MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

Corporate Governance (assessment circa la conformità alle linee guida EBA in materia di internal governance EBA/GL/2017/11)

Rapporto 2018_76

Siena,

Direzione Chief Audit Executive
Area Revisione Specialistica
Servizio Corporate & Control Governance Audit

La presente revisione, inserita nell'ambito della pianificazione annuale di audit per l'anno 2018 di Capogruppo, svolta in assistenza al Collegio Sindacale, è indirizzata a verificare la conformità alle linee guida dell'EBA in materia di internal governance (EBA/GL/2017/11), pubblicate in data 26 settembre 2017[1] ed entrate in vigore dal 30 giugno 2018.

Le nuove linee guida EBA specificano le disposizioni, i processi e i meccanismi che gli Istituti di Credito e le imprese di investimento devono implementare in conformità all'articolo 74, paragrafo 1, della Direttiva 2013/36/UE (cd. CRD IV) ai fini di una gestione efficace e prudente dell'ente con riferimento ai seguenti titoli:

» *TITOLO I - Proporzionalità*
» *TITOLO II - Ruolo e composizione dell'organo di amministrazione e dei comitati*
» *TITOLO III - Quadro di governance*
» *TITOLO IV - Cultura dei rischi e codice etico*
» *TITOLO V - Quadro e meccanismi di controllo interno*
» *TITOLO VI - Gestione della continuità operativa*
» *TITOLO VII - Trasparenza.*

Nello specifico sono stati valutati, con riferimento a Banca MPS, le principali novità introdotte dalle predette Linee Guida EBA, nei seguenti ambiti:

TITOLO IV EBA GL - Cultura del rischio e codice etico;
TITOLO V EBA GL - Quadro e meccanismi di controllo interno; focus sulla funzione Risk Management, in termini di assetto organizzativo e reporting verso gli Organi di Vertice (in particolare verso il Comitato Rischi).

L'intervento non ha invece riguardato i seguenti aspetti:

- *la modalità di gestione dei conflitti di interesse, ricompresa nel Titolo IV EBA GL;*
- *la «New product approval policy», ricompresa nel Titolo V EBA GL.*

Per quanto riguarda i titoli delle Linee Guida EBA non oggetto della presente revisione, la Direzione CAE valuterà la programmazione di futuri interventi nell'ambito della pianificazione pluriennale.

1. La versione in lingua italiana delle Linee Guida è stata pubblicata dall'EBA in data 21/03/2018 con il titolo «Orientamenti sulla governance interna».

Overview

Anagrafica Intervento

Intervento: Corporate Governance (assessment circa la conformità alle linee guida EBA in materia di internal governance EBA/GL/2017/11).

Obbligatorietà: NO

Unità auditata/e: BMPS

Tipologia di intervento: revisione ordinaria settoriale

Data open meeting: 18/10/2018

Data exit meeting: 17/01/2019

Responsabile Audit Team: Furlani Andrea

Audit Team:

- *Paola Blasutto*
- *Fulvio Formiggini*
- *Mariangela Latina*
- *Michele Sbardellati*
- *Genziana Sigismondi (CIA)*
- *Marco Zamperini (CIA)*

Esito Intervento

Grade Complessivo Intervento

Rating 1 (VERDE)	Rating 2 (GIALLO)	Rating 3 (ARANCIONE)	Rating 4 (ROSSO)

Il Grade complessivo dell'intervento, come previsto dagli Standard di audit, è in funzione della numerosità e rilevanza (bassa-media-alta), oltre che dell'impatto in termini di rischio, dei gap aperti a seguito dell'intervento stesso, come riassunto nella tabella seguente.

Grade	n. complessivo Gap	con n. Gap Alti
Rating 1 (verde)	< 5	0
Rating 2 (giallo)	≥ 5	0
Rating 3 (arancione)	qualsiasi	da 1 a 2
Rating 4 (rosso)	qualsiasi	≥ 3

In sede di attribuzione finale del grade vi è sempre la discrezionalità da parte del CAE di rivedere il giudizio finale sia in termini peggiorativi che migliorativi, motivando opportunamente tale scelta.

Fattore Causale	Distribuzione dei Gap per rilevanza		
	Alta	Media	Bassa
Risorse	-	-	-
Processi	-	-	-
Sistemi	-	-	-
Totale	-	-	-

Precedenti interventi di revisione (se esistenti)

Ambito intervento	Periodo della verifica	N. rapporto	Grade intervento

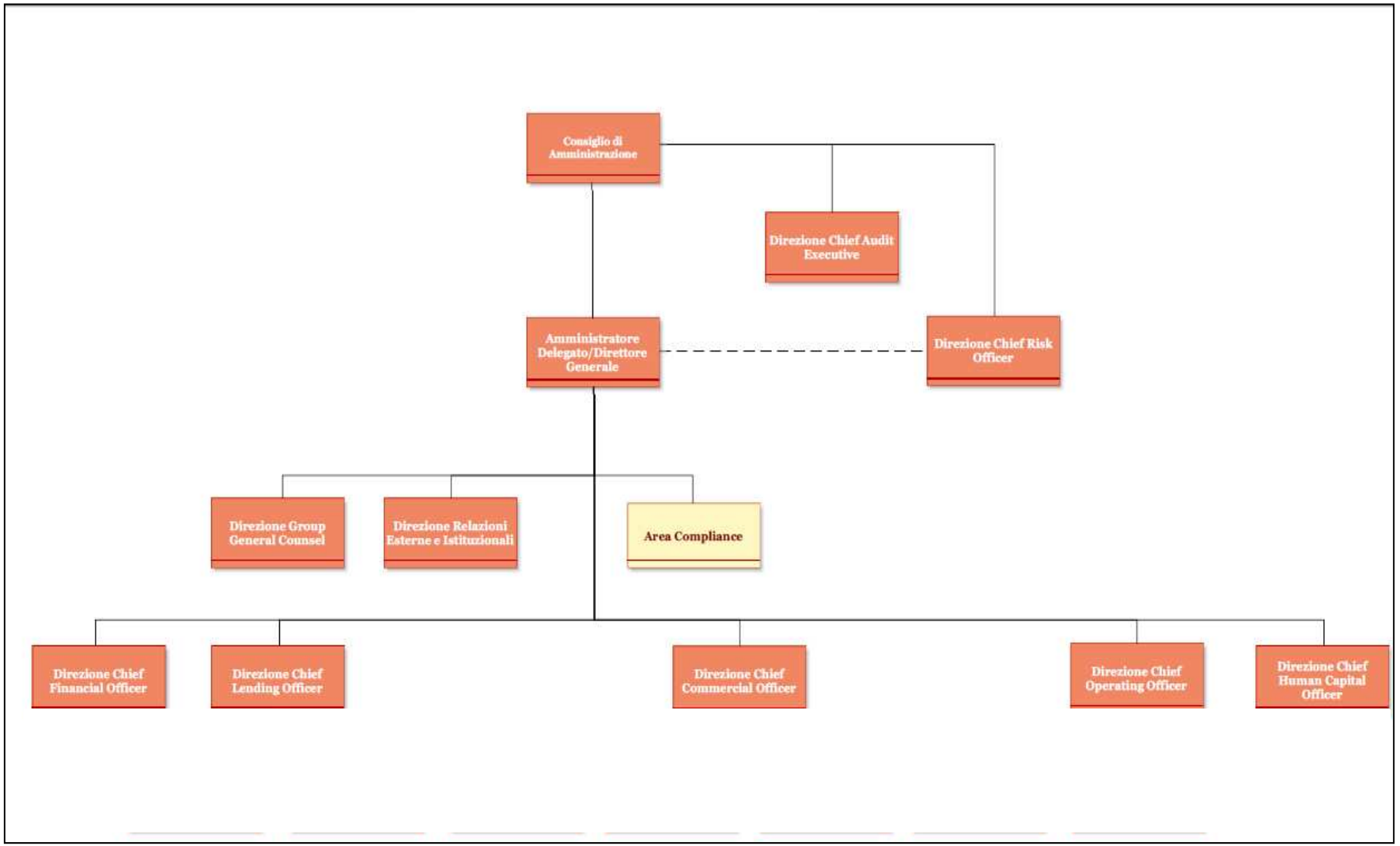
Organi destinatari del presente audit

Legal Entity	Organo Destinatario
BMPS	*Collegio Sindacale*
BMPS	*Comitato Rischi **

* Il rapporto viene inoltrato al Collegio Sindacale in quanto svolto in assistenza a tale Organo di controllo e al Comitato Rischi, vista la rilevanza degli argomenti trattati.

Organigramma Capogruppo

Allegato al Regolamento n.1 - D 751 0098



Executive Summary (1 di 3)

CONTESTO DI RIFERIMENTO

Le Linee guida EBA in materia di Internal Governance pubblicate il 26/09/2017 (in sostituzione di quelle precedenti del settembre 2011) sono entrate in vigore a partire dal 30/06/2018 e mirano ad armonizzare ulteriormente le modalità, i processi e i meccanismi di governance interna delle istituzioni in tutta l'UE, in linea con le nuove esigenze introdotte nella direttiva sui requisiti patrimoniali (CRD IV) e tenendo conto anche del principio di proporzionalità. Le nuove Linee guida pongono maggiore enfasi sui doveri e sulle responsabilità dell'organo di gestione nella sua funzione di supervisione nel controllo dei rischi. Inoltre, è stato ulteriormente sviluppato il quadro di riferimento riguardante il *business conduct*, attribuendo maggiore importanza alla creazione di una cultura del rischio, al codice di condotta e alla gestione dei conflitti d'interesse. In Italia, la Circolare Bankit n.285, beneficiando del lungo periodo in cui il documento EBA è rimasto in consultazione, disciplina già molti degli aspetti di novità introdotti, pertanto la Banca, che nel tempo si è attenuta alle disposizioni contenute nella Circolare n.285, risulta in larga parte conforme alle previsioni delle EBA GL.

TITOLO IV CULTURA DEL RISCHIO E CODICE ETICO

Cultura del rischio

Dalla normativa aziendale primaria emerge chiaro il cd. «*tone at the top*» per sviluppare una sana cultura del rischio a tutti i livelli. Il Reg.1 di BMPS disciplina, per tutte le strutture aziendali, la responsabilità di improntare i comportamenti a principi di eticità delle decisioni, cultura del controllo, basando la pratica su etica e responsabilità. Le Policy e Direttive in materia contengono espliciti richiami alla cultura del rischio.

La consapevolezza delle funzioni di controllo interno nel presidiare la gestione dei rischi risulta - oltre che dalle attività e controlli di competenza - dall'adesione a percorsi di formazione professionalizzanti e dalla partecipazione in qualità di relatori/docenti ad incontri organizzati con il business.

Ad oggi è già indirizzata la necessità di una maggiore azione coordinata da parte delle Funzioni Aziendali della Banca per meglio presidiare il rischio (es. operativo, di mercato, di credito) mediante un sistema integrato di processi, procedure, controlli, metodologie e formazione, rafforzando quindi la reputazione complessiva.

Complessivamente, i corsi di formazione destinati al personale connessi alla cultura del presidio dei rischi sono numerosi e variegati per modalità di fruizione. La Banca, inoltre, ha in essere processi aziendali in base ai quali un mancato completamento dei corsi obbligatori costituisce elemento ostativo per l'attribuzione / permanenza in ruoli di responsabilità, la partecipazione ai corsi esterni o l'erogazione di premi in caso di contest.

E' positiva l'attenzione della Banca verso un ulteriore affinamento dell'offerta formativa rispetto alle esigenze di ruolo, misurate su un livello di esposizione al rischio, competenze richieste e responsabilità connesse. Ciò mediante l'adozione di una metodologia risk based, l'esecuzione di un risk assessment di ruolo ed una skill gap analysis individuale per definire il fabbisogno ed erogare una formazione mirata.

Infine, sono sempre più evidenti gli sforzi per rafforzare il legame tra retribuzione, performance ed assunzione di rischi: l'incorporazione dei macro indicatori di rischio e di performance risk-adjusted coerenti con il RAF nelle politiche di remunerazione e incentivazione del personale rappresenta una ulteriore leva per promuovere la consapevolezza dei comportamenti agiti e l'accrescimento di una sana cultura del rischio.

Valori aziendali e codice etico

Il Codice Etico, destinato alle strutture della Capogruppo Bancaria e alle società controllate, è costituito dall'insieme di principi guida, complementari agli obblighi di legge, dai modelli e dalle norme di comportamento che ispirano l'attività della Banca, orientando le condotte attese in continuità e coerenza con la missione dell'Azienda e dei suoi valori fondamentali: etica della responsabilità, orientamento al cliente, attenzione al cambiamento, imprenditività e proattività, passione per le competenze professionali, spirito di squadra e cooperazione.

Gli obiettivi e le finalità del Codice Etico trovano rappresentazione nell'enunciazione dei:

- ✓ principi e valori etici – che devono ispirare l'attività di coloro che operano per conto della Banca, tenendo conto dell'importanza dei ruoli e delle relative responsabilità;
- ✓ norme comportamentali – mediante la definizione dello standard di «buona condotta» per l'attuazione di politiche e procedure aziendali;
- ✓ formazione dei dipendenti - nell'ottica di favorire i comportamenti attesi e di contribuire ad attuare una politica di responsabilità sociale all'interno del Gruppo. In tal senso il Codice Etico opera indistintamente nei confronti di amministratori, sindaci, dirigenti e dipendenti del Gruppo, nello svolgimento delle proprie funzioni e in relazione alle rispettive responsabilità.

Executive Summary (2 di 3)

TITOLO IV CULTURA DEL RISCHIO E CODICE ETICO

Il Gruppo MPS ha inoltre esplicitato il suo impegno di responsabilità sociale attraverso la «Carta dei Valori», definita in relazione alla «etica della responsabilità», la quale trova espressione nel costante orientamento al servizio, all'integrità, alla trasparenza, alla correttezza negli affari, alla salvaguardia dell'ambiente e al rispetto delle persone; principi ribaditi e ripresi nel Codice Etico.
Oltre alle regole del Codice, il Gruppo si impegna a rispettare le discipline di emanazione esterna a cui aderisce, quali:
1. il Codice di autodisciplina - emanato dal Comitato per la Corporate Governance di Borsa Italiana; 2. l'Alleanza Europea per l'Impresa Competitiva e Sostenibile – con l'obiettivo di incoraggiare l'adesione alla RSI/CSR (Responsabilità sociale d'impresa/ Corporate Social Responsibility) tra le aziende europee; 3. il *Global Compact* delle Nazioni Unite - nato per promuovere la responsabilità sociale d'impresa. In tal senso l'attenzione della Banca si è espressa anche con l'adesione alla norma OHSAS18001 *Occupational Health and Safety Assessment Series*, principale standard di riferimento a livello mondiale sulla sicurezza e la salute dei lavoratori, a cui l'art. 30 del D. Lgs 81/08 riconosce la presunzione di conformità per le parti corrispondenti agli obblighi di legge (cfr. anche D. 884 «Direttiva di Gruppo per la gestione adempimenti prescrittivi in materia di D. Lgs. 231/2001 sulla responsabilità amministrativa»).

Relativamente al citato decreto, il Codice Etico rappresenta un documento fondamentale del modello organizzativo previsto dalla legislazione vigente, tanto da essere oggetto di periodico assessment, generalmente biennale, da parte della Funzione Compliance e della Funzione Legale, che ne valutano l'adeguatezza in ordine alle previsioni legislative e la relativa tenuta con riferimento alla struttura e alle dimensioni aziendali. L'ultimo aggiornamento risale al dicembre 2016 a seguito del recepimento del «sistema interno di segnalazioni delle violazioni» (c.d. *Whistleblowing*).
L'attenzione crescente della Banca all'etica della responsabilità si esprime anche attraverso i diversi percorsi formativi pianificati dalla Direzione CHCO di concerto con la Funzione Compliance, per gli ambiti afferenti il codice etico (trasparenza, usura, conflitti di interessi, antiriciclaggio, ecc.), sempre più orientati ad esigenze di efficacia (diversificazione per ruoli e responsabilità) ed efficienza (tempi formativi limitati alle reali necessità). Inoltre, in tali ambiti, la Funzione Compliance svolge sistematicamente e con differenziata periodicità accertamenti ex ante e controlli ex post in materia di conformità a leggi, a regolamenti e alla normativa interna. Tale attività favorisce, nel contempo, la creazione di valore diretta a promuovere una cultura aziendale improntata a principi di correttezza, trasparenza e al rispetto sostanziale delle disposizioni vigenti. Utile inoltre a stimolare la formazione di presidi adeguati a identificare e controllare preventivamente i comportamenti in violazione di prescrizioni normative e di autoregolamentazione.

Procedure interne di segnalazione (Whistleblowing)

La Banca si è dotata di una procedura di allerta interna conforme a quanto richiesto dalla normativa italiana a partire dal 30/11/2015, incardinata presso la Funzione Antifrode (in seno alla Funzione Audit). La procedura adottata rispetta i principi previsti dalle linee guida EBA in materia di Internal Governance, in particolare, da un lato, per quanto riguarda l'accessibilità e la tracciabilità della procedura stessa e, dall'altro, per la tutela dei soggetti coinvolti (segnalante e segnalato). Le prassi adottate forniscono maggior garanzia del rispetto dei principi previsti, in particolare quella di non divulgare le motivazioni di avvio indagine neanche in caso di avvio di procedimenti disciplinari (tutela del segnalante) e quella di consentire al Collegio Sindacale (titolare di eventuali indagini in capo al personale coinvolto nella gestione della procedura) piena e costante visibilità su tutte le segnalazioni pervenute (informativa diretta e senza indugio verso gli organi per oggetti rilevanti).

TITOLO V QUADRO E MECCANISMI DI CONTROLLO INTERNO

Quadro di controllo interno e di gestione dei rischi; Funzioni Aziendali di Controllo

Il Sistema dei Controlli Interni (SCI) del Gruppo MPS (cfr. D. 793) assume un ruolo strategico per il Gruppo e la cultura del controllo ha una posizione di rilievo nella scala dei valori aziendali, coinvolgendo tutta l'organizzazione. L'attuale configurazione del SCI, in conformità alle nuove EBA GL, prevede l'istituzione delle Funzioni Aziendali di Controllo (Compliance, Risk Management, Convalida interna, Antiriciclaggio e Revisione Interna) che dispongono di autorità, risorse e competenze necessarie per lo svolgimento dei loro compiti. Nel disegno del SCI, l'Amministratore Delegato (e Direttore Generale) è stato nominato anche Amministratore Incaricato del Sistema di Controllo Interno e di Gestione dei Rischi previsto dal Codice di Autodisciplina di Borsa Italiana. Tale soluzione ad oggi in essere nel Gruppo MPS risulta essere anche quella più diffusa tra i player bancari quotati che hanno aderito al suddetto Codice di Autodisciplina.

Executive Summary (3 di 3)

TITOLO V
QUADRO E MECCANISMI DI CONTROLLO INTERNO

Il Risk Management Framework è stato valutato nel corso del 2017, con il supporto di KPMG, con un adeguato livello di conformità ai requisiti normativi. Risultano ad oggi in fase di completamento alcune azioni, conseguenti a tale assessment, volte a rafforzare il processo per la governance dei dati in termini di mappatura delle metriche di rischio nonché alla definizione delle linee guida di produzione del relativo reporting. A tal fine, a gennaio 2018, è stata approvata e pubblicata la nuova Direttiva di Gruppo in materia di «Integrated Risk Reporting» (D.02291) che definisce ruoli, responsabilità e processi, oltre a fornire una mappatura dei principali flussi di reporting diretti agli Organi di vertice e al Senior Management. Tale Direttiva sarà ulteriormente affinata nel corso del prossimo anno, per recepire anche le nuove indicazioni derivanti dal progetto Perdar Risk 2018 predisposto con riferimento ai principi BCBS239 in materia di *Risk Data Aggregation e Risk Reporting*.

Funzione di Risk Management

Una delle principali novità delle EBA GL è la previsione di un maggior coinvolgimento del Risk Management nell'ambito della Corporate Governance, prevedendo strumenti di governo per il responsabile RM per assicurare un effettivo ed efficace challenge sulle decisioni prese dalle funzioni di business. In tal senso, è stata introdotta la verbalizzazione di pareri anche negativi, non vincolanti, su Operazioni di Maggior Rilievo da parte del RM: al 30/09/2018 sono stati rilasciati n. 28 pareri, di cui 2 negativi (uno con override degli Organi competenti). Inoltre, nei casi di superamento delle soglie di tolerance, il RM valuta in maniera indipendente l'efficacia/efficienza delle proposte correttive elaborate dalle funzioni di business, rinviando la decisione in merito agli Organi competenti. E' stato, inoltre, ricercato il rafforzamento del ruolo della funzione RM anche nei momenti di «decision making» per assicurare presidio diffuso e supporto agli Organi di Vertice. Con riferimento a questo aspetto, ad oggi, il CRO partecipa ai comitati gestionali (anche con diritto di voto) e presiede il Comitato Gestione Rischi (non deliberativo) che predispone un'informativa verso il Comitato Direttivo (esecutivo), in precedenza indirizzata al CdA. Al riguardo, nel corso delle verifiche effettuate con il CRO, è emersa la possibilità di adottare scelte organizzative tese a razionalizzare ulteriormente i meccanismi di governance e, quindi, il presidio dei rischi. E' stata altresì rilevata una maggiore interazione tra lo stesso e il Comitato Rischi endoconsiliare, in risposta ad uno degli elementi rafforzativi previsti dalle nuove EBA GL. A tale proposito si evidenzia che, dal mese di maggio 2018, il CRO inoltra anche al Presidente del Comitato Rischi la reportistica mensile, predisposta e discussa in Comitato Gestione Rischi, arricchendo così il patrimonio informativo del Comitato Rischi endoconsiliare al fine di rendere più proattivo il suo ruolo verso il CdA. Infine si evidenzia che è in corso di completamento l'aggiornamento e la pubblicazione del D.1915, che disciplina i flussi informativi scambiati tra le funzioni di controllo e gli Organi aziendali.

Funzione di Compliance

La Funzione Compliance di Banca MPS svolge attività in servicing per le controllate bancarie italiane[1] del Gruppo allo scopo di garantire con modalità uniformi il presidio della conformità alle normative vigenti. I requisiti richiesti dalle EBA GL sono ottemperati, in particolare i processi di monitoraggio legislativo e aggiornamento del quadro normativo sono documentati e standardizzati. E' prevista l'attività di consulting normativo a supporto del CdA che viene svolta a beneficio di altre strutture aziendali che utilizzano i pareri ricevuti come supporto nelle loro comunicazioni verso i vertici aziendali. E' inoltre previsto ed è oggetto di tracciatura il coinvolgimento della Funzione anche nella validazione dei nuovi prodotti e del materiale promozionale. Particolare attenzione è riservata a garantire che il personale sia in possesso di adeguate competenze ed esperienze attivando percorsi formativi volti a sanare eventuali carenze. Le interazioni con le altre funzioni di controllo sono avvantaggiate dalla partecipazione a Comitati quali il Comitato Rischi, il Comitato Gestione Rischi ed il Comitato di coordinamento delle Funzioni di Controllo, mentre l'informativa verso gli Organi (CdA e Collegio Sindacale) è garantita, oltre che da precise periodicità di reporting, anche dalla possibilità, accordata al Responsabile della Funzione di Conformità, di comunicare con essi (e con il Comitato Rischi) nel continuo senza restrizioni ed intermediazioni.

Funzione di Internal Audit

La funzione di Internal Audit è collocata a livello gerarchico alle dirette dipendenze del CdA e senza responsabilità diretta di aree operative sottoposte a controllo. La Funzione informa regolarmente gli Organi Aziendali in merito alle risultanze emerse nel corso delle proprie attività ed allo stato di avanzamento delle relative azioni di rimedio tramite una puntuale attività di monitoraggio («follow-up»).

