Regolamento di Indirizzo e Coordinamento di Gruppo per i processi in ambito ICT

Regolamento approvato dal Consiglio di Amministrazione del 10 Maggio 2022

SOMMARIO

1 PREMESSA

La disciplina del conglomerato finanziario stabilisce che siano adottati all'interno del conglomerato, tra l'altro, adeguati meccanismi di coordinamento e di controllo interno oltre a procedure di presidio gestione dei rischi.

Banca Mediolanum S.p.A. ha adottato indirizzi e indicazioni (gli "Indirizzi e Indicazioni di Conglomerato") al fine di disciplinare le necessità di coordinamento del Conglomerato (il "*Regolamento di Indirizzo e Coordinamento del Gruppo Mediolanum*", approvato dal Consiglio di Amministrazione della Banca del 20 gennaio 2022).

Tale regolamento disciplina gli ambiti rilevanti per il coordinamento di Gruppo e le funzioni di capogruppo responsabili di svolgere le attività di indirizzo e coordinamento.

In considerazione della rilevanza che i processi in ambito ICT rivestono sotto il profilo strategico, di funzionamento, di rischio e di controllo, il presente regolamento declina quanto previsto dal citato Regolamento di indirizzo e coordinamento di conglomerato, al fine di dettagliarne i processi di attuazione.

Quest'ultimo disciplina in particolare, al capitolo 4:

- gli ambiti specifici in cui si esplica il processo di indirizzo e coordinamento di Gruppo Bancario / Conglomerato;
- le principali attività relative a ciascun ambito;
- le previsioni sulla tipologia di autonomia attribuita alle società controllate per le attività identificate;
- le strutture organizzative dell'Impresa Madre coinvolte e il ruolo assegnato a ciascuna di esse.

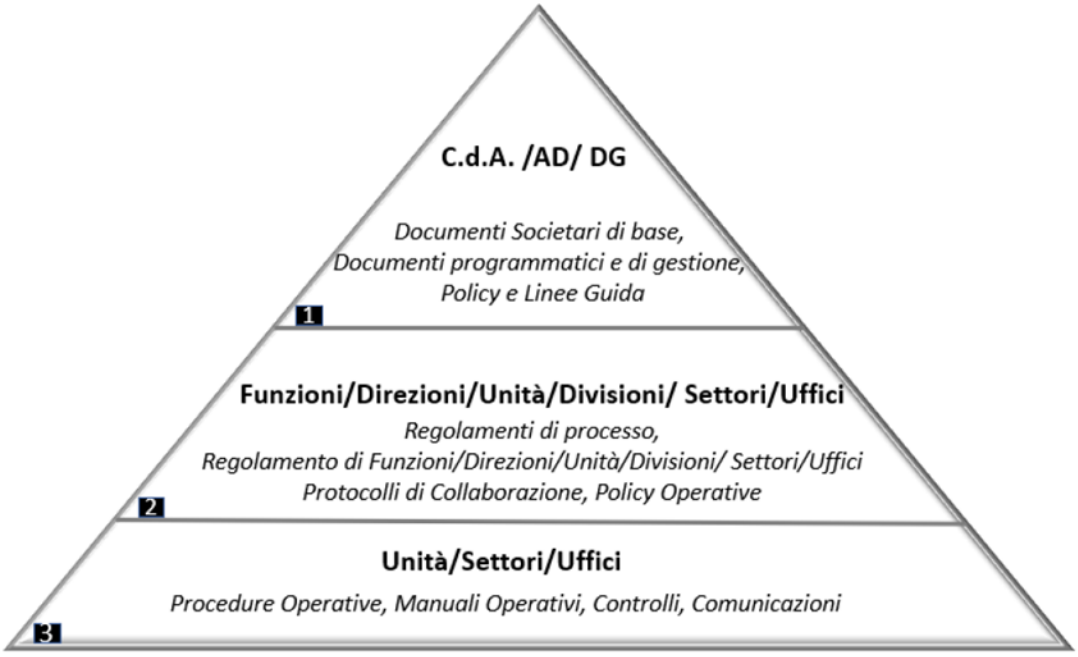
1.1 OBIETTIVO DEL DOCUMENTO

In tale contesto, la Divisione ICT, nell'esercizio della propria attività di indirizzo e coordinamento per le tematiche ICT, ha elaborato il presente regolamento che, fermi gli indirizzi e le indicazioni di Conglomerato, stabilisce con maggior dettaglio le modalità di coordinamento tra la funzione ICT di Capogruppo e le omologhe funzioni delle controllate.

