MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

Protocollo Sisifo: **8254818\20**

Siena, 31/08/2018

FUNZIONI COMPILATRICI:
Segreteria Tecnica CAE - MPS

Comunicazione per:
Consiglio Di Amministrazione - MPS

OGGETTO:

Azioni di miglioramento conseguenti agli esiti dell'attività di audit e forensic sul processo di segnalazione di diamanti da investimento alla clientela e ai recenti interventi normativi da parte dell'Autorità di Vigilanza: identificazione e pianificazione di ulteriori iniziative di rafforzamento dei presidi deliberativi, di processo e di controllo.

1. MOTIVAZIONE

In data 27 luglio 2018, l'Amministratore Delegato (di seguito, AD) ha approvato la proposta, portata alla sua attenzione in data 24.07.2018 da parte delle Funzioni Internal Audit e Compliance, avente ad oggetto il «*Piano di azioni di miglioramento conseguenti agli esiti dell'attività di revisione e forensic sul processo di segnalazione di diamanti da investimento alla clientela e ai recenti interventi normativi da parte dell'Autorità di Vigilanza*».

Tale proposta trae origine dall'informativa inviata dallo stesso AD alle sopra citate funzioni in data 19.03.2018 nella quale veniva richiesto di individuare specifiche azioni migliorative/di rimedio per assicurare che i processi e i comportamenti inerenti alle attività di individuazione, produzione e gestione, commercializzazione e monitoraggio/controllo prodotti (con riferimento anche, ma non solo, alle cd. "*attività connesse*"), da un lato, tengano conto delle evidenze emerse dalle attività svolte di *audit* e *forensic* in tema di segnalazione di diamanti da investimento alla clientela (completatesi con la presentazione da parte di Deloitte Forensic dell'*Elaborato Tecnico Conclusivo* del 28.05.2018 in Consiglio di Amministrazione in data 31.05.2018) e, dall'altro, vengano effettuati in modo adeguato e conforme a quanto contenuto nella comunicazione di Banca d'Italia dell'8 marzo scorso[1], ovvero conseguentemente alle indicazioni della vigilanza europea in materia di *governance* e controllo sui prodotti offerti alla clientela, in particolare "*retail*".

La suddetta proposta, che riporta in particolare gli esiti degli approfondimenti condotti dalle Funzioni compilatrici unitamente a un gruppo di lavoro operativo interfunzionale allo scopo costituito, ha sviluppato un piano di azioni teso a migliorare i seguenti ambiti:

- ✓ i processi di approvazione, commercializzazione, monitoraggio e controllo dei nuovi prodotti e di eventuali "attività connesse" esercitabili dalla Banca;
- ✓ le modalità tecnico-operative e comportamentali da adottare da parte dei dipendenti in materia di archiviazione della posta elettronica e della documentazione di lavoro sui *server* aziendali e ciò per garantire una migliore salvaguardia e tutela del patrimonio informativo della Banca, oltre che una adeguata profondità storica e una maggior facilità di accesso in casi di esigenze di revisione.

Le linee guida associate al suddetto piano hanno come principale obiettivo quello di ridurre al minimo il rischio potenziale che fenomeni come quelli rilevati nel caso dei diamanti da investimento possano in futuro ripresentarsi senza essere immediatamente intercettati, governati e controllati nel modo più opportuno.

[1] *Attività connesse esercitabili dalle banche*", Banca d'Italia, lettera dell' 08.03.2018.
[2] *Orientamenti sulla governance interna*", EBA, 26.09.2017, pubblicato in lingua italiana in data 21.03.2018: rif. par. 18 "*Nuovi prodotti e modifiche significative*" (gli orientamenti si applicano dal 30.06.2018) e "*Orientamenti sui dispositivi di governance e di controllo sui prodotti bancari al dettaglio*", EBA, pubblicati in data 22.03.2016, che invece si applicano a partire dal 03.01.2017.

A seguito dell'approvazione da parte dell'AD di tali linee guida, queste ultime sono state prese in carico dalle rispettive Funzioni *owner* (Direzioni CCO e COO), compilatrici della presente informativa unitamente alla Direzione CAE e all'Area Compliance, che hanno quindi avviato un'attività progettuale volta alla loro effettiva realizzazione sulla base di un piano dettagliato nei tempi e nei modi di seguito rappresentato.

Obiettivo della presente informativa è quindi portare all'attenzione del Consiglio di Amministrazione (di seguito, CdA) il piano definitivo di interventi delineato e i relativi ruoli di responsabilità identificati.

2. ELEMENTI CHIAVE DELL'INFORMATIVA

Portare a conoscenza del CdA:

- ✓ gli esiti degli approfondimenti interni condotti in materia di individuazione delle linee guida relative alle azioni di miglioramento conseguenti alle evidenze emerse dalle attività di internal audit e *forensic* in tema di segnalazioni di diamanti da investimento alla clientela e concernenti:
  - il processo di *product approval & governance* attinente alle fasi di approvazione, commercializzazione, monitoraggio e controllo dei nuovi prodotti offerti alla clientela e/o di eventuali "attività connesse" esercitabili dalla Banca;
  - il rafforzamento delle modalità tecnico-operative e le norme comportamentali di archiviazione della posta elettronica e della documentazione di lavoro;
- ✓ il piano di azione con l'individuazione delle Funzioni responsabili volto a finalizzare le azioni correttive necessarie a rafforzare ulteriormente il sistema dei controlli su tale ambiti comprensivo delle relative tempistiche.

Il CdA sarà coinvolto in specifici passaggi deliberativi concernenti la revisione delle *policy* e dei processi inerenti la realizzazione del piano di azioni migliorative e riguardanti, tra l'altro, anche le nuove responsabilità che esso stesso verrà a ricoprire in tali processi.

3. INFORMAZIONI RILEVANTI

L'esigenza di definire un piano di interventi, richiesto dall'AD con la citata lettera del 19.03.2018, scaturisce, oltreché dai contenuti della sopra citata lettera di Banca d'Italia in materia di "attività connesse" e delle più recenti linee guida emanate dall'EBA in materia di *corporate governance* e di controlli sui prodotti bancari, anche dalle evidenze emerse all'esito degli interventi eseguiti dalle funzioni di *audit* interno[3] e da Deloitte *Forensic*[4] sul processo di segnalazione a società terze di

[3] I documenti pubblicati dalla Direzione CAE e le relative date di passaggio in CdA sono di seguito evidenziati:

- » *Rapporto 228/2017, pubblicato in data 05.12.2017 - Assessment sul processo di segnalazione a società terze di clientela interessata all'acquisto di diamanti da investimento e conformità dei comportamenti agiti, CdA del 12.12.2017;*
- » *Rapporto 229/2017, pubblicato in data 05.12.2017 - Assessment sul processo di segnalazione a società terze di clientela interessata all'acquisto di diamanti da investimento e correttezza dei comportamenti agiti dai principali responsabili, CdA del 12.12.2017;*
- » *Rapporto 120/2018, pubblicato in data 20.03.2018 - Segnalazione a società terze di clientela interessata all'acquisto di diamanti da investimento, Integrazione Assessment 228/2017 Passaggi Formali e Comitati, CdA 22.03.2018;*
- » *Aggiornamento del rapporto n.120/2018, pubblicato in data 05.04.2018 - Segnalazione a società terze di clientela interessata all'acquisto di diamanti da investimento., CdA del 17.04.2018.*

[4] Di seguito invece quanto prodotto da Deloitte Forensic e le date di passaggio in CdA:

- » *Project Ice - Elaborato tecnico preliminare, datato 12 gennaio 2018, CdA del 16.01.2018;*
- » *Project Ice - Ulteriori approfondimenti condotti, datato 20 marzo 2018, CdA del 22.03.2018;*
- » *Project Ice – Elaborato Tecnico conclusivo, datato 28 maggio 2018, CdA del 31.05.2018.*

clientela interessata all'acquisto di diamanti da investimento, svoltosi nel periodo gennaio 2013 febbraio 2017, e riconducibile a una cd. "attività connessa" (tali evidenze emerse dalle attività di audit e *forensic* sono riepilogate al successivo paragrafo 6 in cui sono riportati rispettivamente gli ambiti di miglioramento identificati con riguardo ai processi relativi a nuovi prodotti e attività connesse e all'archiviazione della posta e documenti elettronici).