1) Le controllate estere mantengono la propria F. Compliance autonoma

Overview obiettivi di controllo SSM

Pillar	Processo	Numero Obiettivi di controllo
Internal Governance & SCI	Gestione societaria	8
	Gestione del rischio di non conformità	1
	Presidio dei Rischi	2
	Pianificazione e Rendicontazione dei rischi	1
TOTALE		**12**

A	B	C	D	NA
8				
1				
2				
1				
12				

ID	Obiettivi di controllo	Percentuale di completamento	Rating	GAP Associati
IG.1.1	Verificare che il Gruppo/la Banca sia dotato di un documento di governance (es: policy) che descriva la ripartizione di ruoli e responsabilità tra i diversi organi aziendali (e relativi Comitati) ed il ruolo delle principali aree organizzative interne	100%	**A**	
IG.1.2	Verificare la presenza una chiara divisione dei poteri e delle responsabilità a tutti i livelli, dalle singole unità organizzative agli organi aziendali. Accertare inoltre che siano chiaramente definite le linee di riporto e il collocamento gerarchico dell'intera struttura organizzativa, nel rispetto del principio di segregation of duties e dei vincoli normativi esistenti (es: collocamento gerarchico delle Funzioni Aziendali di Controllo)	100%	**A**	
IG.1.3	Verificare, in caso di Gruppo Bancario, l'esistenza di un documento da cui si rilevi con chiarezza la struttura societaria del Gruppo, il ruolo della Capogruppo, le modalità con le quali la Capogruppo intende svolgere le funzioni di direzione e coordinamento, i legami tra le diverse Legal Entity ed il relatvo ruolo all'interno del modello di governance complessivo di Gruppo (ruolo degli organi aziendali delle Controllate, etc.)	100%	**A**	
IG.2.1	Verificare che l'Organo con funzione di supervisione strategica stabilisca i principi di governance, i valori societari e gli standard appropriati	100%	**A**	
IG.2.3	Verificare che le strategie e le politiche adottate siano comunicate a tutto il personale interessato e che la cultura del rischio sia applicata a tutti i livelli dell'ente	100%	**A**	
IG.3.20	Verificare che i flussi di reporting verso gli Organi di Vertice siano adeguatamente formalizzati, chiari, completi e utili. Inoltre, verificare che le tempistiche di elaborazione degli stessi siano coerenti con le esigenze degli Organi	100%	**A**	
IG.3.21	Verificare che l'esistenza di un'efficace ed efficiente cooperazione tra l'Organo con Funzione di Supervisione Strategica, l'Organo con Funzione di Gestione e le Funzioni Aziendali di Controllo (Internal Audit, Compliance, Risk Management) al fine di pervenire ad un quadro generale dei rischi a cui è esposta la Banca	100%	**A**	
IG.6.1	Verificare che il Gruppo/ la Banca adotti un framework di integrazione e dei meccanismi di coordinamento tra le diverse Funzioni di Controllo in cui si evidenzi al contempo la chiara indipendenza delle stesse, attraverso la chiara distinzione e separatezza delle responsabilità, nonché la dovuta integrazione volta a fornire al Vertice Aziendale un'assurance complessiva sul Sistema dei Controlli aziendali	100%	**A**	
IG.6.4	Verificare che il Gruppo/ la Banca abbia adottato una politica di gestione del rischio di non conformità e che sia stata istituita una Funzione di conformità alle norme che rispetti i requisiti previsti dalla normativa di riferimento	100%	**A**	
IG.6.13	Verificare che la posizione gerarchica e funzionale della Funzione di controllo dei rischi all'interno della struttura organizzativa permetta alla Funzione di svolgere la sua attività in totale indipendenza e autorità. A tal proposito verificare se la Funzione riporta all'Organo con funzione di supervisione strategica o all'organo con funzione di gestione. Indipendentemente dalla sua collocazione gerarchica, verificare che la funzione di controllo dei rischi riesca a mantenere dei legami appropriati con le linee operative	100%	**A**	
IG.6.14	Verificare che il Gruppo/ la Banca adotti un Regolamento della Funzione di controllo dei rischi approvato dall'Organo con Funzione di Supervisione Strategica che specifica gli obiettivi e lo scopo della Funzione, cosi come il posizionamento organizzativo, la composizione, le competenze e le responsabilità	100%	**A**	
IG.6.15	Verificare che la Funzione di controllo dei rischi abbia accesso diretto agli Organi Aziendali. Verificare, inoltre, l'esistenza di un processo periodico di reporting nei confronti dei suddetti Organi	100%	**A**	

La scala di rating si articola su quattro livelli a criticità crescente («A»; «B», «C», «D»). Lo stato «NA» (Non applicabile) è indicato qualora non è espresso alcun rating sull'Obiettivo di controllo, che seppur selezionato in fase di pianificazione dell'intervento non è stato oggetto di specifica verifica in corso di accertamento

Agenda

1. Contesto di riferimento
2. Attività svolta

Allegati

1 Contesto di riferimento: *principali evoluzioni normative in tema di Governance* *(1 di 4)*

2011

27/09/2011 Pubblicazione EBA «Guidelines on Internal Governance»
12/2011 World Bank «How to Develop a Strong Risk Culture within Financial Institutions Leveraging on an Economic Capital Framework and BASEL III"

2012

22/11/2012 Pubblicazione EBA «Guidelines on the assessment of the suitability of members of the management body and key function holders»

2013

01/2013 Pubblicazione BCBS « Principles for effective risk data aggregation and risk reporting»
02/2013 FSB «Thematic Review on Risk Governance»
06/2013 UK Parliamentary Commission on Banking Standards "Changing banking for good" (report su cultura e standard professionali bancari)
07/2013 15° aggiornamento della Circolare n. 263/2006
10/2013 Inizio dell'AQR da parte della BCE; Chartered Institute of Management Accountants "Risk Culture in Financial Organization"
17/12/2013 Emanazione della Circolare 285 Banca d'Italia (che abroga la Circolare n. 263/2006)

2014

09/2014 Pubblicazione IMF working paper: «Reforming the Corporate Governance of Italian Banks»
04/11/2014 Entrata in vigore del SSM

2015

02/2015 Avvio «Thematic Review on Governance & Risk Management» da parte della BCE-Banking Supervision
07/2015 Pubblicazione versione aggiornata BCBS «Guidelines - Corporate governance principles for banks »

2016

01/01/2016 Inizio operatività del SRM (Single Resolution Mechanism)
28/10/2016 Pubblicazione aggiornata EBA «Guidelines on Internal Governance» (consultazione)
28/10/2016 Pubblicazione aggiornata EBA /ESMA «Guidelines on the assessment of the suitability of members of the management body and key function holders» (consultazione)

2017

05/2017 BCE - Guida alla verifica dei requisiti di professionalità e onorabilità
01/08/2017 Schema di decreto ministeriale recante il regolamento in materia di requisiti e criteri di idoneità allo svolgimento dell'incarico degli esponenti aziendali (Draft)
26/09/2017 Pubblicazione aggiornata EBA /ESMA Guidelines on the assessment of the suitability of members of the management body and key function holders (final report)
26/09/2017 Pubblicazione Final Report EBA «Guidelines on Internal Governance» (EBA/GL/2017/11)
31/10/2017 Avvio della Consultazione EBA sulle Linee Guida SREP ove è fatto specifico richiamo all'Internal Governance e alle novità legislative in materia, in quanto uno degli elementi chiave per la valutazione delle banche

2018

21/03/2018 Orientamenti sulla Governance Interna (EBA/GL/2017/11) entrata in vigore il 30/06/2018
19/07/2018 Pubblicazione «Guidelines on the revised common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing», riferite alla Consultazione avviata il 31/10/2017 (e conclusa il 31/01/ 2018)

1 Contesto di riferimento: *le «nuove» linee guida EBA (2 di 4)*

- ✓ Le Linee guida EBA in materia di Internal Governance pubblicate il 26/09/2017 (in sostituzione di quelle precedenti del settembre 2011) e entrate in vigore in data di recente (30/06/2018), si inseriscono in un'articolata successione di disposizioni normative e regolamentari nonché in una fitta serie di standard di settore dedicati al governo societario, al sistema di gestione dei rischi e dei controlli interni, emanati a seguito degli eventi registrati in ambito di governance bancaria tra il 2007 e il 2010.
- ✓ Le nuove Linee guida pongono maggiore enfasi sui doveri e sulle responsabilità dell'Organo di gestione nella sua funzione di supervisione nel controllo dei rischi. Inoltre, è stato ulteriormente sviluppato il quadro di riferimento riguardante il *business conduct*, attribuendo maggiore importanza alla creazione di una cultura del rischio, al codice di condotta e alla gestione dei conflitto d'interesse.
- ✓ Le Linee guida mirano ad armonizzare ulteriormente le modalità, i processi e i meccanismi di governance interna delle istituzioni in tutta l'UE, in linea con le nuove esigenze introdotte nella direttiva sui requisiti patrimoniali (CRD IV) e tenendo conto anche del principio di proporzionalità.

...in Italia

BANCA D'ITALIA

La Circolare n. 285 del 17 dicembre 2013 nei suoi plurimi aggiornamenti, beneficiando del lungo periodo in cui il documento EBA è rimasto in consultazione, disciplina già molti degli aspetti di novità introdotti.

Titoli delle nuove EBA GL

- » I - Proporzionalità
- » II - Ruolo e composizione dell'organo di amministrazione e dei comitati
- » III - Quadro di governance
- » IV - Cultura dei rischi e codice etico
- » V - Quadro e meccanismi di controllo interno
- » VI - Gestione della continuità operativa
- » VII - Trasparenza.

Highlights

Assicurare la supervisione strategica: più efficace, efficiente e consapevole definizione delle strategie aziendali

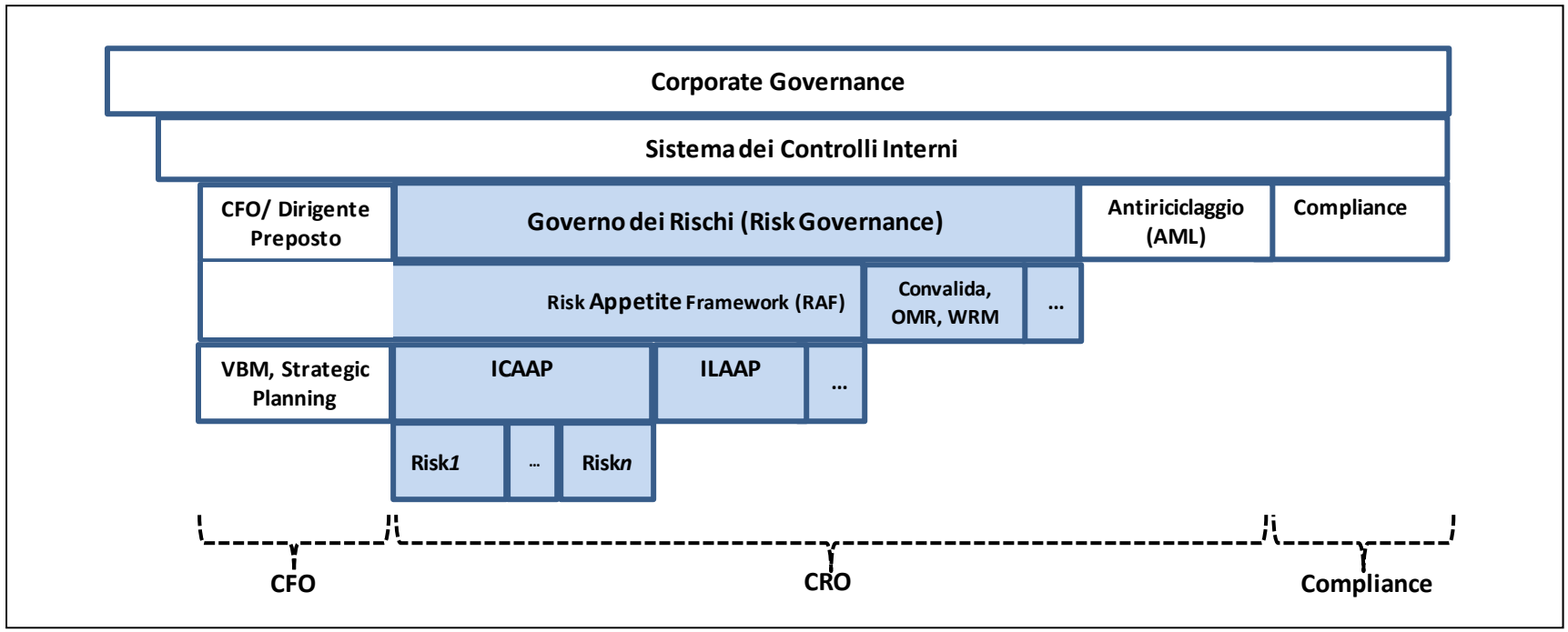
Comitati endoconsiliari: ruolo più proattivo dei Comitati Endoconsiliari, in particolare del Comitato Rischi in materia di rischi e risk strategy

Ruolo della funzione di Risk Management: Da "*Risk Control Function*" a "*Risk Management Function*»

Visione integrata dei controlli interni e della gestione dei rischi

Entrata in vigore delle EBA GL: 30/06/2018

1 Contesto di riferimento: *Il sistema dei controlli e di gestione dei rischi all'interno della Corporate Governance di BMPS (3 di 4)*



Fonte: D1114 Policy in materia di Risk Management

Nel Gruppo MPS si evidenzia un assetto organizzativo e normativo teso a garantire una governance attiva in cui, partendo dalla definizione delle strategie, assume rilievo il rafforzamento e l'integrazione del sistema di controlli interni e di governo dei rischi anche attraverso un ruolo più attivo dei Comitati endoconsiliari e, più in particolare, tra questi, del Comitato Rischi.
In tale ambito, assumono rilievo i meccanismi di reporting e le modalità di interrelazione tra i diversi attori della Corporate Governance.
L'intero sistema è impostato ricercando nel continuo la coerenza con i requisiti normativi, di autodisciplina e di *leading practices* per il settore finanziario, garantendo contemporaneamente la compatibilità con il profilo di rischio del Gruppo, il monitoraggio della corretta implementazione ed esecuzione dei *commitment* connessi al Piano di Ristrutturazione 2017-2021 nonché la sostenibilità per l'azienda di obiettivi coerenti con gli interessi dei diversi *stakeholders*.
Tutti i processi di Corporate Governance ricomprendono gli obiettivi di Risk Culture abbinati all'applicazione dei principi etici e di comportamento, delle linee guida in tema di conflitto di interessi e di *Whistleblowing*.

1 Contesto di riferimento: *Valori aziendali e Codice Etico (4 di 4)*

L'attenzione crescente riservata ai valori etici che devono ispirare la condotta della Banca è da riferire alla nuova concezione del ruolo dell'impresa nella società, nel senso di un più ampio riconoscimento delle sue responsabilità verso il contesto in cui opera.

In particolare con l'emanazione dell' ex D. Lgs n. 231, dell'8 giugno 2001 che ha introdotto per la prima volta in Italia la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, si è andata definendo una «moralità dell'organizzazione», quale parte integrante dei criteri per valutare la performance aziendale, strettamente correlata alla creazione nelle aziende di strutture di governo e di reporting capaci di istituzionalizzare l'etica.

Di seguito la rappresentazione sintetica della normativa nazionale e internazionale alle quali si riferisce il codice etico aziendale, i valori ai quali si ispira e gli obiettivi da perseguire.

Normativa esterna di riferimento

- Codice di autodisciplina;
- Codici di condotta specifici per settore di attività;
- Global Compact delle Nazioni Unite;
- Alleanza europea sulla responsabilità d'impresa

Obiettivi

- Definire standard di «buona condotta»;
- Informare i dipendenti circa i comportamenti attesi;
- Contribuire ad attuare la politica di responsabilità sociale del Gruppo;
- Contribuire a rendere compatibili gli obiettivi del Gruppo con gli interessi della società civile.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Cultura del rischio (1/6)*

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
Effettuare un assessment in relazione agli orientamenti sulla governance interna contenuti nel Titolo IV EBA/GL/2017/11 – Cultura del Rischio e Codice Etico.	Perimetro: BMPS Metodologia: » analisi della normativa interna ed esterna; » interviste al personale delle strutture interessate; » acquisizione evidenze documentali.	Rischio di non conformità alle EBA GL.

RIFERIMENTO EBA GL	ESITI
«*Una cultura del rischio sana e coerente dovrebbe essere un elemento chiave nella gestione efficace dei rischi da parte degli enti e consentire a questi ultimi di prendere decisioni adeguate e informate.* *Gli enti dovrebbero sviluppare una cultura del rischio integrata ed estesa a tutto l'ente, basata sulla piena comprensione e su una visione olistica dei rischi a cui fanno fronte e di come tali rischi vengono gestiti, alla luce della propensione al rischio dell'ente*» (art. 94-95).	Il Reg.1 di Banca MPS – che definisce il modello e l'assetto organizzativo - disciplina distintamente che tutte le strutture aziendali hanno la responsabilità di improntare i comportamenti a principi di eticità delle decisioni e cultura del controllo e di favorire nel quotidiano la pratica di una cultura basata su etica e responsabilità. Pertanto, al fine di garantire la diffusione di una cultura aziendale improntata al rispetto della legalità e del codice etico, i Responsabili delle strutture della Capogruppo (Direzioni, Aree, Servizi e Staff) sono da considerarsi presidi di compliance, chiamati a porre in essere le misure opportune per garantire la conformità delle materie loro attribuite dal presente Regolamento e segnalare alla funzione Compliance ogni eventuale situazione di rilevante non conformità, con particolare attenzione alla correttezza delle relazioni Banca/cliente. Il citato Reg. 1 prevede, altresì, che la Funzione Risk Management supporti le Funzioni di Business, contribuendo alla diffusione della cultura del rischio nella Filiale, e che la Direzione Chief Human Capital Officer (CHCO) valorizzi il capitale umano e favorisca lo sviluppo di valori e cultura di Gruppo.
«*Gli enti dovrebbero sviluppare una cultura del rischio attraverso politiche, comunicazione e formazione del personale riguardo alle attività, alla strategia e al profilo di rischio dell'ente e dovrebbero adattare la comunicazione e la formazione del personale per prendere in considerazione le responsabilità di quest'ultimo nell'assunzione e nella gestione dei rischi*» (art. 96).	Di seguito si riportano le azioni di dettaglio attuate dalla Banca che esplicitano le 3 principali modalità attraverso cui sviluppare la cultura del rischio: 1. politiche, 2. comunicazione (cfr. slide successive), 3. formazione del personale (cfr. slide successive). Con riguardo alle Politiche aziendali, e posto quanto previsto dal Reg.1 (cfr. sopra), dall'analisi della normativa interna di più alto livello (Policy e Direttive) si riscontra positivamente la presenza di espressi richiami alla cultura del rischio e alla cultura aziendale. A titolo esemplificativo e non esaustivo, si citano la Policy in materia di Risk Management Governo dei Rischi (D.1114), la Direttiva sul Governo del RAF (D.1930) e la Policy in materia di Sistema dei Controlli Interni (D.793). Inoltre, la cultura del controllo è presente nelle Linee Guida SCI (D.1635) e la cultura di gestione del rischio trova esplicitazione nella Direttiva di Gruppo in materia di Gestione dei Rischi Operativi (D.906), mentre la Policy e Direttiva sul rischio di non conformità contengono i principi base della cultura aziendale (D.2163, D.1277). In questa overview, si annoverano anche la Direttiva di Gruppo su D.Lgs.231/2001 (D.884) e le Regole per la prevenzione della corruzione (D.2330), quest'ultima con lo specifico obiettivo di diffondere la cultura dell'anticorruzione.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Cultura del rischio (2/6)*

RIFERIMENTO EBA GL	ESITI
«*Il personale dovrebbe essere pienamente consapevole delle proprie responsabilità in merito alla gestione dei rischi. La gestione dei rischi non dovrebbe essere confinata agli esperti in materia di rischi o alle funzioni di controllo interno. Le unità operative, sotto la sorveglianza dell'organo di amministrazione, dovrebbero essere principalmente responsabili della gestione dei rischi su base quotidiana, in linea con le politiche, le procedure e i controlli dell'ente, tenendo in conto la sua propensione al rischio e la sua capacità di rischio*» (art. 97).	Dalla documentazione acquisita e dagli incontri tenuti con le Funzioni di controllo interno in corso di revisione, emerge in modo netto la consapevolezza delle medesime nel presidio della gestione dei rischi aziendali: sia attraverso lo svolgimento delle attività e dei controlli di competenza che nell'adesione a percorsi di formazione professionalizzanti. In tema di formazione continua e specializzata per le Funzioni di Direzione Generale e delle Società, si citano il percorso professionalizzante ABI in Risk Management e Compliance, il percorso AIIA per funzioni di controllo, percorso avanzato ABI per specialisti AML, la certificazione per gli internal auditor (CIA), i diplomi specialistici AIIA per auditors, oltre alla partecipazione a corsi esterni su tematiche di business e controlli (*). E' positivo, inoltre, che tale approccio formativo professionalizzante sia confermato anche per l'anno 2019 con una estensione sistematica di percorsi formativi ad elevata specializzazione per funzioni di controllo e governo (Compliance, CRO e trasversale sul cyber risk). Il senso di responsabilità nella diffusione della cultura del rischio dimostrato dalle Funzioni di controllo trova riflesso anche nella partecipazione in qualità di relatori/docenti ad incontri organizzati con il personale della Banca. Si riportano le seguenti casistiche esemplificative: • la DCRO interviene direttamente nei corsi per il Middle Management; redige induction sia per il Board su specifici rischi che per la Rete Commerciale sul rischio di credito; ha realizzato una survey conoscitiva su tematiche di mitigazione del rischio (diretta a tutto il personale in modo volontario e anonimo); sta collaborando con la Direzione CHCO per definire un palinsesto di attività di comunicazione e informazione al fine di favorire la conoscenza e la condivisione delle attività formative organizzate sulla cultura del rischio; • la Funzione AML/CFT effettua periodiche docenze in aula con risorse della rete, specialisti filiera estero e deliberanti del credito; • specialisti della Funzione Compliance hanno partecipato in qualità di relatori ad iniziative formative organizzate da società specializzate e da ABI; • la DCAE effettua incontri periodici con la rete commerciale al fine di migliorare il presidio dei rischi e favorire la diffusione della cultura del rischio (su AML/CFT, rischi di credito e operativi, frodi e Whistleblowing, …); conduce verifiche in assistenza al Collegio Sindacale sulle Direzioni Territoriali – al termine delle quali sono condivisi gli esiti delle attività poste in essere dall'audit per il presidio dei rischi; effettua verifiche sulla formazione degli auditati in ambito cultura del rischio; conduce audit comportamentali su specifiche tematiche atte ad accertare gli scostamenti tra comportamenti attesi e comportamenti agiti; • complessivamente, le Funzioni di Controllo assicurano la propria collaborazione alla Funzione Formazione nella strutturazione dei corsi di pertinenza (es. corso Risk Master per Area Manager e AML/CFT per Titolari). La Funzione Formazione, inoltre, sta realizzando sia uno specifico Tableau de Bord per i Vertici Aziendali sulla formazione erogata/programmata che KRI operativi.

