

**MANUALE METODOLOGICO E OPERATIVO**

**DELLA**

**FUNZIONE COMPLIANCE**

**Approvato dal Consiglio di Amministrazione**

**Matrice delle revisioni**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Ed | Data | Rev | Data | Descrizione | Emesso da | Approvato da |
| 01 | 09/02/2022 | 00 | 09/02/2022 | Prima emissione | Funzione Compliance | Consiglio di Amministrazione |

**INDICE**

[**1.Premessa e obiettivi del documento** 4](#_Toc82186870)

[**2. Modello operativo della Funzione Compliance** 5](#_Toc82186871)

[2.1 Definizione e aggiornamento del framework metodologico 6](#_Toc82186872)

[*2.2 Alerting* normativo e aggiornamento della *Legal inventory* 7](#_Toc82186873)

[*2.3 Impact Analysis* 8](#_Toc82186874)

[2.3.1 Valutazione del rischio inerente 9](#_Toc82186875)

[2.3.2 Valutazione complessiva di conformità dei presidi organizzativi e di controllo 10](#_Toc82186876)

[2.3.3 Valutazione del rischio residuo e determinazione della priorità di intervento 12](#_Toc82186877)

[2.4 Pianificazione delle attività di compliance 13](#_Toc82186878)

[2.4.1 *Compliance Risk Assessment* 14](#_Toc82186879)

[2.4.1.1 Fattori di prioritizzazione per la pianificazione annuale 14](#_Toc82186880)

[2.4.2 *Compliance Need* 16](#_Toc82186881)

[2.5 Interventi di compliance 16](#_Toc82186882)

[2.6 Monitoraggio carenze – *Follow up* 19](#_Toc82186883)

[2.7 Altre attività di compliance 20](#_Toc82186884)

[2.7.1 Consulenza 20](#_Toc82186885)

[2.7.2 Formazione 21](#_Toc82186886)

[2.8 Reporting……. 22](#_Toc82186887)

# **Premessa e obiettivi del documento**

Il rischio di non conformità è un rischio diffuso a tutti i livelli dell’organizzazione aziendale, pertanto l’attività di prevenzione deve svolgersi in primo luogo dove il rischio viene generato. Un’efficace ed efficiente gestione del rischio di non conformità richiede in particolare:

* una chiara e formalizzata individuazione e distinzione di ruoli e responsabilità ai diversi livelli dell’organizzazione;
* l’istituzione di un’apposita Funzione Compliance incaricata, nell’ambito dei controlli di secondo livello, della gestione del rischio di non conformità;
* la predisposizione di un framework che definisca le modalità operative e il modello di controllo adottato dalla Funzione Compliance;
* la redazione di documenti periodici di programmazione e di reporting delle attività condotte dalla Funzione Compliance indirizzati ai vertici aziendali al fine di consentire la valutazione del presidio del rischio di non conformità.

I principi sopra richiamati sono finalizzati alla corretta gestione del rischio di non conformità e allo sviluppo di una complessiva “cultura della compliance” che consenta di ottimizzare la gestione del business e di soddisfare al meglio i bisogni dei clienti nell’ottica del miglioramento continuo delle prestazioni e della creazione di valore.

L’individuazione e la valutazione delle aree sensibili al rischio di compliance avviene utilizzando un approccio:

* focalizzato sui processi, al fine di poter intervenire efficacemente su un unico ambito di operatività, tramite *know how* specialistico e, di conseguenza comprendere i rischi e le anomalie peculiari dei diversi ambiti normativi di riferimento;
* guidato dai rischi (*risk based*), in cui gli obiettivi e le attività di compliance sono definiti in funzione dei rischi di non conformità associati a ciascun ambito di operatività;
* caratterizzato da strumenti e tecniche standard al fine di assicurare omogeneità di analisi e di rappresentazione dell’attività.

Pertanto, il presente “*Manuale metodologico e operativo*” descrive le modalità con cui la Funzione Compliance (di seguito “Funzione”) di Confeserfidi Soc. cons. a r.l. (di seguito “Confidi” o “Confeserfidi”) assicura la gestione del rischio di non conformità; nello specifico il modello di controllo consta delle seguenti fasi:

* identificazione delle norme di etero regolamentazione (leggi e regolamenti) e autoregolamentazione (codici di condotta, codici etici) che determinano l’esposizione a rischi di non conformità;
* individuazione e valutazione, con cadenza almeno annuale, dei principali rischi di compliance;
* definizione di un programma annuale di verifiche che tenga conto dei rischi di compliance individuati;
* conduzione di verifiche di compliance relativamente ai processi sulla base della valutazione dei rischi precedentemente condotta;
* monitoraggio dei piani di intervento nei quali vengono riepilogate le azioni correttive da intraprendere ed attraverso cui vengono definiti tempi, priorità e responsabilità delle attività;
* attivazione di un sistema di reporting idoneo a rappresentare i rischi di compliance al Consiglio d’Amministrazione, al Collegio Sindacale, all’Amministratore Delegato, alle Funzioni di Controllo, alle Strutture operative ed all’Autorità di Vigilanza.

# **Modello operativo della Funzione Compliance**

Nell’ambito delle attività assegnate alla Funzione Compliance assume primario rilievo l’attribuzione di funzioni di controllo finalizzate alla gestione del rischio di non conformità, quali:

* verifica, in via preventiva, dell’adeguatezza dei presidi organizzativi adottati ai fini di assicurare il rispetto della normativa di riferimento (c.d. verifica di adeguatezza);
* verifica, nel continuo, dell’effettiva adozione dei presidi organizzativi previsti e della conformità dei processi aziendali (c.d. verifica di efficacia).