Nei successivi paragrafi si intende altresì evidenziare come le linee guida di tale piano proposte all'AD e dal medesimo approvate si inseriscano all'interno di un processo di *product approval & governance* e di un sistema dei controlli interni che, principalmente nel corso dell'ultimo biennio, si è evoluto in modo sostanziale e che ha già di fatto portato a un rafforzamento dei presidi operativi tale da creare di per sé una totale discontinuità con la situazione in essere nel periodo relativo all'attività di segnalazione di diamanti da investimento alla clientela.

Di seguito (par. 4) sono riportati gli aspetti principali di questa evoluzione, nonostante i quali si evidenzia, nel proseguo della presente Comunicazione (par. 5), la necessità di procedere ad ulteriori aggiornamenti dei processi e delle procedure aziendali per essere non solo conformi alle nuove disposizioni della vigilanza europea e nazionale e garantire un adeguato presidio di tali materie, ma soprattutto per tener conto delle "*lesson learnt*" come conseguenza delle attività di audit e *forensic* effettuate nell'arco temporale compreso tra il 1° agosto 2017 e fine maggio 2018.

La presente Comunicazione illustra il citato piano di azione indirizzato a mitigare le criticità rilevate tale da permettere di assicurare che sia i processi e i comportamenti inerenti alle attività di individuazione, produzione e gestione, commercializzazione e monitoraggio/controllo prodotti (con riferimento anche, ma non solo, alle cd. "*attività connesse*"), sia le modalità tecnico-operative e i relativi comportamenti inerenti l'archiviazione della posta elettronica e della documentazione di lavoro, vengano effettuati in modo adeguato e in conformità a quanto contenuto nelle disposizioni normative e siano quindi di conseguenza tali da garantire che evidenze quali quelle riscontrate nel caso dell'attività di segnalazione di diamanti da investimento alla clientela non possano più ripresentarsi nelle medesime modalità (par. 7 e 8).

4. – EVOLUZIONE DEL SISTEMA DEI CONTROLLI INTERNI NELL'ULTIMO BIENNIO

Le funzioni di controllo nel corso dell'ultimo biennio hanno subito varie modifiche organizzative e di assetto che hanno contribuito a rafforzarne i relativi presidi sui vari ambiti di interesse. Ulteriori contributi sono pervenuti dalla stessa Autorità di Vigilanza a seguito di attività ispettive in loco (*On Site Ispection* - OSI) e/o verifiche a distanza (*Thematic review*) in termini di azioni di rimedio realizzate. Miglioramenti infine riguardo ai meccanismi relazionali hanno permesso di efficientare i flussi informativi tra le stesse funzioni di controllo così come tra queste e gli Organi di supervisione e controllo della Banca.

Particolare rilevanza rispetto a questa evoluzione è attribuibile ai risvolti positivi derivanti dalle valutazioni esterne di *Quality Assurance Review* (di seguito QAR), condotte sulle funzioni di controllo di secondo (Risk Management e Antiriciclaggio) e terzo livello (Internal Audit) da primarie società di consulenza che hanno permesso di individuare ambiti di miglioramento specifici e livelli di efficacia ed efficienza da rafforzare rispetto ai requisiti normativi e alle *best practice* adottate dal sistema.

In particolare sulla Funzione di Internal Audit, già oggetto di una valutazione esterna nel 2014, è stata condotta nel 2017 un'attività di *follow-up* che si è configurata come un vero e proprio nuovo *assessment*, attraverso l'analisi documentale, l'esame della metodologia, degli strumenti operativi di controllo e della reportistica. Tale analisi ha consentito di constatare, dopo due anni dal precedente QAR, il livello di conformità dell'attività di audit nonché di valutarne l'efficienza e l'efficacia e la capacità di adattamento al contesto in evoluzione, sia interno che esterno, anche

mediante il confronto con le principali *best practice* di settore. In tale contesto sono state altresì rilevate alcune ulteriori aree di potenziale sviluppo evolutivo, sulle quali la Funzione si è adoperata a finalizzare le relative azioni correttive, in particolare la rivisitazione del *framework* metodologico di valutazione del sistema dei controlli interni e la conseguente evoluzione dello schema di *reporting* attraverso la definizione di meccanismi di raccordo tra il modello di audit in uso e gli obiettivi di controllo ricavati dai pilastri del processo SREP e il rafforzamento del *set* di strumenti di controllo a distanza, tramite l'ampliamento del novero di indicatori definiti sui processi di rete.

Anche sulla Funzione di Risk Management nel corso del 2017 è stato condotto un *assessment* teso a valutare il *framework* interno rispetto ai principali requisiti normativi, alle aspettative del supervisore e alle *best practice* di mercato. I risultati della valutazione hanno evidenziato un ampio livello di conformità rispetto ai requisiti normativi per gli ambiti di *Risk Internal Governance e Risk Management Framework & Risk Culture*. Da rafforzare invece, se confrontato con i *competitor* rilevanti, l'ambito inerente la *Risk Infrastructure, Data and Reporting*. Sull'insieme di tali ambiti la Direzione CRO ha in corso specifiche attività progettuali.

Un esercizio di *assessment* condotto nel periodo novembre 2017 - gennaio 2018 anche sulla Funzione Antiriciclaggio (AML) ha permesso di valutarne la robustezza del modello interno dei presidi in essere in termini di posizionamento nell'organizzazione della Capogruppo, assetto organizzativo, esecuzione di *benchmarking* presso *peer* comparabili, adeguatezza delle metodologie di gestione del rischio di riciclaggio e modello di *governance* adottato ed efficacia nel presidio delle attività AML. L'esito ha individuato varie priorità di intervento in particolare relativamente ad ambiti di *governance* societaria (modalità di accentramento/decentramento sia dei presidi AML delle singole Società del Gruppo sia della valutazione della clientela a rischio alto), e operativi e di presidio di altre strutture della Banca (attività formative, razionalizzazione della struttura dei controlli di I livello; sviluppo della reportistica). Gli ambiti di miglioramento sono stati indirizzati nel piano di azione 2018 della Funzione AML e si completeranno nel corso del 2019.

E' infine a programma il completamento della valutazione delle funzioni di controllo di secondo livello con l'avvio nell'ultimo trimestre 2018 di uno specifico QAR anche sulla funzione Compliance.

Relativamente agli assetti organizzativi e ai relativi incarichi di responsabilità, in meno di due anni in ottica, di *change management*, sono stati avvicendati la quasi totalità dei responsabili delle funzioni di controllo[5].

Nell'ambito delle richieste dell'Autorità di Vigilanza a seguito di attività ispettive (cfr. OSI-32-33), particolare rilevanza ha assunto, quale rafforzamento dei presidi di primo livello, la costituzione deliberata dal CdA in data 21.11.2016 dell'Area Controlli, Conformità e Reclami a diretto riporto del CCO, con competenza sul perimetro delle filiali e dei centri[6]. Sin dalla sua costituzione, ha esercitato il proprio riporto funzionale per indirizzare le attività dei Settori già esistenti nelle Aree Territoriali e riportanti gerarchicamente al loro Responsabile. Le principali attività progettuali hanno già permesso di realizzare alcuni importanti interventi tra cui la mappatura dei controlli di 1° livello esistenti in Rete (attinenti ambiti di conformità, antiriciclaggio, comportamentali, sui servizi di investimento, ecc.), il relativo monitoraggio e una semplificazione accompagnata all'accentramento di una parte di essi direttamente nei presidi di controllo, rafforzando altresì lo scambio di flussi informativi da/verso le funzioni di controllo di 2° e 3° livello.

