica prevede l'esecuzione di analisi documentali e verifiche campionarie atte a valutare, con il supporto di opportune matrici, il valore complessivo dei presidi posti in essere e ad attribuire un valore di rischio residuo al processo analizzato.

I processi oggetto di verifica vengono sottoposti a ricognizione per valutare il loro allineamento ai requirement normativi di riferimento per ciò che attiene all'adeguatezza dell'impianto, al corretto disegno dei presidi e al loro effettivo funzionamento.
Nello specifico, l'attività viene svolta tramite:

- la verifica che quanto disposto dalla normativa esterna di riferimento sia correttamente trasposto nella normativa interna;
- l'analisi di dettaglio del processo/attività;
- interviste con il/i Responsabile/i delle unità aziendali interessate;
- verifiche dirette su base campionaria tramite estrazioni informatiche o analisi documentale.

Le verifiche possono essere di "**impianto**" e/o di "**funzionamento**" a seconda degli obiettivi del controllo e sono, come citato in precedenza, definite preliminarmente nel Piano di Lavoro.
Nello specifico, le verifiche di "impianto", o di adeguatezza, sono finalizzate ad accertare:

- una corretta e chiara assegnazione di ruoli e responsabilità tra le strutture organizzative;
- meccanismi decisionali e sistemi di deleghe interni;
- l'esistenza e l'adeguatezza dei presidi organizzativi;
- la formalizzazione di specifica normativa interna;
- l'adeguatezza degli applicativi informatici;
- l'esistenza di un'adeguata formazione delle risorse umane su tematiche di conformità e della consapevolezza dei rischi che originano dall'operatività.

Le verifiche di "funzionamento", o di efficacia, sono invece finalizzate ad accertare la presenza, la correttezza e l'efficacia dei presidi organizzativi e dei processi decisionali attraverso la verifica diretta, anche su base campionaria, dell'applicazione delle procedure di prevenzione e controllo dei rischi di non conformità.

Nel corso delle verifiche vengono individuati e valutati i presidi al rischio di non conformità che consentono l'eliminazione o la mitigazione del rischio gravante sul singolo processo

oggetto di controllo. In particolare, è necessario valutare la funzionalità e l'affidabilità dei controlli di primo livello rispetto al rischio di subire sanzioni amministrative, pecuniarie o penali.

Le **modalità di esecuzione** delle verifiche ex-post possono ricomprendere:

- verifiche documentali: prevedono l'esame delle evidenze disponibili nell'ambito del sistema dei controlli (a titolo di esempio: documentazione progettuale, documenti di analisi funzionale, analisi andamento KCI se pertinenti, eventuali pareri o valutazioni di conformità emessi dalla Funzione, ecc.);
- interviste alle strutture aziendali owner dei processi tramite la richiesta di informazioni specifiche sui controlli eseguiti.
- reperforming di attività e controlli di I° livello.

Le modalità di esecuzione della verifica, l'approccio utilizzato e gli esiti dell'intervento, vengono formalizzati nei documenti denominati Report e Allegato tecnico della verifica svolta.

A conclusione dell'attività di verifica, la Funzione Compliance fornisce alle aree interessate le risultanze dell'intervento, anche mediante **exit meeting** di condivisione e provvede a richiedere, qualora necessario, l'effettuazione degli interventi volti a sanare nel più breve tempo possibile eventuali gap normativi riscontrati.

3.4.1.3. Valutazione della verifica

La valutazione dei controlli da parte della Funzione Compliance è definita in relazione a specifici fattori connessi all'adeguatezza del processo aziendale oggetto di verifica, nonché all'efficacia e all'efficienza del sistema dei presidi adottati dalla Società.

Per ogni compliance risk di riferimento, le valutazioni comprendono tre principali dimensioni:

- *Process*: l'insieme delle normative interne (per esempio, policy, procedure, manuali operativi), dei relativi controlli con la relativa descrizione dei ruoli e delle responsabilità e verifica della corretta applicazione degli stessi;
- *System*: l'insieme delle procedure di carattere informatico o manuale che supportano lo svolgimento di un processo ed i relativi controlli di linea e verifica della corretta applicazione degli stessi;
- *People*: l'insieme dei programmi e delle attività di formazione sul personale addetto allo svolgimento di un determinato processo o al presidio di un determinato ambito normativo e verifica della corretta applicazione degli stessi.

