



**MONTE
DEI PASCHI
DI SIENA**
BANCA DAL 1472

Audit Plan 2018

Direzione Chief Audit Executive

Indice

PREMESSA.....	3
EXECUTIVE SUMMARY	4
1. OBIETTIVI STRATEGICI E PIANIFICAZIONE PLURIENNALE.....	7
APPROCCIO METODOLOGICO.....	10
2. IL PIANO DI AUDIT 2018	14
DATA QUALITY ASSURANCE	14
ANALISI CONSOLIDATA DI GRUPPO	15
CONTROLLI DI 1° LIVELLO.....	15
ANALISI COMPORTAMENTALE.....	16
JOINT AUDIT	16
INTERVENTI DI REVISIONE	18
• CREDITO.....	19
• MACCHINA OPERATIVA	20
• FINANZA PROPRIETARIA.....	20
• DISTRIBUZIONE COMMERCIALE.....	20
• GOVERNANCE, CONTROLLO RISCHI E CONFORMITÀ.....	21
• INFORMATION TECHNOLOGY	21
ATTIVITÀ DI CONSULTING	22
ANALISI A DISTANZA.....	22
ATTIVITÀ DIREZIONALE E RELAZIONALE.....	22
ATTIVITÀ DIVERSE.....	23
PROGETTI GESTITI E COORDINATI DALLA DIREZIONE CHIEF AUDIT EXECUTIVE	23
FORMAZIONE.....	23

Premessa

In coerenza con gli standard internazionali, la pianificazione delle attività costituisce il momento in cui il Responsabile della Direzione Chief Audit Executive individua gli obiettivi da raggiungere, le modalità di realizzazione, la relativa tempistica e frequenza, nonché le conseguenti risorse da impiegare.

Con quest'anno ha inizio un nuovo ciclo di revisione pluriennale che, nell'arco temporale triennale 2018-2020, si pone l'obiettivo di assicurare un adeguato livello di copertura dell'*audit universe* secondo una logica *risk based* al fine di valorizzare il ruolo ex ante della funzione di audit e, al contempo, considerando talune linee guida che essa intende perseguire.

La profonda e rapida evoluzione del contesto di riferimento sta avendo forti impatti sulle realtà bancaria e di conseguenza sulla sfera di azione dell'internal audit con l'introduzione di nuove e complesse materie di indagine e con l'incremento degli interventi richiesti dal supervisore europeo.

Al fine di cogliere in modo efficace le nuove sfide, il Piano di Audit per il 2018 introduce alcuni sostanziali elementi innovativi:

- rappresenta il primo anno di un nuovo approccio pluriennale (2018-2020) che si estende in arco Piano di Ristrutturazione;
- è allineato agli obiettivi strategici previsti nel Piano di Ristrutturazione e ne è a diretto e specifico supporto;
- tiene conto dei *commitment* della Commissione Europea (CE) e quindi dei possibili impatti derivanti per l'attività di internal audit dalla concessione degli aiuti di Stato;
- è stato definito sulla base di un approccio metodologico *SREP oriented* e tiene conto sia delle priorità 2018 del meccanismo unico di vigilanza (SSM-*Single Supervisory Mechanism*) sia dello specifico piano di vigilanza presentato dal JST per il Gruppo MPS;
- prevede interventi di maggiore ampiezza e articolazione effettuati in *joint audit* da team misti;
- contempla un approccio consolidato a livello di Gruppo su macrotematiche di particolare rilievo.

Allo stesso tempo, la nuova pianificazione conferma e consolida l'attenzione dell'internal audit sui seguenti ambiti:

- processi creditizi;
- controlli di 1° livello (in particolare in ambito filiera commerciale e creditizia) e di 2° livello (in particolare in ambito antiriciclaggio e compliance);
- analisi comportamentale;
- *Conduct Risk* e *Risk Culture* aziendale.

Executive Summary

Il Piano di Audit 2018 è stato predisposto come primo anno di un approccio triennale (2018-2020) in arco Piano di Ristrutturazione sulla base di taluni *driver* che la Direzione Chief Audit Executive ha individuato anche alla luce degli esiti del *Quality Assurance Review* (QAR) straordinario effettuato nella prima parte del 2017.

La revisione degli obiettivi di audit pluriennali originariamente definiti nel piano avviato nel 2016 si è resa necessaria a seguito del rapido evolversi degli scenari interni/esterni che hanno interessato il Gruppo MPS e che hanno condotto all'ingresso del MEF nell'assetto proprietario della Banca.

L'insediamento del nuovo Consiglio di Amministrazione e la messa a terra del Piano di Ristrutturazione suggeriscono di mantenere un certo grado di flessibilità nella definizione delle attività che permetta di rispondere tempestivamente a eventuali ulteriori esigenze di *assurance* che dovessero rendersi necessarie nel corso dell'anno.

Il piano è stato sviluppato applicando la metodologia consolidata di *Risk Control Assessment* assicurando una copertura in linea con l'arco Piano, considerando, altresì, una serie di input prioritari tra cui le **aspettative/priorità della vigilanza (BCE), i commitment CE**, gli eventuali vincoli derivanti dalla **concessione degli aiuti di Stato**, nonché gli ulteriori **ambiti di attenzione regolamentare**.

L'approccio adottato è stato esteso a tutte le società controllate, i cui piani sono stati condivisi e approvati dalla Direzione Chief Audit Executive.

Consistente l'impatto degli interventi "obbligatori" (23) richiesti dalla normativa e/o dalla supervisione europea, tra cui rileva la presenza di interventi in ambito di **data quality assurance**. Il tema della plausibilità e della correttezza del dato, intesa come verifica che le informazioni fornite rispondano fedelmente alla situazione vigente al momento della trasmissione dello stesso, hanno acquistato una crescente attenzione da parte della vigilanza europea che, in vari ambiti tra i quali da ultime le linee guida della TRIM (*Targeted Review of Internal Models*), attribuisce alla funzione di internal audit un ruolo particolare nel complesso processo di *data quality assurance* per quanto riguarda i modelli interni e gestionali per la stima dei requisiti di capitale.

Sono, altresì, contemplate verifiche ai fini del conseguimento delle attività richieste dalla BCE a seguito dei *finding* evidenziati negli esiti (a tutt'oggi ancora in forma di *draft follow-up letter*) della OSI-1238 su "*Credit and counterparty risk management and risk control system*".

Le **priorità di vigilanza per il 2018** esplicitate dal SSM hanno impattato direttamente sugli obiettivi di audit, convergendo le mire per il prossimo esercizio anche su buona parte delle tematiche "*core*" individuate dal supervisore europeo e relative nello specifico a: **modelli di business; rischio di credito** (in particolare recupero degli NPL); **analisi dei modelli interni** (TRIM); introduzione del principio contabile **IFRS9**. Sono state altresì considerate le attività di vigilanza 2018 pianificate per il Gruppo MPS e recentemente presentate dal JST, in particolare i perimetri e i tempi delle annunciate attività ispettive *on-site* (quali le ispezioni sull'*IT Risk* e sul rischio tasso del portafoglio bancario e la *Internal Model Investigation* sulle modifiche al modello interno AIRB per la determinazione dei requisiti patrimoniali per il rischio di credito) così come il dettaglio delle varie attività di supervisione (*deep dive*, ecc.) da effettuarsi in corso d'anno.

Lo stesso *assessment* di QAR effettuato da Deloitte nel 2017 ha evidenziato, tra le aree di miglioramento evolutive, come il cambiamento in atto del contesto di riferimento e le rinnovate aspettative da parte del supervisore europeo, richiedano alla funzione di internal audit di estendere la propria attività di revisione interna a temi innovativi, che a loro volta presuppongono l'adozione di strumenti e tecniche orientati al processo *SREP*.

Allo scopo di perseguire al meglio tali molteplici obiettivi, la Direzione CAE ha avviato un percorso di rivisitazione del proprio assetto organizzativo nonché dell'intero *framework* metodologico adottando un **approccio SREP oriented**.

La nuova impostazione presuppone la riconduzione ai pilastri *SREP* dell'*audit universe* mappato nell'albero dei processi del Gruppo. Gli obiettivi di controllo *SREP* identificati sulla base delle linee guida *EBA* e di ulteriori informazioni derivanti dall'azione regolamentare della vigilanza sono stati associati ai processi aziendali permettendo una previsione di copertura in ottica *SREP*.

In fase di consolidamento dei risultati di audit sarà fornita, in aggiunta al giudizio complessivo espresso per ogni revisione, anche una valutazione dei singoli obiettivi di controllo *SREP* impattati, sulla base della mappatura definita nel *framework*. Ciò permetterà di ottenere un'evidenza complessiva della valutazione degli obiettivi di controllo *SREP* che potrà costituire un efficace strumento di controllo nell'interazione con l'Autorità di vigilanza.