(*) Formazione destinata ai ruoli specialistici di Funzioni di Controllo di Direzione Generale e Società Controllate (Risk Management, AML, Compliance, Audit); sui singoli moduli la partecipazione è estesa alle filiere Credito, Organizzazione e Commerciale.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Cultura del rischio (3/6)*

RIFERIMENTO EBA GL	ESITI
(segue) «*Il personale dovrebbe essere pienamente consapevole delle proprie responsabilità in merito alla gestione dei rischi. La gestione dei rischi non dovrebbe essere confinata agli esperti in materia di rischi o alle funzioni di controllo interno. Le unità operative, sotto la sorveglianza dell'organo di amministrazione, dovrebbero essere principalmente responsabili della gestione dei rischi su base quotidiana, in linea con le politiche, le procedure e i controlli dell'ente, tenendo in conto la sua propensione al rischio e la sua capacità di rischio*» (art. 97).	*(segue)* Nel corso degli accertamenti è stata acquisita evidenza delle numerose attività formative condotte nell'ultimo biennio dalle Funzioni aziendali della Banca nei confronti del Business e della Rete al fine di diffondere la cultura del rischio e la corretta gestione dello stesso. Oltre alle iniziative formative descritte nei paragrafi precedenti, in cui le Funzioni di controllo hanno svolto un ruolo attivo in qualità di relatori / docenti, i corsi di formazione connessi alla gestione dei rischi e destinati al personale della Banca sono numerosi e variegati per modalità di fruizione - in aula, online, obbligatori e non, trasversali, distinti per ruolo. I contenuti hanno il comune obiettivo di fornire strumenti idonei per gestire i rischi aziendali. A titolo d'esempio, si citano i corsi su AML/CFT, MiFID, IVASS (*), credito NPL, D.Lgs. 231/01, GDPR privacy, trasparenza bancaria, FATCA/CSR, market abuse, safety, sicurezza delle informazioni aziendali, frodi e Whistleblowing. Nell'ottobre 2017, infine, è stato erogato a tutti i dipendenti il corso realizzato da ABI sulla «cultura e governo dei rischi» in materia di gestione e mitigazione dei rischi, normative di riferimento e metodologie di misurazione, concluso con successo dall'87% del target. Anche per il 2019 si rileva una strutturata offerta formativa ad elevata specializzazione che prevede – ad esempio – corsi (con certificazione finale) per le Funzioni di Governo e Controllo su competenze tecnico professionali (cyber risk, risk management, compliance, servizi di investimento, gestione dei conflitti di interesse), due nuovi percorsi di audit sulle competenze relazionali/manageriali e sull'assurance sul II livello di controllo ed iniziative formative distinte su AML/CFT nei confronti delle figure di rete, in considerazione del diverso grado di responsabilità previsto nei processi aziendali (approccio risk based). Rilevano, infine, le attività condotte dalla Funzione Comunicazione Interna, impegnata in una sistematica campagna informativa per diffondere la consapevolezza dell'impegno aziendale e delle persone coinvolte, e dalla Funzione Formazione che monitora regolarmente la fruizione dei corsi e porta avanti iniziative sull'evoluzione delle competenze manageriali, specialistiche e su tematiche volte a trasmettere la cultura del presidio di specifici rischi. E' altresì positiva l'attenzione che la Banca sta ponendo verso un ulteriore affinamento dell'offerta formativa rispetto alle specifiche esigenze di ruolo, misurate su un livello di esposizione al rischio, competenze richieste e responsabilità connesse. Ciò mediante l'adozione di una metodologia risk based - secondo un processo bottom-up – con l'obiettivo di creare attività formative diversificate rispetto al ruolo e quindi al diverso grado di responsabilità previsto dal processo aziendale. Con questo approccio viene svolto un risk assessment di ruolo ed una *skill gap analysis* annuale individuale (**) per definire il fabbisogno ed erogare una formazione mirata, preventivamente condivisa con l'owner di processo. In tal senso si segnala la formazione su AML/CFT per la quale il corso non è più inteso come adempimento amministrativo ma diventa efficace gestione del rischio aziendale per individuare / approfondire i corretti comportamenti e le conoscenze tecniche che soddisfino le aspettative aziendali in termini di normativa e processi aziendali.

(*) Nel rispetto del Reg. ISVAP n. 5/2006 e del Reg. IVASS n. 6/2014 circa la formazione del personale addetto all'attività di intermediazione assicurativa (rif. D.2009).
(**) Es.: la *skill gap analysis* «trasparenza in Banca» per Titolari MPS e «antiriciclaggio» per Area Manager, Titolari, Responsabili Centri, Sostituiti Premium.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Cultura del rischio (4/6)*

RIFERIMENTO EBA GL	ESITI
«*Una forte cultura del rischio dovrebbe anche prevedere quanto segue:* *a. l'adozione di una linea dall'alto: l'organo di amministrazione dovrebbe essere responsabile della definizione e della comunicazione dei valori chiave e delle aspettative dell'ente. Il comportamento dei suoi membri dovrebbe riflettere i valori adottati. La dirigenza dell'ente, compresi i titolari di funzioni chiave, dovrebbero favorire la comunicazione interna al personale dei valori chiave e delle aspettative. Il personale dovrebbe agire in osservanza di tutte le leggi e di tutti i regolamenti applicabili e segnalare prontamente le situazioni non conformi osservate all'interno o all'esterno dell'ente (ad esempio all'autorità competente mediante una procedura di denuncia delle irregolarità). L'organo di amministrazione dovrebbe continuamente promuovere, monitorare e valutare la cultura del rischio dell'ente, valutare l'impatto di tale cultura sulla stabilità finanziaria, sul profilo di rischio e sulla solida governance dell'ente, nonché apportare modifiche laddove necessario*» (art. 98, a).	Dai flussi informativi analizzati appare acquisita la volontà di adottare una «linea dall'alto» che tenga conto di una corretta gestione dei rischi e promuova la diffusione della cultura del rischio a tutti i livelli aziendali, anche mediante l'azione congiunta delle Funzioni di Governo. La reportistica periodica e ad evento redatta nei confronti dei Vertici aziendali è prevista, ad esempio, nel D.1915 «Flussi Informativi» in fase di aggiornamento, nel D.2291 «Direttiva in materia di Integrated Risk Reporting» e mediante board induction. Essa contribuisce a fornire una visione olistica dell'attuale presidio dei rischi (cfr. slide seguenti), delle prospettive future e offre uno strumento utile per valutare gli impatti sulla governance. In tal senso, rileva il coinvolgimento dei Resp. delle Funzioni aziendali nell'effettuazione periodica dei *risk self assessment* - in materia D.Lgs.231/01, rischi operativi, 262 ed i cui esiti sono portati all'attenzione dei Vertici aziendali – e il processo interno adottato per monitorare le azioni correttive a fronte delle criticità rilevate dalle Funzioni di controllo, oggetto di monitoraggio da parte del Comitato per il Coordinamento delle Funzioni con compiti di controllo e periodica rendicontazione agli Organi Apicali. Come illustrato nei paragrafi precedenti, la normativa interna redatta su tematiche di rischio e sistema dei controlli interni (Policy e Direttive *in primis*) contengono espressi rischiami alla cultura del rischio, confermando un chiaro "tone at the top" aziendale e la volontà di diffondere tali principi a tutta l'organizzazione. A tal proposito le Funzioni Aziendali della Banca hanno preso consapevolezza della necessità di una maggiore azione coordinata (CRO, COO, CLO, CCO, CHCO, ecc.) per meglio presidiare la cultura del rischio, intesa nelle sue diverse articolazioni (operativo, di mercato, di credito, ecc), ciò mediante un sistema integrato di processi, procedure, controlli, metodologie e azioni info-formative per gestire e mitigare in modo consapevole il rischio, rafforzando la reputazione complessiva (*). Dal punto di vista di formazione del personale, è stato attuato un piano definito attraverso un processo totalmente «bottom-up» con l'erogazione di una formazione specialistica (funzioni di controllo, risk management, risorse umane, credito, commerciale e organizzazione) e ritagliata sulla posizione ricoperta (ruoli di rete, neo assunti, neo titolari e titolari advanced (**), ..) così da favorire anche la comunicazione delle aspettative e valori. Rileva positivamente che per il 2018 è continuata la formazione finalizzata ad accrescere la cultura del presidio dei rischi e proseguirà anche per il 2019. In tale contesto, in Banca ha attivato canali riservati per la segnalazione di possibili infrazioni o violazioni che il personale ritenga di comunicare come in caso di infrazioni al codice etico, ai sensi del D.Lgs. 231/01, per operazioni sospette AML/CFT e market abuse. Dal 2015 è attiva anche la procedura di Whistleblowing per i cui dettagli si rimanda alle apposite slide.

(*) cfr. Sisifo per CdA del 30.10.2018 «Cultura del rischio: aggiornamento».
(**) Per i titolari di filiale sono attivi due percorsi in aula, base e advanced, (ciascuno 5 gg) centrati sul presidio del rischio di credito, operativo, di mercato e riflessi sul conto economico. Le attività prevedono anche elementi utili al consolidamento di comportamenti efficaci.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Cultura del rischio (5/6)*

RIFERIMENTO EBA GL	ESITI
«*Una forte cultura del rischio dovrebbe anche prevedere quanto segue:* *b) Responsabilità: il personale pertinente di ogni livello dovrebbe conoscere e comprendere i valori chiave dell'ente e, nella misura necessaria per il ruolo rivestito, la propensione al rischio e la capacità di rischio dell'ente. Dovrebbe essere in grado di svolgere il proprio ruolo ed essere consapevole che sarà ritenuto responsabile delle proprie azioni riguardo al comportamento dell'ente relativo all'assunzione del rischio*» (art. 98, b)	Gli esiti delle verifiche rendicontate nei paragrafi precedenti hanno avuto l'obiettivo di evidenziare una piena consapevolezza nella gestione dei rischi e nella diffusione della cultura del rischio da parte del Board e delle principali Funzioni Aziendali e di Controllo. Ciò, ad esempio, mediante l'adozione di politiche aziendali, la partecipazione attiva ad iniziative formative e la co-predisposizione di corsi destinati al personale. Resta comunque nella responsabilità del dipendente effettuare e concludere i corsi formativi a cui è iscritto per migliorare la capacità di comprendere i propri rischi, gestirli correttamente e, per quanto possibile, evitare che si reiterino. La Banca, d'altro canto, ha in essere processi aziendali collegati all'avvenuta fruizione dei corsi obbligatori in base ai quali un mancato completamento costituisce elemento ostativo per l'attribuzione e/o la permanenza in ruoli di responsabilità, la partecipazione ai corsi esterni oppure l'erogazione di premi in caso di contest (cfr. D.2222 Gestione Contest, Stage Formativi e Workshop) . Al contempo, la Funzione Risorse Umane presidia le attività di formazione e la valutazione delle competenze/comportamenti, curandone in modo integrato le ricadute anche in termini gestionali mentre la Funzione Commerciale presidia le attività di monitoraggio qualitativo dell'azione commerciale svolta dalle strutture territoriali e la valutazione gestionale sui rischi operativi da essa conseguenti.
«*Una forte cultura del rischio dovrebbe anche prevedere quanto segue:* *c. Comunicazione e messa in discussione efficaci: una cultura del rischio solida dovrebbe promuovere un ambiente dove viga una comunicazione aperta e una messa in discussione efficace, in cui i processi decisionali incoraggiano pareri ampiamente diversificati, consentono di testare le pratiche attuali, stimolano un atteggiamento critico costruttivo fra il personale e promuovono un ambiente all'insegna di un impegno aperto e costruttivo nell'intera organizzazione*» (art. 98, c).	L'analisi dei flussi informativi codificati nella normativa interna (es. D.1915) evidenzia la predisposizione di una strutturata reportistica destinata ai Vertici Aziendali e ai Comitati con funzioni di supporto al CdA. A questi si aggiungono i report prodotti in occasione delle riunioni dei Comitati di Gestione durante i quali le Funzioni di Controllo, ad esempio, condividono le principali evidenze sui rischi di competenza e contribuiscono a fornire una visione globale dei rischi. Per ulteriori dettagli sulla reportistica prodotta per relazionare i Comitati si rimanda alle slide sul Titolo V delle EBA GL ed, in particolare, alle analisi condotte sul Risk Management. A latere, inoltre, si segnala che le EBA GL demandano agli Enti la possibilità di istituire, oltre ai comitati obbligatori (Comitato Rischi, Comitato Nomine e Comitato Remunerazioni), anche altri comitati quali il Comitato Etico, Comitato di Condotta e Comitato di Conformità (cfr. par. 41 EBA GL). Di fatto la Banca ha già istituito Comitati che assolvono in buona sostanza a quanto auspicato dalle EBA GL: Comitato di Coordinamento delle Funzioni di Controllo, OdV 231 e Commissione Affari Disciplinari.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Cultura del rischio (6/6)*

RIFERIMENTO EBA GL	ESITI
«*Una forte cultura del rischio dovrebbe anche prevedere quanto segue:* *d. Incentivi: incentivi appropriati dovrebbero svolgere un ruolo chiave nell'allineamento del comportamento di assunzione del rischio con il profilo di rischio dell'ente e il suo interesse a lungo termine*[21]» (art. 98, d).	In tema di remunerazione ed incentivi, le Politiche di Remunerazione del Gruppo MPS (*), nell'accrescere la governance aziendale, hanno anche l'obiettivo - tra gli altri - di: • essere in linea con i valori, le strategie e gli obiettivi aziendali di lungo periodo; • essere coerenti con i livelli di capitale e di liquidità necessari a fronteggiare le attività intraprese; • evitare incentivi distorti che possano indurre ad un'eccessiva assunzione di rischi per l'intermediario ed il sistema finanziario nel suo complesso. Il rafforzamento del legame tra retribuzione, performance ed assunzione di rischi è tema quanto mai all'attenzione ed oggetto di esplicita previsione sia nelle su citate Politiche che nella Policy in materia. In dettaglio, la funzione Risk Management della Banca salvaguarda la sostenibilità delle politiche di remunerazione e produce una relazione a supporto del Comitato Rischi che, a sua volta, accerta - attraverso un parere per il Comitato Remunerazione – la coerenza tra gli incentivi sottesi al sistema di remunerazione e incentivazione del Gruppo con il RAF. Ad esempio, il Premio Variabile di Risultato (PVR) ed il *Management by Objectives* (MBO) sono parametrati ad indicatori di performance misurati al netto dei rischi ed attivati solo in caso di raggiungimento di obiettivi economico-patrimoniali. Pertanto, l'incorporazione dei macro indicatori di rischio e di *performance risk-adjusted* coerenti con il RAF nelle politiche di remunerazione e incentivazione del personale rappresenta un'ulteriore leva per promuovere la consapevolezza dei comportamenti agiti da tutte le risorse e l'accrescimento di una sana cultura del rischio. Quanto sopra esposto trova riscontro nel "*Sistema di Talent & Performance Management*" adottato dalla Banca che, complessivamente, impatta sui piani di sviluppo e formazione, remunerazione (es. esclusione da contest) e piani gestionali di mobilità. Peraltro, a partire dal 2017, tale sistema di valutazione delle performance dei dipendenti è stato implementato di tre modifiche per considerare le tematiche di rischio ed il suo presidio nell'attività ordinaria (**). Infine, si cita il sistema sanzionatorio ex post adottato dalla Banca nei casi di irregolarità rilevate a carico del personale, ovvero i richiami interni e le sanzioni discusse in sede di Commissione Affari Disciplinari (CAD) per fatti di particolare gravità, che annoverano anche motivazioni direttamente o indirettamente connesse alla cultura del rischio (violazioni di normative, scarsa diligenza, anomalie nella gestione del rischio di credito, omessi o inefficaci controlli,…).

Nota 21: Si rimanda anche agli orientamenti dell'ABE su sane politiche di remunerazione ai sensi dell'articolo 74, paragrafo 3, e dell'articolo 75, paragrafo 2, della direttiva 2013/36/UE e sull'informativa ai sensi dell'art.450 del regolamento (UE) n. 575/2013 (ABE/GL/2015/22), disponibili all'indirizzo https://www.eba.europa.eu/regulation-and-policy/remuneration.
(*) per dettagli, cfr. Relazione sulla Remunerazione anno 2018.
(**) Nell'ambito del processo valutativo, è stata aggiunta per tutta la popolazione del Gruppo la valutazione della competenza inerente ai "Rischi connessi all'attività" e incluso nel comportamento «Rigore e Professionalità» l'attenzione al presidio dei rischi.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (1/12)*

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
Assessment circa gli orientamenti sulla governance interna contenuti nel Titolo IV EBA/GL/2017/11 – Cultura del Rischio e Codice Etico_ Valori aziendali e Codice Etico	Perimetro: BMPS Metodologia: » analisi della normativa interna ed esterna; » interviste al personale delle strutture interessate; » acquisizione evidenze documentali.	Rischio di non conformità alle EBA GL.

RIFERIMENTO EBA GL

Linee guida EBA GL/2017/11
Valori aziendali e Codice Etico

Art. 99 – *L'organo di amministrazione dovrebbe sviluppare, adottare, rispettare e promuovere le necessità e le caratteristiche specifiche dell'ente e dovrebbe garantirne l'attuazione (mediante un codice etico e uno strumento analogo). Dovrebbe anche monitorare il rispetto di tali standard da parte del personale. Laddove applicabile, l'organo di amministrazione può adottare e attuare gli standard relativi al gruppo dell'ente o gli standard comuni pubblicati da associazioni o altre organizzazioni pertinenti*

ESITI

Il Codice Etico del Gruppo Montepaschi, approvato dal Consiglio di Amministrazione della Banca, è stato aggiornato in data 16 dicembre 2016 per introdurre le previsioni normative riferite al «sistema interno di segnalazione delle violazioni» (c.d. Whistleblowing).

Il documento, destinato alle strutture della Capogruppo Bancaria e alle società controllate, dispone che queste ultime provvedano al relativo recepimento con atto deliberativo dell'Organo competente e a uniformare la propria normativa interna ai principi ispiratori del citato codice.

In tal senso sono state condotte specifiche verifiche che hanno consentito di rilevare il puntuale recepimento del documento in vigore, da parte delle controllate del Gruppo MPS, a fronte dell'aggiornamento normativo citato.

Il Codice etico è costituito dall'insieme dei principi guida, complementari agli obblighi di legge, dai modelli e dalle norme di comportamento che ispirano l'attività della Banca, orientando le condotte attese in continuità e coerenza con la missione dell'Azienda e dei suoi valori fondamentali: etica della responsabilità, orientamento al cliente, attenzione al cambiamento, imprenditività e proattività, passione per le competenze professionali, spirito di squadra e cooperazione.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (2/12)*

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
Assessment circa gli orientamenti sulla governance interna contenuti nel Titolo IV EBA/GL/2017/11 – Cultura del Rischio e Codice Etico_ Valori aziendali e Codice Etico	Perimetro: BMPS Metodologia: » analisi della normativa interna ed esterna; » interviste al personale delle strutture interessate; » acquisizione evidenze documentali.	Rischio di non conformità alle EBA GL.

RIFERIMENTO EBA GL

ESITI

In tempi relativamente recenti si è andata affermando una nuova concezione del ruolo dell'impresa nella società, nel senso di un più ampio riconoscimento delle sue responsabilità verso il contesto in cui opera.

La consapevolezza di una «responsabilità sociale» delle aziende, è espressione di un mutamento nelle aspettative della società nei confronti delle imprese. In particolare con l'emanazione dell'ex D. Lgs n. 231 dell'8 giugno 2001 che ha introdotto per la prima volta in Italia la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, si è andata definendo una «moralità dell'organizzazione» che ha determinato un'attenzione crescente in materia di valori etici, quale parte integrante dei criteri per valutare la performance aziendale. La stessa si esprime non solo in termini di redditività e di crescita, ma contemperando gli interessi di lungo periodo di molteplici stakeholders, la cui collaborazione è essenziale per il successo dell'impresa. Prospettiva quest'ultima che è strettamente correlata alla creazione nelle aziende di strutture di governo e di reporting capaci di istituzionalizzare l'etica.

In tal senso l'adozione da parte della banca e delle società controllate del Gruppo MPS del Codice Etico, rappresenta la piena adesione ai valori che lo stesso esprime e la modalità attraverso la quale l'impresa e il suo management può mostrare la «due diligence» nell'esercizio delle proprie responsabilità.

Gli obiettivi e le finalità del Codice etico trovano rappresentazione nell'enunciazione dei:

- **principi e valori etici** – che devono ispirare l'attività di coloro che operano per conto della Banca, tenendo conto dell'importanza dei ruoli e delle relative responsabilità;
- **norme comportamentali** – mediante la definizione dello standard di «buona condotta» per l'attuazione di politiche e procedure aziendali;
- **formazione dei dipendenti -** nell'ottica di favorire i comportamenti attesi e di contribuire ad attuare una **politica di responsabilità sociale** all'interno del Gruppo.

In tal senso il Codice Etico opera indistintamente nei confronti dei seguenti destinatari:

- amministratori, sindaci e dirigenti del Gruppo, nello svolgimento delle proprie funzioni ed in relazione alle rispettive responsabilità;
- dipendenti di ogni ordine e grado.

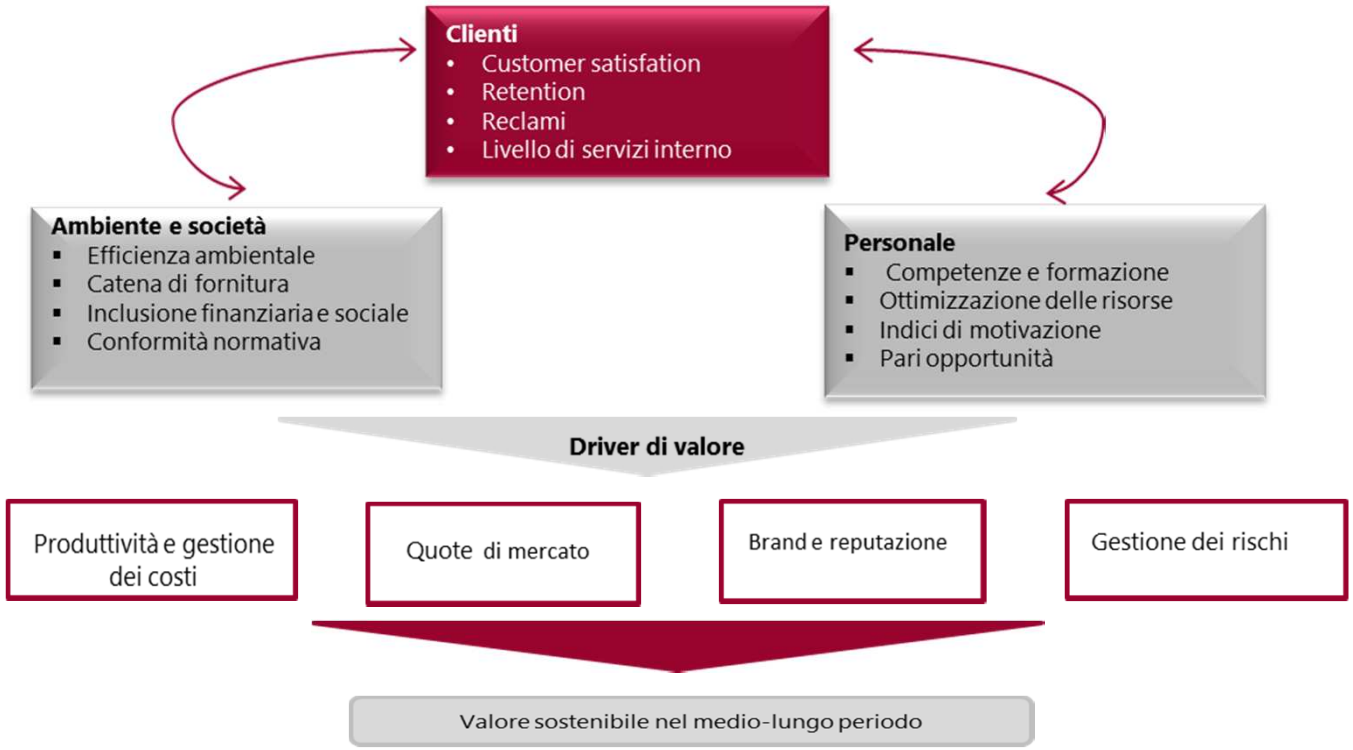
2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (3/12)*

Il Gruppo MPS ha inoltre esplicitato il suo impegno di responsabilità sociale attraverso la «Carta dei Valori», definita in relazione all'«etica della responsabilità», la quale si esprime con un costante orientamento al servizio, all'integrità, alla trasparenza, alla correttezza negli affari, alla salvaguardia dell'ambiente e al rispetto delle persone; principi ripresi, ribaditi e sviluppati nel Codice Etico.

Quest'ultimo, in particolare, sottolinea per il Gruppo MPS, la centralità della creazione di valore per gli azionisti, ponendo un'attenzione prioritaria alla soddisfazione dei clienti, favorisce inoltre lo sviluppo professionale delle persone e sostiene l'importanza del citato concetto di responsabilità sociale, che si esprime rispondendo alle attese e agli interessi degli azionisti e degli altri stakeholder.

