Audit Plan 2017

GRUPPOMONTEPASCHI

Siena, 8 febbraio 2017

Direzione Chief Audit Executive
Responsabile: Pierfrancesco Cocco

Obiettivo del documento è quello di presentare le linee guida e le attività di audit previste dalla Direzione Chief Audit Executive per l'esercizio 2017.

La pianificazione complessiva, dopo aver recepito le indicazioni del Collegio Sindacale, verrà sottoposta al Comitato Rischi e presentata per l'approvazione al Consiglio di Amministrazione.

Il piano include gli interventi obbligatori previsti dalla legge e dalla regolamentazione nonché le verifiche specificamente richieste dalle Autorità di Vigilanza.

Executive summary

LINEE GUIDA 2017

- il 2017 è il secondo anno del ciclo di audit della durata di 4 anni: la pianificazione delle revisioni si inserisce quindi in un'ottica pluriennale di copertura del rischio aziendale
- la profonda evoluzione del contesto interno ed esterno, nonché le aspettative del ***Single Supervisory Mechanism*** (SSM) hanno necessariamente impattato gli obiettivi pluriennali individuati, correggendone le mire per il prossimo anno e permettendo il conseguimento di un più efficace *focusing*
- la pianificazione considererà le linee guida del nuovo ***Piano Industriale***, prevendendo attività di *assurance* e di *consulting* sul roll out delle attività previste
- specifico focus riguarderà la componente strategica, con l'inserimento di verifiche sul ***business model*** in ottica ***SREP oriented***
- il modello di internal audit è volto a valutare la complessiva efficacia dei processi di controllo del ***Conduct Risk*** facendosi attore e promotore della ***risk culture*** aziendale
- ove si ravvisino sinergie e possibilità di economie di scopo è incentivata l'esecuzione di attività di audit in joint tra le strutture
- il piano di attività è consistente con l'***evoluzione organizzativa della funzione di IA*** per allineamento al nuovo contesto interno ed esterno

PROCESSI CENTRALI E SOCIETA'

- gli interventi sui processi centrali e società consentiranno una view più complessiva delle attività/strutture auditate, con analisi orientate alla verifica dell'intero processo e non focalizzate a livello di fase.
- il piano contempla tutte le attività cd ***obbligatorie*** perché prescritte dalle Autorità di Vigilanza
- consueto effort sarà dedicato al mondo IT, con particolare attenzione agli aspetti di ***cybersecurity***
- l'approccio integrato consente l'analisi congiunta dei risultati emersi sulle Società con le evidenze di Capogruppo, al fine di individuare ambiti di intervento comuni e massimizzare le economie di scopo

RETE TERRITORIALE

- i nuovi obiettivi di audit prevedono lo sviluppo di azioni sinergiche tra settori specialistici e settori che verificano i processi sulla Rete territoriale, al fine di accrescere l'efficacia dell'internal audit in ottica di ***continuos monitoring***
- un differente approccio metodologico di presidio sulla Rete prevede, quale riferimento per l'audit, una struttura territoriale superiore (DTM) con un eventuale accesso alle singole dipendenze volto a completare la valutazione complessiva della struttura di riporto gerarchico. Questo cambio di passo, adottato anche a seguito delle indicazioni ECB, ***riduce sensibilmente il numero di audit sulla Rete.***
- la presenza sul territorio continua ad essere un fattore vincente per il rafforzamento della ***risk culture***

Agenda

1 *Linee guida Audit Plan 2017*

2 Interventi di audit 2017

1 Linee guida Audit Plan 2017: *aspettative del SSM*

- Il ***Single Supervisory Mechanism (SSM)***, nel corso delle attività rientranti nel Comprehensive Assessment, ha individuato specifici punti di attenzione in relazione ai quali si attende una maggiore focalizzazione da parte dall'internal audit
- La Direzione Chief Audit Executive non può prescindere dal cogliere tale ulteriore sfida sotto il profilo evolutivo e strategico
- Il piano di audit per il 2017 è stato pertanto calibrato all'accoglimento delle principali aspettative del Supervisor

- assurance sulla qualità dei dati con rinnovata attenzione nei confronti dei ***rischi IT***, in particolar modo quelli derivanti dall'uso di nuove tecnologie (cybercrime, digital and mobile banking)
- focus su attività di ***stress test e scenario analysis*** sempre più considerati come strumenti di vigilanza
- attenzione alla ***governance interna*** quale bilanciamento di poteri tra Organi apicali, processi decisionali e informativi
- adozione di strumenti di studio e verifica della vulnerabilità del ***modello di business***, nonché dei modelli di governo e ***gestione del rischio strategico***
- valutazione del grado di conformità dei ***processi di recovery & resolution*** definiti dalla Banca al fine della coerenza con i *key indicators* prescelti
- rispondenza dell'***ILAAP*** ai canoni SREP, l'internal audit ne deve valutare l'integrazione con l'impianto ICAAP e l'utilizzo di entrambi i processi nella determinazione delle politiche di gestione dei rischi
- adozione di modelli di internal audit volti a valutare la complessiva efficacia dei processi di controllo del ***Conduct Risk*** al fine di promuovere ed accrescere la ***Risk Culture*** a tutti i livelli aziendali

1 Linee guida Audit Plan 2017 : *piano SREP oriented*

Il piano di audit per il 2017 è stato definito prevedendo la copertura di tutti i 4 componenti fondamentali dello SREP