La presente sezione descrive, per le diverse fasi del processo di gestione del rischio di non conformità, le modalità operative cui la Funzione è tenuta ad attenersi nello svolgimento delle attività di propria competenza. Nello specifico, il ciclo di attività della Funzione Compliance può essere sintetizzato in:

* definizione e aggiornamento del framework metodologico;
* *alerting* normativo e aggiornamento del *legal inventory;*
* *impact analysis;*
* pianificazione delle attività;
* *compliance risk assessment*;
* *compliance need;*
* interventi di compliance;
* monitoraggio delle carenze e *follow – up*;
* attività straordinarie di compliance:
* consulenza;
* formazione;
* reporting.

# **Definizione e aggiornamento del framework metodologico**

La Funzione Compliance ha il compito di definire e aggiornare nel continuo il complessivo framework metodologico utilizzato per la valutazione del rischio di non conformità del Confidi.

Nello specifico, l’attività di definizione e aggiornamento del framework metodologico della Funzione consiste nel:

* definire e aggiornare il perimetro/ciclo delle attività da svolgere;
* definire e aggiornare la metodologia di valutazione del rischio di non conformità;
* definire e aggiornare gli strumenti operativi volti a supportare le attività della Funzione in linea con la metodologia definita (e.g. matrici di rischio, schede di reporting ordinario);
* definire e aggiornare la reportistica della Funzione mediante la quale viene rappresentata, agli Organi aziendali e al Confidi nel suo complesso, una complessiva valutazione in base all’esposizione al rischio di non conformità.

A seconda dei casi, l’aggiornamento del framework metodologico della Funzione può configurarsi quale:

* attività di gestione: qualora le modifiche risultino non strutturali (e.g. aggiornamento delle matrici di rischio con inserimento di nuovi requisiti e/o rischi; revisione dei valori target degli indicatori di rischio);
* attività di innovazione: qualora le modifiche risultino strutturali (e.g. revisione del perimetro/ciclo delle attività della Funzione e della metodologia di valutazione del rischio; introduzione e revisione degli strumenti di controllo e del reporting della Funzione).

# ***Alerting* normativo e aggiornamento della *Legal inventory***

La Funzione Compliance ha il compito di identificare i rischi di non conformità alle norme derivanti dagli ambiti normativi di diretta competenza del Confidi.

Ai fini dell’identificazione dei presidi attuabili sui diversi ambiti normativi rilevanti nella gestione del rischio di non conformità, le norme ritenute applicabili trasversalmente al Confidi considerano:

* fattori esogeni, ovvero dipendenti dall’evoluzione del contesto normativo esterno di riferimento (i.e. normativa primaria e normativa di Vigilanza);
* fattori endogeni, ovvero dipendenti dall’evoluzione del modello di business e operativo del Confidi, esponendo lo stesso a nuovi rischi di non conformità.

La Funzione è sempre coinvolta in qualsiasi iniziativa strategica di Confeserfidi finalizzata all’evoluzione del modello di business e operativo al fine di poter valutare correttamente l’esposizione al rischio di non conformità alle norme. Inoltre, al fine di poter identificare per tempo i rischi di non conformità alle norme, la Funzione Compliance è tenuta ad effettuare un monitoraggio costante dell’evoluzione normativa esterna.

Nello specifico, la fase in esame si sostanzia nelle seguenti attività e prevede l’utilizzo degli strumenti di seguito elencati:

* individuare le normative applicabili: a seguito del verificarsi di uno dei fattori esogeni e/o endogeni precedentemente specificati, la Funzione Compliance effettua un’analisi dettagliata, finalizzata a comprendere il perimetro delle nuove normative applicabili al Confidi. Tale attività può prevedere il coinvolgimento, a titolo consultivo, di altre Funzioni aziendali;
* integrare la *Legal Inventory* delle norme applicabili: la Funzione Compliance provvede ad integrare la *Legal Inventory* delle normative applicabili. In particolare, occorre specificare l’ambito ed il corrispettivo riferimento normativo, ovvero la regolamentazione che è stata introdotta al verificarsi di fattori esogeni o che risulta applicabile al Confidi in ragione di fattori endogeni.

# ***Impact Analysis***

A seguito dell’aggiornamento della *Legal Inventory*, la Funzione Compliance pone in essere un’analisi degli impatti (*impact analysis*) derivanti dalla normativa applicabile al Confidi. L’obiettivo dell’analisi di impatto è di rappresentare in modo sintetico:

* il contesto della nuova norma emanata, indicando:
* ambito normativo;
* provvedimento normativo;
* oggetto del provvedimento normativo;
* *requirement* di riferimento;
* una valutazione sintetica degli impatti, indicando, per ogni *requirement* normativo:
* processo/i impattato/i;
* Struttura/e e/o Funzione/i impattate;
* livello di impatto in relazione a:
* rischio inerente, calcolato come il prodotto tra la probabilità di accadimento dello scenario di rischio ed il relativo impatto in termini di effetti economico – patrimoniale e/o reputazionale sull’intermediario o sui processi di quest’ultimo e del danno potenzialmente derivante dalla manifestazione dello scenario di rischio e dalla sanzione correlata[[1]](#footnote-1);
* conformità complessiva dei presidi organizzativi e di controllo basata sulla valutazione della completezza e dell’adeguatezza del contesto aziendale definito *ex ante* dal Confidi, derivante dalla valutazione complessiva di: *i)* strategie e politiche di rischio (i.e. le linee strategiche e indirizzi da parte degli Organi aziendali e delle politiche di rischio); *ii)* governance, organizzazione e Sistema dei Controlli Interni (i.e. il modello di governance adottato, la formalizzazione dei ruoli e responsabilità delle Funzioni aziendali e il Sistema dei Controlli Interni); *iii)* processi, procedure e corpus normativo adottato; *iv)* comunicazione e formazione (i.e. i flussi informativi definiti e del livello di formazione professionale delle Strutture interessate/impattate); *v)* sistemi informativi (i.e. le procedure informatiche e supporti tecnologici utilizzati);
* rischio residuo, calcolato come il prodotto tra la valutazione del rischio inerente e la valutazione complessiva di conformità dei presidi organizzativi e di controllo;
* azioni di mitigazione individuate e priorità d’intervento richiesto.