Con particolare riferimento alle attività di verifica effettuate dall'Unità ICT Compliance e Advisory & Controls Flowe della Capogruppo con riferimento al perimetro ICT, 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 le best practice per le materie ICT, oltre che l'adeguatezza delle misure di sicurezza previste e il loro efficace funzionamento, ove significativo.

La valutazione delle tre dimensioni sopra elencate è espressa secondo la seguente riconduzione:

- Adeguatezza: si riferisce al corretto disegno del sistema dei presidi rispetto alle rischiosità da gestire, ossia alla capacità potenziale di ridurre il rischio ad un livello accettabile: la valutazione è espressa assegnando uno score a quattro livelli (1 – Inadeguato; 2 – Parzialmente Inadeguato; 3 – Parzialmente Adeguato; 4 – Adeguato);
- Efficacia: si riferisce al regolare rispetto dei comportamenti aziendali conformemente a quanto previsto dal disegno del sistema dei presidi e dalla normativa interna: la valutazione è espressa assegnando uno score a quattro livelli (1 – Inefficace; 2 – Parzialmente Inefficace; 3 – Parzialmente Efficace; 4 – Efficace).

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

La valutazione complessiva del sistema dei presidi in termini di adeguatezza ed efficacia è espressa tramite una scala valutativa, o score, a quattro livelli:

- 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			

Sulla base dei risultati ottenuti da tale valutazione, è applicato l'abbattimento del Rischio Inerente di Processo (RI Processo) al fine di ottenerne il Rischio Residuo (RR Processo),

anch'esso declinato in una scala a 4 livelli. In particolare, la valutazione del Rischio Residuo di Processo è regolamentata dalla seguente tabella:

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			

La valutazione complessiva sopra indicata del sistema dei presidi per processo, in termini di adeguatezza e funzionamento, è ottenuta quindi sulla base delle valutazioni assegnate 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, ed è espressa tramite una scala valutativa, o score a 4 livelli:

- 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, gli esiti del confronto mediante "exit meeting" con le Unità Aziendali soggette a verifica, l'impatto del processo sul modello di business della Società, variazioni nel corpus normativo, raccomandazioni/interventi delle Autorità Vigilanza.

3.4.2 AZIONI DI MITIGAZIONE

A fronte dello svolgimento delle verifiche di adeguatezza e di funzionamento, ove sia riscontrato un gap normativo rispetto a quanto richiesto, gli analisti preposti alle attività di

controllo identificano le opportune azioni di mitigazione assegnando un livello di priorità riconducibile alla rischiosità dell'anomalia rilevata. Tali azioni vengono condivise con i responsabili delle strutture aziendali interessate, unitamente alla data termine per il rispettivo recepimento.

In funzione della rilevanza del processo analizzato, della criticità rilevata e della tipologia di azione di rimedio richiesta, per ogni intervento viene definito, in accordo con le Unità Aziendali responsabili della risoluzione del gap, un livello di priorità dell'intervento stesso e una data termine per il completamento della soluzione identificata.

Le azioni di mitigazione sono classificate in base alla priorità rilevata su una scala di 4 livelli:

- Alto
- Medio Alto
- Medio Basso
- Basso

e sono registrate sull'applicativo gestionale, con indicazione della tempistica prevista per la loro risoluzione e dell'owner di competenza.

La Funzione Compliance monitora nel continuo lo stato avanzamento delle attività fino al completamento degli interventi panificati, attraverso:

- allineamenti, confronti e monitoraggi periodici con le strutture responsabili dell'implementazione delle azioni di mitigazione definite;
- partecipazione diretta alle attività progettuali / SAL di progetto, nel caso in cui l'azione di mitigazione abbia richiesto l'avvio di un progetto aziendale;
- analisi degli aggiornamenti e della documentazione ricevuti dalle strutture responsabili delle soluzioni;
- esecuzione di verifiche di follow-up.

L'attività di monitoraggio si sostanzia principalmente in:

- appurare che le competenti strutture aziendali stiano realizzando misure di superamento dei gap riscontrati;
- siano rispettate le relative scadenze;
- le misure adottate risultino sempre idonee al superamento delle criticità rilevate.