L'*Audit Plan* 2018, sulla base della nuova metodologia adottata, prevede la copertura di 37 processi selezionati dal catalogo di Gruppo BMPS e individuati sulla base della loro rilevanza *SREP*; la copertura del totale obiettivi *SREP* conseguita verificando tutti gli obiettivi di controllo sottostanti tali processi risulterà per l'anno pari a un massimo circa del 61%.

Taluni processi centrali ad alto impatto (nello specifico, 5) saranno, per la prima volta, oggetto di **analisi consolidata a livello di Gruppo** e ricompresi, quindi, nell'*Audit Plan* della Capogruppo:

- 1) Gestione fornitori, attività negoziale e contratti;
- 2) Compliance: modello accentrato di Gruppo con *focus* su Widiba e MPS CS;
- 3) AML (SOS-Segnalazione Operazioni Sospette) su BMPS, Widiba e MPS Fiduciaria;
- 4) MiFID II (processo/modello/modalità distributive/controlli di 1° livello);
- 5) Ethical Hacking su BMPS, filiale di NY e Widiba.

Il piano ricomprende le attività per le società dove la funzione di internal audit è stata accentrata nella Capogruppo (Widiba, MPS Fiduciaria, Microcredito di Solidarietà, Magazzini Generali di Mantova e Integra).

A livello consolidato rileva evidenziare che la predisposizione del piano di audit delle controllate-Italia ed estere e delle filiali estere – approvati dalla scrivente funzione - ha necessariamente tenuto conto dei *commitment* CE connessi alla concessione degli aiuti di Stato e degli obiettivi strategici di Gruppo in termini di mantenimento ovvero dismissione delle partecipazioni detenute.

La nuova pianificazione presenta accertamenti più estesi in termini di perimetro e maggiormente integrati, prevedendo una costante e sempre più stringente azione sinergica tra settori specialistici e settori che verificano i processi sulla Rete territoriale e sui canali distributivi, con l'individuazione di interventi svolti in **joint audit** da team misti al fine di sfruttare le possibili sinergie e accrescere l'efficacia dell'internal audit.

Per la Rete si conferma l'attenzione verso le strutture di presidio territoriale con particolare focus sui **controlli di 1° livello**. Il tema del corretto svolgimento delle attività da parte delle strutture operative, la prima linea di difesa del processo di gestione dei rischi, sarà costante in tutti gli ambiti che comportano presidi «di linea» (Credito, Servizi di investimento, AML, etc.) quale fattore qualificante ed elemento trasversale della pianificazione 2018.

Prosegue e si estende l'attività di consulenza alla Rete finalizzata al rafforzamento della cultura del rischio. L'attività di audit sarà, pertanto, volta a valutare la complessiva efficacia dei processi di controllo del *Conduct Risk*, facendosi promotrice della **risk culture** aziendale.

L'analisi dei principali processi agiti dalla Rete sarà incentrata su **ambiti di natura comportamentale** e tale approccio sarà previsto nell'ambito delle revisioni a piano ogniqualvolta se ne renderà possibile e opportuna l'applicazione.

Un'importante aliquota del tempo/risorse è allocata per attività di **analisi a distanza** sui principali fenomeni di rischio osservati e per il rafforzamento dell'azione volta a rimuovere le anomalie riscontrate nell'operatività e nel funzionamento dei controlli (*follow-up*).

E' stato pianificato un congruo numero di giornate/uomo per l'attività di *fraud detection*, *fraud investigation* e per la gestione delle segnalazioni (*whistleblowing*) da parte dei dipendenti.

Gli obiettivi per il 2018 sono stati illustrati preventivamente al Collegio Sindacale che ha richiesto supporto su importanti ambiti di rischio per lo svolgimento delle attività di verifica dell'Organo di controllo. Alcuni accertamenti sono stati, altresì, rappresentati all'Organismo di vigilanza 231/2001 per la valutazione dell'effettività e dell'efficacia del modello. Il piano di audit, una volta approvato, sarà presentato al *Joint Supervisory Team (JST)* della BCE.

L'introduzione nel piano di nuovi elementi valutativi così come di nuove aree di indagine caratterizzate da rilevanti complessità (quali, ad esempio, le attività di *data quality validation*), unitamente all'incremento del numero di interventi richiesti obbligatoriamente e all'implementazione di un approccio metodologico *SREP oriented* ha, inoltre, comportato la necessità di un'evoluzione in corso d'anno dell'assetto organizzativo della Direzione CAE un cui primo *step* ha già avuto luogo nella prima metà del 2017.

Uno specifico fondo di 350 mila euro, a finalità strategico-direzionale, è stato stanziato a disposizione del Chief Audit Executive per permettere alla funzione di rispondere tempestivamente alle sfide del nuovo contesto, anche in considerazione delle aspettative dell'Autorità di vigilanza. Nell'ambito delle iniziative progettuali per il 2018, è stato previsto un *plafond* di 290 mila euro per gli interventi prioritari relativi ai Sistemi Informativi di Audit (ESC Audit; FDS).

Il piano formativo 2018 prevede un *budget* di circa 120 mila euro. Particolare attenzione viene rivolta alla crescita professionale e al continuo aggiornamento degli auditor, incentivando il conseguimento delle certificazioni di categoria e contemplando l'erogazione di formazione e percorsi volti al conseguimento di diplomi su tematiche specialistiche erogati dall'AlIA (*Associazione Italiana Internal Audit*).

Come da regole definite, dei risultati delle attività svolte, sull'utilizzo delle risorse e sul *follow-up* sarà fornita periodica rendicontazione agli Organi aziendali.

1. Obiettivi strategici e pianificazione pluriennale

Il rapido evolversi degli scenari interni/esterni che hanno interessato il Gruppo MPS nel corso degli ultimi anni, in particolare nel 2017, e che ha condotto alla concessione di aiuti di Stato, nonché gli elementi caratterizzanti il Piano di Ristrutturazione, hanno richiesto una significativa rivisitazione degli obiettivi di audit pluriennali originariamente individuati, tanto da comportare l'interruzione, con due anni di anticipo, della vigente pianificazione pluriennale avviata nel 2016.

Il 2018 rappresenta, pertanto, il primo anno di un nuovo ciclo di revisione triennale (2018-2020) nel corso del quale la Direzione Chief Audit Executive si prefigge la copertura dell'intero *audit universe* in stretta correlazione con il contesto di riferimento e a diretto supporto degli obiettivi strategici di Gruppo.

La pianificazione pluriennale definisce gli obiettivi di audit da perseguire nell'orizzonte di medio termine individuati prioritariamente sulla base del "fattore rischio", pur tenendo comunque in considerazione il "fattore tempo", allo scopo di assicurare soglie minime di copertura per tutti i processi aziendali.

L'obiettivo è la copertura di tutti i rischi rilevanti nell'orizzonte triennale, secondo differenti approcci di analisi e valutazione, funzionali a ciascuna tipologia di rischio, non soffermandosi esclusivamente sui rischi associati al *business*, ma allargando lo scenario di valutazione anche alle altre fattispecie, ivi compresi il rischio reputazionale e strategico.

Il nuovo piano di audit è predisposto, dunque, applicando la consolidata metodologia di *Risk Control Assessment* e con l'obiettivo di assicurare uno sviluppo pluriennale in linea con l'arco Piano, considerando, altresì, alcuni presupposti fondamentali per l'individuazione delle attività di revisione da condurre come di seguito rappresentato.



Resta inteso che l'insediamento del nuovo Consiglio di Amministrazione e l'attuazione del Piano di Ristrutturazione (2017-2021) suggeriscono di mantenere un certo grado di flessibilità che permetta di rispondere tempestivamente ad eventuali esigenze attualmente non prevedibili che dovessero rendersi via via necessarie nel periodo.

Alla luce, infatti, della profonda e rapida evoluzione del contesto di riferimento che sta producendo rilevanti impatti sulle realtà bancaria e, di conseguenza, anche sul perimetro di azione dell'internal audit, la stessa è oggetto di un processo evolutivo che la condurrà a ricoprire un ruolo sempre più di interlocutore primario del supervisore europeo e, quindi, una sorta di "*internal secondary supervisor*". Tale posizione consente, peraltro, di focalizzare le mire sui temi maggiormente all'attenzione della vigilanza, nonché di valutare il posizionamento della Banca rispetto alle aspettative del supervisore.

La funzione di internal audit è chiamata a fornire *assurance* al proprio vertice aziendale, da un lato favorendo l'adozione di opportuni e preventivi interventi di adeguamento in riferimento ai possibili esiti del processo *SREP*, dall'altro consentendo l'acquisizione di evidenze di supporto nella formulazione di controdeduzioni a eventuali *finding* rilevati dalle iniziative ispettive della vigilanza.