Determinato il livello di impatto della nuova norma applicabile al Confidi, la Funzione Compliance comunica le novità introdotte e gli esiti delle valutazioni condotte alle Strutture impattate.

# **Valutazione del rischio inerente**

La valutazione del rischio inerente rappresenta la valutazione sintetica del singolo evento rischioso la cui manifestazione potrebbe provocare un danno diretto o indiretto di natura economico – finanziaria, patrimoniale, sanzionatoria o d’immagine verso l’esterno. Suddetto rischio è rilevato nell’ambito del processo di compliance ed è indipendente dai presidi e dalle misure poste a mitigazione dello stesso.

Il rischio inerente è definito sulla base di considerazioni qualitative con riferimento:

* all’impatto, ossia l’effetto economico – patrimoniale e/o reputazionale sull’intermediario o sui processi di quest’ultimo e del danno potenzialmente derivante dalla manifestazione dello scenario di rischio e dalla sanzione correlata, determinato sulla base di driver valutativi quali: *i)* governance e assetto organizzativo, *ii)* processi di funzionamento, *iii)* strumenti e metodologie operativi;
* alla probabilità di accadimento, ossia la possibilità che il singolo scenario di rischio possa manifestarsi in un periodo temporale determinato in funzione della sua tipologia.

Nello specifico, il rischio inerente è definito come:

in cui la probabilità di accadimento dello scenario di rischio oggetto di valutazione e l’impatto vengono definite su quattro livelli secondo la seguente scala di giudizi:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IMPATTO** | | | | **+** | **PROBABILITA’ DI ACCADIMENTO** | | | |
| **Giudizio** | **Impatto** | **Valore** | **Valore ponderato (60%)** | **Giudizio** | **Descrizione** | **Valore** | **Valore ponderato (40%)** |
| **Alto** | >100.001 € | 100 | 60 | **Certa** | L’evento accade sicuramente. | 100 | 40 |
| **Medio Alto** | Da 40.001 a 100.000 € | 80 | 48 | **Probabile** | L'evento ha buone probabilità di manifestarsi. | 75 | 30 |
| **Medio Basso** | Da 15.001 a 40.000 € | 40 | 24 | **Possibile** | L'evento ha possibilità di accadere. Dipende da una circostanza che può o meno verificarsi, pertanto con una ridotta probabilità di realizzazione. | 50 | 20 |
| **Basso** | < 15.000 € | 10 | 6 | **Remota** | L'evento ha scarsissime o nulle possibilità di verificarsi; ovvero potrà accadere solo in situazioni eccezionali, pertanto la probabilità di accadimento è prossima allo zero. | 25 | 10 |

Dalla combinazione dell’impatto derivante dalla manifestazione del singolo scenario di rischio e della relativa probabilità di accadimento, il rischio inerente è determinato sulla base di una scala a quattro livelli, così come di seguito rappresentato:

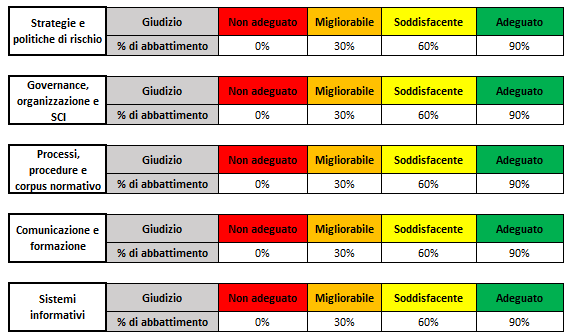
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **PROBABILITA’ DI ACCADIMENTO** | | | |  | **RISCHIO INERENTE** | |
| **Remota** | **Possibile** | **Probabile** | **Certa** | **Giudizio** | **Valore** |
| **IMPATTO** | **AltO** | **Elevato** | **Elevato** | **Molto Elevato** | **Molto Elevato** | **Molto elevato** | 81 – 100 |
| **Medio Alto** | **Moderato** | **Elevato** | **Elevato** | **Molto Elevato** | **Elevato** | 61 – 80 |
| **Medio Basso** | **Contenuto** | **Moderato** | **Moderato** | **Elevato** | **Moderato** | 36 – 60 |
| **Basso** | **Contenuto** | **Contenuto** | **Moderato** | **Moderato** | **Contenuto** | 0 – 35 |

# **Valutazione complessiva di conformità dei presidi organizzativi e di controllo**

Dopo aver valutato il rischio inerente occorre procedere alla rilevazione e valutazione dei presidi organizzativi e di controllo adottati dall’intermediario al fine di mitigare il rischio connesso a possibili aree di non conformità. La valutazione complessiva di conformità dei presidi organizzativi e di controllo è determinata dalla media dei giudizi attribuiti a:

* strategie e politiche di rischio, ovvero la definizione di linee strategiche ed indirizzi da parte degli Organi aziendali e delle politiche di rischio;
* governance, organizzazione e Sistema dei Controlli Interni, ovvero la definizione di un modello di governance, ivi inclusa la formalizzazione di ruoli e responsabilità delle Funzioni aziendali e del Sistema dei Controlli Interni nel suo complesso;
* processi, procedure e corpus normativo;
* comunicazione e formazione professionale delle risorse in organico;
* sistemi informativi, ovvero la presenza di procedure informatiche e supporti tecnologici.