Sempre con riferimento alle funzioni di controllo di 1° livello, sono stati costituiti il Servizio

[5] Il responsabile dell'Area Compliance (2° liv) è in carica dal 01.07.2015, mentre, per quanto riguarda le altre funzioni di controllo, il nuovo responsabile della Direzione CAE (3° liv) è in carica dal 15.11.2016, il nuovo responsabile della Direzione CRO (2° liv) è in carica dal 13.03.2018 e il nuovo responsabile del Servizio AML-CFT (2° liv) è in carica dal 04.12.2017.

[6] La suddetta Area ha subito provveduto alla mappatura della situazione *as is* ed alla relativa *gap analysis*, predisponendo un progetto presentato al Comitato Direttivo del 26.04.2017. Ciò andava incontro alle richieste pervenute dall'Autorità di Vigilanza a seguito di accertamenti ispettivi, indicazioni contenute nel *finding* #5 della OSI-32-33 relativamente ai controlli di 1° livello.

Qualità Processo Creditizio (febbraio 2017) e il Servizio Supporto Specialistico e Qualità Crediti Non Performing (ottobre 2017), con il compito, tra gli altri, di garantire il monitoraggio della qualità del processo e del portafoglio creditizio su posizioni rispettivamente in gestione ordinaria e *non performing*.

Ulteriori rafforzamenti sono stati richiesti a seguito degli esiti della OSI-32-33 anche alle Funzioni Compliance e AML-CFT[7] che hanno portato alla finalizzazione di specifiche attività nel corso del 2017. Nello specifico, si è proceduto ad accentrare presso la Funzione Compliance di Capogruppo sia i Presidi Specialistici di conformità[8] sia le Funzioni Compliance presenti presso le Società controllate italiane (MPS Capital Services, Consorzio Operativo GMPS, Widiba, MPS Leasing Factoring, MPS Fiduciaria). Con riferimento invece al piano di azione sull'antiriciclaggio, si è proceduto a rafforzare i controlli di 1° livello (cfr. quanto riportato sopra sull'Area Controlli, Conformità e Reclami), i meccanismi di coordinamento con le filiali e controllate estere, la definizione di iniziative per diffondere la consapevolezza delle tematiche AML presso la rete delle filiali, un incremento di organico presso la Funzione AML-CFT da un punto di vista sia qualitativo che quantitativo, l'attivazione di un'informativa periodica verso gli Organi aziendali su carenze individuate/azioni correttive e sull'alimentazione dell'Archivio Unico Informatico (AUI).

Riguardo infine al rafforzamento dei meccanismi informativi tra le funzioni di controllo, la partecipazione delle stesse ai vari Comitati endoconsiliari, di gestione e operativi si è intensificata nel corso dell'ultimo anno permettendo una maggiore sinergia e un adeguato scambio informativo su temi di reciproco interesse[9].

Per quanto riguarda in particolare la partecipazione delle funzioni di controllo ai comitati endoconsiliari, e nello specifico al Comitato Rischi, a seguito di una richiesta da parte del JST-BCE avanzata a seguito della "*Thematic review on risk governance and appetite*" del 2015 con la quale era stata evidenziata la necessità che il CRO avesse accesso diretto e incondizionato a tale Comitato, si è provveduto ad apportare le opportune azioni correttive in base alle quali non solo il CRO (da maggio 2016), ma anche il CAE (da marzo 2017) e il responsabile della Funzione Compliance (da novembre 2017) vengono istituzionalmente e regolarmente tenuti al corrente dell'ordine del giorno delle riunioni del Comitato e possono decidere discrezionalmente di parteciparvi, cosa che di fatto si verifica a ogni adunanza di tale Organo.

Il responsabile della DCAE presenzia inoltre regolarmente alle adunanze del Collegio Sindacale su invito del suo Presidente.

È stato infine rafforzato il ruolo del Comitato per il Coordinamento delle Funzioni con Compiti di Controllo il quale, come noto, si configura come un momento di sintesi e di confronto tra le varie funzioni aziendali di controllo di 2° e 3° livello. Nella riunione del Comitato dello scorso 28 giugno è stato infatti deliberato di estenderne la partecipazione alle funzioni di controllo di 1° livello (del CCO e del CLO) al fine di rafforzare ulteriormente i meccanismi relazionali e i relativi presidi su materie di interesse, così da favorire una valutazione complessiva del presidio dell'intero sistema dei controlli sui processi aziendali. Sono state inoltre recentemente rafforzate alcune responsabilità del Comitato, tra cui quella di coordinare le diverse iniziative progettuali connesse al sistema dei controlli con l'intento di ottimizzare gli interventi identificando possibili sinergie, sovrapposizioni e aree di razionalizzazione in ottica di costi/benefici. In tale contesto particolare importanza assume

[7] Cfr. *finding* #4 della OSI-32-33 sulla Funzione Compliance e *finding* #9 della OSI-32-33 sulla Funzione AML-CFT.

[8] Ad eccezione di quelli che presidiano le aree normative di "salute e sicurezza sui luoghi di lavoro" e "*tax compliance*" i quali mantengono le responsabilità di gestione del rischio di non conformità per le materie di competenza presso le proprie strutture organizzative.

[9] Comitato Gestione Rischi: il responsabile della Funzione di Internal Audit è sempre stato invitato quale membro senza diritto di voto mentre il responsabile della Funzione Compliance, è membro effettivo dal mese di novembre 2015 e votante e da ottobre 2017 a tutte le sessioni programmate (sessioni Credit, Financial e Operational Risk). Il responsabile della Funzione AML-CFT è invece membro effettivo e votante della sola Sessione Operational Risk dal mese di ottobre 2017. Comitato Direttivo: dal mese di ottobre 2016 e da inizio 2017 vi partecipano rispettivamente anche il CAE e il Responsabile della Funzione Compliance (il CRO partecipa da più tempo).

anche la condivisione dei *gap* e/o delle azioni di rimedio rivenienti non solo da tutte le funzioni di controllo, ma anche dalle Autorità di Vigilanza a seguito di attività ispettive o comunque tali da generare iniziative della specie, con l'intento di valutarne la rilevanza e gli impatti della relativa mitigazione e conseguentemente definire le strategie di intervento complessive in ottica integrata di gestione delle iniziative nel rispetto dei requisiti di indipendenza delle singole funzioni partecipanti.

5. – NORMATIVE E POLICY INTERNE

Il sistema normativo aziendale si caratterizza per la presenza di diversi documenti volti a disciplinare i processi di approvazione dei prodotti ed è stato oggetto di recente aggiornamento in relazione all'entrata in vigore da inizio 2018 della MiFID II con riferimento, in particolare, ai prodotti di investimento. Di seguito viene riepilogata la cronologia della principale normativa di riferimento in base alla data del più recente aggiornamento o della relativa emanazione.