Al fine di traguardare tali obiettivi, la Direzione CAE ha dunque avviato nel corso del 2017, quale intervento conseguente alle raccomandazioni del QAR 2017, un percorso di rivisitazione dell'intero *framework* metodologico adottando un approccio di natura *SREP oriented* (Cfr. All. 1 - *Framework* pianificazione *SREP oriented*: supporto metodologico).

Il nuovo modello metodologico si fonda su una preliminare mappatura degli obiettivi di controllo per ciascuno dei 4 pilastri del *framework SREP*, condotta sulla base delle Linee Guida *EBA* e delle linee guida/orientamenti *EBA* su specifiche tematiche richiamate all'interno delle stesse Linee Guida *SREP* (es. orientamenti sull'organizzazione interna, orientamenti sulle politiche e prassi di remunerazione, *IT Risk*, ecc.).

Sulla base di tale *framework SREP* sono stati mappati, al momento, 285 obiettivi di controllo così ripartiti:

- 33 obiettivi di controllo per il 1° pilastro *SREP - Business Model Analysis*,
- 137 obiettivi di controllo per il 2° pilastro *SREP - Internal Governance*,
- 73 obiettivi di controllo per il 3° pilastro *SREP - Risk To Capital*,
- 42 obiettivi di controllo per il 4° pilastro *SREP - Risk To Liquidity*.

Oltre agli obiettivi di controllo specificatamente individuati, si è tenuto conto di ulteriori informazioni di rilievo derivanti dall'azione ispettiva e dall'azione regolamentare della vigilanza europea interamente riconducibili al *framework SREP*, quali le *SSM 2018 supervisory priorities*; le attività di vigilanza 2018 pianificate dal JST per il Gruppo MPS; i finding del JST conseguenti agli esiti di *OSI/IMI*, *thematic review* e *deep dive analysis*; la timeline regolamentare BCE e i documenti in consultazione emanati dalla BCE/EBA, oltre ovviamente agli esiti del processo annuale di valutazione *SREP* (*SREP decision*).

Per quanto ovvio, gli obiettivi di controllo sono regolarmente mantenuti e aggiornati al fine di rendere il nuovo *framework* costantemente allineato agli eventuali nuovi requisiti normativi che dovessero essere introdotti.

L'adozione dell'approccio *SREP oriented* presuppone la riconduzione ai pilastri *SREP* dell'*audit universe* mappato nell'albero dei processi del Gruppo MPS (ARIS). Gli obiettivi di controllo *SREP* identificati sono stati, pertanto, associati ai processi aziendali, pur con la consapevolezza che tali obiettivi di controllo sono riconducibili solo a un sotto-insieme del complessivo *audit universe* che, nel suo complesso, comprende ulteriori ambiti di azione non riconducibili direttamente allo *SREP*.

Dal punto di vista metodologico, la prioritizzazione dei processi è stata definita sulla base del livello di rilevanza *SREP* attribuito a ciascun di essi¹. Tale rilevanza è direttamente correlata al numero degli obiettivi di controllo associati al processo stesso. Il nuovo approccio permette così, nella definizione del piano di audit, di assicurare un adeguato livello di copertura degli obiettivi di controllo *SREP*.

In fase di determinazione dei risultati dell'attività di audit sarà fornita, in aggiunta al giudizio complessivo espresso per ogni revisione effettuata, anche una valutazione dei singoli obiettivi di controllo *SREP* impattati dalla verifica stessa sulla base della mappatura definita nel *framework*. Ciò permetterà di ottenere nell'anno e, soprattutto, nell'arco del ciclo triennale, un'evidenza complessiva, organica e coerente della valutazione degli obiettivi di controllo *SREP* che potrà fornire un efficace strumento di controllo nell'interazione con l'Autorità di vigilanza.

¹ Il livello di rilevanza è rappresentato con una scala di valutazione su 4 livelli a criticità crescente (R1 Verde; R2 Giallo; R3 Arancione; R4 Rosso).

Inoltre, in fase di consuntivazione dei risultati, si perverrà a una valutazione del complessivo Sistema dei Controlli Interni circoscritta anche ai pilastri del *framework SREP*.

Tra le fonti informative considerate, sono particolarmente rilevanti le priorità di vigilanza SSM 2018, sia in generale che nello specifico per il Gruppo, che permettono di individuare specifici punti di attenzione in relazione ai quali la funzione di internal audit deve necessariamente assicurare un *focus* mirato.

I modelli di *business* e le determinanti della redditività delle banche si confermano una priorità per il meccanismo unico di vigilanza nel 2018.

Priorities 2018	Attività per il 2018 e oltre	Timelines		
		2018	2019	2020
Modelli di business e determinanti della redditività	Analisi di redditività delle banche	■	■	■
	Analisi di sensibilità al rischio di tasso di interesse sul portafoglio bancario	■	■	■
Rischio di credito	Esame delle strategie per gli NPL delle banche (es. deep dives/OSI) Verifica della tempestività degli accantonamenti e delle cancellazioni per gli NPL	■	■	■
	Esame delle esposizioni verso il settore immobiliare Analisi delle prassi di gestione e valutazione delle garanzie	■	■	■
Gestione dei rischi	TRIM-proseguimento attività in materia di modelli di rischio di credito, mercato e controparte	■	■	■
	Miglioramento dell'ICAAP e dell'ILAAP	■	■	■
	Monitoraggio dell'applicazione dell'IFRS 9 Esame dello stato di preparazione ad altre modifiche regolamentari	■	■	■
Azione caratterizzata da dimensioni multiple di rischio	Preparativi per la Brexit	■	■	■
	EU-wide (biennale) e SSM-wide esercizi di stress test	■	■	■

La vigilanza conferma, inoltre, di presidiare su base continuativa gli ambiti connessi ai rischi informatici e alla cybersecurity.

Sono altresì considerate le attività di vigilanza pianificate dal JST a livello di Gruppo MPS per il 2018, in particolare i perimetri e i tempi delle annunciate attività ispettive *on-site* (quali le ispezioni sull'*IT Risk* e sul rischio tasso del portafoglio bancario e la *Internal Model Investigation* sulle modifiche al modello interno AIRB per la determinazione dei requisiti patrimoniali per il rischio di credito) così come il dettaglio delle varie attività di supervisione (*deep dive*, ecc.) da effettuarsi in corso d'anno.

Il processo di pianificazione non può, inoltre, prescindere dal considerare l'impatto sull'attività di audit dei vincoli legati alla concessione di aiuti di Stato, in quanto potrebbero esplicitarsi specifiche richieste di intervento/controlli di audit. Si pone quindi la necessità per la Direzione CAE di identificare a priori e rafforzare attività da condurre su tematiche potenzialmente impattate dai reati di corruzione come il processo di negoziazione acquisti e i rapporti con i fornitori.

Infine, a livello consolidato, rileva evidenziare che la predisposizione del piano di audit da parte delle controllate italiane ed estere e delle filiali estere tiene necessariamente conto dagli obiettivi strategici di Gruppo in termini di mantenimento ovvero dismissione delle partecipazioni detenute/in chiusura.

In particolare nel caso delle controllate in vendita/chiusura/incorporazione, il piano è funzionale esclusivamente all'evento in questione; per le filiali estere in chiusura (Londra, New York e Hong Kong) il piano prevede interventi mirati con natura di *due diligence* aventi l'obiettivo di fare un esame complessivo dei processi in essere alla data di vendita/chiusura/trasferimento alla Capogruppo.

I piani di audit delle controllate che proseguiranno la propria attività ordinaria e quello della filiale estera di Shanghai seguono invece le medesime linee guida valide per la Capogruppo.

L'introduzione di nuovi elementi valutativi così come di nuove aree di indagine caratterizzate da rilevanti complessità (quali, ad esempio, le attività di *data quality validation*), unitamente all'incremento del numero di interventi richiesti obbligatoriamente ha, inoltre, comportato la necessità di un'evoluzione in corso d'anno dell'assetto organizzativo della Direzione CAE, un cui primo *step* ha già avuto luogo nella prima metà del 2017.

Approccio metodologico

La metodologia sottostante al processo di pianificazione è basata su di un *framework* che associa dati quantitativi di rischio alla valutazione qualitativa riveniente dall'attività di *Risk Control Assessment* (RCA) interna, al fine di ottenere un piano di azione costantemente allineato ai cambiamenti aziendali e del contesto esterno e interno.

Il modello agisce sostanzialmente su 4 fasi consecutive in sintesi rappresentate nel sottostante *flow chart*:



- STEP 1: RCA macroprocessi

Valutazione quali/quantitativa della rischiosità dei macroprocessi aziendali di *business* e non di *business* presenti in ARIS (attualmente 43 nel perimetro di audit e in continuo aggiornamento).