Ogni presidio è definito su una scala a quattro livelli (i.e. Non adeguato, Migliorabile, Soddisfacente, Adeguato), a cui è stata attribuita una percentuale di abbattimento:



La valutazione complessiva di conformità dei presidi può essere effettuata direttamente dai *Process owner* di primo livello. Di seguito è riportata la descrizione di ciascuno dei quattro giudizi attribuibili ai presidi:

|  |  |
| --- | --- |
| **Giudizio** | **Descrizione** |
| **Non adeguato** | * Mancata formalizzazione dei presidi * Mancata pertinenza e/o copertura del presidio rispetto al rischio oggetto di analisi (e.g. inesistenza di controllo automatico/manuale) |
| **Migliorabile** | * L’attività di presidio oggetto di analisi risulta essere parzialmente formalizzata in termini di ruoli e responsabilità, tipologia, frequenza e strumenti (anche informatici), organicità della normativa interna e ritardi nell’aggiornamento della stessa rispetto ad evoluzioni organizzative ed operative aziendali * Parziale pertinenza e/o copertura del presidio rispetto al rischio oggetto di analisi in termini di strumenti, frequenza, separatezza dei ruoli, sia in caso di controllo formalizzato sia di prassi consolidata (e.g. il controllo, automatico o manuale, è da aggiornare a causa di adeguamenti normativi) |
| **Soddisfacente** | * L’attività di presidio oggetto di analisi risulta essere formalizzata, tuttavia risultano essere presenti margini di miglioramento circa la definizione degli attributi del controllo in termini di tipologia, frequenza e strumenti (anche informatici), organicità della normativa interna ed aggiornamenti formali * Il presidio copre adeguatamente il rischio oggetto di analisi in termini di separatezza dei ruoli, strumenti (e.g. il controllo, anche se non automatico, potrebbe essere migliorato tramite l'inserimento di driver di anomalia o trigger di analisi ulteriori in grado di coprire maggiormente il rischio presidiato) e frequenza |
| **Adeguato** | * Gli elementi del presidio oggetto di analisi risultano essere formalizzati in termini di ruoli e responsabilità, tipologia, frequenza e strumenti anche informatici * Il controllo (automatico o manuale) copre adeguatamente il rischio oggetto di analisi in termini di strumenti, frequenza, rilevazione preventiva, separatezza dei ruoli |

# **Valutazione del rischio residuo e determinazione della priorità di intervento**

Il rischio residuo rappresenta la valutazione qualitativa del rischio a cui il Confidi risulta essere esposto nonostante i presidi organizzativi e di controllo adottati a mitigazione del rischio inerente. Viene definito autonomamente come la combinazione delle valutazioni di “rischio inerente” e “conformità complessiva dei presidi organizzativi e di controllo”.

Pertanto, il rischio residuo è determinato sulla base di una scala a quattro livelli (i.e. Alto, Medio Alto, Medio Basso, Basso), così come di seguito rappresentato:

|  |  |
| --- | --- |
| **RISCHIO RESIDUO** | |
| **Giudizio** | **Valore** |
| **Alto** | 80,01 – 100 |
| **Medio Alto** | 50,01 – 80 |
| **Medio Basso** | 20,01 – 50 |
| **Basso** | 0 – 20 |

Determinato il rischio residuo per ogni *requirement* normativo, la Funzione Compliance identifica eventuali azioni di mitigazione e definisce la priorità d’intervento (i.e. Nessuna priorità, Alta, Media, Bassa).

# **Pianificazione delle attività di compliance**

La pianificazione delle attività costituisce il momento in cui la Funzione Compliance individua gli obiettivi da raggiungere, le attività da svolgere e le relative modalità di realizzazione, tempistiche e frequenza, nonché l’*effort* richiesto.

Il piano annuale descrive le attività che saranno condotte dalla Funzione con riferimento agli ambiti normativi rientranti nel perimetro di competenza della stessa. Al riguardo, la Funzione Compliance avvia la predisposizione del piano di Compliance relativo all’anno successivo, durante l’ultimo trimestre di ciascun anno solare in corso.

Inoltre, l’attività di pianificazione della Funzione Compliance deve garantire l’idonea integrazione con la pianificazione delle altre Funzioni aziendali di Controllo (i.e. Funzione Internal Audit e Funzione Controllo Rischi).

In via generale, nella definizione del Piano Annuale si tengono in considerazione le seguenti informazioni:

* attività di gestione, con particolare riferimento a:
* evoluzione organizzativa interna;
* manutenzione delle procedure, delle metodologie e degli strumenti operativi di controllo;
* attività ordinarie, per ciascun ambito normativo rientrante nel perimetro di controllo della Funzione, si fornisce una descrizione dell’attività di:
* *alerting* normativo e aggiornamento del *legal inventory*;
* *impact analysis* e *gap analysis*;
* c*ompliance risk assessment*;
* attività di consulenza e formative rivolte alle Strutture interne;
* reporting e *follow up*;
* eventuali altre attività ordinarie;
* attività straordinarie, con particolare riferimento a:
* attività poste in essere a fronte di nuove iniziative (e.g. nuovi prodotti e/o servizi);
* attività di controllo di carattere straordinario richieste dagli Organi aziendali;
* attività di controllo di carattere straordinario richieste dalle Autorità di Vigilanza.