- D 1098 - *Distribuzione derivati OTC.* Il documento norma le attività di distribuzione dei derivati OTC nel rispetto delle regole interne di distribuzione previste nel documento normativo D1820 (vedi oltre) e di quelle esterne. Ultimo aggiornamento **26.05.2017**.
- D2241 - *Direttiva in materia di Governance e controllo su prodotti bancari retail.* La Direttiva recepisce le linee guida emanate dall'EBA in data 22.03.2016 (cfr. "*Orientamenti sui dispositivi di governance e di controllo sui prodotti bancari al dettaglio*"). Emanata in data **12.09.2017**.
- D1444 - *Gestione collaboratori con reti alternative.* Il documento norma le modalità di contrattualizzazione e di gestione degli accordi con le reti terze, intese come intermediari (mediatori creditizi) che presentano i requisiti necessari per veicolare prodotti e servizi bancari alla clientela, in particolare mutui e finanziamenti destinati a privati e aziende. Ultimo aggiornamento 0**9.10.2017**.
- D1820 - *Direttiva di Gruppo in materia di operatività in derivati OTC con la clientela*. Il documento definisce il modello organizzativo adottato dal Gruppo (principi e responsabilità) per il processo "Operatività in derivati OTC con la clientela". Il processo ha l'obiettivo di presidiare la definizione del modello di *business* previsto per la commercializzazione dei derivati di tipo *over the counter* (OTC), le modalità di distribuzione in base alla tipologia di clientela interessata e i criteri per la distribuzione di tali prodotti. Ultimo aggiornamento **30.11.2017**.
- D2277 - *Direttiva di Gruppo in materia di governance e controllo su prodotti finanziari per la clientela*. Emanata in data **21.12.2017**, la Direttiva recepisce i principi, applicabili a partire dal 03.01.2018 e relativi alla *governance* e controllo su strumenti finanziari di cui alla Direttiva Europea 2014/65/UE (MiFID II), agli artt. 9 e 10 della Direttiva delegata n. 2017/593 della Commissione Europea del 07.04.2016 e al *Final Report* ("*Guidelines Product Governance*") dell'ESMA del 02.06.2017, cui deve attenersi il Gruppo MPS.
- D2272 *Policy di Gruppo in materia di prodotti*. La *Policy*, il cui ultimo aggiornamento è del **22.12.2017**, definisce modelli e principi generali adottati per il macro processo prodotti che riguarda l'ambito dello sviluppo, acquisizione e gestione dei nuovi prodotti o servizi, sviluppo di nuove attività, ingresso in nuovi segmenti operativi o di mercato, sia destinati alla clientela del Gruppo che ai portafogli di proprietà.
- D920 - *Direttiva di Gruppo in materia di sviluppo, acquisizione e gestione prodotti*. La Direttiva declina il modello organizzativo adottato per il processo di sviluppo, acquisizione e gestione prodotti, riferito ai prodotti destinati alla clientela e ai portafogli di proprietà. Ultimo aggiornamento **22.12.2017**.

- D752 - *Regolamento n. 3 – Deleghe di autonomia in materia di prodotti e condizioni*. Il documento definisce le autonomie in materia di condizioni, inclusi tassi, abbuoni alla clientela e rettifiche per errori/disguidi nell'applicazione di condizioni, fissandone le norme, i criteri, le modalità e i limiti di attribuzione. Ultimo aggiornamento **09.02.2018**.
- D1817 - *Sviluppo, acquisizione e gestione prodotti*. Documento di processo oggetto di revisione in data **16.04.2018** per implementare le sezioni di cui alla fase di studio di fattibilità di nuovi prodotti prevedendo, nei casi di impatto sul profilo di rischio, un adeguato *risk assessment*, nonché l'approvazione da parte del Comitato Gestione Rischi.
- D2335 - *Regole in materia di determinazione e transcodifica del Target Market dei prodotti finanziari*. Emanato in data **29.06.2018** e afferente il "*Target Market* dei prodotti finanziari" (documento di tipo operativo). Rimangono a oggi ancora da definire alcuni processi 'minori' in attesa della pubblicazione delle linee guida ABI sul tema.
- D2113 - *Direttiva di Gruppo in materia di consulenza sugli investimenti*. Il documento definisce il modello organizzativo adottato dal Gruppo (principi, responsabilità e processi) per il processo di "consulenza sugli investimenti". Ultimo aggiornamento del **30.06.2018**.
- D2262 - *Compendio organizzativo MiFID II e Regolamento PRIIPs*. Emanato in data **13.08.2018**, il documento norma gli adempimenti da eseguire a seguito dell'entrata in vigore della Direttiva Europea 2014/65/UE del 15.05.2014 (MIFID II), del Regolamento (UE) n. 600/2014 (MiFIR), del Regolamento (UE) n. 1286/2014 (PRIIPs) e del Regolamento Delegato n. 653/2017 con i relativi allegati, in tema di servizi di consulenza in materia di investimenti, collocamento/distribuzione ed intermediazione di prodotti finanziari (inclusi i prodotti finanziari emessi da imprese di assicurazione).

Rimangono peraltro da aggiornare altri documenti normativi/di processo afferenti macro categorie specifiche di prodotti o riguardanti tematiche non esclusivamente attinenti alla 'filiera produzione – distribuzione'.

Per quanto riguarda la normativa di vigilanza rileva nello specifico che, dal 30.06.2018, si applicano gli Orientamenti EBA sulla *Governance* interna che raccomandano, tra l'altro, l'adozione di una politica aziendale per l'approvazione di nuovi prodotti e ingresso in nuovi mercati (la cd. NPAP, *New Product Approval Policy*) approvata dal CdA[10]. Tali orientamenti entrano nel dettaglio delle caratteristiche e del perimetro di tale *policy* stabilendo che essa «*dovrebbe inoltre includere le definizioni di 'nuovo prodotto/mercato/attività' e 'modifiche significative' da utilizzare nell'organizzazione e indicare le funzioni interne da coinvolgere nel processo decisionale*.» Tra le questioni che la NPAP deve trattare, gli Orientamenti dell'EBA elencano: (1) il rispetto della normativa interna ed esterna, (2) gli aspetti contabili, (3) il ruolo delle funzioni di controllo[11] e i relativi modelli di quantificazione del rischio, (4) l'impatto sul profilo di rischio, l'adeguatezza

[10] «*Gli enti dovrebbero disporre di una politica aziendale per l'approvazione di nuovi prodotti (New Product Approval Policy, NPAP) ben documentata, approvata dall'organo di amministrazione, che fa fronte allo sviluppo di nuovi mercati, prodotti e servizi e alle modifiche rilevanti apportate a quelli esistenti, nonché alle operazioni straordinarie*.» Gli Orientamenti prevedono inoltre che tale politica «*dovrebbe garantire che i prodotti e le modifiche approvati siano compatibili con la strategia di rischio e la propensione al rischio dell'ente nonché con i limiti corrispondenti, o che vengano effettuate le necessarie revisioni*.», EBA, *Orientamenti sulla governance interna*, versione italiana del 21.03.2018 (versione originaria inglese del), par. 18 "Nuovi prodotti e modifiche significative", pag. 37.

[11] «*La funzione di gestione dei rischi e la funzione di conformità dovrebbero partecipare all'approvazione dei nuovi prodotti o delle modifiche significative ai prodotti, processi e sistemi esistenti. Il loro contributo dovrebbe prevedere una valutazione esaustiva e oggettiva dei rischi derivanti da nuove attività in diverse ipotesi di scenario, delle potenziali carenze nei quadri di gestione dei rischi e di controllo interno dell'ente, e della capacità dell'ente di gestire efficacemente eventuali nuovi rischi. La funzione di gestione dei rischi dovrebbe avere anche una chiara visione d'insieme del processo di introduzione di nuovi prodotti (o delle modifiche significative apportate ai prodotti, processi e sistemi esistenti) nei diversi portafogli e linee di business, e il potere di richiedere che le modifiche ai prodotti esistenti siano sottoposte al processo formale previsto nella politica aziendale per l'approvazione di nuovi prodotti*.», EBA, Orientamenti sulla governance interna, versione italiana del 21.03.2018 (versione originaria inglese del 26.09.2017), par. 18 "Nuovi prodotti e modifiche significative", pag. 38.

patrimoniale e la redditività, (5) la disponibilità di risorse adeguate per le attività di *front*, *back* e *middle-office* e infine (6) la disponibilità di adeguati strumenti interni, risorse e competenze per la comprensione, la gestione e il monitoraggio dei rischi associati.

Con la lettera dell'8 marzo 2018 avente per oggetto "*Attività connesse esercitabili dalle banche*", Banca d'Italia ha da ultimo delineato da parte sua le specifiche cautele che le banche sono chiamate a seguire qualora intendano intraprendere una operatività in cd. "attività connesse" che ricoprono però una valenza di tipo più generale indirizzabile al complesso dei prodotti che le banche intendono collocare/segnalare ai propri clienti. Nello specifico, oltre a ricordare le specifiche attribuzioni delle funzioni aziendali di controllo (*compliance*, *risk management* e antiriciclaggio) chiamate ad esprimersi preventivamente all'avvio dell'operatività nonché a garantirne il regolare controllo, Banca d'Italia indirizza le seguenti specifiche cautele: (1) identificazione, valutazione e controllo delle diverse tipologie di tutti i rischi potenziali, inclusi controlli sulle controparti alle quali le banche ricorrono per distribuire prodotti alla clientela; (2) definizione di regole comportamentali volte ad assicurare che il servizio sia svolto secondo criteri di correttezza, professionalità e attenzione ai fabbisogni della clientela (*target* clientela, limiti di operatività, verifica sulla congruità dei prezzi, trasparenza sui costi e commissioni applicate, sulla liquidabilità e sui rischi degli investimenti); (3) l'adozione di modalità operative atte a prevenire comportamenti distorsivi da parte della rete commerciale in tema di remunerazione.