A tal fine, al capitolo 4 del presente Regolamento sono riportate le Tabelle di Dettaglio di Conglomerato declinate per gli ambiti ICT.

Nello stabilire i Principi e Linee Guida, sono altresì richiamati i ruoli e responsabilità dei principali attori coinvolti nell'attività di direzione e coordinamento, in relazione all'assetto organizzativo.

Con riferimento alla "Policy sulle modalità di redazione, approvazione, diffusione ed aggiornamento della normativa interna", il presente documento si colloca al primo livello della piramide documentale richiamata nello schema seguente.



1.2 Struttura del documento

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

Capitolo 2: Gli attori coinvolti

Obiettivo del Capitolo è descrivere ruoli e responsabilità degli attori coinvolti nel processo oggetto del presente documento, esclusivamente con riferimento alle attività svolte nel processo stesso, facendo riferimento alle specifiche “figure” definite all’interno del processo.

Capitolo 3: Attività di indirizzo e coordinamento

Obiettivo del Capitolo è descrivere le modalità di indirizzo e coordinamento specifiche per gli ambiti ICT

Capitolo 4: Ambiti di dettaglio del processo di indirizzo e coordinamento

Obiettivo del Capitolo è individuare per ciascun ambito in cui si esplica il processo di indirizzo e coordinamento di Gruppo le specifiche strutture organizzative coinvolte e il ruolo da esse assunte.

Capitolo 5: Il contesto normativo

Obiettivo del Capitolo è descrivere il quadro normativo di riferimento per il processo oggetto di regolamentazione.

2 PRINCIPALI ATTORI COINVOLTI

2.1 DIVISIONE ICT DI BANCA MEDIOLANUM

La Divisione ICT in qualità di Divisione di capogruppo definisce le linee guida e gli indirizzi in ambito ICT a livello di Gruppo, e ne monitora l'attuazione da parte delle società.

Con riferimento alle Società Coordinate è compito della Divisione ICT di Banca Mediolanum verificare la coerenza di indirizzi e linee guida con la più ampia strategia del Conglomerato.

La Divisione ICT ha il compito di:

- trasmettere alle società componenti il Gruppo le disposizioni e linee guida emanate dalla Capogruppo per ciascun ambito di indirizzo e coordinamento individuato, e di quelle necessarie per dare attuazione alle istruzioni di carattere generale e particolare impartite dalle Autorità di Vigilanza, nell'interesse della stabilità del Gruppo;
- presidiare la reale attuazione delle disposizioni e linee guida emanate dalla Banca per ciascun ambito di indirizzo e coordinamento individuato;
- presidiare la corretta attuazione di azioni derivanti da attività progettuali relative a sviluppi/evoluzioni, adeguamenti normativi, modifiche di standardizzazione e di efficientamento a livello di Gruppo;
- favorire lo sviluppo di modelli idonei a soddisfare le esigenze organizzative del business di riferimento, coerentemente con gli obiettivi definiti a livello di Gruppo;
- supervisionare la corretta implementazione dei processi IT.

La Divisione ICT, ha il compito di informare tempestivamente l'Amministratore Delegato, il Direttore Generale e ogni altra Direzione/Funzione aziendale interessata per competenza, in presenza di:

- eventi rilevanti riguardanti le società controllate, derivanti da attività di monitoraggio;
- punti di attenzione rispetto alle attività per cui viene richiesta una opinion.

2.1.1 CHIEF INFORMATION OFFICER - CIO

Il Responsabile della Divisione ICT ricopre il ruolo di Chief Information Officer ("CIO") a livello di Conglomerato.
Il CIO, in coerenza con il piano strategico della Banca in qualità di Capogruppo e con l'evoluzione degli scenari tecnologici:

- definisce gli obiettivi, le politiche ed i piani di sviluppo informatico del Conglomerato, sostenendo le iniziative aziendali a supporto della definizione e attuazione della strategia;
- supporta la pianificazione e lo sviluppo strategico del Conglomerato, riportando l'andamento delle Società Controllate, italiane e estere al Comitato di Coordinamento di Gruppo e Sviluppo Strategico;
- presidia l'effettiva attuazione delle modalità di raccordo tra gli organi, le strutture e le funzioni aziendali della Banca, approvando "Binding / Non binding opinion" ove previsto, per gli ambiti di propria competenza, dove necessario può sottoporre la relativa tematica al Comitato di Coordinamento di Gruppo e Sviluppo Strategico;
- rappresenta il riferimento aziendale per le tematiche tecnologiche, presidia la gestione e lo

sviluppo dei Sistemi Informativi e cura la comunicazione con le strutture ICT delle Controllate;

- amplia, crea e mantiene relazioni basate sulla fiducia con gli stakeholder chiave sia all'interno che all'esterno dell'azienda;
- presidia l'esecuzione di eventuali attività volte alla mitigazione del rischio ICT;
- coordina la definizione del piano strategico ICT delle Controllate, promuovendo l'allineamento con gli obiettivi della Capogruppo anche in termini di costi, rischi e piani di investimento;
- presidia il governo delle tematiche relative alla sicurezza ICT.