Pertanto, in base alle risultanze della fase di identificazione e valutazione dei rischi di non conformità, il piano delle verifiche definito deve considerare:

* le priorità di intervento emerse nella fase di valutazione dei rischi;
* la necessità di preservare una logica di copertura temporale dei processi aziendali in considerazione della rilevanza delle norme ad essi applicabili;
* le indicazioni che dovessero emergere in fase di altre verifiche, eventualmente condotte da altre Funzioni di Controllo.

Ad integrazione di quanto sopra riportato, la Funzione Compliance nell’ambito dell’attività di revisione del processo di valutazione aziendale dell’adeguatezza patrimoniale (*Internal Capital Adequacy Assessement Process -* ICAAP), effettua una verifica sul processo, volta ad assicurare che le procedure ed i processi aziendali finalizzati alla determinazione della posizione patrimoniale siano coerenti con le disposizioni normative per tempo vigenti.

# ***Compliance Risk Assessment***

Sulla base delle matrici di rischio definite e del modello metodologico adottato per la valutazione del rischio di non conformità, la Funzione Compliance provvede a svolgere l’attività di *Compliance Risk Assessment*.

Al fine di valutare il rischio di non conformità cui è esposto l’intermediario, la Funzione definisce un’apposita metodologia interna mediante la quale per ciascun ambito normativo giunge ad una valutazione di rischiosità “netta”.

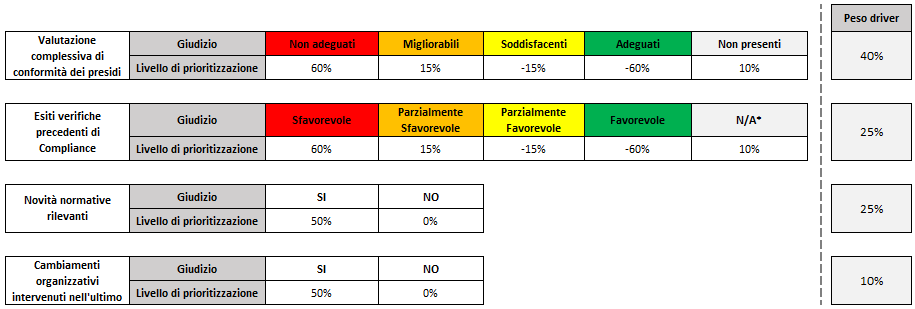
La valutazione del rischio si sostanzia nella valutazione del rischio inerente[[2]](#footnote-2) e nella successiva integrazione di fattori di prioritizzazione (i.e. fattori vincolanti e driver di prioritizzazione).

# **Fattori di prioritizzazione per la pianificazione annuale**

Le valutazioni di rischio inerente relative a ciascun ambito normativo, sono successivamente integrate sulla base di fattori di prioritizzazione che permettono di evidenziare peculiari esigenze di intervento utili a definire un livello di prioritizzazione delle attività di controllo da pianificare.

I fattori di prioritizzazione presi in considerazione sono riconducibili a tre macro-categorie:

* fattori vincolanti: esprimono una necessità inderogabile di pianificare l’attività di verifica. Nello specifico: i) attività obbligatorie previste dalla normativa di Vigilanza; ii) richieste ed esigenze di approfondimento espresse da parte degli Organi aziendali; iii) richieste straordinarie formulate dalle Autorità di Vigilanza successive ad eventuali ispezioni condotte dalle stesse. Il verificarsi di una tra queste fattispecie comporta una prioritizzazione assolutae pertanto un rating priorità di intervento “Alta”;
* driver di prioritizzazione:evidenziano delle peculiari esigenze di intervento, mediante la valutazione di: i) valutazione complessiva di conformità dei presidi organizzativi; ii) esiti di attività di verifica condotte dalla Funzione Compliance; iii) novità normative rilevanti; iv) cambiamenti organizzativi intervenuti nell’ultimo esercizio. I driver sopra citati, sono stati definiti su una scala di giudizi a cui è stata attribuita una percentuale inerente il livello di prioritizzazione e rispetto peso di ponderazione, come di seguito rappresentato:



* *override* qualitativo della Funzione Compliance: discrezionalità lasciata alla Funzione di attribuire un elemento di prioritizzazione finale sulla base di specifici elementi a sua conoscenza. L’*override* presenta carattere di complementarietà rispetto all'esito della prioritizzazione derivante da fattori quantitativi e pertanto può variare in aumento o in diminuzione il *rating* priorità di intervento con il limite di 3 fasce in aumento e 2 fasce in diminuzione. La Funzione Compliance dovrà motivare gli eventuali scostamenti rispetto ai risultati ottenuti con il metodo quantitativo.

# ***Compliance Need***

Le valutazioni di rischio, integrate sulla base di fattori di prioritizzazione, permettono di evidenziare peculiari esigenze di intervento utili a definire un livello di prioritizzazione delle attività di controllo da pianificare.

Il *Compliance Need,* determinato con riferimento a ciascun ambito normativo,rappresenta la priorità di intervento utile alla definizione della pianificazione *risk based*, tenendo anche in considerazione la *capacity* della Funzione.

# **Interventi di compliance**

In coerenza con il piano di compliance, a seguito delle risultanze emerse dal *Risk Assessment*, la Funzione Compliance programma ed organizza le singole attività di verifica da svolgere.