Le tecniche per il monitoraggio a distanza ricomprendono ad esempio i solleciti e i contatti con le strutture responsabili dell'intervento e/o la ricezione di comunicazioni di aggiornamento ricevute dalle strutture.

Una volta ottenuti gli opportuni riscontri della completa implementazione delle iniziative, la Funzione provvede a porre in stato di "Chiusa" l'azione di mitigazione in esame. In caso di mancata esecuzione degli interventi, la Funzione valuta le motivazioni per le quali la struttura non ha ottemperato a quanto richiesto e ne richiede specifiche motivazioni e/o nuova una ripianificazione della data di completamento dell'intervento.

Le attività di monitoraggio sono oggetto di specifica **rendicontazione** periodica agli Organi Aziendali. Tale reportistica contiene, tra l'altro, informazioni quali: il livello di priorità dell'azione, l'owner preposto alla realizzazione delle azioni correttive e della Direzione/Unità organizzativa di appartenenza, la scadenza prevista, l'eventuale data di ripianificazione e la relativa motivazione.
In tale ambito, al fine di perseguire una sempre maggiore uniformità nelle modalità di rappresentazione degli esiti dei controlli, la Capogruppo Banca Mediolanum si è dotata del *Regolamento del processo di gestione dei rilievi emessi dalle Funzioni Aziendali di Controllo*, che prevede l'applicazione anche alle società controllate del Gruppo Bancario, inclusa Flowe, con l'obiettivo di:

- descrivere le diverse fasi del processo che le competenti strutture aziendali devono attuare 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 omogenee tra le Funzioni Aziendali di Controllo.

Tale 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.

3.4.3 REPORTING DELLE ATTIVITA' DI CONTROLLO

Le attività di verifica svolte vengono formalizzate in uno specifico Report, corredato dell'Allegato tecnico, che contiene le seguenti sezioni principali:

- **EXECUTIVE SUMMARY:** contiene la sintesi degli esiti della verifica condotta con l'evidenza delle eventuali azioni di mitigazione identificate
- **REPORT DI DETTAGLIO**:
  - il contesto normativo di riferimento
  - l'obiettivo e il perimetro della verifica
  - le Unità Aziendali coinvolte
  - gli applicativi informatici
  - il quadro normativo di riferimento
  - l'aggiornamento sulle azioni di mitigazione in corso
  - i pareri emessi dalla Funzione Compliance
- **RISULTATI DELL'INTERVENTO**:
  - perimetro dell'intervento ed esito delle verifiche
  - conclusioni
  - tabelle di sintesi
- **FOLLOW UP**, sezione presente nel caso in cui la verifica in esame ricomprenda anche il follow up di una verifica precedente e che contiene una descrizione sintetica dell'esito e dei controlli effettuati.

L'Allegato Tecnico al Report contiene il dettaglio delle analisi effettuate ed i relativi esiti, in termini di adeguatezza ed efficacia per la valutazione dei presidi adottati al fine di mitigare i rischi di non conformità.

Le risultanze sintetiche delle verifiche condotte vengono sottoposte all'attenzione degli Organi Apicali in occasione delle periodiche relazioni della Funzione Compliance.

3.4.4 INDICATORI DI RISCHIO

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 in diretto di natura sanzionatoria, finanziaria o reputazionale. L'impiego, nell'ambito del framework di Compliance, di indicatori di rischio consente di osservare fenomeni o

comportamenti specifici al fine di completare la visione dei rischi di non conformità a cui Flowe è esposta.

3.4.4.1 Key Compliance Indicators - KCI

Nell'ambito del complessivo framework di controllo e mitigazione dei rischi, la Funzione Compliance per il tramite dell'Unità Framework Reporting & Coordinamento di Gruppo 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).

I risultati del monitoraggio degli indicatori vengono mensilmente trasmessi alla Funzione Compliance, per opportuno allineamento e per supportare le rispettive attività di advisory e di controllo e sono oggetto di apposita reportistica trimestrale a beneficio delle altre Funzione Aziendali di Controllo.

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.