2.2 IT GOVERNANCE

L'unità IT Governance si avvale di una struttura di IT Governance di conglomerato che supporta il CIO nell'esercizio delle sue attività attraverso:

- definizione dei processi di IT Governance;
- coordinamento dei processi IT;
- diffusione della normativa interna a supporto dei processi definiti;
- standardizzazione di un modello di valutazione dei fornitori;
- standardizzazione di un modello di rendicontazione della spesa;
- standardizzazione di template.

L'IT Governance di conglomerato inoltre:

- monitora le attività di follow up su iniziative concordate con i responsabili delle controllate;
- coordina i flussi informativi con le controllate.

2.2.1 CHIEF INFORMATION SECURITY OFFICER - CISO

Il CISO, sviluppa ed attua le strategie ed i piani complessivi di governo della sicurezza informatica, in linea con quanto disciplinato dalle politiche di Capogruppo e dagli obblighi normativi vigenti[1].

In particolare:

- definisce il quadro di riferimento metodologico e di controllo di primo livello per il presidio e per il governo della sicurezza informatica condividendolo con le strutture del Gruppo interessate;
- definisce e pianifica il piano della sicurezza informatica, come parte integrante del piano strategico ICT e dei piani operativi annuali ICT;
- presidia il recepimento delle evoluzioni normative in materia di sicurezza informatica;
- presidia la coerenza delle misure di sicurezza informatica implementate rispetto alle policy

[1] Circolare n. 285 di Banca d'Italia del 17 dicembre 2013 e successivi aggiornamenti, Capitolo 4 – Il sistema informativo, Sezione II – Governo e organizzazione del sistema informativo, 5. La sicurezza informatica e Sezione IV – La gestione della sicurezza informatica, 2. Policy di sicurezza.

divulgate;

- presidia l'esecuzione di eventuali attività di rafforzamento delle procedure di sicurezza informatica;
- definisce i requisiti e le guideline in materia di sicurezza informatica per la realizzazione di nuovi servizi ICT (security by design e privacy by design);
- definisce i requisiti e le guideline in materia di sicurezza informatica per le esternalizzazioni e ne valuta i rischi di sicurezza informatica al fine di identificare le misure di sicurezza da implementare e/o richiedere nell'ambito dell'affidamento di servizi a Terze Parti;
- presidia l'applicazione delle policy di sicurezza nell'esecuzione dei processi IT.

Il CISO assume il ruolo di CISO di Conglomerato e tale ruolo è ricoperto dal responsabile IT Governance.

2.3 ICT SOCIETÀ CONTROLLATE

Sulla base degli indirizzi ricevuti e di quanto definito dalla Divisione ICT di Banca Mediolanum, operano all'interno del processo di indirizzo e coordinamento secondo due possibili livelli di autonomia nell'adozione delle soluzioni di attuazione delle disposizioni emanate dalla Capogruppo:

- **autonomia decisionale**: le società controllate declinano e personalizzano gli indirizzi strategici e le linee guida definiti dalla Capogruppo nel rispetto delle normative locali e in base alle proprie esigenze di business e di mercato, individuando le soluzioni più idonee a garantire la coerenza fra le linee guida e gli indirizzi strategici ricevuti e le specifiche realtà ed esigenze locali;
- **autonomia esecutiva**: le società controllate definiscono le modalità operative attraverso le quali attuare le linee guida e gli indirizzi strategici definiti dalla Capogruppo, seguendo le eventuali indicazioni di dettaglio ricevute.

Il dettaglio del livello di autonomia per gli specifici ambiti di indirizzo e coordinamento individuati è riportato al successivo Capitolo 4.

3 ATTIVITÀ DI INDIRIZZO E COORDINAMENTO

Il processo di indirizzo e coordinamento di Gruppo può prendere avvio secondo due differenti modalità:

a) direttamente dalla Capogruppo, la quale nel suo ruolo attivo nei confronti delle società controllate definisce e fornisce le linee guida e gli indirizzi strategici, per gli ambiti individuati e descritti nel presente paragrafo;

b) su iniziativa delle società controllate, le quali possono richiedere alla Capogruppo di fornire le indicazioni strategiche per specifici ambiti di interesse.