La programmazione operativa del singolo intervento di verifica prevede l’attuazione delle seguenti attività:

* analisi dell’ambito normativo da sottoporre a verifica, al fine di provvedere alla definizione del perimetro di compliance, dei limiti dell’attività, degli obiettivi da perseguire e dell’approccio, ovvero delle modalità e del livello di dettaglio con cui sono condotte le attività di verifica, sulla base delle valutazioni preliminari effettuate sul rischio di non conformità afferente la specifica operatività;
* identificazione dei controlli associati al rischio di non conformità relativo al singolo ambito normativo presente nel *Risk Assessment*;
* previsione dei *deliverable* da produrre;
* pianificazione delle tempistiche necessarie alla conduzione dell’attività, in linea con la definizione del calendario delle interviste dirette alle Funzioni/Strutture operative coinvolte e il reperimento della documentazione interna di riferimento.

Nel corso delle attività di compliance, la Funzione ha cura di mantenere traccia, tra le carte di lavoro, delle interviste condotte, nonché delle attività di controllo effettuate.

Il processo di raccolta di dati ed informazioni è autonomo. Nel caso sia necessario richiedere il supporto di strutture terze del Confidi per l’estrazione dei dati (e.g. da sistemi informativi), la Funzione Compliance predispone apposita e formale richiesta di documentazione, trasmessa tramite email al Responsabile della Struttura operativa quale *owner* dell’informazione. Le informazioni raccolte devono consentire il raggiungimento degli obiettivi definiti nel piano di intervento, essere convalidate da idonea documentazione a supporto e rispettare i principi fondamentali, rispetto agli obiettivi dell’incarico; nello specifico, devono rispettare i seguenti principi:

* sufficienza: devono essere concrete, adeguate e convincenti al fine di permettere a chiunque di essere informato e di giungere alle stesse conclusioni della Funzione;
* affidabilità: devono essere fondate e ottenute attraverso l’uso di tecniche appropriate;
* attinenza: sono coerenti con l’obiettivo dell’incarico e danno fondamento ai rilievi ed alle osservazioni;
* utilità: possono aiutare l’organizzazione a raggiungere le proprie finalità.

L’insieme delle informazioni raccolte deve essere utilizzato dalla Funzione Compliance per pervenire alle conclusioni sull’incarico attraverso opportune analisi e valutazioni, nel rispetto dei generali principi di obiettività e competenza.

In funzione delle attività di controllo, la Funzione Compliance può applicare le seguenti tecniche di analisi:

* intervista: si sostanzia nel domandare al proprio interlocutore informazioni sui controlli eseguiti, al fine di rilevare informazioni descrittive. La tecnica in oggetto non può ritenersi esaustiva per supportare conclusioni sul concreto funzionamento di uno specifico controllo. Al riguardo, può essere proficuamente utilizzata in combinazione con altre tecniche di *test* al fine di comprendere la consapevolezza del soggetto intervistato circa le attività di controllo poste in essere, nonché l’azione di mitigazione che tali controlli hanno, rispetto al rischio di non conformità su un determinato ambito normativo oggetto di verifica;
* analisi della documentazione interna: consiste nell’analisi documentale (e.g. *policy*, procedure, circolari, regolamenti) ed in generale di tutta la normativa interna disponibile;
* esame delle evidenze (ispezione): si sostanzia nell’esame delle evidenze del controllo, le quali possono essere rappresentate, a titolo esemplificativo e non esaustivo, da *report* di eccezioni, da documenti di *follow-up*, da tabulati di spunta, da note esplicative scritte. L’utilizzo di tale tecnica è finalizzato a testare i controlli per cui è ragionevole che sia disponibile un’evidenza. Nel caso in cui nel corso dell’intervento si riscontri l’assenza di evidenze da testare che potrebbe indicare il mancato svolgimento del controllo previsto dalla normativa interna, la Funzione è tenuta ad adottare ulteriori attività di verifica, al fine di rilevare se il controllo in oggetto risulti altrimenti documentabile e pertanto concretamente svolto.

Al riguardo, la Funzione Compliance, sulla base dei risultati conseguiti con le verifiche di compliance perviene alla valutazione dei presidi sui rischi di non conformità, sulla base di una scala di giudizi articolata su 4 livelli:

* conforme: i presidi sono coerenti con la normativa di riferimento e con i rischi derivanti da essa, in termini di esistenza ed adeguatezza degli stessi ad assicurare il rispetto delle disposizioni normative; oppure i presidi sono regolarmente applicati ed i comportamenti risultano assolutamente aderenti alle disposizioni normative;
* prevalentemente conforme: i presidi sono prevalentemente coerenti con i rischi presidiati, infatti, pur in presenza di limitati e specifici interventi migliorativi, gli stessi sono in grado di assicurare il rispetto delle disposizioni normative; oppure i presidi sono prevalentemente applicati in maniera corretta ed i comportamenti risultano sostanzialmente aderenti alle disposizioni normative;
* prevalentemente non conforme: i presidi sono incompleti ovvero sono a volte incoerenti con i rischi presidiati, pertanto richiedono adeguati interventi migliorativi per assicurare il rispetto delle disposizioni normative; oppure i presidi non sono applicati correttamente ed i comportamenti risultano prevalentemente non aderenti alle disposizioni normative;
* non conforme: non sono presenti presidi volti ad assicurare il rispetto delle disposizioni normative ovvero quelli esistenti non sono assolutamente coerenti con i rischi presidiati; oppure le attività eludono la normativa.

Tali valutazioni sono di natura “discrezionale” ovvero scaturiscono dal giudizio professionale del valutatore.

Terminata l’attività di analisi, la Funzione formalizza il c.d. “*Report di compliance*”, nel quale definisce le principali evidenze emerse dall’incarico, i punti di attenzione/carenze emerse nel corso dell’attività di controllo, i possibili interventi di miglioramento e la data entro cui dovranno essere risolte eventuali carenze riscontrate.