6. – LE PRINCIPALI RISULTANZE DELLE VERIFICHE DI AUDIT E FORENSIC IN MATERIA DI SEGNALAZIONE DI DIAMANTI DA INVESTIMENTO ALLA CLIENTELA

Le verifiche condotte dalla Funzione di Internal Audit e da Deloitte *Forensic* in materia di segnalazione di diamanti da investimento alla clientela hanno consentito di identificare alcuni ambiti di miglioramento riconducibili alle seguenti macro aree di interesse.

» ***Processo autorizzativo***

- Codifica puntuale a livello di *policy* approvata dal CdA della definizione di "nuovo prodotto / nuovo mercato / nuovo *target* clientela", delle loro "modifiche significative" e del relativo livello deliberativo (chiara identificazione delle delibere in materia in capo al CdA).
- Introduzione di un processo strutturato regolante l'espletamento di procedure competitive volte alla selezione di *business partner*, che tenga conto anche delle valutazioni di cui al punto successivo.
- Introduzione di un processo di *due diligence* strutturata sul *business partner* volta a meglio apprezzare preliminarmente lo *standing* complessivo dello stesso.
- Miglioramento dei presidi in tema di rispetto dei tempi e ordine nei passaggi autorizzativi al Comitato Guida Investimenti e Prodotti ai sensi del D920 e documenti collegati.

» ***Valutazione materiale per commercializzazione e attività di formazione interna***

- Presa visione del materiale contrattuale e commerciale della società terza per cui la Banca decide di svolgere l'attività di segnalazione/distribuzione.
- Valutazione critica dei contenuti delle *brochure*, materiale pubblicitario e commerciale e loro distribuzione alla Rete.
- Valutazione attenta della documentazione commerciale interna contenente informazioni, sulle caratteristiche dell'investimento o comunque dell'attività (es.: liquidità, quotazioni, disinvestimento, ecc.).

- Introduzione di iniziative strutturate di formazione del personale di Rete sul ruolo della Banca, sulle attività in concreto da svolgere e sui rischi possibili derivanti da comportamenti non conformi.

» ***Normativa e Procedure***

- Emanazione della normativa di riferimento in tempi coerenti con l'effettivo avvio delle vendite.
- Presenza di istruzioni operative dettagliate e di adeguata informativa sui potenziali rischi reputazionali e legali per la Banca derivanti dall'assunzione di comportamenti non conformi.
- Garanzia di un'attività strutturata e critica di tracciatura, monitoraggio (di volumi e commissioni) e archiviazione delle segnalazioni effettuate.

» ***Antiriciclaggio***

- Effettuazione di *assessment* strutturati in sede di introduzione di nuovi servizi/prodotti, anche di natura non finanziaria, finalizzati all'individuazione ed eventuale introduzione di presidi restrittivi su *target* di clientela.
- Miglioramento del processo di affinamento e customizzazione degli "scenari" applicati dalla Banca nell'ambito dei *continuos monitoring*.

» ***Comportamentale***

- Introduzione/miglioramento di un processo approvativo strutturato per la codificazione di nuove voci gestionali di conto economico, l'assegnazione di obiettivi commerciali, l'attivazione di meccanismi incentivanti e/o monitoraggi presso le strutture di Rete.

A seguito anche della citata lettera di Banca d'Italia datata 8 marzo 2018 relativa alla cd. "*attività connesse*", nel mese di aprile c.a. è stato inoltre attivato un gruppo di lavoro sull'argomento all'interno del quale è stato avviato un cantiere operativo finalizzato all'analisi della situazione "*as-is*", all'identificazione degli ambiti di miglioramento (tenuto conto anche delle novità normative nel frattempo introdotte), nonché alla definizione dei conseguenti interventi, con *focus* sul processo di *product approval* indirizzati a mitigare le criticità sopra riportate.

Dall'insieme di tali evidenze è scaturito il piano di lavoro riportato nel successivo paragrafo 7.

Ulteriori ambiti di attenzione sono stati identificati sempre dall'attività svolta da Deloitte Forensic relativamente ad aspetti di sicurezza informatica legati alle dotazioni strumentali e agli strumenti di informatica personale assegnati ai dipendenti della Banca. In particolare, gli aspetti di maggiore attenzione identificati sono sintetizzabili come segue:

1) mancanza di cifratura e di *backup* periodici sui dati memorizzati sui computer personali;
2) impossibilità di effettuare ricerche storiche negli archivi della posta elettronica aziendale;
3) utilizzo da parte di alcuni dipendenti di dispositivi non forniti dalla Banca e la mancanza di una *policy* che regolamenti il BYOD ("*Bring Your Own Device*");
4) mancata regolamentazione delle attività da svolgere all'atto di riconsegna dei dispositivi informatici da parte dei dipendenti al momento della cessazione del rapporto di lavoro; in particolare il riferimento riguarda:

   a. il divieto di utilizzo dei dispositivi stessi,
   b. il divieto di alterarne il contenuto,
   c. il divieto di estrarre i dati per scopi personali,
   d. l'obbligo di restituire i dispositivi integri e funzionanti.

7. – PIANO DI AZIONI MIGLIORATIVE IN MATERIA DI PRODUCT GOVERNANCE & APPROVAL

Come sopra riportato, per l'implementazione delle azioni migliorative in materia di *product governance* e *product approval* è stato definito un piano degli interventi con il dettaglio delle singole scadenze, delle funzioni responsabili (CCO e, per la componente Formazione, Area Talent & Knowledge Management) e delle funzioni contributrici (CRO, CFO, Area Organizzazione, Area Compliance, Area Legale e Societario, COG-Demand, COG-IT).

In particolare la Direzione CCO ha individuato come Funzione Responsabile dell'attività di coordinamento del Piano degli interventi l'Area Controlli, Conformità e Reclami che, in continuità con i contributi specifici cui viene chiamata ordinariamente per il proprio ruolo, garantirà:

- la complessiva supervisione del piano stesso e del rispetto delle scadenze, unitamente al coordinamento dei contributi delle Funzioni interne al perimetro della Direzione di appartenenza, per assicurare la piena coerenza di tutte le attività condotte dalla Funzione Commerciale;
- il confronto con tutte le altre Funzioni coinvolte, anche in merito agli approfondimenti necessari;
- il progressivo adattamento delle attività di controlli e di indirizzo secondo gli aggiornamenti introdotti;
- la regolare informativa sullo stato di avanzamento delle attività da portare all'attenzione del Comitato Direttivo e quindi del Comitato Rischi e del CdA.

Il Piano degli interventi in questione, avviato in forma di gruppo di lavoro per garantirne la tempestiva attivazione, sarà subito trasformato in progetto, al fine di garantire:

- il formale monitoraggio delle scadenze e dei rilasci, secondo le metodologie in vigore;
- l'individuazione dei fabbisogni in termini di risorse e *capacity*, soprattutto IT, per procedere alla richiesta di un apposito finanziamento di budget in sede di programmazione annuale.

La funzione Organizzazione, in particolare, fornirà supporto garantendo che le modifiche ai processi e alle normative da parte delle funzioni di *business* avvengano in coerenza con il modello dei processi e della normativa di Gruppo (D1691 - *Regolamento di governo operativo del Gruppo* e D1823 - *Policy in materia di normativa interna e processi*) e siano eventualmente declinate per singola tipologia di prodotto.