Ciascun Responsabile di Area/Servizio della DCAE esprime per ciascun macroprocesso aziendale un giudizio di rischiosità² valutandone:

- rilevanza aziendale
- impatto evoluzione contesto interno
- impatto evoluzione normative esterne
- efficacia del sistema dei controlli.

Al fine di ottenere una valutazione allineata ai mutamenti del profilo di rischio aziendale vengono forniti a supporto del giudizio espresso i seguenti elementi quantitativi sintetici:

- "*Risk Appetite Monitoring*": verifica andamentale RAF al 30.09.2017. Fornisce un monitoraggio per ciascun indicatore del RAF del rispetto degli obiettivi di Risk Appetite e dell'eventuale superamento delle soglie di *Risk Tolerance/Capacity*.
- "*Risk Relevance Classification*": classificazione dei rischi in fase di definizione del RAF sulla base della loro rilevanza.

L'integrazione delle valutazioni espresse porta alla formulazione di una graduatoria degli ambiti da presidiare, con l'individuazione di 19 macroprocessi rischiosi (di *business* e non di *business*), rientranti nelle classi di score R4 Rosso e R3 Arancione, da sottoporre allo *step* successivo, così come qui di seguito riportato:

² Cfr. Nota 1.

MACROPROCESSI DI BUSINESS (<i>catalogo dei processi di Gruppo ARIS</i>)
Credito
Gestione dei crediti problematici
Servizi di investimento
Gestione ordinaria del credito
Governo del credito
MACROPROCESSI NON DI BUSINESS (<i>catalogo dei processi di Gruppo ARIS</i>)
Contrasto al riciclaggio e al finanziamento del terrorismo
Data governance
Compliance
Erogazione ICT
Politiche Commerciali
Risk Management
Contabilità, fiscale e vigilanza
Demand
Sviluppo ICT
Risorse Umane
Prodotti
Canali di contatto con la clientela
Organizzazione
Organizzazione e Demand

- STEP 2: RCA processi

Valutazione qualitativa della rischioosità dei processi (di business e non di business).

La seconda fase di RCA prevede la valutazione qualitativa dei processi sottostanti ai macroprocessi risultati a maggior rischio nello STEP 1. Il giudizio di rischioosità è espresso dai Responsabili di Area/Servizio della DCAE sulla base della medesima scala di *rating* a criticità crescente³, utilizzata nello STEP 1.

A ulteriore supporto per la valutazione dei processi sono fornite le seguenti informazioni in ambito di *SREP coverage* rivenienti dal nuovo *framework SREP oriented* sviluppato dalla funzione:

- numerosità degli obiettivi di controllo associati a ciascun processo;
- livello di rilevanza attribuito a ciascun processo in base alla numerosità degli obiettivi di controllo associati.

Ciò consente di identificare i processi maggiormente impattati dal *framework* e, conseguentemente, di misurare il livello di copertura degli obiettivi di controllo *SREP*. Dal punto di vista metodologico, qualora tale livello di copertura non risulti soddisfacente, si rende necessario rivedere il perimetro dei processi da auditare prevedendone ulteriori ad alto impatto *SREP* (maggior numero di obiettivi di controllo collegati).

Per l'individuazione e la prioritizzazione dei processi da auditare rilevano, ovviamente, anche gli esiti di precedenti interventi di audit.

La fase di identificazione delle attività a maggior rischio ha evidenziato 29 processi di business e 12 processi non di business in fascia critica con score R4 Rosso e R3 Arancione.

Relativamente agli ambiti "di business" è risultato prioritario il presidio dei processi del Credito (Gestione massiva dei crediti problematici, Gestione recupero crediti a contenzioso, Definizione indirizzi e metodologie

³ Cfr. Nota 1.

in materia di crediti problematici). E' stato, inoltre, ritenuto necessario condurre accertamenti in materia di Servizi di investimento sul processo di Consulenza sugli Investimenti.

L'attività sul comparto delle filiali estere sarà strettamente legata agli sviluppi degli obiettivi strategici di Gruppo e ai commitment CE che ne prevedono, per 3 di loro (Londra, New York e Hong Kong), la chiusura entro il 2018.

Relativamente ai processi "non di *business*", sono stati valutati come maggiormente rischiosi i processi riconducibili agli adempimenti in materia di riciclaggio e finanziamento al terrorismo. Particolare attenzione dovrà essere rivolta ai presidi dei canali di contatto con la clientela (WEB e *mobile banking*) e, in ambito di politiche commerciali, al processo di analisi commerciale di mercato (prodotti, *pricing*, canali).

- **STEP 3: Focusing**

Integrazione con Mandatory Audit /SREP Coverage/Pianificazione annuale JST/Copertura RA JST

La fase di *focusing* ha permesso l'identificazione dei singoli interventi di audit che andranno a comporre la pianificazione 2018, individuati a presidio dei processi critici segnalati in fase di RCA ed integrati sulla base di:

- Mandatory Audit
- ambiti di attenzione regolamentare ed eventuali richieste delle Autorità di vigilanza
- impatti del progetto ARGO 3 (*finding* della OSI-1238) e *follow-up* ARGO 2 e altre *remedial action* conseguenti ai *finding* di vigilanza
- *SREP coverage*
- indicazioni/richieste ricevute dal Collegio Sindacale e dall'OdV 231
- aspetti di criticità emersi sulla base di indirizzi strategici.

Sono stati, inoltre, considerati anche processi collegati a taluni macroprocessi non evidenziati come critici dal risultato del framework di RCA, ma per i quali si reputa comunque necessario intervenire (erogazione ICT connessa agli aspetti di cybersecurity, sistema antifrode, data governance, data quality).

In linea generale, la copertura è assicurata, contemporaneamente, da verifiche sui processi centrali e da interventi capillari sugli stessi processi agiti dalla Rete territoriale - in ottica di *continuous monitoring* e di presidio della complessiva *Risk Culture* aziendale. Per la Rete, oltre a tenere conto dei risultati del modello di *Risk Control Assessment*, sono stati anche considerati gli obiettivi strategici in un'ottica di medio termine e valutati gli esiti degli accertamenti effettuati nei precedenti esercizi.

L'*effort* sulla Rete è quindi orientato al processo centrale, con interventi sempre più specifici sulle singole unità, ma ricondotti a una visione d'insieme volta a fornire *assurance* sulla complessiva gestione dei processi. I nuovi obiettivi di audit prevedono lo sviluppo sempre più stringente di azioni integrate tra settori specialistici e settori che verificano i processi sulla Rete territoriale, al fine di rafforzare le possibili sinergie ed accrescendo l'efficacia dell'*internal audit*.

A livello di Gruppo MPS viene utilizzato un approccio integrato per la pianificazione delle attività di audit che coinvolge sia la Direzione Chief Audit Executive sia le corrispondenti funzioni di *internal audit* presso le società controllate.

La componente qualitativa di analisi e valutazione della rischiosità dei macroprocessi impattati dallo specifico *business* di ciascuna società, finalizzata all'individuazione dei principali ambiti da sottoporre ad audit, è quindi estesa alle *legal entity*, pur nell'esigenza di individuare un piano di attività per il 2018 che sia coerente con gli obiettivi strategici di Gruppo che prevedono la cessione/chiusura/incorporazione di alcune società.

Il piano assicura, inoltre, il pronto recepimento delle segnalazioni di allerta provenienti dal sistema di *fraud detection* (FDS) e da eventuali *whistleblowing* che possono dare luogo a specifici interventi.

- STEP 4: Meeting con Top Management, Organi di controllo e apicali

I criteri e le priorità assegnate sono stati oggetto di confronto con l'Amministratore Delegato a seguito del quale sono state accolte ulteriori indicazioni su specifiche aree di attenzione.

Per arrivare alla definizione del Piano di Audit 2018 sono stati, infine, tenuti incontri dedicati con il Collegio Sindacale e inviate informative all'Organismo di Vigilanza 231/2001 al fine di coglierne le eventuali richieste di intervento su particolari ambiti di rischio.

Il piano di audit, successivamente all'approvazione, sarà presentato al JST BCE.

2. Il piano di audit 2018

Il piano annuale è la sintesi dell'insieme delle attività di audit da condurre nell'anno di riferimento, con l'indicazione della tipologia, delle modalità, dei tempi e della frequenza di realizzazione, nonché delle conseguenti risorse.

Il piano di audit per il 2018 si colloca al primo anno di un nuovo ciclo di revisione triennale per il quale sono stati definiti i macroambiti di copertura in arco Piano, diventandone fattore di calibrazione/correzione per l'orizzonte del singolo esercizio sulla base sia degli esiti rivenienti dal *framework* di *Risk Control Assessment* sia delle linee guida di vigilanza espresse dal supervisore europeo.