L'impianto di KCI in essere, come anticipato nei paragrafi precedenti, viene utilizzato sia in fase di pianificazione che in fase di esecuzione delle verifiche di Compliance. In fase di pianificazione, il responsabile dei controlli:

- tiene in considerazione eventuali evidenze emerse in corso d'anno riferite ai business process in perimetro nel momento in cui identifica i processi da includere nel nuovo piano;
- in corso d'anno, valuta l'integrazione del piano di attività approvato con eventuali "verifiche extra-piano" nel caso in cui dovessero emergere situazioni di particolare allerta/anomalia.

In fase di esecuzione, invece, l'analista incaricato di eseguire la verifica può considerare, ove opportuno, gli indicatori riferiti al processo in esame, osservandone l'andamento ed eventualmente riferendosi agli stessi in fase di formulazione degli esiti.

La Funzione può decidere di modificare/integrare indicatori esistenti laddove lo ritenga opportuno, anche sulla base delle risultanze delle attività di verifica stesse.

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 FR&CG e, nel caso di eventuali azioni correttive, coinvolgimento delle unità Advisory & Business Impact Controls
Alto	Attivazione analisi di dettaglio FR&CG ed informativa alle unità Advisory & Business Impact, che, se del caso, 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. Vengono tempestivamente interessate anche le strutture di business preposte alla supervisione del processo in esame, al fine di concordare congiuntamente gli approfondimenti e le azioni necessarie.

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.

3.5 REPORTING

Di seguito si descrivono le attività di reporting agli Organi Aziendali e alle Autorità di Vigilanza.

3.5.1 REPORTING AGLI ORGANI AZIENDALI

Con frequenza almeno semestrale, attraverso relazioni che riportano la sintesi delle attività concluse nel periodo, la Funzione Compliance fornisce un aggiornamento sullo stato di avanzamento del piano annuale delle verifiche, delle azioni di mitigazioni gestite nel periodo ed eventuali altre informazioni significative (come, ad esempio, le ispezioni e/o le interazioni significative con l'Autorità di Vigilanza). La produzione della relazione annuale, svolta dalla Funzione con il supporto dell'Unità Framework, Reporting e Coordinamento di Gruppo, viene trasmessa, secondo la normativa vigente, anche alle competenti Autorità di Vigilanza.

Nello specifico, vengono predisposte e condivise con gli Organi Aziendali:

- Relazioni periodiche sull'attività svolta, che illustrano, tra l'altro:
    - sintesi delle verifiche effettuate e dei risultati emersi;
    - interventi correttivi proposti per la rimozione delle anomalie riscontrate ed il loro stato di avanzamento;
    - attività ex-ante svolte nel periodo, come gli *alert* normativi, le valutazioni preventive, l'emissione di pareri, le validazioni di normativa interna, le *gap analysis;*
    - approfondimenti sugli ambiti per i quali la vigente normativa prevede obblighi di reporting periodici verso gli Organi Sociali e/o le Autorità di vigilanza, come ad esempio in relazione alle tematiche di Product Governance, dei Reclami ricevuti dalla Società per le attività sia ex-ante che ex-post;
    - pianificazione triennale delle verifiche, con focus sul primo anno (contenuta unicamente nella Relazione annuale).

- Relazioni "ad hoc" predisposte dalla Funzione aventi ad aggetto:
    - violazioni o carenze rilevanti riscontrate, che possono comportare un alto rischio di sanzioni regolamentari o legali, perdite finanziarie di rilievo o significativi impatti reputazionali;
    - rapporti con le Autorità di Vigilanza o comunicazioni di rilievo da queste ultime ricevute.

3.5.2 REPORTING ALLE AUTORITA' DI VIGILANZA

Dopo l'esame da parte dei competenti Organi Aziendali, la reportistica prodotta viene quindi trasmessa, ove previsto, alle Autorità di Vigilanza competenti, nazionali ed europee.

L'attività di invio risulta in carico alla Funzione, con il supporto dell'Unità Framework Reporting & Coordinamento di Gruppo che assicura la puntuale trasmissione della reportistica, ove previsto e secondo la periodicità stabilita.

3.5.3 GESTIONE RAPPORTI CON AUTORITA' DI VIGILIANZA NAZIONALI

L'attività è svolta in outsourcing dalla Capogruppo Banca Mediolanum e consiste nella gestione dei rapporti di natura ordinaria e straordinaria con le Autorità di Vigilanza nazionali, per le materie di competenza della Funzione Compliance che si coordina, ove opportuno, con le altre Funzioni di Controllo e con la Divisione Affari Societari della Banca.