Nello specifico le politiche e gli obiettivi di *Corporate Social Responsibility (CSR)* sono intesi come driver per la creazione di valore per l'azienda e la gestione attiva dei c.d. CSR Intangible Asset (fattori di sviluppo e motivazione del personale, qualità di gestione, livelli di servizio ai clienti e soddisfazione relativa, investimenti nel sociale e nei sistemi territoriali) che rappresenta un mezzo per esaltare le performance economico-finanziarie dell'azienda.

Di seguito un modello di misurazione dei Csr Intangible Asset – schema logico



2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (4/12)*

Il documento che disciplina la materia (*) delinea le c.d. «regole di condotta», che trovano espressione soprattutto in determinati ambiti normativi, di seguito indicati:

- gestione del personale e ambiente di lavoro;
- relazioni con i clienti;
- rapporti con i fornitori;
- correttezza e trasparenza negli affari (concorrenza sleale, integrità, conflitto di interessi, lotta alla corruzione, gestione delle informazioni);
- uso di asset aziendali;
- organi amministrativi, direttivi e di controllo;
- rapporti con organizzazioni esterne (autorità e istituzioni pubbliche, organizzazioni sindacali e politiche, organizzazioni della società civile, organi d'informazione e relazioni pubbliche;
- responsabilità verso la «società» (opposizione ad attività criminose, creazione di valore per gli azionisti e gli altri stakeholder, impegno verso la comunità, tutela dall'ambiente).

In merito a quest'ultimo punto, l'attenzione della Banca si è espressa anche mediante l'adesione alla norma OHSAS18001 *Occupational Health and Safety Assessment Series*, principale standard di riferimento a livello mondiale sulla sicurezza e la salute dei lavoratori. L'art. 30 del D. Lgs. 81/08 la indica per la conformità alle disposizioni di tale articolo. Tale adesione è esimente della relativa responsabilità amministrativa di cui al D. Lgs 231/01.

Oltre alle regole del Codice, il Gruppo si impegna a rispettare anche le discipline di emanazione esterna a cui aderisce, come:

- **Codice di autodisciplina (**)**– emanato dal Comitato per la Corporate Governance costituito, nell'attuale configurazione, nel giugno 2011 ad opera delle Associazioni di Impresa (ABI, ANIA, Assonime, Confindustria) e di investitori professionali (Assogestioni), nonché da Borsa Italiana SpA;

- **Alleanza Europea per un'Impresa Competitiva e Sostenibile** – nata nel 2006 con l'obiettivo di incoraggiare l'adesione alla RSI/CSR tra le imprese europee, dare maggiore supporto e riconoscimento al suo contributo per lo sviluppo sostenibile e per le strategie finalizzate alla crescita economica e all'occupazione;

- **Global Compact delle Nazioni Unite** – è un'iniziativa volontaria lanciata nel 1999 con l'obiettivo di promuovere su scala globale la cultura della responsabilità sociale d'impresa. E' quindi una rete che unisce governi, imprese, agenzie delle Nazioni Unite, organizzazioni sindacali che realizza un «economia globale più inclusiva e sostenibile» attraverso la condivisione, l'implementazione e la diffusione dei principi e dei valori promossi dall'iniziativa.(***)

(*) D. 1186 Codice Etico del Gruppo MPS (vers. 3 del 16.12.2016);
(**) Il Codice di Autodisciplina è stato aggiornato al Luglio 2018;

(***) I principi del Global Compact, estrapolati da trattati internazionali come la «Dichiarazione Universale dei Diritti Umani», la «Dichiarazione sui Principi Fondamentali e i Diritti nel Lavoro» dell'ILO, la «Dichiarazione sull'Ambiente e lo Sviluppo» di Rio de Janeiro, sono: 1) promuovere e rispettare i diritti umani universalmente riconosciuti nell'ambito delle rispettive sfere di influenza; 2) assicurarsi di non essere, seppur indirettamente, complici negli abusi dei diritti umani; 3) sostenere la libertà di associazione dei lavoratori e riconoscere il diritto alla contrattazione collettiva; 4) eliminazione di tutte le forme di lavoro forzato e obbligatorio; 5) effettiva eliminazione del lavoro minorile; 6) eliminazione di ogni forma di discriminazione in materia di impiego e professione;7) Sostenere un approccio preventivo nei confronti delle sfide ambientali; intraprendere iniziative che promuovano una maggiore responsabilità ambientale; 9) incoraggiare lo sviluppo e la diffusione di tecnologie che rispettino l'ambiente; 10)contrastare la corruzione in ogni sua forma, incluse l'estorsione e le tangenti.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (5/12)*

Linee guida EBA GL/2017/11
Titolo IV – Valori aziendali e codice etico

Art. 100. Gli standard attuati dovrebbero mirare a ridurre i rischi ai quali l'ente è esposto, in particolare i rischi di tipo operativo e reputazionale, che possono avere un impatto considerevolmente negativo sulla redditività e sostenibilità dell'ente sotto forma di ammende , spese di contenzioso, restrizioni imposte dalle autorità competenti o altre sanzioni finanziarie o penali e la perdita di valore del marchio e della fiducia del cliente.
Art. 101 L'organo deliberante dovrebbe adottare politiche chiare e documentate per delineare le modalità con le quali tali standard dovrebbero essere rispettati. Tali politiche dovrebbero:
c. Stabilire principi e fornire esempi in merito a comportamenti accettabili o inaccettabili legati, in particolare, a informazioni inesatte o illeciti professionali in ambito finanziario, reati economici e finanziari (fra cui frode, riciclaggio di denaro e pratiche anti-trust, sanzioni finanziarie, corruzione, manipolazione di mercato, vendita di prodotti inadeguati e altre violazioni della normativa che tutela i consumatori.
d. Chiarire che, oltre al rispettare le disposizioni giuridiche e regolamentari e le politiche interne, il personale è chiamato a comportarsi in modo onesto ed integro e a svolgere i propri doveri con la dovuta capacità, attenzione e diligenza; e
e. Garantire che il personale sia consapevole delle potenziali azioni disciplinari interne ed esterne, delle azioni legali e delle sanzioni che possono seguire comportamenti scorretti o inaccettabili.

Un incentivo alla diffusione nelle imprese italiane dei codici etici è avvenuto con l'emanazione dell'ex D. Lgs n. 231, dell'8 giugno 2001 (*) che ha introdotto per la prima volta in Italia la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica per gli illeciti amministrativi dipendenti da reato.

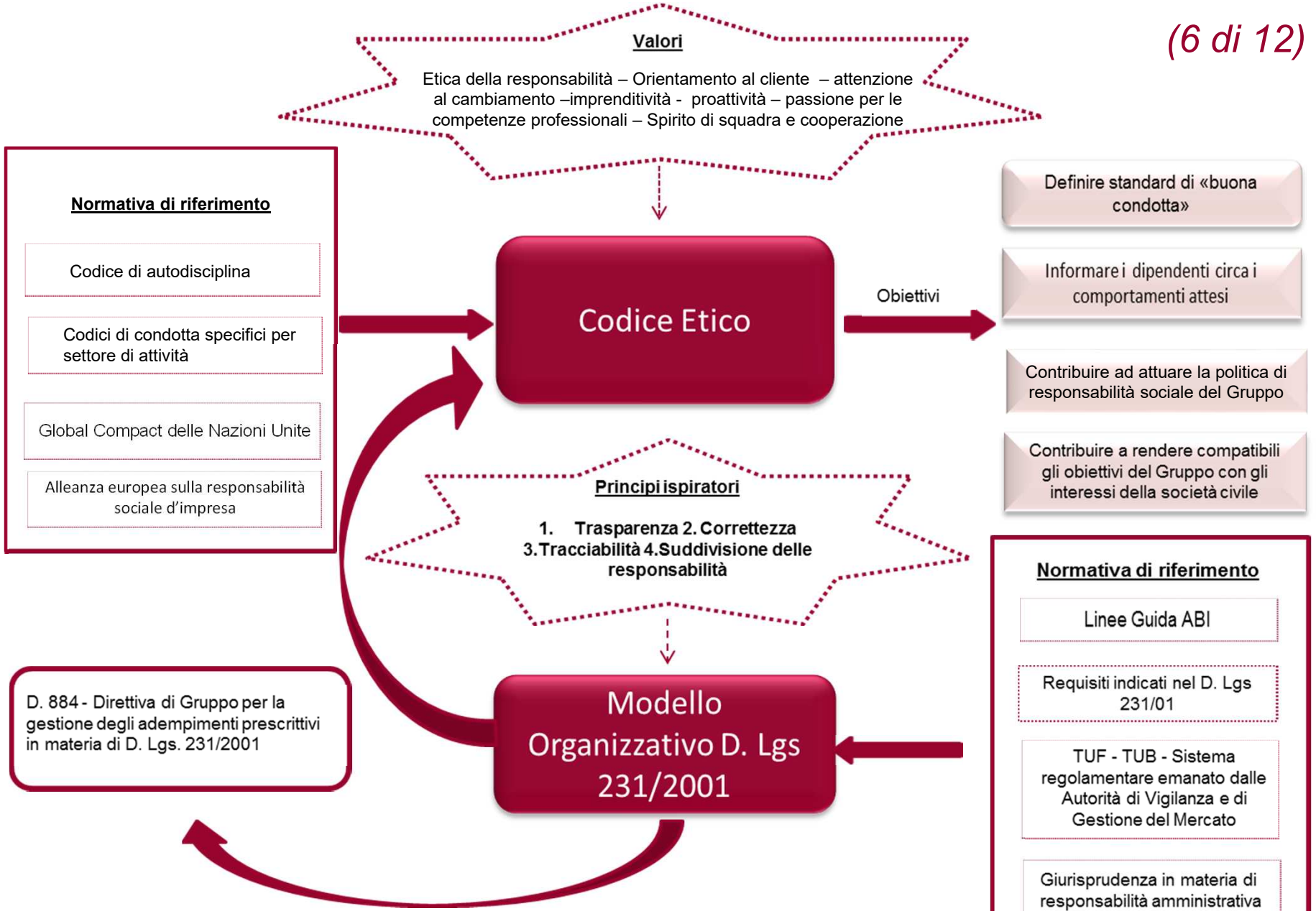
L'art. 5 del decreto stabilisce che l'ente «è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti menzionati al punto precedente.
L'art. 6 nello stesso tempo contempla, una specifica forma di esonero qualora l'ente dimostri, nel caso di reati commessi da soggetti apicali, che: a) l'organo dirigente ha adottato e efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire i reati previsti dal citato decreto; b) il compito di vigilare sul funzionamento dei modelli sia stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione; d) non vi è stata omessa e insufficiente vigilanza da parte dell'organismo dedicato.

I modelli di organizzazione e di gestione idonei a prevenire reati devono rispondere ad una serie di esigenze: a) individuare le attività nel cui ambito possono essere commessi reati; b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire; c) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di reati; d) prevedere obblighi di informazione neo confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza di modelli; e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate dal modello.

L'adozione e l'attuazione da parte delle imprese di modelli di organizzazione e gestione idonei a prevenire i reati si deve basare su un'etica aziendale che abbia un approccio globale e vada al di là della richiesta di conformità alla legge, fondato sull'idea di «integrità morale» che coniughi l'attenzione per la responsabilità morale manageriale.
Una strategia basata sul principio di integrità morale permette di stabilire uno standard di condotta più solido mentre il principio di conformità alle leggi si basa sulla necessità di evitare sanzioni legali. Inoltre, il principio di integrità si fonda sull'idea dell'autogoverno e di responsabilità del management in conformità a una serie di principi e valori guida.
In tale ottica il Codice Etico, parte integrante del Modello Organizzativo ex D.Lgs 231/2001 è oggetto di un assessment periodico, di norma biennale, da parte della Funzione Compliance unitamente alla Funzione Legale, che ne valutano l'adeguatezza in ordine alle disposizioni legislative vigenti e alla relativa tenuta da riferire alla struttura e alle dimensioni aziendali.

L'ultimo aggiornamento del Codice risale al dicembre 2016 a seguito del recepimento del «sistema interno di segnalazioni delle violazioni (c.d. «Whistleblowing»). Nella slide a pag. 23 viene evidenziata la correlazione tra Codice Etico e Modello Organizzativo 231, con i relativi riferimenti normativi.

(*)Emanato in attuazione della delega contenuta nella Legge n. 300 del 29 settembre 2000. Quest'ultima ratifica le Convenzioni OCSE e UE contro la corruzione nel commercio internazionale e contro la frode ai danni della Comunità Europea


Valori
Etica della responsabilità – Orientamento al cliente – attenzione al cambiamento –imprenditività - proattività – passione per le competenze professionali – Spirito di squadra e cooperazione
Normativa di riferimento
Codice di autodisciplina
Codici di condotta specifici per settore di attività
Global Compact delle Nazioni Unite
Alleanza europea sulla responsabilità sociale d'impresa
Codice Etico
Obiettivi
Definire standard di «buona condotta»
Informare i dipendenti circa i comportamenti attesi
Contribuire ad attuare la politica di responsabilità sociale del Gruppo
Contribuire a rendere compatibili gli obiettivi del Gruppo con gli interessi della società civile
Principi ispiratori
1. Trasparenza 2. Correttezza 3.Tracciabilità 4.Suddivisione delle responsabilità
Modello Organizzativo D. Lgs 231/2001
D. 884 - Direttiva di Gruppo per la gestione degli adempimenti prescrittivi in materia di D. Lgs. 231/2001
Normativa di riferimento
Linee Guida ABI
Requisiti indicati nel D. Lgs 231/01
TUF - TUB - Sistema regolamentare emanato dalle Autorità di Vigilanza e di Gestione del Mercato
Giurisprudenza in materia di responsabilità amministrativa delle Società – Reati 231

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (7/12)*

La Banca, negli ultimi anni, ha riservato una particolare attenzione al tema della formazione del personale su temi afferenti il Codice Etico e la Cultura del Rischio, in relazione all'evolversi dello scenario economico-normativo di riferimento .

In tal senso la Direzione CHCO ha pianificato, nel biennio 2017/2018(*), diverse attività formative (in aula, on line, etc.) estese a tutto il personale (Capogruppo e Rete) al fine di garantire con sistematicità un costante aggiornamento sugli ambiti di maggior rilievo. Di seguito uno schema riepilogativo delle diverse tipologie di corsi realizzati, più strettamente attinenti agli argomenti trattati dal Codice Etico.

Linee Guida EBA GL/2017/11 Titolo IV «Valori Aziendali e codice etico

Art. 101 L'organo di amministrazione dovrebbe adottare politiche chiare e documentate per delineare le modalità con le quali tali standard dovrebbero essere rispettati. Tali politiche dovrebbero:

a. Ricordare ai lettori che tutte le attività dell'ente dovrebbero essere condotte in conformità del diritto applicabile e dei valori aziendali dell'ente;

b. Promuovere la consapevolezza del rischio attraverso una forte cultura del rischio, in linea con la sezione 9 degli orientamenti, trasmettendo il messaggio secondo cui l'organo di amministrazione si aspetta che le attività non si spingeranno oltre la propensione al rischio e oltre i limiti definiti dall'ente e le rispettive responsabilità del personale.

c. Art. 102 Gli enti dovrebbero monitorare il rispetto di tali standard e garantire la sensibilizzazione del personale, ad esempio mediante la sua formazione

(*) Periodo preso in esame

Formazione 2017/2018 "Argomenti inerenti il Codice Etico"

Iniziativa	Contenuti	Target	SAL
GDPR Privacy (1h)	o Nuovo Regolamento UE in ambito Privacy, applicazione in MPS (normativa e comportamenti efficaci).	Tutti i dipendenti del Gruppo (c.a. 23.000 risorse)	88% formati (iscrizioni 2018)
Responsabilità Amministrativa delle società - D.Lgs. 231/01 (3 h)	o Contenuti del D. Lgs. 231/2001 e fattispecie di reati; o Presidi adottati dal Gruppo MPS e protocolli di controllo; o Comportamenti utili al fine di non incorrere nelle sanzioni previste dalla normativa vigente.	Tutti i dipendenti del Gruppo (c.a. 23.000 risorse)	90% formati (iscrizioni 2017)
Trasparenza (1h30)	o Normativa vigente, rapporto con il cliente e principali suo diritti. Informativa e schema contrattuale; o Tecniche di comunicazione commerciale.	Tutti i dipendenti del Gruppo (c.a. 23.000 risorse)	97% formati
Whistleblowing	o Cos'è il Whistleblowing: come e cosa segnalare; la tutela del segnalante; monitoraggio e custodia delle segnalazioni.	Tutti i dipendenti del Gruppo (c.a. 23.000 risorse)	Avviato nel IV trimestre 2018
Skill Gap Analysis - Trasparenza in Banca	o Misurazione dello stato di conoscenza delle risorse su normative, processi e operatività della Trasparenza;	Titolari MPS (1.500 risorse)	88% partecipanti (2018)
Skill Gap Analysis - Antiriciclaggio per la Rete	o Misurazione dello stato di conoscenza delle risorse su tematiche Antiriciclaggio (Presidio del ruolo e responsabilità: i comportamenti - verifica della clientela - Alimentazione archivio unico - Limitazione uso contante - Segnalazione operazioni sospette).	Area manager, Titolari MPS, Responsabili Centri, Sistituti Premium (ca 2.250 risorse)	90% partecipanti (2018)
Antiriciclaggio	o Aggiornamento su IV Direttiva AML per Titolari e ODS (1 g. aula + on line per tutti); o Percorso ad elevata specializzazione con certificazione finale (3 gg) - realizzato con ABI.	Titolari e ODS (ca 800 aula) Tutta la rete (16.000 online) 120 specialisti DG e società	40% formati (in corso) In erogazione da nov. 18
IVASS ex art. 40/18 del nuovo Regolamento (cfr. D. 1174 "Gestione di collocamento prodotti di finanziamento al consumo")	o Aggiornamento normativa su Bancassicurazione con specifici richiami a Trasparenza, Antiriciclaggio, corretta profilatura del cliente (30h).	Tutti i Collocatori di Polizze (ca 13.000 risorse in ruoli di Rete)	60% formati
Servizi di Investimento (MIFID)	o Aggiornamento in conformità al disposto del Regolamento Intermediari 20307 CONSOB, che prevede in termini generali la mitigazione del rischio operativo di non conformità (30h) o Si affrontano anche il Rischio di Mercato, Richio di Credito, Rischio di Liquidità.	Ruoli di Rete (ca 12.500 risorse)	93% formati (dato novembre 2018)

Fonte: Servizio Knowledge Management e Formazione (dati aggiornati a novembre 2018)

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (8/12)*

Di seguito una rappresentazione schematica dei corsi di formazione in materia di antiriciclaggio e contrasto al terrorismo, per l'anno 2017.

Sintesi attività formativa AML_CFT anno 2017

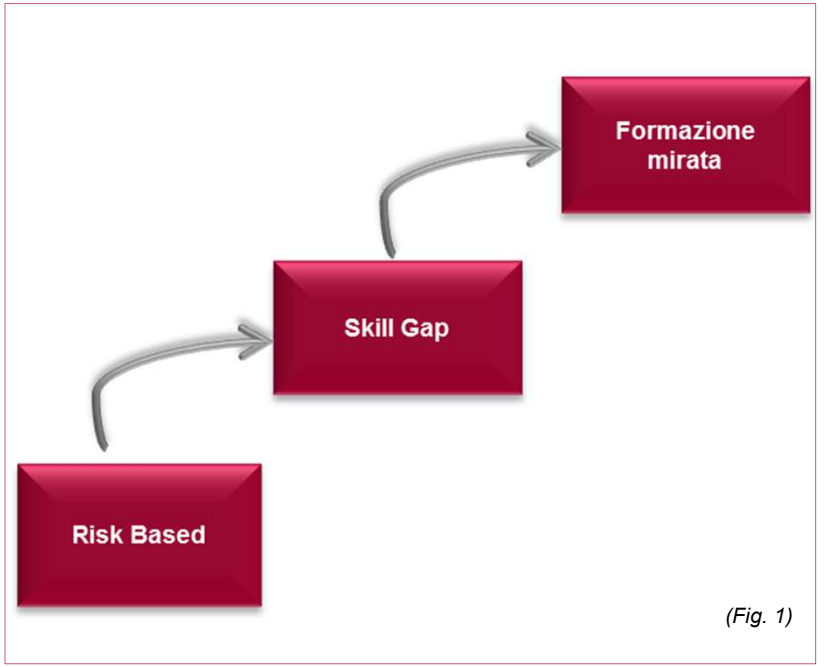
AULA	Nr. Persone	Durata (h)	% Fruizione	ONLINE	Nr. Persone	Durata (h)	% Fruizione
Neo-assunti: antiriciclaggio normativa e operatività bancaria (4 h)	30	120	100%	Antiriciclaggio normativa e operatività (2h)	644	1288	95%
Antiriciclaggio e contrasto al terrorismo - neo titolare di filiale (5)	32	160	100%	Antiriciclaggio normativa e operatività per i responsabili di filiale e centri (1h30)	234	351	93%
Antiriciclaggio e contrasto al terrorismo - corso per OdS (7h30)	1749	13118	95%	Antiriciclaggio normativa e operatività per i responsabili di Direzione DG (1h30)	268	402	87%
Antiriciclaggio normative e operatività rete (15h)	779	5843	99%	La IV Direttiva antiriciclaggio: adempimenti e responsabilità (Nuovo corso per DG - 2h)	384	768	17%
Antiricilaggio normative e operatività di rete (7h30)	40	600	100%	Online - Gianos 3D	437	437	65%
Antiriciclaggio follow up IV Direttiva (5h)	50	375	100%	Online antiriciclaggio: segnalazioni delle operazioni sospette nel settore assicurativo (1h)	1039	1039	99%
Kyc persone giuridiche (5h)	148	740	100%				
Antiriciclaggio e contrasto al finanziamento del terrorismo internazionale (3h)	25	125	100%				
Training e contrasto al finanziamento del terrorismo internazionale (3h)	88	264	90%				
Training on the Job (durata variabile)	24	481	100%				
Workshop "le nuove prospettive di contrasto al finanziamento del terrorismo" (3h)	50	150	100%				
	3.015	**21.976**			**3.006**	**4.285**	

Fonte: Servizio Knowledge Management e Formazione

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (9/12)*

Nel corso del 2018 l'attività di formazione, in ambiti particolarmente sensibili (antiriciclaggio/contrasto al terrorismo AML/CFT) si è evoluta introducendo una nuova metodologia risk-based strutturata su nuove logiche (cfr. fig. n. 1), sempre più orientate a creare un piano formativo efficace (diversificazione per ruoli e responsabilità) ed efficiente (tempi formativi limitati alle reali necessità), al fine di:

- concepire la formazione come uno dei presidi al rischio;
- prevedere attività proporzionate al rischio insito nel ruolo;
- garantire lo svolgimento di programmi permanenti di formazione finalizzati alla corretta applicazione AML-CFT, al riconoscimento di operazioni connesse al riciclaggio o al finanziamento del terrorismo e all'adozione di comportamenti e delle procedure per il rispetto della normativa.



(Fig. 1)

Coerentemente alla metodologia adottata, è stata prevista:

- la compilazione di un questionario specialistico in materia di contrasto al riciclaggio destinato a Titolari di Filiale e ai Responsabili dei Centri Specialistici (maggio 2018);
- un'offerta formativa flessibile, con **nuove edizioni in aula** per la rete al fine diffondere le novità derivanti dal recepimento della IV Direttiva Antiriciclaggio; nuovi **corsi on line, webinar, eventuali newsletter tematiche e/o pillole formative, community;**
- corsi in aula per Direttori di Filiale, in tale ambito sono previsti spazi dedicati al tema «Fraud Risk» e al «Rischio di Credito»;
- nuove edizioni dei corsi in aula a docenza interna altamente qualificata;
- percorso avanzato in house progettato con ABI Formazione per specialisti AML.