La pianificazione annuale è stata definita individuando come base un impiego medio di 215 giorni/uomo per FTE.

L'Audit Plan 2018 sulla base della metodologia *SREP oriented* prevede nel complesso la copertura di 37 processi declinati nel catalogo dei processi di Gruppo ARIS e individuati sulla base della loro rilevanza *SREP*; verificando tutti gli obiettivi di controllo sottostanti tali processi, si consegue una copertura massima di circa il 61% del totale obiettivi.

I processi a maggior rilevanza *SREP*, inclusi nella pianificazione 2018, sono i seguenti:

- Governo del *Risk Appetite Framework*
- Gestione del rischio di liquidità
- Valutazione dell'adeguatezza patrimoniale (ICAAP - *Internal Capital Adequacy Assessment Process*)
- *Corporate Governance* (assessment della conformità alle linee guida dell'EBA in materia di *internal governance* EBA/GL/2017/11 che entreranno in vigore dal 30.06.2018)
- Valutazione dell'adeguatezza della liquidità (ILAAP - *Internal Liquidity Adequacy Assessment Process*)
- Attuazione delle politiche di remunerazione e incentivazione.

La quota principale delle attività di audit è assorbita dagli interventi di revisione (cd. attività "*core*"); sono, inoltre, previste tutte le diverse tipologie di attività contemplate dagli *standard* professionali, tra cui quella di *consulting* con lo scopo di rafforzare il ruolo consulenziale dell'internal audit e di *follow-up*, con l'obiettivo di efficientare ulteriormente il processo di mitigazione dei *finding* individuati.

Il piano ricomprende tutte le ispezioni cd. "*mandatory*" previste dalla regolamentazione interna ed esterna, alla quale si aggiungono le eventuali richieste del JST della BCE (*finding* OSI, *thematic review*, esiti valutazione *SREP*, ecc.).

Una consistente quota dell'attività sarà dedicata alle tematiche creditizie e, in particolare, alla verifica della realizzazione degli interventi previsti a seguito dei *finding* rilevati nell'OSI-1238 "*Credit and counterparty risk management and risk control system*" (Progetto ARGO 3).

Data Quality Assurance

Negli ultimi anni è considerevolmente aumentata l'attenzione delle Autorità di vigilanza al complesso processo di gestione dei dati all'interno degli istituti bancari. Patrimonio informativo, tecnologie e sistemi, tuttavia, non rappresentano che una visione parziale e incompleta del complesso mondo delle decisioni aziendali.

Il passaggio dal dato inteso come informazione alla conoscenza si basa, tra gli altri, su due presupposti fondamentali: la cultura aziendale e il *data quality*. Per questo, specie nel più ampio perimetro del processo *SREP*, alla funzione di internal audit viene chiesto sempre più spesso di condurre interventi di analisi e revisione dove, accanto ai tradizionali aspetti di natura prettamente IT ("*Accuracy*" e "*Reliability*",

"Completeness", "Punctuality", "Consistency" e "Stability"), si affianca, in maniera spesso preponderante, il tema della plausibilità del dato (affrontato solitamente con metodi statistici) e della sua correttezza⁴, intesa come verifica che le informazioni fornite rispondano fedelmente ("*faithful mirroring*") alla situazione vigente al momento della trasmissione dei dati.

Questi interventi di riconciliazione tra basi dati diverse acquistano sempre maggiore rilevanza e impegno soprattutto se confrontati con l'approccio delle Autorità di vigilanza, le quali stanno adottando sempre più una visione di sintesi che ingloba sia i sistemi di natura contabile-amministrativa sia quelli gestionali-direzionali indirizzati al monitoraggio e controllo degli aspetti commerciali, di *risk management* e di analisi della redditività. In questo contesto rilevano sia esperienze di natura "*on-demand*" quali ad esempio il *SSM Liquidity Exercise* effettuato nel 2017 sia interventi più istituzionali come la revisione sui modelli interni (TRIM) nelle cui linee guida è messo in particolare evidenza il ruolo attribuito alla funzione di Internal Audit nel complesso processo di *data quality assurance* per quanto riguarda i modelli interni per la stima dei requisiti di capitale⁵.

In considerazione, pertanto, della rilevanza della materia e delle aspettative della vigilanza europea, sono stati pianificati per il 2018 due specifici interventi di *data quality assurance* per testare la riconciliazione dei dati in materia di PD e LGD. Un congruo *buffer* di giornate uomo è stato considerato per potenziali ulteriori richieste su tale fronte da parte di BCE.

Analisi consolidata di Gruppo

Talune macrotematiche a forte impatto in termini di rischio saranno, per la prima volta, oggetto di analisi a livello consolidato impattando contemporaneamente su più entità del Gruppo.

Tale tipologia di analisi consolidata è stata prevista per gli interventi a piano della Capogruppo sui seguenti 5 macro ambiti:

- 1) Gestione fornitori, attività negoziale e contratti;
- 2) Compliance: modello accentrato di Gruppo con focus su Widiba e MPS CS;
- 3) AML (Segnalazione Operazioni Sospette) su BMPS, Widiba e MPS Fiduciaria;
- 4) MiFID II (processo/modello/modalità distributive/controlli di 1° livello);
- 5) Ethical Hacking su BMPS, filiale di New York e Widiba.

L'approccio consolidato sarà perseguito anche nella gestione delle criticità rilevate nel corso di tutte le revisioni a piano. Ciascun gap evidenziato su di uno specifico processo sarà diffuso a livello di Gruppo in modo che ne sia presa coscienza anche da parte delle entità non coinvolte nella revisione ma che, agendo sullo stesso processo, potrebbero beneficiare delle azioni di rimedio proposte senza attendere l'intervento specifico da parte della funzione di audit.

In tale ottica possono essere individuati ambiti di condivisione e sinergie da portare a fattor comune per la mitigazione delle criticità.

Controlli di 1° livello

Il tema dell'adeguatezza dei controlli di 1° livello è l'elemento trasversale della pianificazione 2018.

⁴ "Supervisory Data Quality Framework", BCE, Presentazione alla *Supervisory Reporting Conference* 28.11.2016.

⁵ *Guide for the Targeted Review of Internal Models - TRIM*, BCE, febbraio 2017.

L'attenzione al corretto svolgimento delle attività da parte delle strutture di linea, le prime responsabili del processo di gestione dei rischi, sarà costante in tutti gli ambiti che comportano presidi di primo livello (Credito, Servizi di investimento, AML, ecc.) anche laddove non siano stati pianificati interventi specifici.

Per la Rete commerciale, l'adeguatezza dei controlli di 1° Livello sarà oggetto di particolare *focus* negli interventi sulle Strutture di Presidio Territoriale (Direzioni Territoriali).

Al fine di sfruttare in maniera efficace le possibili sinergie tra auditor specialistici e auditor di Rete è prevista un'attività in *joint* in ambito MiFID II, sempre sulla corretta esecuzione delle attività di linea.

Analisi comportamentale

Prosegue e si consolida l'attività di consulenza alla Rete finalizzata al rafforzamento della cultura del rischio.

L'attività di audit sarà, pertanto, volta a valutare la complessiva efficacia dei processi di controllo del *Conduct Risk*, facendosi promotrice della *risk culture* aziendale.

Il ricorso all'analisi comportamentale sarà previsto nell'ambito delle revisioni a piano ogniqualvolta se ne renderà possibile e opportuna l'applicazione.

Specifiche attività di *assessment* in ambito comportamentale riguarderanno il Processo di Gestione Anticipi e la tematica MiFID II.

Joint audit

La pianificazione 2018 prevede un numero di interventi di audit ridotto rispetto agli scorsi anni, privilegiando tipologie di attività più estese in termini di perimetro e profondità di analisi.

Tale nuovo approccio richiede e incentiva una maggiore integrazione fra le due Aree della funzione (specialistica e Rete/canali distributivi) favorendo la creazione di *team* misti tra risorse specializzate sugli interventi di processo e auditor di Rete/canali distributivi.

Sono, al momento, identificati i seguenti interventi da effettuare in *joint audit*:

- MiFID II (processo/modello e modalità distributive/controlli di 1° livello)
- *Covered Bond*
- SIRIO: piattaforma gestione contenzioso (processo esternalizzato)
- IFRS9
- Gestione processo successioni.

Per quanto concerne la filiera distributiva, la pianificazione contempla, altresì, il presidio *in servicing* sui canali di Widiba (Negozi/Consulenti Finanziari e Negozi Axa) e sui Presidi Territoriali Specialistici BMPS (Centri Private, Family Office).