# **Monitoraggio carenze – *Follow up***

La fase in oggetto può originare da una pluralità di eventi:

* individuazione di azioni di mitigazione (i.e. interventi correttivi di adeguamento) a seguito di una specifica attività di *gap analysis*;
* *Compliance Risk Assessment* da cui emergono gap di impianto e di funzionamento;
* eventuali segnalazioni di non conformità per le quali, a seguito di approfondimenti e di specifiche analisi da parte della Funzione, emerge la necessità di avviare azioni di mitigazione *ad hoc*;
* attività di verifica periodiche.

In generale, si definiscono “gap di non conformità” le anomalie e criticità che possono esporre il Confidi al rischio di violare disposizioni di legge, di vigilanza e di autoregolamentazione. Un gap di conformità può essere generico, pertanto si evince la necessità di dettagliarlo, circoscriverlo e correlarlo ad un obbligo regolamentare di riferimento.

Ogni gap rilevato è associato ad un livello di rilevanza, il quale viene attribuito sulla base del rischio connesso all’anomalia rilevata e classificato su una scala a quattro livelli:

* alta, in caso di:
* gravi violazioni di norme cogenti che richiedono immediate azioni correttive;
* anomalie segnalate dalle Autorità di Vigilanza;
* necessità di coinvolgere gli Organi aziendali;
* medio – alta, in caso di gap che hanno un elevato rischio potenziale e che, se non sanati tempestivamente, possono comportare danni rilevanti per il Confidi;
* medio – bassa, in caso di gap a cui sono associati rischi potenziali importanti;
* bassa, in caso di gap con un rischio potenziale non rilevante.

Una volta individuati uno o più gap di non conformità e formalizzati gli stessi all’interno della matrice di rischio a supporto, la Funzione Compliance procede alla condivisione degli interventi proposti con la Struttura *owner* responsabile della relativa risoluzione. L’assegnazione del gap deve risultare univoca e, di conseguenza, riferita ad un’unica Struttura aziendale, la quale si assumerà la responsabilità della mitigazione. Qualora fosse necessario, la Struttura *owner* indica anche il coinvolgimento di uno o più soggetti che, nell’ambito delle proprie competenze, dovranno partecipare alla realizzazione dell’intervento.

Nella fase di condivisione la Funzione Compliance ha il compito di raggiungere una posizione comune con la Struttura *owner* in merito a:

* evidenze delle attività di controllo;
* caratteristiche delle criticità riscontrate;
* modalità di mitigazione.

In particolare, la Funzione Compliance condividerà:

* l’assunzione della responsabilità delle attività di mitigazione da parte della Struttura *owner*;
* la rilevanza del gap;
* la soluzione correttiva suggerita;
* la *deadline* per la risoluzione del gap.

Tutti i gap rilevati, a prescindere dalla loro natura, sono gestiti mediante ricorso ad uno strumento *ad hoc* che dovrà essere monitorato e aggiornato nel continuo dalla Funzione.

Pertanto, il *follow-up* è la verifica operativa tramite la quale la Funzione Compliance si assicura che gli interventi correttivi siano stati realizzati e che questi stiano ottenendo i risultati desiderati, oppure in alternativa, che gli Organi aziendali abbiano accettato il rischio di non attivare azioni correttive, assumendosi la responsabilità di tale decisione. La Funzione dovrà condurre un’attività di *follow – up* con frequenza almeno annuale.

# **Altre attività di compliance**

# **Consulenza**

La Funzione Compliance, in linea con il proprio ruolo all’interno dell’organizzazione aziendale e dei compiti ad essa attribuiti, è tenuta a rilasciare pareri (c.d. *Compliance Opinion*) ad ogni Organo aziendale, Funzione e/o Struttura aziendale che ne faccia richiesta, aventi ad oggetto la compliance normativa.

L’attività di consulenza è articolata nelle seguenti fasi operative:

* ricezione della richiesta di consulenza: le richieste di consulenza possono essere distinte in: *i)* consulenza spot/ordinaria; *ii)* consulenza progettuale, volta alla definizione di linee guida operative per lo sviluppo di interventi di mitigazione del rischio di non conformità;
* istruttoria: nello specifico, la Funzione: *i)* analizza la normativa di riferimento, individuando i requisiti normativi applicabili; *ii)* recepisce ed esamina l’eventuale documentazione interna disponibile sull’argomento; *iii)* analizza gli impatti della normativa sulle attività aziendali e sulle Strutture del Confidi;
* erogazione della consulenza: a seconda del tipo di richiesta pervenuta, possono variare il percorso ed i tempi di erogazione della consulenza. In particolare, la Funzione fornisce pareri in merito ai quesiti posti, soddisfacendo le richieste di consulenza. Le tempistiche necessarie per fornire risposta alla struttura aziendale richiedente sono stabilite in base alle caratteristiche della richiesta (e.g. complessità, innovatività, urgenza) ed ai carichi di lavoro;
* archiviazione documentale: la documentazione a supporto del processo di erogazione della consulenza è archiviata in modo da consentirne un facile e tempestivo recupero;
* *follow up*: la Funzione conduce attività di monitoraggio su eventuali carenze emerse e/o proposte formulate in sede di rilascio del parere.

# **Formazione**

La formazione e l’evoluzione delle *skill* professionali costituiscono aspetti rilevanti per la qualità delle attività che le Strutture sono espressamente chiamate a svolgere sulla base della vigente normativa di vigilanza. Pertanto, la Funzione Compliance ha il compito di “*collaborare nell’attività di formazione del personale 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*”[[3]](#footnote-3).