In sintesi l'attività formativa AML/CFT realizzata nel 1° Semestre 2018:

Formazione AML/CFT 1° semestre 2018

Interventi formativi AULA	Rete		DG/AT		Formazione on line	Rete		DG/AT	
	nr. Partecipanti	Ore	nr. Partecipanti	Ore		nr. Partecipanti	Ore	nr. Partecipanti	Ore
Titolare (7,5 h)	0	0	0	0	Online Resp. Filiale e Centri	26,00	39,00	6,00	9,00
Aula OdS (7,5h)	164	1.230	0	0	Online personale di Rete (2hh)	79,00	158,00	2,00	4,00
Neo Titolari (5h)	30	150			Online Resp. DG e funzioni specialistiche DG (2hh)	1,00	-	1.417,00	2.834,00
Formazione per Credito (Target: delib. Reperto High Risk; Delib. Erogazione; Prep. Rep. High Risk; Prep. Rep. Erogazione)	145	1.088	51	383	Online personale di Rete (5hh)	4,00	20,00	-	-
Incontri formativi	35	143,5	19	92,5	Antiriciclaggio:SOS nel settore assicurativo (1h)	20,00	20,00	-	-
Questionari orientamento (AML_CFT 2018 - 1,5h) per Tit. e Resp. Centri	1.935	2.902	2	3	Antiriciclaggio e terrorismo internazionale percorso personale di rete (3,5h)	2,00	7,00	1,00	1,00
					GIANOS 3D - modulo GPR (1h)	54,00	54,00	2,00	2,00
	2.309,00	**5.513,50**	**72,00**	**478,50**		**186,00**	**298,00**	**1.428,00**	**2.850,00**

Fonte: Servizio Knowledge Management e Formazione

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (10/12)*

Nell'ambito degli argomenti evidenziati dalle regole di condotta del Codice Etico, la funzione Compliance esegue, sistematicamente e con differenziata periodicità, accertamenti ex-ante e controlli ex-post avvalendosi, per questi ultimi, di una piattaforma dedicata (piattaforma compliance). I controlli ex ante si sostanziano in validazioni/pareri effettuati nel continuo difficilmente quantificabili (stimati circa 400 pareri nel 2017); mentre ex-post vengono svolte verifiche in materia di conformità a leggi, a regolamenti e alla normativa interna (cfr. all.to n. 1). Tale attività favorisce, nel contempo, la creazione di valore diretta a promuovere una cultura aziendale improntata a principi di correttezza, trasparenza e al rispetto sostanziale delle disposizioni vigenti. Utile inoltre a stimolare la formazione di presidi adeguati a identificare e controllare preventivamente i comportamenti in violazione di prescrizioni normative e di autoregolamentazione.

Di seguito uno schema riepilogativo delle principali verifiche eseguite dalla funzione per le materie correlate al tema in argomento.

	Compliance Plan 2017 - Piano Controlli			***Compliance Plan 2018 (fino al 30.06.18) - Piano Controlli***	
Nr.	**Materia**	**Periodicità**	**Nr.**	**Materia**	**Periodicità**
6	Antiusura	una tantum	18	Antiusura	trimestrale
2	Antiusura	trimestrale			
8	**Totale controlli antiusura**		**18**	**Totale controlli antiusura**	trimestrale
1	Trasparenza CIV	una tantum	2	Trasparenza -CIV	trimestrale
2	Trasparenza-informativa precontrattuale	una tantum	3	Trasparenza - informativa precontrattuale	trimestrale
1	Trasparenza reclami	annuale	1	Trasparenza e reclami	trimestrale
2	Trasparenza mutui	una tantum	1	Trasparenza - processi di vendita	trimestrale
16	Trasparenza -IRC	trimestrale			
1	Trasparenza - anatocismo	una tantum			
23	**Totale controlli trasparenza**		**7**	**Totale controlli trasparenza**	
1	Intermediazione assicurativa	semestrale	9	Intermediazione assicurativa	trimestrale
12	Intermediazione assicurativa	mensile			
13	**Totale controlli intermediazione assicurativa**		**9**	**Totale controlli intermediazione assicurativa**	
4	Privacy - IRC	trimestrale	1	Responsabilità sociale d'impresa	trimestrale
5	Privacy	una tantum	**1**	**Totale controlli responsabilità sociale d'impresa**	
4	Privacy	semestrale			trimestrale
13	**Totale controlli Privacy**				
1	Sistemi di pagamento	una tantum	1	Sistemi di pagamento	trimestrale
1	**Totale sistemi di pagamento**		**1**	**Totale sistemi di pagamento**	
1	Responsabilità amministrativa Enti	una tantum	2	Responsabilità amministrativa enti	trimestrale
1	**Totale responsabilità amministrativa Enti**		**2**	**Totale responsabilità amministrativa Enti**	
59	**Totale controlli codice etico**		**38**	**Totale controlli codice etico**	

Fonte: Funzione Compliance (Piattaforma Compliance)

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (11/12)*

OBIETTIVO

Assessment circa gli orientamenti sulla governance interna contenuti nel Titolo IV EBA/GL/2017/11 – Cultura del Rischio e Codice Etico_ Valori aziendali e Codice Etico.

PERIMETRO/ METODOLOGIA

Perimetro: BMPS

Metodologia:

» analisi della normativa interna ed esterna;
» interviste al personale delle strutture interessate;
» acquisizione evidenze documentali.

RISCHI IMPATTATI

Rischio di non conformità alle EBA GL.

RIFERIMENTO EBA GL

Linee Guida EBA GL/2017/11
Valori aziendali e codice etico

Art. 102. …. Gli enti dovrebbero definire la funzione responsabile del monitoraggio della conformità al codice etico o a uno strumento analogo e valutarne le violazioni, nonché un processo per gestire i casi di non conformità. L'organo di amministrazione dovrebbe essere informato periodicamente sul risultato.

ESITI

Al fine di un monitoraggio puntuale e compiuto in tema di conformità al codice etico, è stata condivisa con la funzione di Compliance l'opportunità di predisporre un «indice» in ordine ai temi/normative interessate trasversalmente dal citato Codice per una valutazione complessiva riferita a tutti gli ambiti interessati (*), da rappresentare in una sezione dedicata del tableau de bord. Tale elaborato, prodotto con cadenza trimestrale, fornisce una rappresentazione dettagliata dell'attività di controllo e di monitoraggio svolte dalla funzione, nonché degli esiti e delle relative azioni di mitigazione, negli ambiti interessati da accertamenti di conformità.

Il tableau de bord (TdB) viene predisposto in due distinti report in relazione al perimetro di riferimento (Capogruppo bancaria e Società controllate italiane/estere/filiali estere).

In particolare il TdB di Banca MPS riporta le seguenti informazioni:
1 il quadro sinottico del rischio residuo per area normativa; 2. la conformità dei macro-processi e delle linee di business di BMPS; 3. l'esposizione al rischio per area normativa; 4. consuntivo attività e controlli; 5. Gap di conformità; 6. perdite operative.

L'informativa viene fornita a tutte le funzioni apicali della banca. Dall'analisi del tableau de bord al 30.06.18 è evidente l'attenzione posta dalla funzione sui temi oggetto di recenti aggiornamenti normativi (ad es.: MiFID II) e sugli ambiti di «Governance societaria».

La Funzione Compliance, inoltre, unitamente ai controlli di conformità eseguiti periodicamente, svolge trimestralmente un monitoraggio sugli indicatori di rischio (IRC), in ambiti specifici, ad es.: i reclami.

(*) A titolo esemplificativo non esaustivo si forniscono gli ambiti interessati dal Codice Etico: 1.Antiriciclaggio e antiterrorismo, 2.conflitti di interessi, 3. contrasto all'usura, 4. diritti del lavoro, 5. distribuzione prodotti assicurativi non finanziari, 6. Finanza e mercati finanziari, 7. Gestione del risparmio, 8. Governance societaria, 9. Politiche retributive e incentivanti, 10. Salute e sicurezza sui luoghi di lavoro e tutela ambientale. 11. Servizi e prodotti di investimento, 12. Trasparenza servizi e prodotti bancari, 13.Trasparenza servizi e prodotti di finanziamento, 14. Trasparenza servizi e prodotti di pagamento, 15. Tutela dei dati personali (privacy).

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 - Valori aziendali e Codice Etico (12/12)*

OBIETTIVO

Assessment circa gli orientamenti sulla governance interna contenuti nel Titolo IV EBA/GL/2017/11 – Cultura del Rischio e Codice Etico_ Valori aziendali e Codice Etico.

PERIMETRO/ METODOLOGIA

Perimetro: BMPS

Metodologia:
- » analisi della normativa interna ed esterna;
- » interviste al personale delle strutture interessate;
- » acquisizione evidenze documentali.

RISCHI IMPATTATI

Rischio di non conformità alle EBA GL.

RIFERIMENTO EBA GL

ESITI

Per le nuove previsioni normative di fonte europea rappresentate da: Regolamento (UE) n. 1286/2014 (Regolamento PRIIPs), Direttiva (UE) 2016/97 «Insurance e Distribution Directive» (IDD) e Regolamento Delegato n. 653/2017 in tema di servizi di investimento, collocamento/distribuzione ed intermediazione di prodotti finanziari, adeguatamente declinate nella normativa interna (*), la Funzione Compliance, coinvolta in un GdL a presidio dell'operatività inerente, ha svolto specifiche attività di supporto e di verifica di conformità per quanto di seguito rappresentato:

- questionario Demand&Needs: individuati i requisiti affinché la procedura intercetti le esigenze della clientela e la indirizzi verso uno solo dei prodotti assicurativi attualmente a catalogo;
- POG: valutata la coerenza e la conformità dei documenti normativi interni emanati per adeguarsi al disposto normativo in tema di approvazione dei prodotti;
- DIP danni e altri documenti di trasparenza: validati i documenti informativi da consegnare/mettere a disposizione dei clienti, valutandone la conformità, chiarezza e esaustività;
- Responsabile della distribuzione assicurativa: è in corso la nomina di un «responsabile» dell'attività distributiva della Banca, che dovrà garantire il corretto svolgimento dell'attività di intermediazione assicurativa;
- polizze dormienti: verificata la possibilità di concedere al cliente il diritto di indicare in forma nominativa i beneficiari della polizza ed eventuale terzo diverso beneficiario.

Oltre le attività sopra descritte la Funzione Compliance ha provveduto ad implementare blocchi a sistema per evitare che colleghi non formati possano collocare polizze, disattendendo in tal modo il disposto normativo.

(*) D. 2234 «Collocamento delle polizze assicurative» - D. 2355 Direttiva di Gruppo in materia di distribuzione di prodotti assicurativi di protezione - D 1093 Prodotti di investimento assicurativo - D. 2262 Compendio Organizzativo MiFID II.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 – Procedure interne di segnalazione (1/2)*

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
Effettuare un assessment in relazione agli orientamenti sulla governance interna contenuti nel Titolo IV EBA/GL/2017/11 – Cultura del Rischio e Codice Etico.	Perimetro: BMPS Metodologia: » analisi della normativa interna ed esterna; » interviste al personale delle strutture interessate; » acquisizione evidenze documentali.	Rischio di non conformità

RIFERIMENTO EBA GL	ESITI
13 Procedure interne di segnalazione Art. 117 Adozione procedura, oggetto e documentazione segnalazione	La Banca ha attivato a partire dal 30/11/2015 un sistema interno di segnalazione delle violazioni (cd. Whistleblowing) alla luce della normativa italiana (art. 52 bis del TUB, Circ. 285 Banca d'Italia) che recepisce la normativa comunitaria. Il sistema ha valenza per le società italiane facenti parte del Gruppo. Circa l'attendibilità della segnalazione, la normativa esterna non prevede obblighi di documentazione in capo al segnalante, conformemente la Banca presuppone la sola buona fede del segnalante, precisando peraltro che una falsa segnalazione caratterizzata da comprovati elementi di dolo o colpa grave comporta conseguenze disciplinari.
Art. 118 Canale segnalazione e protezione dati soggetti coinvolti	La procedura definita dalla Banca e resa pubblica al suo interno (D.2064 e manuale M.182) specifica sia i destinatari ordinari delle segnalazioni (Funzione Antifrode all'interno della Funzione Audit) sia il destinatario (Collegio Sindacale) qualora oggetto della segnalazione sia personale coinvolto nella Funzione Antifrode stessa o diretti superiori. Il principio di protezione dei dati è espresso nella normativa interna, inoltre a maggior tutela l'identità del segnalante è «schermata» attraverso l'uso di credenziali fittizie mentre la conoscenza dei segnalati è ristretta ad un ridotto numero di soggetti abilitati a lavorare le segnalazioni (n. 8 in fase di impianto incluso Collegio Sindacale).
Art. 119 Accessibilità procedura	La procedura è inserita all'interno della intranet aziendale, accessibile pertanto a ciascun soggetto dotato di abilitazione. Sono abilitati anche gli esterni (es. tecnici/consulenti/promotori) ai quali sia stata conferita abilitazione ad accedere alla intranet aziendale. L'attribuzione di tale abilitazione è «prova» di un inserimento «in pianta stabile» del singolo all'interno dell'organizzazione aziendale tale da risultare conforme alla definizione di «personale» richiesta dalla normativa esterna, che non si esaurisce nel perimetro dei soggetti con rapporto di lavoro subordinato, ma contempla ogni forma di rapporto che determina l'inserimento all'interno dell'organizzazione aziendale.
Art. 120 Escalation ai vertici	La normativa interna, in coerenza con la normativa di vigilanza, prevede che il Responsabile della procedura riferisca "direttamente e senza indugio agli organi aziendali le informazioni oggetto di segnalazione, ove rilevanti". La possibilità di segnalare in forma anonima è stata esclusa in sede di definizione della procedura, che è accedibile solo previo riconoscimento del soggetto all'interno della intranet aziendale. L'identità del segnalante è comunque «schermata» dalla generazione di credenziali automatiche da parte della procedura: la possibilità di risalire al nominativo ove richiesto ad esempio dalla magistratura sussiste ma non è in autonomia (tecnica ed autorizzativa) della Funzione Antifrode. Circa la messa a disposizione delle informazioni ai vertici, accanto alla facoltà del Responsabile della procedura di comunicare direttamente ai vertici eventuali casistiche eccezionali, il Collegio Sindacale mantiene piena visibilità di ciascuna segnalazione pervenuta in procedura. La Funzione redige inoltre una relazione annuale, accessibile a tutto il personale come richiesto dalla normativa italiana.

2 Attività svolta: *Assessment Tit. IV EBA GL/2017/11 – Procedure interne di segnalazione (2/2)*

RIFERIMENTO EBA GL	ESITI
Art. 121 Tutela segnalante	La normativa interna prevede e specifica il principio previsto dalla GL EBA. Dal punto di vista pratico la tutela è garantita dalla riservatezza del nominativo del segnalante, di fatto ignoto alla struttura di indagine. Ulteriore garanzia è data dalla prassi della Funzione Antifrode di non rivelare, in caso di deferimento alla Commissione Affari Disciplinari, che l'indagine scaturisce da una segnalazione Whistleblowing: dato che i casi sono esposti basandosi su prove documentali, la presenza o meno di una segnalazione all'origine è ininfluente per la valutazione del caso.
Art. 122 Tutela segnalato	La normativa interna prevede e specifica il principio previsto dalla GL EBA, evidenziando peraltro gli esiti in cui incorre colui che effettua una segnalazione dolosamente, con effetti diffamatori. Solo a fronte di evidenze concrete sono presi provvedimenti, peraltro comunicando al segnalato l'avvio di un procedimento disciplinare. Qualora non emergano evidenze, constatata la buona fede del segnalante, la segnalazione viene archiviata. Ad ulteriore garanzia di riservatezza e tutela del nominativo segnalato, il numero dei soggetti che possono visionare le segnalazioni in corso è strettamente limitato.
Art. 123 Sintesi caratteristiche procedura	La procedura risulta documentata, come richiesto dalle Linee Guida: accanto ai documenti normativi pubblicati sono presenti documentazioni interne alla Funzione Audit contenenti ulteriori dettagli relativi alle prassi operative generalmente utilizzate dalla Funzione Antifrode. Le garanzie sulla riservatezza della segnalazione e delle persone coinvolte sono presenti, in particolare la tutela del segnalante da atti di vittimizzazione è garantita dalla normativa e dalla prassi di non divulgare le motivazioni di avvio indagine neanche in caso di avvio di procedimenti disciplinari. Le segnalazioni sono rendicontate annualmente, inoltre il Collegio Sindacale ha accesso diretto alla procedura di segnalazione, con visibilità sia delle pratiche che coinvolgono il personale della Funzione Antifrode ed i loro diretti superiori (per le quali ha compiti di indagine), sia delle pratiche curate dalla Funzione Antifrode, a scopo informativo. La procedura prevede la comunicazione al segnalante sia della presa in carico della segnalazione sia della conclusione delle verifiche (ma non degli esiti delle stesse): ciò ovviamente qualora il segnalante acceda in un secondo tempo alla procedura con le proprie credenziali fittizie. Le segnalazioni ricevute, sono registrate in ordine progressivo e conservate. In assenza di indicazioni più specifiche sulle tempistiche di conservazione, si applicano i criteri di conservazione previsti per le indagini ordinarie della Funzione Antifrode (fino a 10 anni di conservazione su archivi separati a disposizione di eventuali richieste della magistratura, salvo procedimenti penali in corso).

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Quadro e meccanismi di controllo interno (1/4)*

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
Effettuare un assessment in relazione agli orientamenti sulla governance interna contenuti nel Titolo V EBA/GL/2017/11 - Quadro e meccanismi di controllo interno	Perimetro: BMPS Metodologia: » analisi della normativa interna ed esterna; » interviste al personale delle strutture interessate; » acquisizione evidenze documentali.	Rischio di non conformità alle EBA GL.

RIFERIMENTO EBA GL

15 Quadro di controllo interno
16 Attuazione di un quadro di controllo interno

Art. da 126 a 135 EBA GL

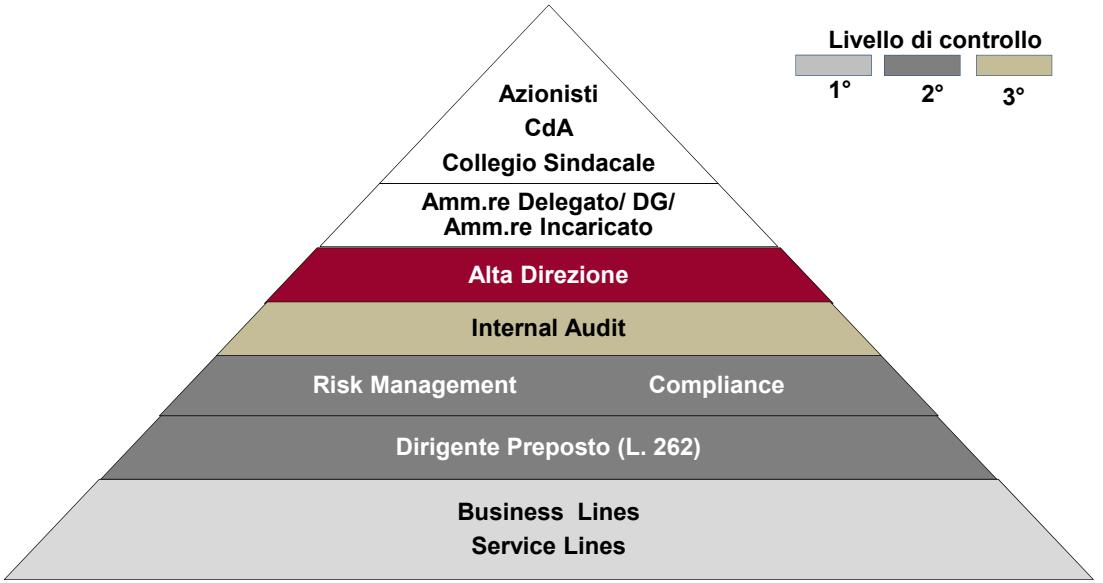
Cfr. Doc normativo D.793

ESITI

Il Sistema dei Controlli Interni (di seguito anche SCI) adottato dal Gruppo MPS è costituito dall'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure volte ad assicurare la sana e prudente gestione. Il SCI riveste un ruolo centrale nell'organizzazione aziendale, ovvero:

- rappresenta un elemento fondamentale di conoscenza per gli organi aziendali in modo da garantire piena consapevolezza della situazione ed efficace presidio dei rischi aziendali e delle loro interrelazioni;
- orienta i mutamenti delle linee strategiche e delle politiche aziendali e consente di adattare in modo coerente il contesto organizzativo;
- presidia la funzionalità dei sistemi gestionali e il rispetto degli istituti di vigilanza prudenziale;
- favorisce la diffusione di una corretta cultura dei rischi, della legalità e dei valori aziendali.

In sintesi, si riporta una rappresentazione grafica delle principali componenti del SCI:



2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Quadro e meccanismi di controllo interno (2/4)*

RIFERIMENTO EBA GL	ESITI
	Per tali caratteristiche, il SCI assume un ruolo strategico per il Gruppo e la cultura del controllo assume una posizione di rilievo nella scala dei valori aziendali, coinvolgendo tutta l'organizzazione aziendale (organi aziendali, strutture, livelli gerarchici, personale) nello sviluppo e nell'applicazione di metodi, logici e sistematici, per identificare, misurare, comunicare e gestire i rischi. Il CdA della Capogruppo approva la costituzione delle Funzioni Aziendali di Controllo (Compliance, Risk Management, Internal Audit, Convalida, Antiriciclaggio), i relativi compiti e responsabilità, le modalità di coordinamento, i flussi informativi tra tali Funzioni e tra queste e gli Organi Aziendali. Per supportare il concreto espletamento di tali compiti all'interno del CdA sono costituiti specifici Comitati con funzione di supporto. Al fine di favorire la diffusione di una cultura interna dei controlli, il CdA approva, inoltre, un codice etico – cui sono tenuti a uniformarsi i componenti degli organi aziendali e i dipendenti - che definisce i princìpi di condotta a cui deve essere improntata l'attività aziendale (per dettagli si rinvia all'apposita sezione del Rapporto sul Codice Etico). Nell'attuale configurazione del SCI, l'Amministratore Delegato (e Direttore Generale) è stato nominato anche Amministratore Incaricato del Sistema di Controllo Interno e di Gestione dei Rischi previsto dal Codice di Autodisciplina di Borsa Italiana. Tale soluzione ad oggi in essere nel Gruppo MPS è anche quella più diffusa tra i player bancari quotati che hanno aderito al suddetto Codice di Autodisciplina. Gli ambiti di miglioramento rilevati, in un'ottica di gestione integrata dei rischi, sono portati a conoscenza delle funzioni con compiti di controllo in relazione agli specifici ambiti di competenza anche per il tramite di meccanismi di coordinamento e di condivisione tra le stesse. Inoltre, sono oggetto di sistematico *follow up.* Risultano, inoltre, in progressivo miglioramento le relazioni tra Funzioni di Controllo e Funzioni Owner, al fine di individuare tempo per tempo tutte le possibili contromisure per assicurare la compiuta realizzazione delle attività di mitigazione dei gap entro le scadenze fissate I controlli sono presenti in maniera diffusa all'interno di ogni processo aziendale e livello gerarchico e coinvolgono, pertanto, tutte le Funzioni Aziendali. Sono normati, inoltre, gli aspetti attinenti ai flussi informativi e ai rapporti interfunzionali in ottica di gestione integrata delle informazioni finalizzata a promuovere la piena valorizzazione dei diversi livelli di responsabilità all'interno dell'organizzazione aziendale, con particolare attenzione al reporting per l'Alta Direzione e gli Organi Aziendali, al fine di favorire i processi decisionali e di governo. Infine, si evidenzia come il Gruppo è impegnato nel continuo ad implementare le azioni di mitigazione contenute nei piani annuali delle Funzioni di Controllo di Capogruppo approvati dal CdA (Risk Plan, Compliance Plan, AML Plan, Validation Plan, Internal Audit Plan), allo scopo di migliorare i processi e le metodologie di gestione dei rischi, mitigare le perdite operative e rischi di «condotta» diffondendo la cultura dei controlli e rafforzando la reputazione complessiva.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Quadro e meccanismi di controllo interno (3/4)*

RIFERIMENTO EBA GL	ESITI
17 Quadro di gestione dei rischi Art. da 136 a 146 EBA GL	Il Governo dei Rischi (o Risk Governance) è la componente della più generale Corporate Governance finalizzata ad una corretta definizione e gestione dei rischi. Per rafforzare la Risk Governance del Gruppo è fondamentale il ruolo dell'organo con funzione di supervisione strategica (Consiglio di Amministrazione e del Comitato Rischi endoconsiliare della Capogruppo) al fine di garantire il massimo coinvolgimento nella valutazione e nella promozione di una forte cultura del rischio all'interno di tutte le funzioni, stabilire e monitorare correttamente la propensione al rischio e la sua trasmissione all'organizzazione, attraverso una chiara e completa dichiarazione di propensione al rischio (RAS, Risk Appetite Statement). Il Governo dei Rischi del Gruppo MPS si estrinseca nell'adozione e applicazione di sani e saldi principi al fine di garantire che l'assunzione dei rischi sia in linea con la capacità dell'istituto di assorbire le perdite e sostenere la sua redditività di lungo periodo; coinvolge in modo specifico il Consiglio di Amministrazione, il Top Management, le funzioni di gestione e controllo del rischio e le attività di integrazione e raccolta delle informazioni di rischio (Risk Data Aggregation e Reporting) a supporto del processo decisionale del management. Il modello è basato sui seguenti principi guida: • responsabilità degli Organi Aziendali e dell'Alta Direzione (senior management) della Capogruppo e delle Controllate nella definizione, implementazione e supervisione dei sistemi di governo e gestione del rischio e di controllo interno; • indipendenza dei controlli, con chiara separazione delle responsabilità ed eliminazione/minimizzazione dei conflitti d'interesse tra funzioni aziendali di controllo e funzioni di business; • chiara attribuzione delle responsabilità a tutti i livelli organizzativi, mirata ad una corretta implementazione e presidio del sistema di governo dei rischi ("pervasività" della cultura del rischio e dei controlli) ed alla minimizzazione delle sovrapposizioni e inefficienze organizzative; • pervasività dei principi che ispirano tutte le componenti del sistema dei controlli interni e di gestione dei rischi. Nel corso del 2017 la Banca MPS ha svolto, in collaborazione con KPMG e con il coordinamento della Funzione di Internal Audit, un assessment sul Framework del Risk Management. Lo scopo della valutazione è stato quello di mappare il quadro di gestione del rischio in relazione ai vari requisiti normativi, le aspettative dei Supervisor e le best practice di mercato, anche in linea con la metodologia SREP. I risultati dell'attività svolta hanno dimostrato un ampio livello di conformità con i requisiti normativi del Risk Internal Governance e del Risk Management Framework e Culture, pur con alcuni ambiti di miglioramento, parte dei quali sono stati completati nel tempo (ad es. aggiornamento policy di rischio, formalizzazione doppio riporto – gerarchico e funzionale, del CRO, miglioramento del processo di gestione dei limiti in ambito RAF); ad oggi risultano da completare le azioni programmate per rafforzare il processo per la governance dei dati e delle informazioni in termini di mappatura delle metriche di rischio nonché quello di definizione delle linee guida di produzione di reporting sui rischi. Più in particolare, a gennaio 2018 è stata approvata dal CdA, e pubblicata in normativa interna, la nuova Direttiva di Gruppo in materia di Integrated Risk Reporting (D.02291) che definisce ruoli, responsabilità e processi, oltre a fornire una mappatura dei principali flussi di reporting in materia di Risk Management diretti agli Organi di vertice e al Senior Management. (Per dettagli sui flussi informativi si rimanda alle slide successive dedicate al Risk Management).