In tal senso, per lo specifico "macro-processo prodotti", le azioni migliorative avranno impatti sui processi di:

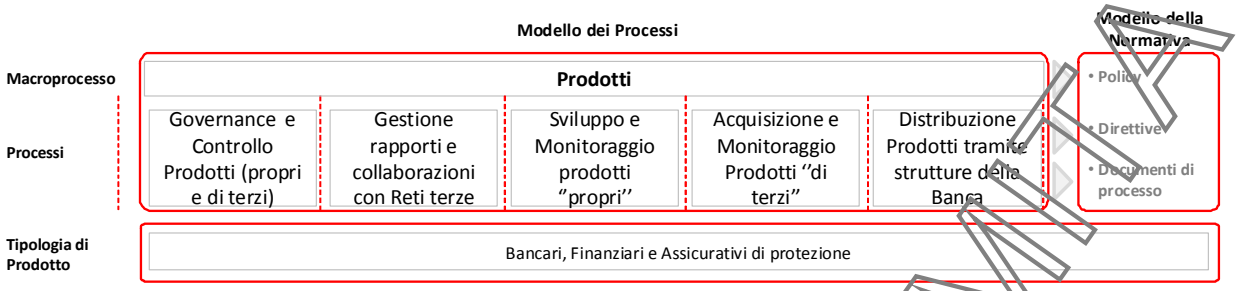
- *governance* e controllo prodotti;
- gestione rapporti e collaborazioni con reti terze;
- sviluppo e monitoraggio prodotti "propri";
- acquisizione e monitoraggio prodotti "di terzi";
- distribuzione prodotti.

L'organo deliberante sarà individuato in conformità alle autonomie previste in materia di normativa (CdA per le *Policy* di natura strategica, AD/Direzione per le Direttive, Area per le norme di processo - cfr. dettagli D2117 – Regolamento deleghe di autonomia in materia di Normativa Interna).

L'analisi di dettaglio potrà evidenziare la necessità di aggiornamenti di processi/normative *extra* perimetro prodotti, oltre a eventuali affinamenti/modifiche rispetto allo schema dei processi ipotizzato.

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

Protocollo Sisifo: **8254818\20**



Di seguito viene riportato il piano degli interventi con i relativi *owner* e le date di finalizzazione delle singole attività previste.

AMBITO	AZIONE	FUNZIONE OWNER	FUNZIONI COINVOLTE	DATA SCADENZA	NOTE
1. Definizione nuovo prodotto/ nuovo mercato/ nuovo *target* di clientela a livello di Gruppo e definizione di "attività connessa"	1.1 Codifica puntuale a livello di *Policy* "strategica" della definizione di "nuovo prodotto/nuovo mercato/ nuovo *target* clientela", delle loro modifiche significative e del relativo livello deliberativo	CCO	CRO (RM+AML) CFO Compliance AO	31.12.2018	Chiara identificazione delle delibere in materia in capo al CdA) La *Policy* dovrà essere approvata dal CdA
	1.2 Definizione di un documento normativo di tipo operativo in tema di *product governance* che definisca puntualmente il processo di *product testing*	CCO	CRO (RM+AML) CFO Compliance AO	31.12.2018	
	1.3 Adozione di un processo *ad hoc* di definizione e valutazione dei nuovi prodotti e delle cd. "attività connesse" che valuti: a) i rischi della nuova operatività; b) il *target market* c) gli impatti in termini di costi, ricavi, risorse e procedure amministrative e contabili d) la capacità dei sistemi informativi di *front/middle* e *back office* di gestire tali prodotti e) gli impatti sui sistemi dei controlli interni *(N.B. valido per tutti e 8 gli*	CCO	CRO (RM+AML) CFO Compliance Legale AO COG/DEMAND	31.12.2018 Attività connesse: settembre 2018 (pubblicazione D1817/D1610)	In relazione al punto d) e al punto e) la data di rilascio degli interventi applicativi verrà individuata a completamento della definizione dei requisiti di *business* In corso di condivisione con il GdL i documenti normativi D1817 e D1610 aggiornati per tener conto delle indicazioni contenute nella lettera Bankit dell'8.3.18 sulle cd. "attività connesse"

	Ambiti)				
	1.4 (i) Definizione dei nuovi processi operativi della *product governance* (chi fa cosa) e di definizione dei documenti metodologici per la definizione del *target market* effettivo e per la transcodifica delle informazioni rese dai *manufacturer*. (ii) Gestione automatizzata del *target market* effettivo per ciascun prodotto in *stock* e a catalogo. *(N.B. valido anche per Ambiti 2 e 7)*	CCO	CRO (RM+AML) CFO Compliance AO COG/DEMAND	31.12.2018	In relazione al punto (ii) la data di rilascio degli interventi applicativi (a cura del COG) verrà individuata a completamento della definizione delle specifiche funzionali da produrre nel corso del progetto
	1.5 Definizione dei nuovi processi operativi della *product governance* (chi fa cosa) nella distribuzione dei prodotti finanziari assicurativi	CCO	CRO (RM+AML) CFO Compliance AO	31.12.2018	
2. Processo istruttorio e di *due diligence*	2.1 Revisione documento di processo reti alternative *(N.B. valido anche per Ambito 3)*	CCO	CRO (RM+AML) Compliance AO	31.12.2018	
	2.2 Definizione di un processo *ad hoc*, autonomo, per prodotti bancari di terzi	CCO	CRO (RM+AML) Compliance AO	31.12.2018	
	2.3 Definizione dei modelli standardizzati e "schede tecniche prodotto" per il rilascio di pareri di conformità, ed estendere il processo di valutazione formale della conformità anche alle operazioni straordinarie	CCO	CRO (RM+AML) Compliance AO COG/DEMAND	31.12.2018	La data di rilascio degli interventi applicativi (a cura del COG) verrà individuata a completamento della definizione delle specifiche funzionali da produrre nel corso del progetto
	2.4 Integrazione del processo definito dall'attuale normativa aziendale con i punti indicati nelle disposizioni normative (ad es. orientamento EBA del 21.03.18). Ad es. le questioni da	CCO	CRO (RM+AML) CFO Compliance AO CHCO	31.12.2018	

	trattare prima della decisione, quali rispetto normativa, contabilità, modelli di quantificazione del rischio, adeguatezza patrimoniale, redditività, impatto sul profilo di rischio, adeguati strumenti, risorse responsabili *(N.B. valido anche per ambito 8)*				
	2.5 Adozione di un'adeguata politica di formazione e abilitazione alla strutturazione e distribuzione di prodotti bancari	Area Talent & Knowledge Management CHCO	AO Compliance	31.12.2018 (definizione dei contenuti e del piano formativo)	L'erogazione della formazione verrà effettuata successivamente alla definizione dei contenuti
	2.6 Implementazione della normativa interna e perfezionamento dei relativi processi in materia di obblighi in capo al produttore e al distributore Adozione di processi di valutazione e monitoraggio dei distributori	CCO	CRO (RM+AML) Compliance AO	31.12.2018	
	2.7 In materia di scomposizione del prezzo (*Fair Value* e costi) rendere coerente - compatibilmente con la normativa vigente - KID, Scheda Strumento Finanziario (SSF) e altri moduli AF (5500)	CCO	CFO Compliance	31.12.2018	
3. Processo deliberativo	*Cfr. in particolare Ambiti 1,1; 1.3 ; 1.5, 2.1, 2.4*	CCO	CRO (RM+AML) CFO Compliance AO	31.12.2018	
4. Ruolo delle funzioni di controllo di 2° livello (…) e dei comitati gestionali nell'ambito del processo deliberativo	4.1 Definizione di un processo formale , sulla base di uno *standard* definito a priori, di: a) valutazione di nuovi prodotti/nuovi mercati/ nuovo *target* clientela quale parte integrante del processo deliberativo b) valutazione delle attività	CCO	CRO (RM+AML) CFO Compliance AO	31.12.2018	Le attività effettuate da parte delle funzioni di controllo di 2° livello nel processo di *product approval & governance* verranno rendi-contate nelle relazioni annuali di tali funzioni unitamente alle