La Divisione ICT ha la responsabilità di definire, per i processi in ambito ICT, le linee guida (es. policy, procedure operative) a cui le controllate devono attenersi ed è inoltre responsabile della divulgazione delle stesse e di verificare il recepimento da parte delle controllate.

3.1 Attività di coordinamento

L'unità competente collabora costantemente con la società controllata fornendo eventuali approfondimenti o dettagli sui contenuti tecnici delle linee guida e degli indirizzi operativo – funzionali forniti, se necessario, anche con il supporto di altre funzioni aziendali competenti, secondo i dettagli riportati al successivo capitolo 4.

In particolare, la Divisione ICT, nell'ambito dei servizi infra-gruppo, eroga la gestione dei sistemi informativi alle Società del Conglomerato Finanziario, che hanno in essere un contratto di prestazione di servizi con la Banca.

L'attività di coordinamento della Divisione ICT nei confronti delle Società Controllate per le quali non eroga la gestione dei sistemi informativi, si sviluppa attraverso i seguenti strumenti:

- Coordinamento continuativo, tramite incontri periodici con le omologhe funzioni delle controllate;
- Ricezione e verifica dei flussi informativi ricevuti dalle controllate (es. per ambiti su cui la controllata non si discosta dalle linee guida, ma su cui la Capogruppo intende effettuare un monitoraggio).

In particolare, i flussi informativi dalle controllate verso la capogruppo devono riportare, su base regolare:

- Andamento del servizio (disponibilità);
- Andamento incidenti IT;
- Andamento Costi IT;
- Macro-pianificazione e andamento progetti strategici ICT;
- Monitoraggio esternalizzazioni;
- Verifiche di audit e compliance;
- HR e relativa organizzazione IT;
- Attuazione delle disposizioni emanate dalla Capogruppo;
- Informative regolamentari (es. Reporting BCE/SRB).

3.2 Attività di indirizzo

La Divisione ICT può essere coinvolta ex ante nel processo in esame, eventualmente anche su richiesta delle società controllate, mediante il rilascio di pareri vincolanti o non vincolanti (c.d. binding opinion – BO / non binding opinion – NBO) in merito alle azioni / scelte che la società controllata desidera intraprendere, comunque nel rispetto della piena responsabilità degli organi con funzione

di supervisione strategica della società controllata stessa.
Nel caso di una non binding opinion, il parere espresso dalla Divisione ICT non è vincolante per la società controllata, la quale nel pieno della propria responsabilità potrà assumere le azioni /decisioni preposte anche in caso di parere "non favorevole".

Secondo quanto previsto dal Regolamento di indirizzo e coordinamento di Conglomerato, l'attività di coordinamento della Divisione ICT nei confronti delle Società Controllate si sviluppa nel perimetro dell'unità competente Direzione Service Operations &ICT, come segue:

Principali macro-attività	Binding /Non Binding Opinion (BO/NBO/NA)	Autonomia delle Controllate	Unità competente	Altre unità/organi coinvolti della Capogruppo
Indirizzi in ambito sistemi informativi (es. strategie, ruoli e responsabilità etc.)	**NA**	**E**	*Direttore Generale / Service, Operations & ICT*	*Comitato Coordinamento di Gruppo e Sviluppo Strategico, Unità organizzative a seconda della tematica*
Processo di pianificazione IT per specificità locali	**BO/NBO**	**E**	*Direttore Generale/Service, Operations & ICT*	*Unità organizzative a seconda della tematica*
Progettualità in ambito IT	**BO/NBO**	**D**	*Direttore Generale/ Service, Operations & ICT*	-
Business Continuity e Disaster Recovery	**BO/NBO**	**E**	*Direttore Generale/Portafoglio Progetti & Sviluppo Organizzativo per BC* *Direttore Generale/ Service, Operations & ICT per DR*	*Comitato Business Continuity, Comitato di Gestione della Crisi*

Per ciascun ambito definito sono state individuate le specifiche attività oggetto di indirizzo e coordinamento da parte della Capogruppo e definiti, per ciascuna attività, i seguenti elementi di dettaglio:

- **Tipologia di autonomia delle società controllate:** si distingue tra autonomia decisionale ("D") o esecutiva ("E") nell'adozione delle soluzioni di attuazione delle disposizioni emanate dalla Capogruppo;
- **Unità competente**: svolge un ruolo di coordinamento delle attività svolte dalle società controllate e di integrazione delle stesse rispetto ai piani e alle scelte strategiche di Gruppo. L'Unità competente è individuata tra le Direzioni/Funzioni di Capogruppo, in base al proprio ambito di competenza per lo specifico ambito di indirizzo e coordinamento, come precedentemente definiti;
- **Unità di supporto/specialistica**: strutture organizzative coinvolte nel processo di indirizzo e coordinamento, a supporto delle unità competenti primarie;
- ***"Binding opinion" – BO***: sono indicate le attività per le quali è previsto che la società controllata richieda la BO alla Capogruppo;
- ***"Non binding opinion" – NBO***: sono indicate le attività per le quali è previsto che la società controllata richieda la NBO alla Capogruppo.

Se prevista per la specifica tematica la richiesta di una "Binding Opinion/Non Binding Opinion" da parte della Capogruppo, il referente della società controllata competente per materia, provvede ad effettuarne opportuna richiesta fornendo tutte le informazioni di dettaglio sulla soluzione specifica che la controllata intende adottare. Tale richiesta deve essere inoltrata tramite mail, all'unità IT Governance che si avvarrà delle diverse unità specialistiche al fine di supportare il CIO nel rispondere alla richiesta di Opinion.

A conclusione dell'implementazione della soluzione operativa identificata per l'adozione degli indirizzi, la società controllata ne fornisce informativa all'IT Governance, unitamente a tutti i relativi dettagli (es. invio normativa interna adottata, etc.).

4 AMBITI DI DETTAGLIO DEL PROCESSO DI INDIRIZZO E COORDINAMENTO DI GRUPPO

Di seguito sono riportate le informazioni di dettaglio relative a:

- gli ambiti di dettaglio in cui si esplica il processo di indirizzo e coordinamento di Gruppo;
- le principali attività specifiche relative a ciascun ambito;
- le previsioni sulla tipologia di autonomia attribuita alle società controllate per le attività identificate;
- le strutture organizzative della Capogruppo coinvolte e il ruolo assegnato a ciascuna, come descritto ai paragrafi precedenti.

3.1 Indirizzi in ambito sistemi informativi (es. strategie, ruoli e responsabilità)

ID	Attività	Binding /Non Binding Opinion (BO/NBO/NA)	Autonomia delle Controllate	Unità competente	Unità di supporto/specialistica
A.1	***Aggiornamento della strategia ICT (inclusa ICT Security) rispetto alla Capogruppo***	**NBO/BO**	**D**	*Divisione ICT*	*IT Governance*
A.2	***Attivazione nuova FEI/NFEI /fornitura a servizio-Cloud ICT***	**NBO**	**D**	*Divisione ICT*	*IT Governance*

La Divisione ICT è inoltre coinvolta dalla Direzione Risorse Umane nell'ambito dei processi di valutazione e rilascio di Non Binding Opinion alle società controllate relativamente alla nomina di figure apicali ICT.

3.2 Processo di pianificazione IT per specificità locali

ID	Attività	Binding /Non Binding Opinion (BO/NBO/NA)	Autonomia delle Controllate	Unità competente	Unità di supporto / specialistica
B.1	***Condivisione Piano Operativo delle iniziative informatiche***	**NBO**	**D**	*Divisione ICT*	*IT Governance*

3.3 Progettualità in ambito IT

ID	Attività	Binding /Non Binding Opinion (BO/NBO/NA)	Autonomia delle Controllate	Unità competente	Unità di supporto/ specialistica
C.1	***Attivazione/approvazione progetti rilevanti che prevedono una spesa di importo rilevante rispetto alla Legal Entity / strategici / che deviano rispetto al piano strategico***	**NBO**	**D**	*Divisione ICT*	*IT Governance*

3.4 Business Continuity e Disaster Recovery.

ID	Attività	Binding /Non Binding Opinion (BO/NBO/NA)	Autonomia delle Controllate	Unità competente	Unità di supporto/specialistica
D.1	***Definizione/aggiornamento piano DR***	**NBO**	**D**	*Divisione ICT*	*IT Operation & infrastructure*

5. PRINCIPALE NORMATIVA DI RIFERIMENTO

5.1 NORMATIVA INTERNA

I principali riferimenti di normativa interna sono le vigenti versioni di:

- Regolamento di indirizzo e coordinamento del Gruppo Mediolanum

5.2 NORMATIVA ESTERNA

- Circolare n. 285 di Banca d'Italia del 17 dicembre 2013 e successivi aggiornamenti