2 **Attività svolta:** *Assessment Tit. V EBA GL/2017/11 – Quadro e meccanismi di controllo interno (4/4)*

RIFERIMENTO EBA GL	ESITI
	Inoltre, sempre nel corso del 2018 è stato avviato un progetto molto ampio di natura pluriennale (Perdar Risk 2018) per aderire ai principi generali BCBS239 in materia di Risk Data Aggregation e Risk Reporting(*). Inizialmente, la Banca ha deciso di applicare i principi BCBS239 nell'ambito esclusivo della Funzione Risk Management e nello specifico partendo dalle attività di Risk Reporting (in particolare due principali report prodotti dalla funzione RM) e con un approccio dichiaratamente di «minimum compliance», essendo tuttavia chiaro che i principi del BCBS239 sono riferiti a tutte le funzioni/dati della Banca e con uno *scope* molto più ampio. Pertanto, in futuro potrebbe essere opportuno valutare possibili evoluzioni progettuali di più ampio respiro nel quadro della Data Governance e di implementazione della Data Strategy del Gruppo. I principali flussi informativi interni in tema di risk management diretti agli Organi di Vertice ed al Senior Management sono formalizzati all'interno del D.2291, riportati sinteticamente nell'Allegato 3. Al riguardo è in corso l'aggiornamento del D.1915 «Flussi informativi» che disciplina il dettaglio dei flussi informativi scambiati tra le funzioni/organi con compiti di controllo e tra queste/i e gli organi aziendali; tale documento è stato oggetto di un ampio processo di revisione nel corso dell'ultimo anno. Gli esiti di tale riesame hanno portato all'integrazione della normativa con l'aggiunta dei flussi informativi che interessano la Funzione Antiriciclaggio, la funzione Risorse Umane, Salute e sicurezza nei luoghi di lavoro e Pianificazione; nonché gli aggiornamenti della nuova regolamentazione sulla GDPR (*General Data Protection Rule*). Il documento è stato altresì analizzato anche dal Comitato di Coordinamento delle Funzioni di Controllo (in vista della pubblicazione) ed è stato reso fruibile alle Funzioni interessate appostandolo su un Team site dedicato. Gli aggiornamenti sono in corso di completamento con l'obiettivo di finalizzare ad inizio 2019.

(*) I principi BCBS239 del Comitato di Basilea forniscono indicazioni utili in tema di risk data aggregation e reporting, tecniche analitiche, Data Management e Visual Analytics per aggregare le componenti di rischio, identificare le concentrazioni significative e innovare il processo di governance.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzioni di controllo interno (1/3)*

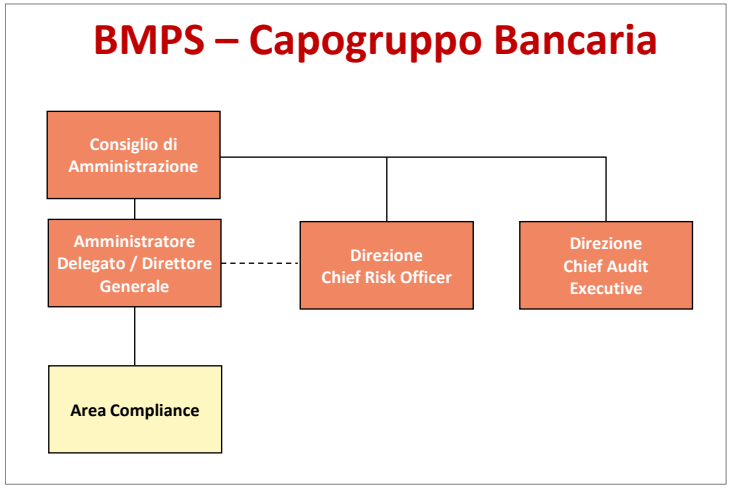
RIFERIMENTO EBA GL	ESITI
19 Funzioni di controllo interno. 19.1 Responsabili delle funzioni di controllo interno 19.2 Indipendenza delle funzioni di controllo interno	Il D.793 prevede, conformemente alle linee guida EBA oggetto di revisione, l'istituzione di cinque Funzioni Aziendali di Controllo permanenti ed indipendenti: - Funzione di conformità alle norme (compliance); - Funzione di controllo dei rischi; - Funzione di convalida interna; - Funzione antiriciclaggio; - Funzione di revisione interna. Le prime quattro attengono ai controlli di secondo livello, la Revisione Interna ai controlli di terzo livello. In tale sede è stato oggetto di disamina le Funzione di conformità alle norme, la funzione di controllo dei rischi e la funzione di revisione interna. Per assicurare il corretto svolgimento dell'attività svolta dalle Funzioni aziendali di controllo, il Gruppo MPS ha definito i seguenti requisiti essenziali da rispettare, valevoli per ciascuna funzione.
Art. 153 e 157 EBA GL	**Nomina e Revoca dei Responsabili** I Responsabili delle funzioni aziendali di controllo – dotati di requisiti di professionalità adeguati – sono nominati e revocati con apposita delibera, motivandone le ragioni, dal Consiglio di Amministrazione, sentito il Collegio Sindacale. In particolare, la nomina/revoca dei Responsabili delle Funzioni Aziendali di Controllo della Capogruppo prevede che gli stessi siano individuati e proposti al CdA dal Comitato Rischi, avvalendosi del contributo del Comitato Nomine. Nello specifico, gli attuali responsabili delle funzioni aziendali di controllo oggetto della presente revisione sono:

Funzione di controllo	Responsabile	Decorrenza incarico
Compliance	Ettore Carneade	01 ottobre 2018
Risk Management	Leonardo Bellucci	13 marzo 2018
Internal Audit	Pierfrancesco Cocco	15 novembre 2016

Art. 154 EBA GL	Si evidenzia che nell'organizzazione dell'attuale Sistema dei controlli interni non sono ad oggi previste funzioni aziendali di controllo esternalizzate per la Banca.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzioni di controllo interno (2/3)*

RIFERIMENTO EBA GL	ESITI
Art. 155, 156 e 158 EBA GL	**Indipendenza e autorevolezza** I Responsabili delle Funzioni Aziendali di Controllo sono collocati in posizioni gerarchico-funzionali adeguate e non hanno responsabilità diretta di aree operative sottoposte a controllo né sono gerarchicamente subordinati ai responsabili di tali aree. In particolare, come recita il D.793 e riportato nella figura a lato: - Il Responsabile della Funzione di Revisione Interna collocato alle dirette dipendenze dell'organo con funzione di supervisione strategica; - Il Responsabile della Funzione di Controllo dei Rischi riporta gerarchicamente all'organo con funzione di supervisione strategica e funzionalmente all'Organo con funzione di gestione; - Il Responsabile della Funzione di Conformità alle Norme è collocato alle dirette dipendenze dell'Organo con funzione di gestione. I responsabili delle funzioni aziendali di controllo riferiscono direttamente agli organi aziendali ed hanno accesso diretto al CdA, al Collegio Sindacale e al Comitato Rischi comunicando con essi nel continuo senza restrizioni e intermediazioni. Graficamente l'organigramma aziendale è così rappresentato:



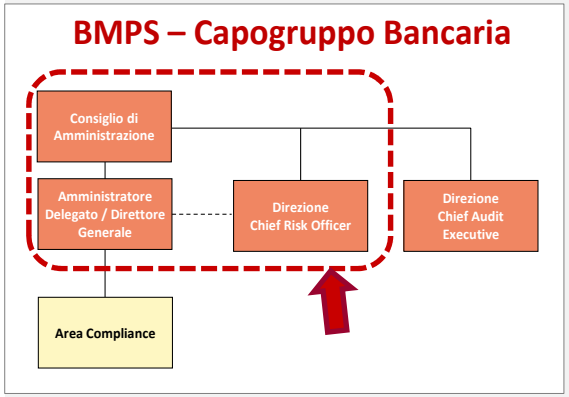
In ordine a tale requisito, dal paragrafo 158 delle linee guida EBA si evince, tra l'altro. che «fatta salva la responsabilità generale dei membri dell'organo di amministrazione per l'ente, il responsabile di una funzione di controllo interno non dovrebbe essere subordinato a una persona responsabile di gestire le attività che la funzione di controllo interno monitora e controlla» (punto c). Al riguardo, fatta salva la conformità del modello di governance della Banca agli orientamenti EBA e Bankit, la funzione di compliance ha richiesto, nel corso delle attività di impact analisys, un approfondimento sul proprio posizionamento, ipotizzando una possibile evoluzione del modello attuale prevedendo il proprio riporto all'Organo con Funzione di Supervisione strategica. Si rimanda alle slide successive per le considerazioni sulla Funzione Compliance.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzioni di controllo interno (3/3)*

RIFERIMENTO EBA GL	ESITI
	Separatezza funzionale L'obiettività e l'indipendenza delle Funzioni Aziendali di Controllo sono garantite da una segregazione organizzativa delle stesse; la relativa declinazione trova formalizzazione nei singoli Regolamenti Aziendali. Il personale che partecipa alle Funzioni Aziendali di Controllo non è coinvolto in attività che sono chiamate a controllare e, pertanto, qualora partecipi a Comitati di Gestione, la Funzione Aziendale di Controllo è senza diritto di voto per le materie in contrasto con detto principio. In merito al funzionamento dei Comitati di gestione si rimanda alle slide successive di approfondimento. **Sistemi di remunerazione e incentivazione** Al fine di non compromettere l'obiettività e l'indipendenza, gli assetti retributivi dei Responsabili delle Funzioni Aziendali di Controllo della Capogruppo sono deliberati dal Consiglio di Amministrazione su proposta del Comitato Remunerazione, che acquisisce preventivamente il parere del Comitato Rischi; per gli aspetti retributivi del Responsabile della Funzione di Revisione interna è altresì chiamato ad esprimere un parere il Collegio Sindacale. Gli assetti retributivi dei Responsabili delle strutture fino al 2° livello organizzativo delle Funzioni Aziendali di Controllo sono deliberati dal Consiglio di Amministrazione su proposta del Comitato Remunerazione.
19.3 Combinazione delle funzioni di controllo interno Art. 159 EBA GL	Le EBA GL prevedono che, pur tenendo conto dei criteri di proporzionalità enunciati al titolo I, la funzione di gestione dei rischi e la funzione di conformità possono essere combinate. La funzione di audit interno non dovrebbe essere combinata con un'altra funzione di controllo interno. Tale fattispecie di combinazione tra le funzioni di controllo non è stata adottata da parte della Banca MPS.
19.4 Risorse delle funzioni di controllo interno Art. 160 EBA GL	Il D.793 prevede che le funzioni di controllo dispongono dell'autorità, delle risorse e delle competenze necessarie per lo svolgimento dei loro compiti. A tal fine viene periodicamente valutata l'adeguatezza quali-quantitativa delle risorse affinché le Funzioni Aziendali di Controllo dispongano di personale adeguato per numero, competenze tecnico-professionali e aggiornamento, anche attraverso l'inserimento di programmi di formazione specialistici nel continuo. Con riferimento alla Funzione RM, è stata visionata la proposta di riorganizzazione dell'assetto dell'Area Risk Management e dell'Area Validazione, Monitoraggio e Risk Reporting, e la conseguente delibera assunta dall'Amministratore delegato, con approvazione delle esigenze e degli impatti di tale riorganizzazione. Al fine di garantire la formazione di competenze trasversali e di acquisire una visione complessiva e integrata dell'attività di controllo svolta, sono incentivati programmi di rotazione delle risorse tra le funzioni di controllo. Sono state verificate le composizioni degli organici e le capacità professionali (anche in ambito formativo) delle principali funzioni di controllo interno. Si rimanda alle slide successive.
Art. 161 EBA GL	**Accesso alle informazioni aziendali** Alle Funzioni Aziendali di Controllo è consentito di avere accesso nel continuo ai dati aziendali e a quelli esterni (eventualmente richiesti *on demand*) necessari per svolgere in modo appropriato i propri compiti. Il Responsabile della Funzione di Revisione Interna ha accesso, su richiesta e correlata a specifiche attività, agli atti del CdA e degli Organi di Controllo.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Risk Management (1/8)*

RIFERIMENTO EBA GL	ESITI
20 Funzione di gestione dei rischi (Risk Management Function) Art. 162 EBA GL	**Istituzione funzione Risk Management** La Funzione aziendale di Controllo dei Rischi (Funzione Risk Management) prevista e disciplinata dalla normativa di Vigilanza, all'interno del Gruppo Montepaschi è svolta dalla Direzione Chief Risk Officer (CRO) della Capogruppo Banca MPS. Di seguito le Principali Responsabilità della funzione RM: - Sviluppo e implementazione del quadro di Governo dei Rischi del Gruppo che comprenda anche la promozione e diffusione di una solida cultura del rischio, la definizione della propensione al rischio e la fissazione dei limiti operativi; - Identificazione, modellizzazione, misurazione, monitoraggio e mitigazione dei singoli rischi, attuali e prospettici, oltre che la loro aggregazione; - Partecipazione alla definizione del RAF e monitoraggio nel continuo del profilo di rischio al fine di verificarne la coerenza con il Risk Appetite e i limiti operativi approvati dal CdA, corrispondenti alle esigenze di capitale e di liquidità. Il ruolo, le responsabilità, l'articolazione ed i compiti sono definiti dal Regolamento n.1. (Cfr. par. 163,164 EBA GL) **Posizionamento gerarchico e Riporto Funzionale** La Direzione Chief Risk Officer della Capogruppo - a riporto gerarchico del Consiglio di Amministrazione e funzionale dell'Amministratore Delegato - si articola nelle seguenti strutture organizzative: ✓ Segreteria Tecnica Chief Risk Officer, ✓ Staff Regulatory Relationship, ✓ Servizio AML-CFT, ✓ Servizio Validazione Sistemi di Rischio, ✓ Area Financial Risk Officer, ✓ Area Lending Risk Officer, ✓ Area Operating Risk Officer Il riporto gerarchico al Consiglio di Amministrazione garantisce la necessaria indipendenza e l'immediata possibilità di escalation da parte del Responsabile della Direzione Chief Risk Officer. Il riporto funzionale nei confronti dell'Amministratore Delegato si realizza prevedendo che il Responsabile della Direzione Chief Risk Officer si rapporti a quest'ultimo organo nell'attuazione delle seguenti macro-responsabilità: – la definizione, trasmissione e monitoraggio degli indirizzi programmatici e strategici di gestione dei rischi per la Capogruppo e le Società controllate del Gruppo; – la definizione del framework dei rischi, il monitoraggio della corretta attuazione delle strategie, delle politiche di governo del rischio e del RAF mediante definizione e analisi di indicatori specifici, nonché reporting sul superamento delle soglie di tolleranza del rischio stabilite; – la rendicontazione periodica delle attività in materia di gestione e controllo dei rischi di Gruppo.



2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Risk Management (2/8)*

RIFERIMENTO EBA GL	ESITI
Art. 165 EBA GL	Il personale all'interno della funzione di gestione dei rischi possiede conoscenze, competenze ed esperienza sufficienti riguardo alle tecniche e alle procedure di gestione dei rischi, nonché ai mercati e ai prodotti, e ha accesso a regolari formazioni. Nell'ambito delle revisioni svolte sulla funzione vengono puntualmente valutate le competenze, anche in termini di anzianità di servizio ed esperienza sul ruolo, e l'aggiornamento in ambito formativo del personale impiegato in ciascun settore. Sono stati acquisite le evidenze degli ultimi interventi svolti nel corso dell'Audit Plan 2018. Gli esiti delle verifiche consentono di concludere che la composizione degli organici e l'anzianità nel ruolo delle risorse appartenenti alle strutture della Direzione CRO non presentano criticità. Le risorse hanno una chiara conoscenza e comprensione della cultura del rischio e la piena consapevolezza delle normative vigenti e delle prassi operative adottate L'analisi dell'elenco dei corsi frequentati dai componenti delle strutture evidenzia che tutte le risorse hanno ricevuto una adeguata formazione specifica in materia di Risk Management. In sintesi:
Art. 166 EBA GL	La funzione di gestione dei rischi interagisce con le funzioni di business, anche con l'obiettivo di responsabilizzazione rispetto alla gestione dei rischi presso tutto il personale. Dagli incontri intercorsi con Il responsabile Area Financial Risk Officer, nell'approccio della funzione RM con le linee di business operative sono previsti momenti di condivisione e formazione atte a trasferire la cultura del rischio con approccio di tipo top down: i vari responsabili della Direzione RM effettuano incontri e corsi formativi verso le linee di business (corsi effettuati a livello di Chief, ma anche di responsabili di Area). Momenti formativi vengono svolti anche con le strutture delle società controllate. Per maggiori dettagli sulle considerazioni in merito alla cultura del rischio si rimanda alle slide precedenti. Nel corso della predetta riunione abbiamo avuto conferma che il CRO partecipa con regolarità alle riunioni del Comitato Rischi, riceve osservazioni nonché richieste specifiche di informativa/approfondimenti.

Servizio/Settore analizzato*	Competenze	Anzianità servizio
SERVIZIO INTEGRAZIONE RISCHI E REPORTING *Settore Integrazione Rischi*	✔ Valutazione positiva	✔ Valutazione positiva
SERVIZIO RISCHI DI LIQUIDITÀ E ALM *Settore Rischi di Liquidità* *Settore Rischi ALM*	✔ Valutazione positiva	✔ Valutazione positiva
SERVIZIO VALIDAZIONE SISTEMI DI RISCHIO *Settore Validazione Sistemi di Rischio Gestionali*	✔ Valutazione positiva	✔ Valutazione positiva

*In tabella sono riportati i Settori/Servizi auditati dal la DCAE nel corso del 2018.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Risk Management (3/8)*

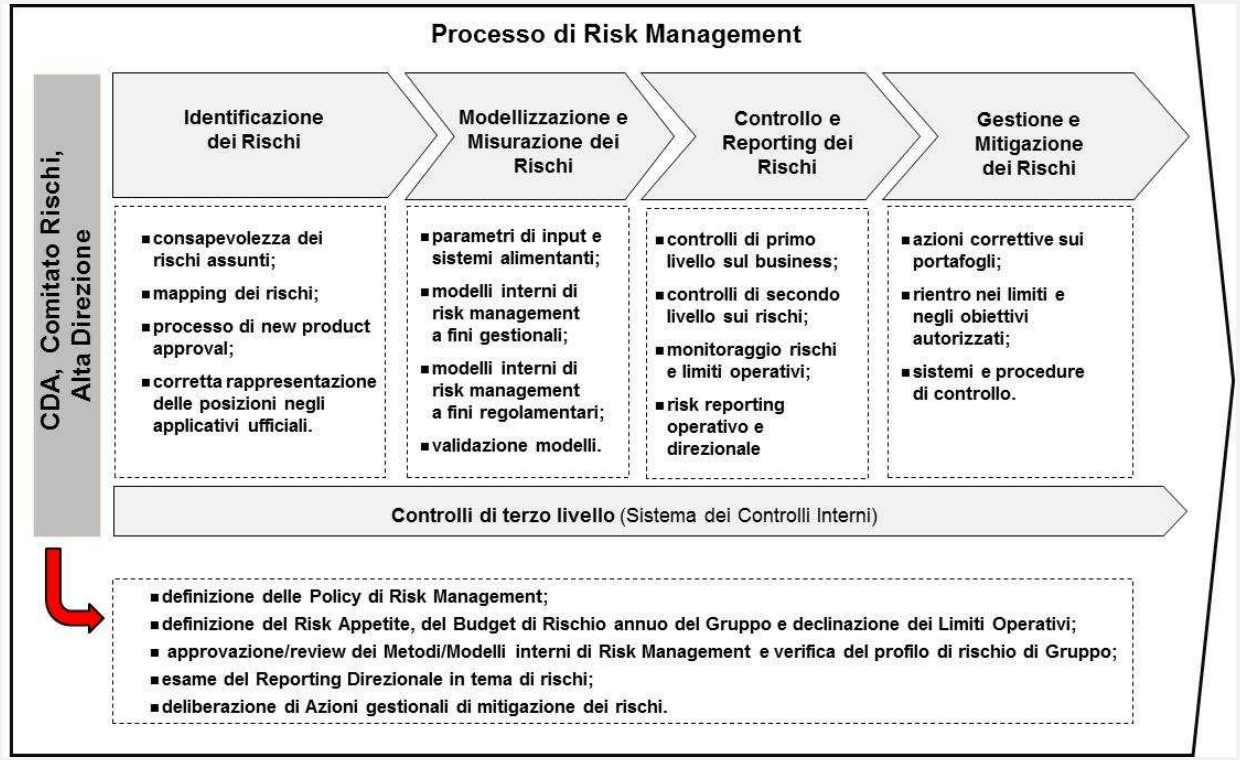
RIFERIMENTO EBA GL	ESITI
Art. 167, 168 EBA GL	Banca MPS ha previsto l'istituzione di una funzione di gestione dei rischi centrale, che si suddivide gerarchicamente in vari settori per competenza, al fine di fornire una visione complessiva di tutti i rischi a livello di ente e di gruppo e garantire che venga rispettata la strategia in materia di rischio. Le strutture organizzative della Direzione CRO, oltre al Responsabile, sono state ristrutturate nel corso del 2017 costituendo tre Aree specifiche in modo da essere partner delle rispettive aree di interesse o di business, e in modo da separare nettamente le strutture che svolgono la funzione di validazione interna dei modelli di rischio e la funzione antiriciclaggio che sono poste a diretto riporto del CRO. Si rimanda all'Allegato 2 per l'organigramma della Direzione CRO. Il modello di Risk Management adottato dal Gruppo Montepaschi è di tipo «Misto» (accentrato per alcune componenti e decentrato per altre, ma sempre infragruppo: si evidenzia che per MPS Banque è in corso la procedura di liquidazione mentre per MPS Belgio è in corso la cessione). Tali società hanno una Funzione di Controllo dei Rischi locale con un Responsabile, che agisce in autonomia pur nel rispetto delle regole di Gruppo a cui tutte le controllate sono assoggettate.
Art. 169 EBA GL	Le linee guida EBA prevedono al par.169 che: «*La funzione di gestione dei rischi dovrebbe fornire informazioni, analisi e pareri di specialisti sull'esposizione ai rischi pertinenti e indipendenti, e consulenza su proposte e decisioni in materia di rischi adottate dalle linee di business o dalle unità interne. Dovrebbe inoltre segnalare all'organo di amministrazione se queste siano conformi alla propensione al rischio e alla strategia in materia di rischio dell'ente. La funzione di gestione dei rischi può raccomandare l'apporto di miglioramenti al quadro di gestione dei rischi e misure correttive per porre rimedio a violazioni delle politiche, delle procedure e dei limiti operativi in materia di rischi*». Al riguardo, il Gruppo MPS prevede che la Funzione Risk Management abbia la responsabilità circa: - lo sviluppo di un sistema di *early warning* o *triggers* per la violazione del Risk Appetite e/o dei limiti operativi; - la valutazione e l'eventuale condizionamento ex-ante della realizzazione delle operazioni che sono in grado di modificare in maniera sensibile il profilo di rischio del Gruppo; - la valutazione dei rischi derivanti dall'introduzione di nuovi prodotti e servizi o l'avvio di nuove attività e di quelli derivanti dall'ingresso in nuovi segmenti operativi e di mercato e la coerenza di questi con la propensione al rischio; - la predisposizione del risk reporting direzionale per il senior management e gli Organi Aziendali, includendo eventuali proposte di mitigazione dei rischi (Cfr. slide successive).