	connesse con specifico riferimento ai rischi ed al ruolo delle funzioni di controllo di 2° livello c) valutazione della compatibilità con le strategie di rischio e la propensione al rischio aziendale (coerente con RAS/RAF) d) monitoraggio nel continuo dei rischi e degli eventuali limiti operativi introdotti e) criteri di contabilizzazione e rappresentazione di conto economico, monito-raggio andamentale e veri-fiche di budget da parte della Funzione Pianifica-zione e Controllo di Gestione in ottica di contabilità analitica *(N.B. valido anche per Ambiti 7 e 8)*				attività di monitoraggio e controllo effettuate nel periodo
5. Tracciatura/ archiviazione obbligatoria	5.1 Tracciatura/archivia-zione obbligatoria dell'iter di approvazione finale *Cfr in particolare ambiti 1.3 e 1.5*	CCO	CRO (RM+AML) CFO Compliance AO COG/DEMAND	31.12.2018 (definizione delle specifiche funzionali)	La data di rilascio degli interventi applicativi (a cura del COG) verrà individuata a completamento della definizione delle specifiche funzionali
6.Predisposizione di un catalogo prodotti	6.1 Predisposizione di un catalogo prodotti in forma di "Documento" a partire dalla tipizzazione di una scheda prodotto (tecnica) multi-contribuita da utilizzare nel processo di approvazione: contenuti (inclusi *target market* ed *economics*), circolarizza-zione e aggiornamento della scheda e del catalogo; censimento organico delle controparti della Banca *Cfr in particolare ambiti 1.3 e 1.5*	CCO	CRO (RM+AML) CFO Compliance AO	31.12.2018	
7. Monitoraggio nel tempo e	7.1 Definizione di un documento normativo	CCO	CRO (RM+AML) CFO	31.12.2018	

rendicontazione periodica (…) da parte delle funzioni di controllo di 1° e 2° livello e del controllo di gestione	operativo sui prodotti bancari che regoli: a) compiti e responsabilità in merito alla verifica puntuale e periodica dei dispositivi di *governance* e di controllo sui prodotti; b) processo di monitoraggio		Compliance AO		
	7.2 Rafforzamento del processo di controllo e monitoraggio dell'offerta di prodotti svolta dai mediatori creditizi, su competenze e al rispetto del *target market*	CCO	CRO (RM+AML) CFO Compliance AO	31.12.2018	
	7.3 Rafforzamento delle procedure per la valutazione di adeguatezza dei prodotti bancari ai sensi delle regole sulla trasparenza bancaria	CCO	CRO (RM+AML) Compliance AO	31.12.2018	
8. Coerenza con il *business model* e impatto sulla *profitability* della Banca	*Cfr. azione 7.1*	CCO	CRO (RM+AML) CFO Compliance AO	31.12.2018	

Il completamento del piano delle suddette attività, pur prevedendo alcune scadenze intermedie, si posiziona come data ultima a dicembre 2018, fatto salvo per i rilasci applicativi che richiedono interventi di tipo 'IT' e che presuppongono quindi per la loro pianificazione la definizione delle relative specifiche funzionali (cfr. colonna Note nella tabella).

Al fine di garantire comunque un immediato efficace presidio dei processi di approvazione di distribuzione nuovi prodotti (propri o di terzi)/ingresso in nuovi mercati e/o nuovi *target* di clientela da indirizzare, verranno da subito adottate alcune modalità operative. Nello specifico, si provvederà a rafforzare la definizione di nuovo prodotto, nuovo mercato di riferimento e sviluppo di nuovi modelli di servizio in modo da garantire, anche con riferimento alle cd. "attività connesse", l'immediata adozione di un processo deliberativo più rigoroso e strutturato che veda coinvolto direttamente il CdA. Rispetto alle definizioni oggi già in uso all'interno della normativa in vigore, si fisseranno i criteri per definire (1) una nuova operatività aziendale quale quella non ancora ricompresa nell'ambito delle attività svolte dalle singole Società del Gruppo, (2) lo sviluppo di nuovi modelli di servizio dedicati a segmenti di clientela non ancora serviti dalle Società del Gruppo tramite modelli di servizio dedicati e/o l'adozione di nuovi canali distributivi per prodotti e servizi e (3) l'ingresso con conseguente avvio di nuova operatività in nuove aree geografiche.

8. – MODALITA' TECNICO-OPERATIVE IN MATERIA DI ARCHIVIAZIONE DELLA POSTA ELETTRONICA E DELLA DOCUMENTAZIONE DI LAVORO SUI SERVER AZIENDALI

Con riferimento a quanto emerso in tema di modalità tecnico-operative in materia di archiviazione della posta elettronica e della documentazione di lavoro del personale della Banca e del relativo eventuale accesso, varie iniziative sono già state realizzate o sono in corso di realizzazione con l'obiettivo specifico di garantire una migliore salvaguardia e tutela del patrimonio informativo della Banca, oltre che una adeguata profondità storica e una maggior facilità di accesso in casi di esigenze di revisione.

Le soluzioni agli aspetti sopra indicati trovano finalizzazione con interventi di tipo applicativo e normativo per lo più ricondotte nell'alveo progettuale denominato *Monte Protect Shield*[12], secondo l'articolazione e i contenuti di seguito illustrati.

1) Mancanza di cifratura e di backup periodici sui dati memorizzati sui computer personali

Gli aspetti relativi alla cifratura sono stati disciplinati in uno specifico documento che regola la materia di utilizzo degli strumenti informatici in corso di pubblicazione e previsto entro il mese di settembre a cura di Area Sicurezza Integrata.

Contestualmente, è in corso il *roll-out*, nell'ambito della Direzione Generale, della funzionalità di protezione dei dati che permette di crittografare l'intero *hard disk* al fine di aumentare la sicurezza dei documenti e dei contenuti multimediali salvati nei PC aziendali.

La crittografia verrà effettuata con l'utilizzo del prodotto *BitLocker*, per il quale a oggi risulta già predisposta l'infrastruttura tecnica a supporto. Per l'attivazione, di cui sono già in corso le verifiche tecniche e di compatibilità, sono stati fissati due obiettivi temporali: il 31.12.2018 per la maggior parte delle postazioni della Direzione Generale e il 30.6.2019 per la Rete delle Filiali.

È comunque attiva per tutte le postazioni aziendali, la procedura *standard* di cifratura dei documenti aziendali che prevede l'utilizzo del programma "*7-zip*" che consente di duplicare un *file* preesistente creandone una copia compressa e cifrata.

Gli aspetti relativi al *back up* sono parimenti disciplinati nel documento di regole in materia di utilizzo degli strumenti informatici che, come sopra già specificato, sarà pubblicato entro il mese di settembre.

In particolare, l'impianto di regole di prossima pubblicazione norma l'utilizzo di ambienti di condivisione appositamente predisposti o di *Team-site* dedicati che garantiscono il mantenimento della documentazione e la condivisione delle informazioni, limitando il rischio di perdita o cancellazione errata dei dati grazie alle operazioni di *backup* schedulate sugli stessi *server* aziendali.

Ulteriori miglioramenti saranno realizzabili attraverso l'implementazione del sistema operativo MS Office 365 (*OneDrive*) che offre diverse opzioni per la sincronizzazione e/o scambio dei dati aziendali su *Cloud*.

2) Impossibilità di effettuare ricerche storiche negli archivi della posta elettronica aziendale

Il CdA del 16.01.2018 ha approvato l'"*Outsourcing* della piattaforma di posta elettronica su *Cloud Microsoft*", che prevede di attivare l'opzione di migrazione delle caselle di posta elettronica aziendale sul *Cloud* (licenze *Microsoft* E3).