Sono stati condivisi e approvati i piani di audit delle società controllate dove è presente una funzione di internal audit decentrata. La pianificazione è risultata allineata alle indicazioni fornite dalla scrivente funzione e coerente con il nuovo Piano di Ristrutturazione e agli obiettivi strategici di Gruppo. Si evidenzia che le attività pianificate saranno suscettibili di potenziali variazioni che potrebbero derivare dall'evoluzione e realizzazione dei citati obiettivi strategici.

Allo stato attuale sono previsti 12 interventi da parte della locale funzione di internal audit per le due società estere, 4 per MPS Leasing & Factoring e 13 per MPS Capital Services.

Per le controllate la cui funzione di internal audit, sulla base di specifici contratti di *service level agreement*, è svolta in *outsourcing* dalla Direzione Chief Audit Executive (Widiba, MPS Fiduciaria, Integra, Magazzini Generali di Mantova SpA, Microcredito) le attività per il 2018 sono ricomprese nella pianificazione della Capogruppo.

Con riferimento invece al Consorzio Operativo di Gruppo, le attività di audit 2018 saranno effettuate prevalentemente dalla Capogruppo in modalità accentrata e ricomprese nella presente pianificazione in ambito *IT e operation*.

Relativamente alle filiali estere per le quali è prevista la cessazione delle attività (Londra, New York e Hong Kong), i piani per il 2018 sono stati condivisi con la Direzione Chief Audit Executive indirizzando l'attività in ottica di *due diligence* sui principali processi delle strutture (HR, *Institutions, Economics, Operations*). Per la filiale di Shanghai, nel cui caso è previsto il prosieguo dell'attività, il piano condiviso con la Capogruppo prevede, per il 2018, 8 attività di audit.

Un ruolo non secondario in termini di *effort* è assorbito dall'azione di rendicontazione e comunicazione verso gli Organi aziendali e di controllo, nonché nei confronti del supervisore europeo.

Particolare attenzione viene dedicata alla formazione delle risorse volta all'accrescimento e al consolidamento delle competenze professionali, nell'ottica di continuo aggiornamento. Gli internal auditor del Gruppo MPS sono incoraggiati a dimostrare la propria competenza conseguendo le opportune certificazioni e qualifiche professionali come quella di "*Certified Internal Auditor*" (CIA) e altre certificazioni rilasciate dal "*The Institute of Internal Auditors*" (IIA) - riferimento internazionale per gli *standard* professionali - nonché da altri organismi professionali riconosciuti.

L'*audit plan* prevede al suo interno un *buffer* di giorni/uomo da utilizzare per garantire un certo grado di flessibilità e adeguati presidi, affinché eventuali situazioni impreviste siano comunque gestite con prontezza e indipendentemente dalla pianificazione ordinaria.

Il dimensionamento *target* per il 2018 è di 175 risorse; la ripartizione dell'attività è stata fatta, in via prudenziale, sulla base di circa 170 risorse, tenuto conto dell'attuale sottodimensionamento dovuto alla consistente riduzione avvenuta nel corso dello scorso anno per adesione al Fondo di Solidarietà (22 risorse) e per trasferimenti ad altre strutture (12 risorse); il previsto ingresso (nel periodo gennaio-marzo) di 14 nuove risorse selezionate con l'iniziativa WOO ("*We Open Opportunities*") comporta un considerevole aumento delle ore destinate alla formazione.

Rileva, inoltre, l'eventuale ulteriore impatto delle nuove adesioni all'esodo previste anche per il 2018 (potenzialmente circa 10 unità) in considerazione del quale si renderà necessario individuare in corso d'anno ulteriori risorse per raggiungere il dimensionamento *target*.

Di seguito si fornisce la sintesi della pianificazione 2018, in termini di giorni/uomo assorbiti da ciascuna tipologia di attività:

RIPARTIZIONE TOTALE ATTIVITA' 2018		
Tipologia attività	GG/uomo	% GG Uomo
Interventi di revisione	20.904	58
Analisi a distanza	2.752	7
Attività direzionali e relazionali	5.042	14
Attività diverse	4.710	13
Attività di consulting	685	2
Progetti gestiti e coordinati dalla Direzione Chief Audit Executive	210	1
Formazione	1.991	5
TOTALI	36.294	100

Interventi di revisione

Gli interventi di revisione programmati per il 2018 risultano 46 (di cui 23 obbligatori) per le società e i processi centrali.

Le attività "core" della funzione sono state definite considerando quale principale driver la volontà di ampliare il perimetro degli interventi favorendo una maggiore integrazione fra le diverse strutture della Direzione CAE e riducendo allo stesso tempo la numerosità degli audit. Tale approccio permette di verificare con maggiore profondità alcuni ambiti utilizzando audit *team* misti, cioè composti sia da auditor specialistici dei processi centrali sia auditor di Rete commerciale.

Tutte le ispezioni obbligatorie, cioè previste dalla regolamentazione interna ed esterna, sono state ricomprese nel piano: convalida sistemi avanzati AIRB e AMA, RAF, Politiche di Remunerazione, *Covered Bond*, ICAAP, ILAAP, Controlli *Privacy* nonché, in ambito *IT*, piano e *test Business Continuity Management* (BCM), *Disaster Recovery* (DR) ed *Ethical Hacking* per la filiale di New York.

A queste si aggiungono gli interventi necessari per garantire il seguimiento dei *finding* rilevati dalla BCE a seguito degli esiti della OSI-1238.

L'effort sulla Rete commerciale e dei canali distributivi è indirizzato ad integrare in maniera sinergica la copertura dei processi a maggior rischio. Per il 2018 si conferma la prevalente attenzione verso le strutture di presidio territoriale (Aree e Direzioni Territoriali) con specifico focus sui controlli di 1° livello (*monitoring e reporting*). Un eventuale accesso alle strutture di livello più basso (le singole dipendenze) è volto a completare la valutazione della struttura di riporto gerarchico.

Il tema dell'adeguatezza dei controlli di 1° livello è uno dei fili conduttori della pianificazione 2018. L'attenzione al corretto svolgimento delle attività da parte delle strutture operative, la prima linea di difesa del processo di gestione dei rischi, sarà costante in tutti gli ambiti che comportano presidi «di linea» (Credito, Servizi di investimento, AML, ecc.) indipendentemente dall'effettuazione di interventi di audit specifici.

Al fine di sfruttare in maniera efficace le possibili sinergie tra auditor specialistici e auditor di Rete, anche sul tema del presidio dei controlli di prima linea, è prevista un'attività in *joint* in ambito MiFID II.

La verifica a distanza (*remote control*) dei principali processi agiti dalla Rete è prevalentemente incentrata su ambiti di natura comportamentale; l'analisi comportamentale verrà utilizzata nell'ambito delle revisioni a piano ogniqualevolta se ne renderà possibile e opportuna l'applicazione.

Ulteriori ambiti di verifica pianificati per il 2018 riguardano, in particolare, la gestione scoperti/sconfinamenti con Istruttoria Veloce, la gestione del processo successioni (*joint audit*) e l'attività d'intermediazione in oro.

Il piano stima, sulla base del *trend* storico, 60 interventi per indagini interne su irregolarità dei dipendenti.

Sono state condivise con il Collegio Sindacale materie di particolare interesse per le quali la funzione di audit fornirà supporto operativo con le seguenti verifiche:

- Gestione fornitori, attività negoziale e contratti
- MiFID II (focus processo/modello e modalità distributiva)
- *Corporate Governance* (*assessment* della conformità alle linee guida dell'EBA in materia di *internal governance* EBA/GL/2017/11 che entreranno in vigore dal 30.06.2018).

Il Collegio Sindacale sarà, altresì, destinatario dei rapporti relativi alle tematiche legate a OSI-1238 (ARGO 3) che saranno seguite dalla Direzione CAE con specifici interventi e per quanto concerne gli ambiti di AML in ottica di monitoraggio delle attività realizzate nel 2017.

In particolare per gli interventi sulle strutture di Rete, la funzione fornirà il consueto supporto operativo al Collegio in 10 verifiche di Direzioni Territoriali (5 ordinarie e 5 di *follow-up*) focalizzate su *origination* del credito, *document management* e adeguatezza dei controlli di 1° Livello (con focus MiFID II).