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Risk Management (4/8)*

RIFERIMENTO EBA GL	ESITI
20.1 Ruolo della funzione di gestione dei rischi nella strategia e nelle decisioni in materia di rischio Art. 170, 171 EBA GL	Il Responsabile della Funzione di Controllo dei Rischi (CRO) supporta il CdA nella supervisione e sviluppo del Risk Appetite Statement (RAS) e nella traduzione del risk appetite in una struttura di limiti operativi. Il CRO insieme al Senior management concorre alla formazione del processo decisionale di Gruppo (pianificazione strategica, capital & liquidity planning, indirizzo strategico in tema di prodotti e servizi, politiche di remunerazione e incentivazione, ecc.). Più in particolare, il RAF è il quadro di riferimento per la definizione degli obiettivi di rischio/rendimento che il Gruppo intende raggiungere, assicurando che il business si sviluppi entro i limiti di rischio definiti, sia in condizione di normale operatività, sia in condizioni di stress. L'organo con supervisione strategica (CdA), supportato dal Comitato Rischi endoconsiliare, approva e monitora le linee strategiche, riportate nel RAS (Risk Appetite Statement), documento formale che contiene la dichiarazione esplicita degli obiettivi/limiti di rischio/rendimento che la banca intende assumere per perseguire le sue strategie. La funzione Controllo dei Rischi partecipa alla definizione del RAF su tutti gli aspetti legati alla misurazione e monitoraggio dei rischi; è, inoltre, responsabile a livello di Gruppo dello sviluppo, manutenzione e redazione del reporting che illustra gli esiti dell'attività di monitoraggio del RAS, secondo il *cascading down* approvato, e differenziato in funzione dei diversi destinatari interessati. Evidenziamo altresì come l'attuale regolamento del Comitato Rischi (D.1788) prevede che il Comitato inviti il CRO a partecipare a tutte le adunanze. Il Comitato svolge funzioni di supporto al Consiglio di Amministrazione in materia di rischi e sistema dei controlli interni; particolare attenzione deve essere riposta nell'ambito del RAF, dove il Comitato svolge attività valutativa e propositiva necessaria affinché l'Organo con Funzioni di Supervisione strategica possa definire e approvare gli obiettivi di rischio (Risk Appetite) e la soglia di tolleranza (Risk Tolerance). Inoltre il Comitato supporta il CdA nella verifica della corretta attuazione delle strategie, delle politiche di governo dei rischi e del RAF. In tale ambito nel corso degli incontri è emerso che sta già avvenendo un progressivo rafforzamento dell'interazione tra CRO e il Comitato endoconsiliare, in risposta ad uno degli elementi rafforzativi previsti dalle nuove EBA GL. In particolare, dal mese di maggio 2018, il CRO effettua l'inoltro anche al presidente del Comitato Rischi, della reportistica mensile predisposta e discussa in Comitato Gestione Rischi (cfr. slide successiva), arricchendo così il patrimonio informativo del Comitato endoconsiliare al fine di rendere più proattivo il suo ruolo verso il CdA. Inoltre, il CRO nel corso del 2018 ha formalizzato dei pareri per il Comitato Rischi, su operazioni di maggior rilievo al fine di valutarne l'impatto in termini di risk appetite. Per dettagli si rimanda alle slide successive (cfr. paragrafo 20.5). Infine, all'interno dell'attuale progettualità Perdar2018 è prevista una migliore definizione del processo operativo di dettaglio che dovrà permettere di «predefinire» le informazioni da fornire al Board in caso di situazione di «Stress/Crisi» su specifici ambiti di rischio, così come il processo che assicurerà il feedback del Board sull'informativa prodotta (valutazione annuale del report E-RMR per assicurare aderenza alle necessità del CdA). Sulla reportistica prodotta si rimanda alle slide successive.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Risk Management (5/8)*

RIFERIMENTO EBA GL	ESITI
20.3 Ruolo della funzione di gestione dei rischi nell'individuazione, misurazione, valutazione, gestione, mitigazione, monitoraggio e segnalazione dei rischi Art. da 174 a 180 EBA GL	Le disposizioni di vigilanza vigenti (Circolare Banca d'Italia n. 285/13) e le normative interne prevedono che l'Organo con Funzione di Supervisione Strategica approvi annualmente la pianificazione annua degli interventi in materia di Risk Management. Il Group Risk Plan 2018 è stato approvato nel corso del primo trimestre 2018 e con esso la Funzione di Controllo dei Rischi di Capogruppo ha illustrato il programma annuale delle attività volte a identificare e valutare i principali rischi a cui il Gruppo Montepaschi è o può essere esposto ed ha delineata la programmazione dei relativi interventi di gestione e mitigazione. Il processo di Risk Management della Banca può essere sintetizzato come segue:

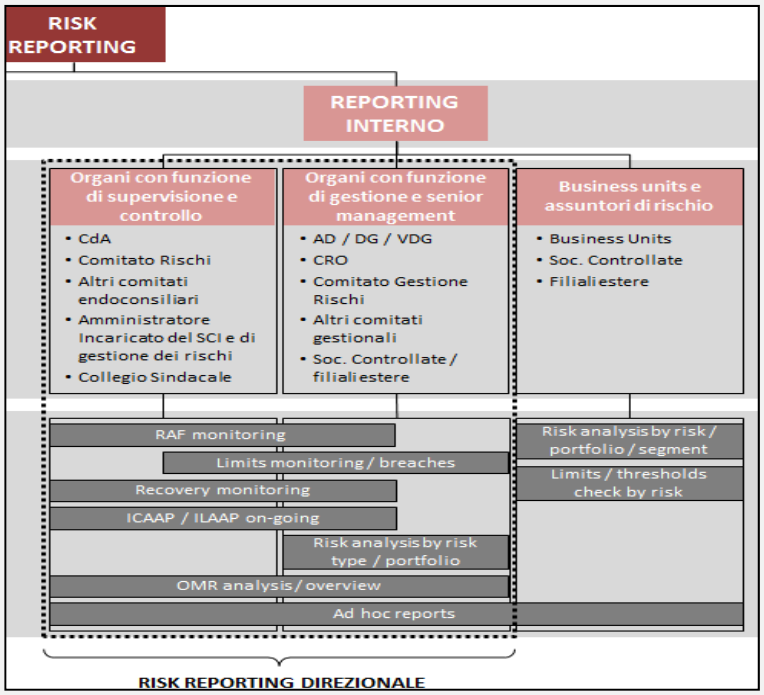


Nell'ambito del macro-processo di Risk Management sopra rappresentato, il Reporting tra le funzioni coinvolte e con gli Organi di Vertice e con il Senior Management assume una notevole rilevanza, anche alla luce delle nuove linee guida EBA.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Risk Management (6/8)*

RIFERIMENTO EBA GL	ESITI

Nei primi mesi del 2018 è stata emanata la «Direttiva di Gruppo in materia di Integrated Risk Reporting» (D2291) al fine di regolare in maniera integrata le modalità con le quali le informazioni di rischio sono rappresentate agli organi e alle funzioni aziendali aventi responsabilità strategiche, decisionali e di controllo.



Il perimetro del Risk Reporting Direzionale comprende i seguenti livelli di reportistica:

- 1° livello di reporting, verso gli organi di vertice aventi funzione di supervisione strategica e controllo; questa reportistica è caratterizzata da un massimo livello di sinteticità;
- 2° livello di reporting, diretto agli organi con funzione di gestione e al senior management, con il dovuto livello di dettaglio e aggregazione utile a valutare i rischi del Gruppo secondo le principali dimensioni di analisi rilevanti.

Esiste inoltre un 3° livello di reporting, indirizzato alle Business Units per finalità di gestione operativa dei rischi, che delimita il perimetro del Risk Reporting Operativo. Tutti i flussi di reporting, con indicazione delle funzioni owner e dei destinatari sono riportati nell'Allegato 3.

Nell'ambito della presente revisione, il focus è stato incentrato sul 1° e 2° livello di reporting; è stata pertanto acquisita e visionata la seguente reportistica:

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Risk Management (7/8)*

RIFERIMENTO EBA GL	ESITI
Controllo e Reporting dei Rischi	*1° livello* ✓ Con riguardo alla fase di identificazione e di modellizzazione/misurazione dei rischi, assume rilievo il **Risk Appetite Statement** (RAS), in cui il CdA, nel 2018, è stato chiamato ad esaminare ed approvare: 1.Le principali modifiche metodologiche introdotte ai modelli di risk management; 2.l'identificazione dei Rischi rilevanti ai fini RAS; 3.la struttura logica dei Key Risk Indicator (KRI) di Gruppo, delle Business Units e delle Legal Entity rilevanti. ✓ **Executive Risk Management Report** (E-RMR), inviato con cadenza trimestrale agli organi di vertice, sintetizza le principali risultanze di altri report/analisi di dettaglio predisposti per il Top Management e per i Comitati gestionali e si articola in specifiche sezioni; ✓ Per il monitoraggio della corretta implementazione ed esecuzione dei Commitment connessi al Piano di Ristrutturazione 2017-2021 viene predisposto e inviato con cadenza trimestrale il Report **ECB Committment** ✓ **Group Risk Plan** e **Group Risk Summary** al fine di illustrare, rispettivamente, la pianificazione annuale e la rendicontazione delle attività svolte dal RM al CdA. *2° livello* ✓ Relativamente ai report di monitoraggio si evidenzia che trimestralmente viene inviato agli Organi competenti il **Risk Appetite Monitoring** (RAM) e il **Recovery Plan Monitoring**, al fine di rendicontare gli stessi in merito alla verifica andamentale degli Indicatori previsti nel Risk Appetite Framework (RAF), agli sconfinamenti ed alle ipotesi di riallocazione della tolerance; all'interno del RAM, viene, tra l'altro, fornito un monitoraggio delle Operazioni di maggior rilievo (OMR) quantificando l'impatto in termini di assorbimenti di capitale sia delle operazioni perfezionate che di quelle ancora «pending». ✓ Con cadenza mensile viene predisposto il **Risk Management Report** (RMR) destinato ai Comitati Gestionali e al Top management, in cui vengono affrontate tutte le principali tipologie di rischio (Credit Risk, Market Risk, IRBB, Liquidity, etc.). Una delle principali novità delle Linee Guida EBA è costituita dalla previsione di un maggior coinvolgimento della Funzione Risk Management nell'ambito della Corporate Governance, prevedendo, in linea generale: 1. strumenti di governance per il responsabile per assicurare un effettivo ed efficace *challenge* sulle decisioni prese dalle funzioni di Business (es. risk opinion vs potere di veto). Per tale aspetto si rimanda alla slide successiva (cfr. paragrafo EBA 20.5). 2. il rafforzamento del ruolo della funzione RM anche nei momenti di «decision making» per assicurare presidio diffuso e supporto agli Organi di Vertice. Con riferimento a questo aspetto, nell'attuale organizzazione della Banca, il Responsabile della Funzione RM partecipa ai comitati gestionali (anche con diritto di voto) e presiede il Comitato Gestione Rischi. Tale Comitato, oggi non esecutivo/deliberativo, è articolato in 3 sessioni (Sessione Financial Risk, Sessione Lending Risk, Sessione Operational Risk) prevedendo la predisposizione di un'informativa verso il Comitato Direttivo (esecutivo), che in precedenza veniva indirizzata al CdA. Al riguardo, nel corso delle verifiche effettuate con il CRO, è emersa la possibilità di adottare scelte organizzative tese a razionalizzare ulteriormente i meccanismi di governance e, quindi, il presidio dei rischi.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Risk Management (8/8)*

RIFERIMENTO EBA GL	ESITI
20.4 Ruolo della funzione di gestione dei rischi in presenza di esposizioni non autorizzate Art. 181, 182 EBA GL	La funzione di gestione dei rischi valuta in maniera indipendente le violazioni o i limiti della propensione al rischio. Dalle verifiche si è potuto appurare che nei casi di superamento di determinate soglie di rischio, la funzione RM proceda a interfacciarsi con le funzioni di business per approfondire le cause e richieda a tali funzioni una proposta per rientrare nei limiti previsti. Il RM valuta l'efficacia/efficienza della proposta correttiva, rinviando la decisione in merito alla autorizzazione agli Organi di Vertice competenti, che poi sarà partecipata tramite la filiera organizzativa /gerarchica alle funzioni di business interessate. Abbiamo ottenuto, a titolo esemplificativo, il report «Risk Appetite Monitoring - Verifica andamentale RAF al 30/06/2018: sconfinamenti e ipotesi di riallocazione tolerance». Con questo report (discusso nei comitati gestionali e validato dal Comitato Rischi), viene indirizzato il CdA della banca a prendere atto dei superamenti delle soglie di tolerance ed a deliberare le linee di indirizzo da applicare. Data Sisifo da parte del RM verso il CDA 30/08/2018; Delibera consiliare in data 06/09/2018.
20.5 Responsabile della funzione di gestione dei rischi Art. da 183 e 186 EBA GL	Le linee guida EBA prevedono che il CRO abbia un ruolo attivo nell'intervenire, alle decisioni prese dalla gestione dell'ente e dal suo organo amministrativo, evidenziando che eventuali obiezioni formulate nelle scelte da parte del RM debbano essere formalizzate; e prevedendo la possibilità di concedere al CRO un potere di veto. Tale possibilità, non è pertanto obbligatoria, ma facoltativa. La valutazione della funzione RM della Banca in merito a tale opportunità è stata di non introdurre il veto (visto anche il fatto che il CRO non è un Amministratore indipendente), prevedendo invece pareri scritti non vincolanti a seguito di verifiche di coerenza su operazioni significative. La Direttiva di Gruppo in materia di Operazioni di Maggior Rilievo (OMR), documento D.1919 stabilisce che la Funzione di Controllo dei Rischi provvede a «formulare pareri preventivi sulla coerenza con il Risk Appetite Framework, tempo per tempo vigente, delle Operazioni di Maggior Rilievo identificate. In sede di valutazione delle operazioni, la Funzione di Controllo dei Rischi può richiedere a tutte le altre Funzioni Aziendali, […], per gli ambiti di loro pertinenza, specifica collaborazione anche attraverso la raccolta di informazioni/pareri sulla rischiosità complessiva dell'operazione (es. aspetti di natura reputazionale, compliance, interpretazione normativa, di redditività, etc.)». Nel corso del 2018 relativamente alle operazioni di maggior rilievo sono stati rilasciati n. 28 pareri (alla data del 30/09/2018), di cui un paio negativi (Arexpo SpA e Fondo Interbancario per la Tutela dei Depositi, aventi per oggetto concessione di nuova finanza; nel primo caso l'operazione è andata comunque avanti ugualmente con override degli Organi competenti). Il parere della Funzione di Controllo dei Rischi attiene alla valutazione di impatto dell'operazione in termini di limiti di appetito al rischio del Gruppo ed esclude ogni considerazione specifica sulla strutturazione dell'operazione o sulle sue caratteristiche generali. In particolare, il parere non fornisce indicazioni o valutazioni nel merito di rischio specifico della singola operazione né in termini di solidità finanziaria della controparte, stipula del contratto, forma tecnica, né in termini di livello di accantonamento e qualità dell'eventuale collaterale a supporto.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Compliance (1/2)*

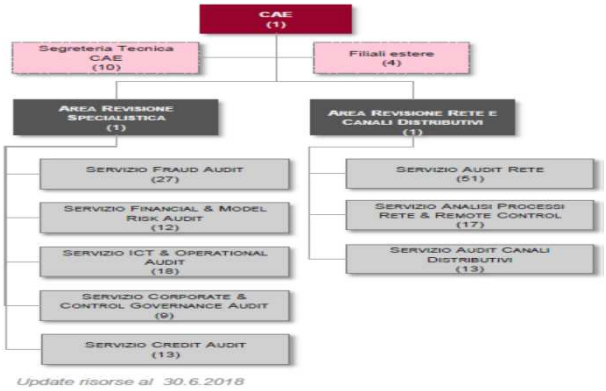
RIFERIMENTO EBA GL	ESITI
21 Funzione di Conformità Art. 187-188 Istituzione e proporzionalità	La Funzione di Conformità è costituita ai sensi della Circolare Banca d'Italia 285 (Tit IV Cap. 3 Sez. III), come indicato nel Reg. n. 1 (D.751, par. 3.7.1.2) aziendale. La mission "*Assolvere alla funzione di controllo di conformità alle norme secondo la definizione della normativa di vigilanza*», è stata recentemente aggiornata il 18 gennaio 2018 (cfr. Reg. 1 v. 87) in funzione del servicing svolto sul tema per le società di Gruppo. Il Responsabile della Funzione è nominato secondo la normativa italiana, inoltre lo stesso è nominato responsabile delle Funzioni Compliance delle società accentrate dai relativi CdA: stante il modello accentrato in uso, il principio di proporzionalità espresso nelle GL per cui la F. Conformità può esser combinata con altre Funzioni nelle realtà minori non trova applicazione.
Art. 189 Autonomia ed indipendenza	L'autonomia e l'indipendenza del Responsabile sono garantite: • dalle modalità di nomina ed approvazione dell'assetto economico (prerogativa del CdA), • dalla rendicontazione periodica al CdA sullo stato di conformità e presentazione annuale del piano degli interventi di mitigazione dei rischi (Compliance Plan) e relativa rendicontazione annuale per approvazione. Al fine di minimizzare i vincoli alla propria indipendenza, il Responsabile della Funzione è collocato a riporto dell'Organo con funzione di gestione ed è previsto che riferisca direttamente agli Organi Aziendali ed abbia accesso diretto al CdA, al Collegio Sindacale e al Comitato Rischi comunicando con essi nel continuo senza restrizioni e intermediazioni (cfr. D 793, come previsto da Circ. 285). In particolare circa il Comitato Rischi è previsto che il Responsabile della F. Compliance: • venga regolarmente tenuto al corrente dell'ordine del giorno delle riunioni del Comitato, • possa decidere discrezionalmente di partecipare alle riunioni a prescindere dagli inviti ricevuti, • possa inserire all'ordine del giorno delle riunioni del Comitato, informandone il Presidente, specifici temi che dovranno conseguentemente presentare con un confronto proattivo all'interno del Comitato. A livello di intera Funzione vige inoltre il principio di separatezza funzionale per il quale il personale che partecipa alle Funzioni Aziendali di Controllo non è coinvolto in attività che sono chiamate a controllare e pertanto, anche nell'ambito di un'eventuale partecipazione a Comitati di Gestione la Funzione è senza diritto di voto per le materie in contrasto con detto principio.
Art. 190 Skills personale	La Funzione di conformità è costituita da n. 60 risorse, 50 delle quali con anzianità in ruolo superiore a due anni o con precedenti esperienze in ruoli analoghi presso società controllate o esterne. La Funzione in occasione dell'introduzione del nuovo Modello Accentrato di Compliance deliberato da Cda di MPS il 27/04/2017 ha preso in carico la responsabilità per numerosi ambiti normativi in precedenza non presidiati: in tale occasione sono state identificate le carenze di competenze da sanare ed avviati una serie di corsi formativi ad hoc per alcune materie. Accanto a tali attività sono stati avviati più corsi metodologici rivolti alle 60 risorse (n. 258 presenze previste sommando i vari corsi), volti a fornire le competenze base per esperire le attività richieste dalla Funzione. Per il 2019 il palinsesto formativo prevede come punti qualificanti i corsi ABI Compliance Management (Base ed Avanzato) e corsi in collaborazione con le Funzioni di controllo su gap (coinvolta Internal audit) e su Cyber risk (coinvolta Direzione CRO). La valutazione del personale è stata per il 93% dei soggetti valutati nel corso del 2017 in ambito positivo, con giudizi pari o superiori a 3 (su una scala di 5).
Art. 191 Monitoraggio attività e norme, politiche di conformità	Il CdA riceve il reporting periodico sullo stato di conformità della banca previsto dal D.1915 «Flussi informativi», in particolare la Relazione annuale, il Plan annuale ed il reporting trimestrale. La normativa aziendale sulle politiche di conformità è pubblicata ed accessibile a tutto il personale, sia per quanto attiene i documenti sulle singole materie di conformità sia riguardo ai documenti quadro (es. Policy di Gruppo D.2163 e documenti metodologici).