L'operazione è stata classificata come "esternalizzazione di Funzione Operativa Importante (FOI)" e come tale è stata trattata in base alle disposizioni di vigilanza (Circ. 285 Bankitalia, Titolo IV, Cap. 3, Sez. IV e V, in particolare, per il Sistema Informativo, il successivo Cap. 4 alla Sez. VI) e

[12] Il Programma *Monte Protect Shield* è articolato in 4 progetti in ambito Capogruppo, COG e Widiba; è stato avviato nell'ottobre 2017 e permetterà entro il 1° trimestre 2019 di migliorare la valutazione attualmente formulata per il rischio della sicurezza IT ("medio"), comunque già in linea con il RAF.

alla specifica normativa interna[13].

Le caratteristiche principali della nuova configurazione sono:

- incremento dimensione della cassetta postale (100 GB) rispetto all'attuale *on premise* (300 MB);
- disponibilità di archivio *on line* su cui ciascun utente può spostare i messaggi contenuti negli archivi locali consentendone l'eliminazione e i relativi *backup*; la dimensione della casella "Archivio" avrà un limite di capacità di 100 GB, ampliabile in modo illimitato;
- introduzione della funzionalità di *Legal Hold*, tramite la quale è possibile conservare senza limiti temporali tutto il contenuto delle cassette postali tra cui gli elementi eliminati e le versioni originali di quelli modificati.

Il completamento del *roll-out* della nuova configurazione delle caselle di posta elettronica in modalità "*Cloud*" è programmato entro il primo semestre 2019.

3) Utilizzo da parte di alcuni dipendenti di dispositivi non forniti dalla Banca e la mancanza di una policy che regolamenti il BYOD ("Bring Your Own Device")

Gli aspetti relativi a questo ambito saranno disciplinati nel documento di regole in materia di utilizzo degli strumenti informatici che sarà pubblicato entro settembre a cura di Area Sicurezza Integrata.

In particolare, sarà previsto che l'accesso alle infrastrutture di rete e ai dati aziendali venga consentito solo nell'ambito delle attività lavorative, utilizzando esclusivamente le modalità e gli strumenti autorizzati dall'Azienda.

4) Mancata regolamentazione delle attività da svolgere all'atto di riconsegna dei dispositivi informatici da parte dei dipendenti al momento della cessazione del rapporto di lavoro

Anche gli aspetti relativi a questo ambito saranno disciplinati nel documento di regole in materia di utilizzo degli strumenti informatici che sarà pubblicato entro il prossimo mese di settembre a cura di Area Sicurezza Integrata. Tali previsioni sono peraltro in parte già trattate in una normativa operativa (D1733) che disciplina i processi di gestione delle esigenze infrastrutturali tecnologiche e strumentali.

In particolare, si prevede che:

- nei casi di restituzione dei dispositivi assegnati all'utente a seguito di cessazione del rapporto di lavoro, la Funzione ICT assicuri la cancellazione sicura dei file contenuti ("*data wipe*") da PC fissi e portatili e dispositivi mobili (*smartphone* e *tablet*) per evitare che gli stessi siano accessibili ad altri utenti che non ne hanno diritto. Quest'ultima operazione non avrà ovviamente effetto sul contenuto della casella di posta elettronica dell'utente censita su "*Cloud*", il cui relativo contenuto rimarrà pertanto inalterato e disponibile per eventuali indagini future;
- nei casi di sostituzione dei dispositivi assegnati all'utente a seguito di modifica dell'incarico e della dotazione o di guasto, la Funzione ICT assicuri la cancellazione sicura dei file contenuti ("*data wipe*") dai PC fissi e portatili e l'utente stesso assicuri la cancellazione dei dati dai dispositivi mobili (*smartphone* e *tablet*).

La cancellazione si rende necessaria sia nei casi di dismissione definitiva dei dispositivi sia nei casi di eventuale riutilizzo degli stessi. Per i dispositivi mobili, come *tablet* e *smartphone*, è possibile ricorrere al *reset* ai dati di fabbrica, mentre per i PC, in accordo con le linee guida del *National*

[13] Direttiva di Gruppo in materia di Presidio dei modelli e delle attività esternalizzate (D1797); Regolamento deleghe di autonomia in materia di esternalizzazione di Funzioni Aziendali (D1867).

Institute of Standards and Technology (NIST), è suggerito l'utilizzo della crittografia come tecnica di cancellazione dei dati.

oooOooo

In conclusione, a completamento delle attività descritte si renderà possibile conservare senza limiti temporali tutto il contenuto delle cassette di posta elettronica, in quanto strumento di lavoro di cui la Banca è di fatto proprietaria e quindi sottoponibile ad audit in ogni momento, e sarà sempre possibile poter accedere (non trattandosi di dati personali) alla documentazione di lavoro e alla posta elettronica dei dipendenti che lasceranno il lavoro per anzianità o per altra motivazione.

9. CONCLUSIONI

Con la presente informativa si intende quindi portare all'attenzione del CdA il piano di interventi delineato (a valenza di Gruppo), il dettaglio delle scadenze e i relativi ruoli di responsabilità identificati. Tale piano di azione è indirizzato a mitigare le criticità rilevate ed è tale da assicurare che sia i processi e i relativi comportamenti inerenti alle attività di individuazione, produzione e gestione, commercializzazione e monitoraggio/controllo prodotti (con riferimento anche, ma non solo, alle cd. "attività connesse"), sia le modalità tecnico-operative e i relativi comportamenti inerenti l'archiviazione della posta elettronica e della documentazione di lavoro, vengano effettuati in modo adeguato e in conformità a quanto contenuto nelle disposizioni normative e siano di conseguenza tali da garantire che evidenze quali quelle riscontrate nel caso dell'attività di segnalazione di diamanti da investimento alla clientela non possano più ripresentarsi nelle medesime modalità.

Le attività finora descritte confluiranno quindi in uno specifico programma, così composto:

- progetto revisione del processo di *product approval*, a guida CCO (che ha indicato come responsabile delle attività l'Area Controlli, Conformità e Reclami);
- azioni di rimedio inerenti le modalità tecnico-operative in materia di archiviazione della posta elettronica e della documentazione di lavoro del personale della Banca e del relativo eventuale accesso, a guida COO.

La declinazione progettuale permetterà di garantire il monitoraggio circa il rispetto dei tempi e gli effettivi rilasci, secondo il percorso e le scadenze già previsti in materia.

Il *kick off* delle attività delineate avverrà a stretto giro e le funzioni coinvolte definiranno all'interno del progetto una *timetable* di dettaglio che porti a rilasci progressivi.

Sempre in conseguenza delle autonomie vigenti, il CdA sarà interessato per la delibera dei documenti normativi di sua competenza, nonché per un regolare e continuo aggiornamento dello stato di avanzamento delle attività. A conclusione del programma, il CdA sarà altresì interessato per la definitiva approvazione delle *policy* e il conseguente aggiornamento indirizzato alle Autorità di Vigilanza.

I contenuti delle delibere consiliari e gli aggiornamenti normativi saranno via via trasmessi alle società del Gruppo, per il recepimento da parte loro nell'ambito delle vigenti regole di *governance*.

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

10. CONDIVISIONI/PARERI PREVENTIVI:

I contenuti della presente Comunicazione sono stati preventivamente condivisi con le seguenti funzioni:

- Chief Human Capital Officer-CHCO
- Chief Financial Officer-CFO
- Chief Risk Officer-CRO
- Group General Counsel-GGC
- Chief Lending Officer-CLO
- Direzione Relazioni Esterne e Istituzionali-DREI
- Consorzio Operativo GMPS-COG

La memoria verrà sottoposta all'esame del Comitato Rischi.

Valutazione impatti contabili/ fiscali/ segnaletici/ di compliance L.262 (SI-NO):

☑ NO: Non esistono impatti contabili/ fiscali/ segnaletici/ di compliance L.262 che richiedano una preventiva analisi da parte delle funzioni preposte.

Parte Correlata o Soggetto Collegato (SI-NO):

☑ NO: La controparte non è individuata come parte correlata/soggetto collegato, a seguito degli opportuni controlli previsti dalla normativa interna in materia.