Relativamente ai reati 231/2001, sono riconducibili alla valutazione dell'efficacia del modello e saranno relazionate all'Organismo di Vigilanza 231 le revisioni su:

- *Gestione fornitori, attività negoziali e contratti*
- *Compliance: modello accentrato di Gruppo con focus su Widiba e MPS Capital Services*
- *AML (Segnalazione Operazioni Sospette) con focus su BMPS, Widiba e MPS Fiduciaria.*

La ripartizione delle revisioni centrali per struttura/processo è riepilogata nella sottostante tabella:

PROCESSO/STRUTTURA	Numero	N. GG.	% GG. Uomo
SOCIETA'/BANCHE ESTERE (di cui IT audit)	8 (2)	715	9
ANALISI CONSOLIDATA DI GRUPPO (di cui IT audit)	5 (1)	1.130	15
PROCESSI CENTRALI	29	5.130	67
IT AUDIT	4	720	9
TOTALE COMPLESSIVO	46	7.695	100

I principali ambiti dell'attività di audit sui processi centrali sono di seguito rappresentati. Negli allegati n. 2 e n. 3 viene fornito il dettaglio degli interventi pianificati per il 2018.

✓ **Credito**

Previsto in primis il presidio per i processi centrali di tutte le tematiche legate alla OSI-1238 BCE (ARGO 3) evidenziate al momento nella draft⁶ *follow up letter* datata 29.11.2017.

Nello specifico il supervisore ha evidenziato criticità in ambito di gestione delle garanzie (*collaterals*) e sul funzionamento del sistema degli *early warnings* (con particolare riferimento all'identificazione del *forbearance*). Per quanto concerne gli NPL sono stati rilevati *finding* relativi alla sottostima delle metriche di calcolo degli accantonamenti e sul mancato aggiornamento dei *Business Plan*.

Tali tematiche saranno seguite dalla Direzione CAE con i seguenti specifici interventi:

- *Double and multicounting collaterals (finding #3 OSI-1238)*
- *Credit Default Detection: efficacia e tempi riguardo al processo di identificazione del forbearance (finding #1, #6 e #7 OSI-1238);*
- *Underestimation of key metrics for calculating loan loss provisions (finding #8 OSI-1238)*
- *Business plan (finding #9 OSI-1238).*

Gli esiti delle verifiche saranno relazionati al Collegio Sindacale, al quale organo il JST ha chiesto di verificare l'implementazione delle azioni di rimedio previste nell'Action Plan.

La Banca è chiamata a fornire una rendicontazione trimestrale sullo stato di avanzamento delle attività previste che dovrà essere accompagnata da una relazione della funzione di internal audit che ne valuti l'appropriatezza.

Si mantiene alto il livello di attenzione sul monitoraggio operativo e sulla gestione dei crediti problematici anche con un intervento su *High Risk* e uno sul *processo gestione massiva crediti Unlikely to Pay*. Un ulteriore accertamento riguarderà il *processo di gestione dei crediti ristrutturati*. Sarà effettuata una verifica su *SIRIO piattaforma gestione del contenzioso* - processo esternalizzato (*joint audit*).

⁶ Al momento in cui il presente piano è redatto non è ancora pervenuta la *final follow-up letter*.

La pianificazione prevede la consueta attività obbligatoria su *covered bond (joint audit)* e, relativamente alle controllate, l'intervento in *servicing* su Microcredito di Solidarietà.

I processi creditizi saranno anche oggetto di verifica negli accertamenti presso le strutture di presidio territoriale (in particolare con *focus* su *origination*, *document management* e adeguatezza dei controlli di 1° livello) e, nel loro complesso, in specifici interventi settoriali/tematici sulle filiali.

Relativamente alla gestione dei prodotti del credito, è prevista un'attività di *assessment* sul *processo di gestione anticipi*. Su tale processo è, inoltre, previsto un intervento di follow up al fine di monitorare lo stato di conseguimento delle attività richieste nella verifica del precedente anno.

✓ **Macchina Operativa**

L'impianto operativo e gestionale del Gruppo MPS sarà valutato con specifici interventi sui macroprocessi ritenuti a maggior rischio.

Il vincolo legato alla concessione di aiuti di Stato ha indotto la funzione di audit a pianificare un intervento specifico sulla *gestione fornitori, attività negoziale e contratti*, ambito fortemente impattabile dai reati di corruzione. L'analisi è una delle 5 che sarà condotta a livello di Gruppo.

In ambito fiscale/contabile l'introduzione del *principio contabile* IFRS 9 e le modifiche regolamentari che ne derivano hanno evidenziato l'esigenza di condurre un accertamento (*joint audit*) sui nuovi schemi contabili considerati ad alto impatto sull'intera operatività della Banca.

Sarà oggetto di un ulteriore intervento la *gestione del processo delle successioni*, esternalizzato a Fruendo. Saranno, inoltre, verificati il *processo fiscale sui servizi di investimento*, la *gestione ATM* e la *dematerializzazione disposizioni operative e firma grafometrica*.

Relativamente al perimetro societario, sarà valutata l'efficacia dei controlli su Magazzini Generali di Mantova.

✓ **Finanza proprietaria**

Gli aspetti di gestione dei portafogli di proprietà saranno presidiati con i seguenti interventi richiesti dai regolamenti specifici:

- *processo di contribuzione alla determinazione del parametro Euribor e Eonia*;
- *processo di segnalazione al FITD (Fondo Interbancario di Tutela dei Depositi)*.

✓ **Distribuzione commerciale**

In tema di politiche commerciali e filiera distributiva è previsto un intervento di processo a livello di Gruppo con focus *MiFID II (joint audit)*.

Una verifica sarà indirizzata a testare l'idoneità della *piattaforma WISE* a supporto della gestione dei servizi d'investimento da parte dei Consulenti Finanziari di Banca Widiba. Un ulteriore intervento sulla controllata avrà ad oggetto la redditività del prodotto mutui. Entrambe le attività saranno effettuate *in servicing* per Widiba secondo quanto disposto dal contratto di *Service Level Agreement*.

La pianificazione su Widiba contempla, altresì, il presidio dei canali distributivi (Negozi/Consulenti Finanziari e Negozi AXA) con circa 40 interventi in loco.

Per quanto riguarda le restanti controllate per le quali la scrivente funzione effettua attività di audit *in servicing*, è stato posto a piano un assessment sui *mandati societari* di MPS Fiduciaria ed un intervento sul *processo carte gestite* da Integra.

Sulla Rete commerciale sono previsti accertamenti volti a verificare la modalità di attuazione dei processi di approccio alla clientela relativi ai servizi di investimento con particolare attenzione al primo livello di controllo. Ulteriori attività riguarderanno il canale distributivo dei Presidi Territoriali Specialistici (Centri Private, Family Office e Uffici Commerciali Territoriali).

✓ **Governance, controllo rischi e conformità**

I processi di *risk management* e *compliance*, con 16 interventi di revisione dedicati, assorbono una cospicua aliquota dell'*effort* sui processi centrali e sono prevalentemente coperti dagli audit "obbligatori". In particolare sulla validazione modelli sono previste le seguenti attività annuali:

- *convalida AIRB*
- *convalida AMA*
- *ICAAP*
- *ILAAP*.

E', inoltre, pianificata una verifica volta a valutare l'efficacia del *processo di definizione del RAF*.

Relativamente agli aspetti di governo e di valutazione del rischio strategico sono stati individuati un intervento sul *business model* e un *assessment* sulla *Corporate Governance*, quest'ultimo per verificare la conformità alle linee guida dell'EBA in materia di *internal governance* (EBA/GL/2017/11) che entreranno in vigore dal 30.06.2018.

In ambito di gestione del rischio di non conformità saranno condotti accertamenti a livello consolidato su *Compliance* (modello accentrato di Gruppo con *focus* su Widiba e MPS Capital Services), *AML – Segnalazione Operazioni Sospette* (con *focus* su BMPS, Widiba, e MP Fiduciaria) e su *MiFID II - processo/modello/modalità distributive/controlli di 1° livello (joint audit)*.

In ottemperanza alle richieste avanzate dal supervisore in tema di qualità dei dati e sulla base di quanto definito dalla TRIM (*Targeted Review of Internal Model*) è stato pianificato un intervento sulla *data quality di riconciliazione LGD*. Sui modelli del credito sarà inoltre effettuata un'*analisi dei modelli PD* anche in ottica *data quality* di riconciliazione correlata al *finding #4* dell'OSI-1238 di BCE (ARGO 3). Tali verifiche, come in precedenza evidenziato, terranno conto anche dell'annunciata *Internal Model Investigation* (IMI) da parte della BCE nell'ambito delle priorità 2018 avente a oggetto l'approvazione delle modifiche apportate al modello interno AIRB per la determinazione dei requisiti patrimoniali per il rischio di credito (ELBE, LGD per le attività in *default*), su cui la Banca ha fatto istanza nel corso del 2017.

Due specifici interventi saranno svolti sull'evoluzione *Pillar 2 (focus modifiche modello IRRB)* - tema indicato dal SSM tra le priorità 2018 in ambito di *business model* e determinanti della redditività e oggetto di una annunciata OSI nel 2018 da parte della BCE- e sui rischi di *controparte e mercato (focus su modello CCR - Credit Counterparty Risk e modifiche market risk FRTB - Fundamental Review of Trading Book)*.