La Funzione Compliance della Capogruppo interagisce inoltre con l'Unità Coordinamento BCE e SRB per tutte le attività, l'informativa, la documentazione e gli incontri riferiti alla gestione dei rapporti con la Banca Centrale Europea e con il Single Resolution Board.

La Funzione Compliance di Flowe gestisce in autonomia i rapporti con le Autorità di Vigilanza di competenza, garantendo un tempestivo reporting e allineamento verso la Funzione Compliance della Capogruppo.

Infine, in caso di verifiche ispettive da parte delle Autorità di Vigilanza, la Funzione Compliance, collabora con le Unità organizzative interessate nella gestione delle stesse.

4. INTERRELAZIONI CON ORGANI, ALTRE SOCIETA' DEL GRUPPO ED ALTRE UNITA' ORGANIZZATIVE

Il Capitolo illustra le modalità di coordinamento della Funzione Compliance con la Funzione Compliance di Capogruppo e le altre Funzioni di Compliance "locali", nonché le principali interazioni con altri Organi ed unità organizzative di Flowe.

4.1 FLUSSI DA E VERSO LA FUNZIONE COMPLIANCE DI CAPOGRUPPO

Si riportano di seguito i principali flussi informativi previsti dalla Funzione Compliance della Capogruppo alla Funzione Compliance di Flowe e viceversa, con indicazione della relativa frequenza. I relativi contenuti vengono tipicamente anticipati e condivisi in specifici incontri appositamente pianificati, aventi finalità informativa e/o di confronto e/o di indirizzo.

Flussi informativi dalla Funzione Compliance di Capogruppo verso la Funzione Compliance di Flowe	
Contenuti delle Policy di ownership della Funzione oggetto di prossima emanazione, preliminarmente ad ogni aggiornamento delle stesse	Ad evento
Iniziative progettuali con impatto sulle Funzioni Compliance delle controllate in termini di processi, strumenti e metodologie in uso	Ad evento
Pianificazione annuale (e triennale) delle attività della Funzione	Annualmente
Eventuali esiti di interesse per le società controllate	Ad evento
Piano di formazione delle risorse	Annualmente

Flussi informativi dalla Funzione Compliance di Flowe alla Funzione Compliance di Capogruppo	
Pianificazione annuale (e triennale) delle attività della Funzione preliminarmente alla approvazione nei rispettivi Organi di Vertice	Annualmente
Stato di avanzamento del piano di attività annuale	Trimestralmente
Stato di avanzamento del recepimento delle policy di ownership di Compliance emesse o aggiornate dalla Capogruppo	Trimestralmente
Esito delle verifiche effettuate, azioni di mitigazione identificate e relativo avanzamento	Trimestralmente
Indicazione delle sedute Consiliari di recepimento delle policy di ownership della Funzione	Ad evento
Evoluzioni delle normative locali che impattino in modo significativo sull'andamento business e/o sul perimetro/entità dei rischi di non conformità complessivamente gestiti	Ad evento
Avvio di nuove ispezioni da parte delle Autorità di Vigilanza locali ed interazioni intercorse con le stesse	Ad evento
Aggiornamento attività di formazione delle risorse	Trimestralmente

Flussi informativi dalla Funzione Compliance di Flowe alla Funzione Compliance di Capogruppo	
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	Ad evento

4.2 INTERRELAZIONI CON ALTRI ORGANI E ALTRE DIREZIONI/DIVISIONI/SETTORI AZIENDALI

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 di Flowe.

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 Conglomerato sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna*".

5 IL QUADRO NORMATIVO DI RIFERIMENTO

Nel presente capitolo si richiama il contesto normativo interno ed esterno, nell'ambito del quale opera la Funzione. L'elenco fornito non si ritiene esaustivo e viene riportato principalmente allo scopo di richiamare l'attenzione sui principali riferimenti a cui la Funzione si attiene nello svolgimento della propria attività.

5.1 CONTESTO NORMATIVO ESTERNO 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 "Disposizioni di vigilanza per le banche" da parte di Banca d'Italia e successivi aggiornamenti;

- 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.

5.2 CONTESTO NORMATIVO INTERNO DI RIFERIMENTO

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

- Compliance Policy;
- 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.