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Compliance (2/2)*

RIFERIMENTO EBA GL	ESITI
Art. 192 Analisi modifiche normative, consulting verso gli Organi	Le modifiche alle normative esterne sono intercettate tramite la fase di "alerting normativo" del processo di Gestione del Rischio di non conformità descritto nel D.1413 omonimo che si avvale tra l'altro di fornitori di informazione esterni (ABICS, Infoproviding Nike) per la segnalazione delle variazioni da sottoporre ad analisi. La fase di «alerting normativo» citata è input di una successiva fase di «gap analysis» tesa a valutare gli impatti di dettaglio della modifiche normative sulle attività dell'azienda. L'attività di consulting è presente e codificata in uno specifico flusso informativo del catalogo pubblicato, il n. 54 "consulenza e supporto su tematiche di conformità" rivolto ad AD, Presidente CdA, Comitato Rischi, OdV231. La versione aggiornata di tale elenco, in fase di pubblicazione al momento della revisione, conferma tale flusso eliminando solo l'OdV231 come destinatario. Va osservato che nell'operatività ordinaria le strutture di Compliance raramente sono ingaggiate per consulting direttamente dai vertici come indicato nella presente GL 192: l'ingaggio avviene usualmente da altre strutture aziendali, che nel caso utilizzano i pareri ricevuti come supporto nelle loro comunicazioni verso i vertici.
Art. 193 Interazione con Risk Function	Il processo di monitoraggio della conformità è strutturato secondo la normativa pubblicata, approvato dal CdA ad inizio anno (documento di pianificazione annuale) e rendicontato sia a cadenza periodica (trimestrale), che al termine del periodo annuale (Relazione conformità). Circa l'interazione con la Funzione Risk è presente un unico flusso da Compliance a Risk, ovvero le "richieste di integrazione delle analisi di scenario" (n. 317). Tale flusso rappresenta un esito della fase di gap analysis del processo di Gestione del Rischio di non Conformità, fase che ha l'obiettivo di identificare, nel continuo, in caso di modifiche alla normativa esterna o all'impianto organizzativo aziendale, l'esistenza o la necessità di intervenire nelle procedure aziendali poste a presidio della conformità, individuando eventuali gap ed attivando le Funzioni competenti per la loro mitigazione. Circa i flussi provenienti da Risk Management e diretti a Compliance sono invece presenti alcuni flussi informativi attinenti ai servizi di investimento. Di maggior rilievo, anche per la selezione degli argomenti trattati, risultano i momenti di coordinamento ai quali le Funzioni di controllo di secondo livello hanno accesso, quali il Comitato Rischi, il Comitato Gestione rischi ed il Comitato di Coordinamento delle Funzioni di controllo.
Art. 194 Nuovi prodotti e procedure	La normativa interna prevede il coinvolgimento della Funzione Compliance in caso di definizione nuovi prodotti (cfr. D.1817 "Sviluppo Acquisizione e Gestione Prodotti) con funzione di validatrice. La Funzione altresì valida il materiale promozionale destinato alla clientela, dando luogo a interscambi frequenti con le funzioni di business: nel periodo gennaio-novembre 2018 sono stata registrate 155 validazioni circa prodotti nuovi/modificati/iniziative commerciali e 129 validazioni di materiale promozionale.
Art. 195 Provvedimenti disciplinari	Il Responsabile della Funzione conformità partecipa alla Commissione Affari Disciplinari con diritto di voto, salvo nel caso che debba svolgere il ruolo di relatore. La normativa interna disciplina le modalità di erogazione delle sanzioni disciplinari previste dal contratto di lavoro.
Art. 196 Filiazioni estere	La normativa interna relativa alla gestione del rischio di non conformità contiene specifiche previsioni per le filiali estere del Gruppo. In ciascuna filiale è prevista la presenza di un Compliance Officer che riporta gerarchicamente ad un settore della Funzione Compliance deputato tra le altre cose a coordinarne l'attività ordinaria come quella straordinaria in occasione del recente progetto di chiusura della maggioranza di tali filiali.

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Internal Audit (1 di 2)*

RIFERIMENTO EBA GL	ESITI
Funzione di audit interno	La Banca ha istituito una Funzione di Internal Audit indipendente ed efficace. La terzietà e l'indipendenza è garantita dal collocamento organizzativo. Il Responsabile della Funzione di Revisione Interna a livello gerarchico è, infatti, posizionato alle dirette dipendenze dell'Organo con funzione di supervisione strategica e non ha responsabilità diretta di aree operative sottoposte a controllo né è gerarchicamente subordinato ai responsabili di tali aree. La Funzione dispone di autorità, peso, risorse, strumenti di audit e metodi di analisi del rischio adeguati alle dimensioni della Banca nonché alla natura, alla portata e alla complessità dei rischi associati al modello di business, alle attività, alla cultura e alla propensione al rischio.



Fonte: QR CAE 3Q2018

Come riportato nei documenti di rendicontazione interna trimestrali, l'organico della Direzione alla data del 22/10/2018 era costituito da n. 177 persone. In termini di formazione Sono state erogate da inizio anno n. 5.017 ore di formazione (circa 28 ore pro-capite). (SCI)
Tutte le componenti del Sistema dei Controlli Interni sono oggetto di un'attività di revisione interna, volta a valutarne l'adeguatezza, la funzionalità e la coerenza con l'evoluzione organizzativa del Gruppo e del quadro normativo esterno.
In tale contesto la Funzione di Revisione Interna svolge un'attività indipendente volta a controllare da un lato, in un'ottica di terzo livello, il regolare andamento dell'operatività e l'evoluzione dei rischi e, dall'altro, a valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del SCI, portando all'attenzione degli Organi Aziendali i possibili miglioramenti, con particolare riferimento al RAF, al processo di gestione dei rischi nonché agli strumenti di misurazione e controllo degli stessi; sulla base dei risultati dei propri controlli formula raccomandazioni agli Organi Aziendali.

L'attività della Funzione di Revisione Interna, definita nel piano di audit annuale, è inquadrata all'interno di un più ampio piano di audit pluriennale che viene sottoposto all'approvazione dell'Organo con funzione di supervisione strategica. Nello svolgimento dei propri compiti la Funzione di Revisione Interna, che ha accesso a tutti i dati aziendali e alle attività esternalizzate, si attiene a quanto previsto dagli standard internazionali della professione, declinati all'interno degli Standard di Internal Audit del Gruppo e del relativo codice deontologico. Gli auditor sono costantemente incentivati al conseguimento della certificazione professionale «Certified Internal Auditor» (CIA) rilasciata dal «*The Institute of Internal Auditors*» (IIA), principale qualifica riconosciuta a livello internazionale per l'esercizio della professione di internal auditor e che identifica in modo univoco i professionisti del settore.
Qualora dalle proprie attività emergano anomalie, la Funzione di Revisione Interna assicura una tempestiva comunicazione e presa in carico da parte delle strutture competenti, monitorandone le modalità/tempistiche di gestione e mitigazione. La Funzione di Revisione Interna informa altresì periodicamente gli Organi Aziendali in merito alle risultanze emerse nel corso delle proprie attività ed allo stato di avanzamento delle attività in «follow up»; fornisce inoltre alle Autorità le dovute rendicontazioni previste dalla normativa di vigilanza.
E' attiva inoltre all'interno della Funzione Audit una struttura dedicata alla Fraud detection, responsabile anche della gestione della procedura di allerta interna (Whistleblowing) aziendale (per dettagli cfr. slide 32-33).

2 Attività svolta: *Assessment Tit. V EBA GL/2017/11 – Funzione di Internal Audit (2 di 2)*

RIFERIMENTO EBA GL

ESITI

Nella tabella sotto riportata sono riepilogati i principali flussi informativi della Funzione di Revisione Interna verso gli organi apicali.

	Destinatari		
Report	**CdA**	**Collegio Sindacale**	**Comitato Rischi**
Audit Plan	x	x	x
Relazione sull'attività svolta Sistema dei controlli interni del Gruppo	x	x	x
Relazione annuale Funzione di Revisione Interna sugli accertamenti condotti in merito ai sistemi AIRB e AMA, al loro utilizzo gestionale ed al processo di convalida interna	x	x	x
Relazione sui Servizi di investimento ai sensi dell'*art. 14, comma 3, Reg. Congiunto Consob-Bankit.*	x	x	x
Relazione sugli accertamenti effettuati presso le Società Controllate	x	x	x
Relazione sulle Funzione esternalizzate	x	x	x
Quarterly Report		x	x
Tableau de Board Internal Audit		x	x

I Report di audit ordinari seguono i criteri di distribuzione dei rapporti di audit, condivisi con il Comitato Rischi e il Consiglio di Amministrazione.

TdB?

Firme e destinatari del rapporto

Ruolo	Cognome e Nome	Firma
Responsabile Audit Team	Furlani Andrea	
Auditors	Paola Blasutto Fulvio Formiggini Mariangela Latina Michele Sbardellati Genziana Sigismondi Marco Zamperini	
V° Responsabile del Servizio Corporate & Control Governance Audit	Furlani Andrea (*ad interim*)	
V° Responsabile dell'Area Revisione Specialistica	Furlani Andrea	
V° Responsabile della Direzione Chief Audit Executive	Cocco Pierfrancesco	

Organi destinatari BMPS	Selezione
Presidente del CdA	
Amministratore Delegato	
Collegio Sindacale	X
Comitato Rischi	X

Altri organi destinatari	
Legal Entity	Organo destinatario

Elenco allegati

- Allegato 1: Normativa inerente il Codice Etico
- Allegato 2: Organizzazione Direzione CRO
- Allegato 3: Risk Management Reporting (D2291)

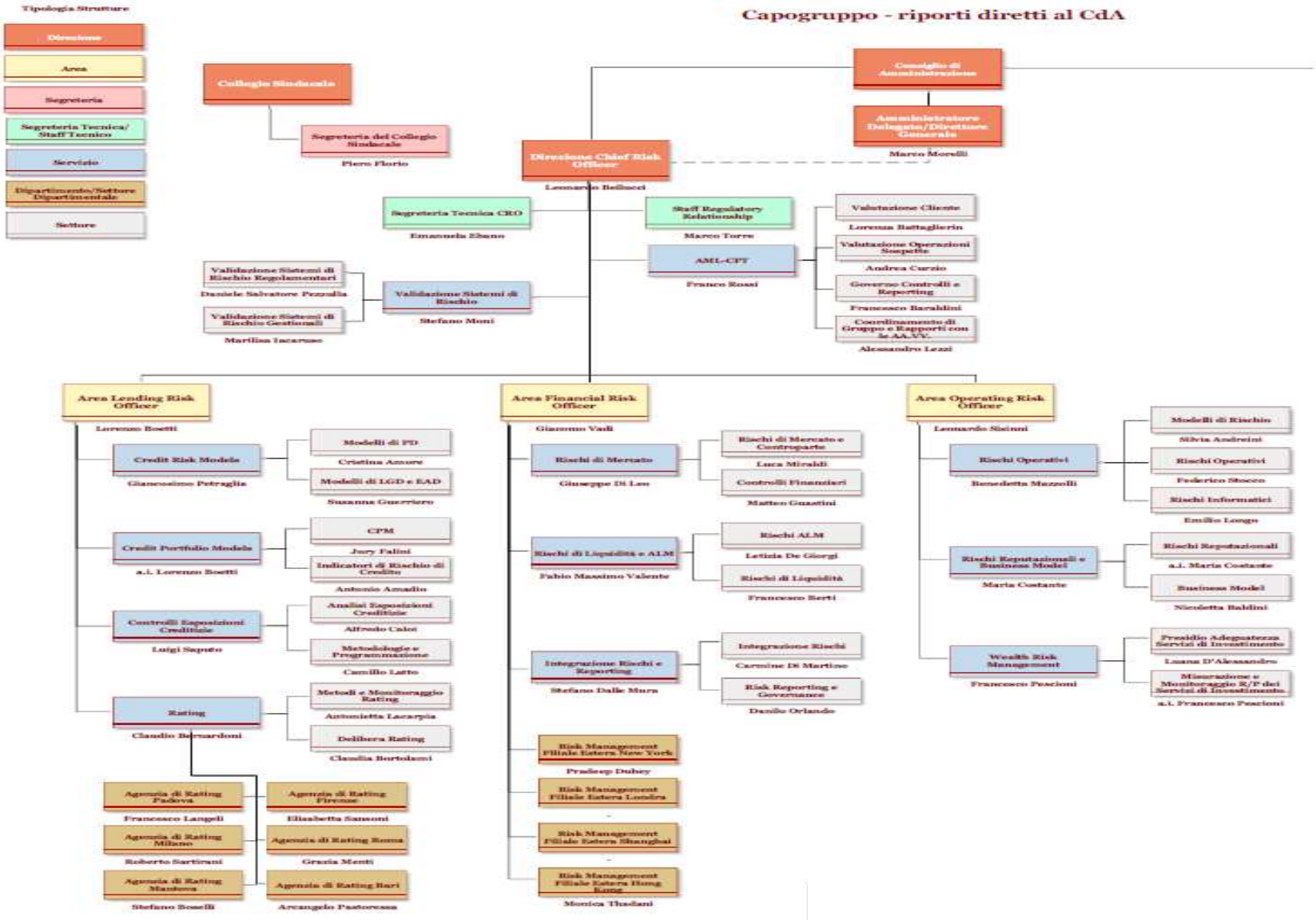
Allegato n. 1 – Normativa inerente il Codice Etico

Normativa inerente il Codice Etico

Gestione del personale e ambiente di lavoro	*D 00505 vers. 6.1 del 29.06.2018* *Direttiva di Gruppo in materia di Presidio e Sicurezza nei luoghi di lavoro* *D 02136 Policy di Gruppo in materia di sicurezza e ambiente* *D 01277 vers. 6.0 del 24.01.2018* *Direttiva di Gruppo in materia di Gestione del Rischio di non conformità (relativamente al "rischio ambiente")* *D 00506 vers. 6.1 del 5.09.2016* *Presidio della salute nei luoghi di lavoro* *U00570 vers. 1.0 del 20.12.2017 Integrazione urgente al documento D 00506 "Presidio della salute nei luoghi di lavoro"* *D 01968 vers. 3 del 28.02.2018* *Regole in materia di metodologia di valutazione del Rischio di non conformità (aspetti inerenti all'ambiente)* *D 01413 vers 6.0 del 28.02.2018* *Gestione del rischio di non conformità* *D 2147 vers. 1.0 del 13.09.2016* *Policy di Gruppo in materia di logistica e servizi ausiliari*	**Lotta alla corruzione**	*D01888 vers. 5.00 del 19.4.2018* *Regole in materia di gestione degli obblighi di segnalazione operazioni sospette* *D02210 vers. 11.00 del 30.10.2018* *Gestione obblighi di adeguata verifica della clientela*
		Gestione delle informazioni	*D 00499 vers. 14.00 del 25.05.2018* *Regole in materia di tutela dei dati personali* *D 01813 vers. 9.2 del 25.5.2018* *Gestione degli adempimenti prescrittivi in materia di dati personali* *D02298 vers. 2.0 del 25.5.2018* *Direttiva di Gruppo in materia di gestione degli adempimenti prescrittivi in materia di tutela di dati personali*
Correttezza e trasparenza negli affari **Conflitto di interessi**	*D01717 vers. 10.1 del 18.03.2018* *Gestione adempimenti prescrittivi in materia di trasparenza* *D 00388 vers. 28.0 del 9.11.2017* *Regole sulla gestion e adempimenti prescrittivi in materia di trasparenza* *D 1850 vers. 2.0 del 24.4.2018* *Policy di Gruppo in materia di privacy* *D01978 vers. 1.2 del 17.02.2015* *Policy inerna di Gruppo in materia di operazioni con parti correlate, soggetti collegati e obbligazioni con esponenti non bancari.* *D01556 vers. 8 del 10.7.2017* *Gestione adempimenti prescrittivi in materia di parti correlate, soggetti collegati e obbligazioni con esponenti bancari*	**Organi amministrativi, direttivi e di controllo** **Opposizione ad attività criminose**	*D02330 vers. 1.0 del 27.06.2018* *Gestione degli adempimenti prescrittivi in materia di D. Lgs 231/2001 sulla responsabilità amministrativa - regole per la prevenzione della corruzione nel Gruppo MPS* *D01455 vers. 1.01 del 5.10.2009* *Direttiva di gruppo in materia di Spese sostenute dai dirigenti* *D 2192 vers. 1.1 del 10.03.2017* *Policy di Gruppo in materia di revisione interna* *D 1594 vers.1.4 del 1. 09.2011* *Gestione della presenza della banca sui social network* *D 01823 vers. 3 del 1.06.2016* *Policy in materia di normativa interna e processi* *D 02345 vers. 1 del 13.08.2018* *Presidio segnalazioni obbligatorie Legge 185/90 (import/export armamenti)* *D 602 vers. 5.0 del 24.01.2018* *Presidio di gruppo in materia di contrasto al riciclaggio e al finanziamento al terrorismo*

Fonte: Normativa interna

Allegato 2) Organizzazione Direzione CRO



Allegato 3) Risk Management Reporting (D2291) (1 di 2)

Risk Management Function Flows
Gruppo Montepaschi
Situation as at Dec-2017

Main Risk Reports

#	Risk Flow Type	Internal/ External	Level	Report Name	Risk Content	Risk Area/ Factors	Frequency	Recipients: CRO	BU	Subsidiary	MC(s)	RMC	CEO	RC	RPC	RemC	AppC	BOD	BoSA	JST	Other Aut.	Market	Communication Mean	Owner
1	Report	Internal	1	Executive Risk Management Report [E-RMR]	Synthetic Risk Report for BoD - Risk Appetite Group KRI - Selected KRI Forward Looking projections - ICAAP/ILAAP on going - Recovery Plan Summary - OMR Summary	ALL	Quarterly	✓						✓				✓		✓			Sisifo	SIRR
2	Report	Internal	1	Exposures to Connected Parties	Connected Parties Limits Monitoring	ALL	Quarterly	✓							✓			✓	✓				Sisifo	SIRR
3	Report	Internal	2	Risk Appetite Monitoring [RAM]	Full cascaded RAS Monitor and OMR summary	ALL	Quarterly	✓			✓	✓	✓	S				S					TS/Sisifo(S)	SIRR
4	Report	Internal	2	Recovery Plan Indicators Monitoring [RPIM]	Group Recovery Indicators Report	ALL	Quarterly	✓			✓	✓	✓	S				S					TS/Sisifo(S)	SIRR
5	Report	Internal	2	Risk Management Report Group [RMR]	Group Report about: - Internal Capital (Equivalent RWA Estimate) - Credit Risk and Limits - IRRBB and Limits - Liquidity position and Limits - Market Risk (Trading + Banking) and Limits - Counterparty Risk - Operational Risk (Q/Q basis) - Wealth Risk Management WRM (Q/Q basis)	ALL	Monthly	✓			✓	✓	✓										Teams Site	SIRR
6	Report	Internal	2	Risk Management Report Subsidiaries/Branches	Individual Risk Report for each Subsidiary/Foreign Branch about all relevant risk factors	ALL	Quarterly	✓		✓													Sisifo	SIRR

Keynote:

BU: Business Units
CRO: Chief Risk Officer
Subsidiary: Individual Legal Entity or Foreign Branch
MC(s): Management Committees (e.g. Comitato Direttivo, Comitato Finanza e Liquidità,..
RMC: Risk Management Committee
CEO: Chief Executive Officer
CR: Risk Committee (BoD Committee)
RPC: Related Parties Committee (BoD Committee)
RemC: Remuneration Committee (BoD Committee)
AppC: Appointments Committee (BoD Committee)
BoD: Board of Directors
BoSA: Board of Statutory Auditors

JST: Joint Supervisory Team (ECB/Bankit)
Other Aut.: Other Authority (e.g. CONSOB, DGComp,...)
Market: General Stakeholders
AFRO: Area Financial Risk Officer [cfr. *Funzione Specialistica di Controllo dei Rischi*]
SIRR: Servizio Integrazione Rischi e Reporting [cfr. *Funzione Risk Reporting*]
SRO: Servizio Rischi Operativi [cfr. *Funzione Specialistica di Controllo dei Rischi*]
SWRM: Servizio Wealth Risk Management [cfr. *Funzione Specialistica di Controllo dei Rischi*]
SRR&BM: Servizio Rischi Reputazionali e Business Model [cfr. *Funzione Specialistica di Controllo dei Rischi*]
Sisifo: Internal Communication Protocol
TS: Collaboration Team Site
OracleCloud: IT environment for Financial Statement management
S: flow in Stressed conditions

Allegato 3) Risk Management Reporting (D2291) (2 di 2)

Risk Management Function Flows
Gruppo Montepaschi
Situation as at Dec-2017

Main Risk Documents

							Recipients																	
							CRO	BU	Senior Manag./ Subsidiaries				Head Office Corporate Bodies						External Recipients					
#	Risk Flow Type	Internal/ External	Level	Report Name	Risk Content	Risk Area/ Factors	Frequency	CRO	BU	Subsidiary	MC(s)	RMC	CEO	BC	RPC	RemC	AppC	BOD	BoSA	JST	Other Aut.	Market	Communication Mean	Owner
7	Document	Internal	1	Group Risk Plan	Risk Activities planned	ALL	Annual	✓						✓				✓					Sirifo	SIRR
8	Document	External	1	Group Risk Summary	Summary of Inherent risks and processes	ALL	Annual	✓						✓				✓		✓			Sirifo	SIRR
9	Document	Internal	2	Individual Risk Plan	Risk Activities planned	ALL	Annual	✓		✓													Sirifo	SIRR
10	Document	Internal	2	Individual Risk Summary	Summary of Inherent risks and processes	ALL	Annual	✓		✓													Sirifo	SIRR
11	Document	External	1	Risks related to Investment Services Summary	Annual Summary about WRM for Consob	WRM	Annual	✓						✓				✓	✓		✓		Sirifo	SWRM
12	Document	External	1	IT Risk Summary	Annual Summary about IT Risk for Bankit	IT Risk	Annual	✓		✓			✓	✓				✓		✓			Sirifo	SRO
13	Document	Internal	1	Risk Appetite Statement [RAS]	- Group KRI - BU/LE KRI Cascading down - Stress Test/Sensitivity Analises	ALL	Annual	✓		✓	✓	✓	✓	✓				✓					Sirifo	AFRO
14	Document	External	1	ICAAP Annual Statement (Package)	- Risks to Capital (Internal/Regulatory Capital) - Capital Adequacy (current, forward and stressed) - Process Adequacy	Risks to Capital	Annual	✓						✓				✓		✓			Sirifo	AFRO
15	Document	External	1	ILAAP Annual Statement (Package)	- Risks to Liquidity (Intraday, Short/Medium/ Long Term) - Liquidity Adequacy (current, forward and stressed) - Process Adequacy	Liquidity	Annual	✓						✓				✓		✓			Sirifo	AFRO
16	Document	Internal	1	RAF-Remuneration Opinion	CRO Opinion about the coherence between RAF and Remuneration Policy	ALL	Annual	✓						✓									Sirifo	AFRO
17	Document	Internal	2	Risk Contribution to Identified Staff Report	Contribution to HR Material Risk Takers identification (Reg. EU 604/14)	ALL	Annual	✓	✓														E-mail	SIRR
18	Document	External	1	Pillar3 Disclosure	External disclosure according to Reg. UE 575/13	ALL	Quarterly	✓			✓		✓	✓				✓				✓	Sirifo	SRR&BM
19	Document	External	1	EC Commitments Monitoring Report	DGComp Commitments Monitoring for Trustee	ALL	Quarterly	✓			✓		✓	✓				✓			✓		Sirifo	SRR&BM
20	Document	Internal	2	Risk Contribution to Financial Statement	Risk analyses for Financial Statement (IPV, FVH,...)	ALL	Quarterly	✓	✓	✓	✓												OracleCloud	SIRR

Keynote:

BU: Business Units
CRO: Chief Risk Officer
Subsidiary: Individual Legal Entity or Foreign Branch
MC(s): Management Committees (e.g. Comitato Direttivo, Comitato Finanza e Liquidità,..
RMC: Risk Management Committee
CEO: Chief Executive Officer
CR: Risk Committee (BoD Committee)
RPC: Related Parties Committee (BoD Committee)
RemC: Remuneration Committee (BoD Committee)
AppC: Appointments Committee (BoD Committee)
BoD: Board of Directors
BoSA: Board of Statutory Auditors

JST: Joint Supervisory Team (ECB/Bankit)
Other Aut.: Other Authority (e.g. CONSOB, DGComp,...)
Market: General Stakeholders
AFRO: Area Financial Risk Officer [cfr. *Funzione Specialistica di Controllo dei Rischi*]
SIRR: Servizio Integrazione Rischi e Reporting [cfr. *Funzione Risk Reporting*]
SRO: Servizio Rischi Operativi [cfr. *Funzione Specialistica di Controllo dei Rischi*]
SWRM: Servizio Wealth Risk Management [cfr. *Funzione Specialistica di Controllo dei Rischi*]
SRR&BM: Servizio Rischi Reputazionali e Business Model [cfr. *Funzione Specialistica di Controllo dei Rischi*]
Sirifo: Internal Communication Protocol
TS: Collaboration Team Site
OracleCloud: IT environment for Financial Statement management
S: flow in Stressed conditions