Al riguardo, la Funzione Compliance si coordina con l’Ufficio Affari Generali e Legali e la Divisione Sviluppo per la gestione e la pianificazione dell’attività di formazione e lo sviluppo professionale del personale dipendente e della rete distributiva.

Nello specifico, la Funzione ha i seguenti compiti:

* programmare, in sede di pianificazione annuale, e dare evidenza degli investimenti destinati all’attività formativa;
* recepire nella pianificazione annuale eventuali esigenze formative;
* concordare con le Strutture sopra citate eventuali modifiche e/o integrazioni al piano annuale, tempo per tempo rivenienti dagli esiti delle attività di verifica sui rischi di Compliance.

Il processo di formazione mira a trasferire alle risorse interne al Confidi la conoscenza, la corretta interpretazione e la comprensione operativa delle normative, ed a garantire l’aggiornamento continuo e gli approfondimenti necessari al fine di costruire una cultura della conformità, trasferendo principi etici e deontologici.

# **Reporting**

L’attività di reporting rappresenta il momento di sintesi formale delle attività di controllo poste in essere dalla Funzione Compliance, sviluppata in relazione alle esigenze informative degli Organi aziendali destinatari e tenendo conto della complessità e della rilevanza degli ambiti di analisi trattati.

Il sistema di reporting è l’insieme delle relazioni e documenti predisposti:

* internamente al Confidi, ai fini dell’informativa aziendale della Funzione Compliance verso il Consiglio di Amministrazione, l’Amministratore Delegato e il Collegio Sindacale, le Funzioni di Controllo e le Strutture operative;
* esternamente al Confidi, ai fini di eventuali informative ai soggetti esterni quali l’Autorità di Vigilanza.

Pertanto, il reporting può essere:

* periodico, in quanto redatto e inviato secondo scadenze prestabilite. In tale tipologia rientrano tipicamente le informazioni periodiche e l’informativa annuale predisposte dalla Funzione Compliance e destinate agli Organi aziendali e alle Funzione di Controllo. Tali informative illustrano, nell’ambito del piano delle attività della Funzione, le verifiche effettuate ed i risultati emersi, le misure adottate per rimediare a eventuali carenze rilevate nonché le attività pianificate. Inoltre, viene riportata la situazione complessiva dei reclami ricevuti sulla base dei dati forniti dalla Struttura competente;
* ad evento, in quanto predisposto e inviato a fronte del manifestarsi di specifici eventi, anomalie e criticità.

Le caratteristiche essenziali del *report* periodico sono:

* periodicità della predisposizione (e.g. annuale, ad evento);
* rilevanza e selettività delle informazioni: deve contenere esclusivamente le informazioni rilevanti necessarie per identificare gli scostamenti rispetto ad indicatori di riferimento o periodi precedenti (e.g. numero di carenze chiuse nel periodo di riferimento, rispetto al periodo precedente);
* comunicazione efficace dei risultati: deve riportare commenti chiari[[4]](#footnote-4), concisi[[5]](#footnote-5), costruttivi[[6]](#footnote-6) e tempestivi[[7]](#footnote-7);
* tracciabilità: deve tracciare con chiarezza il percorso di analisi svolto, il livello di anomalie rilevate e il giudizio di sintesi.

In ogni caso, la Funzione Compliance informa tempestivamente gli Organi aziendali su ogni violazione o carenza rilevante riscontrata (e.g. violazioni che possono comportare un alto rischio di sanzioni regolamentari o legali, significativi impatti sulla situazione finanziaria o patrimoniale, danni di reputazione).

Con cadenza annuale, nello specifico nel corso dell’ultimo trimestre di ciascun ciclo gestionale, la Funzione Compliance predispone una relazione (i.e. “Relazione annuale”) in cui sono illustrate le attività svolte e i relativi esiti con particolare riferimento ai gap rilevati e alle azioni correttive identificate da porre alla valutazione del Collegio Sindacale e alla successiva approvazione del Consiglio d’Amministrazione. Tale relazione contribuisce a formare l’informativa annuale presentata agli Organi aziendali da parte della Funzione.

Inoltre, i *report* trasmessi all’esterno devono essere in versione definitiva e firmati, in formato “copia” non modificabile, contrassegnati con la dicitura “riservato” e da una nota in cui si specifica che ne è vietata la distribuzione ad altri senza la dovuta autorizzazione da parte della Società interessata.

1. Insieme delle sanzioni di natura penale, civile o amministrativa, associate al provvedimento normativo identificato. [↑](#footnote-ref-1)
2. Cfr. paragrafo 2.3.1 del presente Manuale [↑](#footnote-ref-2)
3. Cfr. Circolare della Banca d’Italia n.288 del 3 aprile 2015, Titolo III, Capitolo 1, Sezione III, paragrafo 2 “Funzioni di controllo di conformità” [↑](#footnote-ref-3)
4. Per “chiaro” si intende l’utilizzo di un linguaggio tecnico, privo di espressioni di dubbia interpretazione. [↑](#footnote-ref-4)
5. Per “conciso” si intende il riferimento ad informazioni essenziali per la comprensione dei fenomeni, evitando dettagli superflui. [↑](#footnote-ref-5)
6. Per “costruttivo” si intende l’individuazione pragmatica delle criticità e degli interventi correttivi da avviare. [↑](#footnote-ref-6)
7. Per “tempestivi” si intende la considerazione delle tempistiche necessarie per applicare le azioni di rimedio. [↑](#footnote-ref-7)