Sarà condotta la verifica obbligatoria in materia di tutela dei dati personali sui *Controlli Privacy*.

Ai fini della relazione obbligatoria sulle *politiche e prassi di remunerazione* sarà effettuato il consueto accertamento annuale i cui esiti saranno relazionati al CdA.

✓ **Information Technology**

In materia di Sicurezza *IT*, trasversale alla maggior parte dei processi aziendali, sono stati pianificati su tutto il perimetro di Gruppo 7 interventi. Sono previsti i consueti accertamenti di *Business Continuity Management* e *Disaster Recovery*.

Gli interventi di audit pianificati tengono conto delle attività di vigilanza 2018 annunciate da BCE tra le quali è ricompresa una OSI sull'*IT Risk*.

I *vulnerability test* per attacchi *hacker* saranno effettuati a livello consolidato su tutti i sistemi di BMPS, Widiba e della filiale di New York, quest'ultimo obbligatorio in quanto prescritto dalla FED. Sempre in tema di *cybersecurity* saranno testati i sistemi *antifrode* di Widiba su Home Banking.

Ulteriori verifiche IT *specialized* riguarderanno la *Data Governance* (focus su metodologie, flussi e procedure) e la *Data Quality* (specificatamente in merito alla PD).

Infine, relativamente alle controllate estere, è stato posto a piano un intervento IT su controllo accessi per MP Belgio (in *joint audit* con la locale funzione IA).

Attività di consulting

L'attività di *consulting* è insita nella definizione stessa di attività di internal audit unitamente alla tipica attività di *assurance* (verifiche di audit) e con questa contribuisce al rafforzamento dei processi aziendali nell'ottica della sana e prudente gestione dei rischi.

Questa tipologia comprende l'affiancamento dell'internal audit alle funzioni di *business* su particolari iniziative progettuali relative a tematiche di *compliance*, *governance*, sistema dei controlli, rivisitazione dei processi, ecc..

Analisi a distanza

L'attività a distanza è assorbita prevalentemente dal monitoraggio dei fenomeni rilevanti ed al seguito dello stato realizzativo delle azioni correttive individuate.

Costante l'attenzione posta nell'attività di *follow-up* ai fini dell'efficacia dell'azione di audit; in particolare per quanto concerne la risoluzione delle criticità ancora aperte sui processi centrali, saranno strettamente monitorate le azioni di mitigazione relative agli interventi più datati.

Il *follow-up* sulle strutture di Rete sarà mirato ai soli *gap* di processo riconducibili alle strutture centrali, rilevati sia nel corso delle indagini sulle strutture territoriali, sia in interventi di analisi fenomeni.

Uno dei primari obiettivi per il 2018 è rappresentato dall'efficientamento della gestione a livello consolidato delle anomalie evidenziate nel corso delle revisioni.

Ciascuna criticità rilevata su di uno specifico processo dovrà essere diffusa a livello di Gruppo in modo che ne sia presa coscienza anche da parte delle entità non coinvolte nella revisione ma che, agendo sullo stesso processo, potrebbero presentare uguale anomalia.

Lo scopo della diffusione delle informazioni a livello di Gruppo è quello di divulgare tempestivamente gli ambiti di miglioramento senza attendere l'intervento specifico della funzione di audit.

L'analisi a distanza (*remote control*) dei principali processi agiti dalla Rete sarà incentrata, in particolare, sulla gestione e sull'efficacia dei presidi di controllo in materia AML. Sul processo di gestione anticipi è prevista un'attività di *follow-up* al fine di monitorare lo stato di conseguimento delle *remediation* richieste nella verifica del 2017.

Attività direzionale e relazionale

Tale attività si collega alla produzione di relazioni istituzionali periodiche oltre che di specifiche comunicazioni estemporanee, i cui destinatari sono:

- gli Organi aziendali (es: *report* trimestrali attività svolta, *Audit Plan*, relazioni annuali, ecc.);
- le Autorità di vigilanza, ivi comprese sia le relazioni "obbligatorie" su specifiche tematiche (es. modelli avanzati, società controllate, processi esternalizzati, servizi d'investimento, ecc.), sia il complesso delle comunicazioni, ad evento, da e verso le medesime Autorità a seguito delle ispezioni condotte;

- le altre Funzioni aziendali di controllo (secondo quanto disciplinato per lo scambio dei flussi dal documento normativo D1915).

Nella presente sezione viene, altresì, compreso il complessivo coordinamento delle attività e delle risorse da parte dei responsabili delle strutture della Direzione Chief Audit Executive.

Adeguate reportistica verrà prodotta per la rendicontazione dell'attività in *servicing* (MPS Fiduciaria, Widiba, Microcredito di Solidarietà, Maganizzini Generali di Mantova e Integra).

Attività diverse

In tale tipologia sono incluse, prevalentemente, le attività riconducibili alla gestione segretariale e amministrativa della funzione nel suo complesso (logistica, economato, sicurezze, etc.), ivi compresi il presidio e la manutenzione degli strumenti informatici in dotazione alle risorse, oltre che la gestione dei relativi profili abilitativi.

Rilevante impegno è assorbito dalla gestione delle attività di *fraud detection* e dalla predisposizione della reportistica per la Commissione Affari Disciplinari nei procedimenti in giudizio dei dipendenti.

Un congruo numero di giornate/uomo per l'attività di ricezione e gestione di eventuali segnalazioni di violazioni (*whistleblowing*) inoltrate da parte dei dipendenti tramite la specifica piattaforma.

Progetti gestiti e coordinati dalla Direzione Chief Audit Executive

Una specifico fondo di 350 mila euro è stato stanziato a disposizione del Chief Audit Executive - in ottica strategico direzionale - al fine di permettere alla funzione di rispondere tempestivamente alle sfide del nuovo contesto, individuando soluzioni che garantiscano anche il rispetto delle aspettative dell'Autorità di vigilanza in un'ottica di massima efficienza ed efficacia dei controlli.

Nell'ambito delle iniziative progettuali per il 2018, la Direzione Chief Audit Executive ha provveduto ad individuare e comunicare all'owner del *Master Plan* gli interventi prioritari relativi Sistemi Informativi di Audit (ESC Audit; FDS) a fronte dei quali è stato previsto un *plafond* di 290 mila euro.

Sono, infine, stati stanziati 15 mila euro per la *membership* collettiva all'Associazione Italiana Internal Auditor (AIIA) fruibile da tutte le risorse della funzione e utile al costante aggiornamento professionale.

Nella tabella seguente si riepilogano gli importi di spesa a *budget*:

Tipologia MP	Descrizione attività	Importo (Euro mgl)
MP Spese progettuali	Sviluppo sistemi informativi di audit	290
MP Consulenze	Fondo straordinario a disposizione del CAE	350
MP Logistico Economale	Membership AIIA	15
TOTALE BUDGET		655

Formazione

Complessivamente il piano di formazione della Direzione Chief Audit Executive per il 2018 prevede circa 2.000 gg/uomo per la crescita professionale degli auditor; una consistente aliquota sarà destinata alla formazione delle nuove risorse selezionate con l'iniziativa "*WOO-We Open Opportunities*". Il *plafond* dedicato, approvato tramite la Funzione Formazione, ammonta a 120 mila euro.

In linea con quanto disciplinato dagli *standard* internazionali di categoria, gli internal auditor devono possedere le conoscenze, la capacità e le competenze necessarie all'adempimento delle proprie responsabilità individuali attraverso un aggiornamento professionale continuo.

Il piano di crescita professionale prevede la fruizione di progetti di formazione massiva/diplomi su tematiche specialistiche erogati da AIIA (*Associazione Italiana Internal Auditor*) in continuità con quanto già effettuato con successo nei precedenti anni.

E' stata rinnovata per il 2018 la *membership* alla piattaforma *web* AIIA, il cui accesso è esteso a tutte le risorse della funzione per supporto consulenziale e formativo.

Le risorse sono incentivate al conseguimento della certificazione CIA, rilasciata da AIIA - ufficialmente riconosciuta come affiliazione italiana *dell'Institute of Internal Auditors* – e a oggi la sola qualifica riconosciuta a livello internazionale per l'esercizio della professione di internal auditor.

Siena, 9 febbraio 2018

DIREZIONE CHIEF AUDIT EXECUTIVE

Il Responsabile

Allegati:

- All. 1 - Framework pianificazione *SREP oriented*: supporto metodologico
- All. 2 - Interventi di revisione processi centrali/società anno 2018
- All. 3 - Interventi di revisione Rete territoriale e canali distributivi anno 2018