BUSINESS MODEL	» Valutazione della capacità di generare utili nei successivi 12 mesi (viability) » Valutazione della sostenibilità della strategia della Banca sulla base di una proiezione triennale dei risultati economici	» Revisione RAF » Focus su componente strategica, in particolare sugli aspetti relativi al ***business model***
GOVERNANCE & RISK MANAGEMENT	» Adeguatezza della struttura organizzativa e presenza di una robusta risk culture » Adeguatezza della struttura di remunerazione » Verifica dell'esistenza di un framework di rischio robusto che comprenda: - Risk Appetite Framework - ICAAP e ILAAP - Stress testing » *Appropriatezza del sistema dei controlli interni*	» Revisioni sulla rete territoriale (***risk culture***) » Relazione su politiche e prassi di remunerazione » Revisione ILAAP » Revisione ICAAP » Adeguata verifica » Tutela dati personali » Operazioni Personali » Revisione RAF
RISK TO CAPITAL	» Valutazione del livello di rischio e dei processi di gestione del rischio di: - credito e controparte - mercato - operativo - Interest Rate risk su Banking Book (IRRBB)	» Revisione convalida AMA » Revisione convalida AIRB » Revisione ICAAP » Revisioni LGD/EAD/PD » Attività in GPM » Government & Money Market » Processo di contribuzione al parametro Euribor » Credit Default Detection
RISK TO LIQUIDITY & FUNDING	» Valutazione dell'adeguatezza dei processi di gestione dei rischio di liquidità e funding » Analisi del liquidity contingency plan e dei piani di funding	» Revisione ILAAP » Gestione liquidità operativa e contribuzione parametro Euribor

1 Linee guida Audit Plan 2017 : *coverage mandatory audit*

MANDATORY ACTIVITIES		ORIGINATION	AUDIT REPORT (ON SITE INSPECTION)	RELAZIONI
RISK MGMT	» Processo di adeguatezza patrimoniale (ICAAP)	» CRD4/ Circ. 285	✓	
	» Internal Liquidity Adeguacy Assessment Process (ILAAP)	» Consultation Paper EBA	✓	
	» Processo di convalida AIRB	» CRD4/ Circ. 285	✓	✓
	» Processo di convalida AMA	» CRD4/ Circ. 285	✓	✓
	» Risk Appetite Framework (RAF)	» CRD4/ Circ. 285	✓	
	» Revisioni sui modelli credito (EAD,PD,LGD)	» CRD4/ Circ. 285	✓	
ICT	» Ethical Hacking ICT – New York branch (FED)	» FED	✓	
	» Accessi non autorizzati (prescrizione Garante Privacy)	» Provv. Garante 192/2011	✓	
	» BCM and Disaster Recovery BMPS	» CRD4/ Circ. 285	✓	
	» BCM MP Belgio	» AAVV locali	✓	
	» VISA PIN Security Audit	» VISA	✓	
ALTRE TIPOLOGIE	» Politiche e prassi di remunerazione	» CRD4/ Circ. 285	✓	✓
	» Covered Bond	» CRD4/ Circ. 285	✓	
	» Processi esternalizzati	» CRD4/ Circ. 285		✓

+

ECB RECOMMENDATIONS	
	Revisioni su raccomandazioni in scadenza al 31/12/2016 e nel 2017

1 Linee guida Audit Plan 2017 : *approccio integrato*

Il Gruppo adotta un approccio integrato per la pianificazione delle attività di audit che coinvolge sia la Capogruppo che le Società controllate.

BMPS

- ai fini della definizione del piano di audit è stato consolidato ad utilizzato quale supporto alla pianificazione il modello di *Risk Evaluation* introdotto lo scorso anno che associa alla tradizionale valutazione qualitativa (*judgemental*) - espressa dall'assessment interno - dati quantitativi aziendali definiti per ciascun macroprocesso di business
- interventi su processi centrali con approccio di verifica "top-down" esteso a tutti gli attori e le fasi del processo, partendo dalle attività più strategiche per arrivare a quelle più operative
- rafforzamento delle attività di *joint audit,* tra strutture di revisione su processi specialistici e strutture di revisione sulla rete territoriale al fine di cogliere le possibili economie di scopo
- consolidamento del *continuous monitoring* sui principali fenomeni di rete

SOCIETÀ CONTROLLATE

- utilizzo dello stesso approccio metodologico della Capogruppo per la componente di analisi qualitativa dei processi, finalizzata all'individuazione dei principali ambiti di criticità da indagare
- analisi congiunta dei risultati emersi sulle Società con le evidenze di Capogruppo, al fine di individuare ambiti di intervento comuni e massimizzare le economie di scopo
- per le Società la cui funzione di Internal Audit è svolta dalla Capogruppo sulla base di specifici contratti di outsourcing (Widiba, Fiduciaria e Integra), le attività di audit per il 2017 sono ricomprese nella pianificazione di BMPS

1 Linee guida Audit Plan 2017: *macroprocessi critici*

Step 1

MACROPROCESSI DI BUSINESS	GIUDIZIO DI SINTESI
Credito	ALTO
Finanza	MEDIO ALTO
Prodotti del credito	MEDIO ALTO
Tesoreria e Capital Management	MEDIO
Servizi bancari	MEDIO BASSO
Leasing	MEDIO BASSO
Servizi di Investimento	MEDIO BASSO
Incassi e pagamenti	MEDIO BASSO
Servizi Fiduciari	MEDIO BASSO
Factoring	BASSO
Servizi Accessori	BASSO
Investment Banking	BASSO
Gestione dei crediti problematici*	-
Gestione ordinaria del credito*	-
Governo del credito*	-

» Con riferimento agli altri macroprocessi (non di business) gli aspetti più rilevanti attengono le politiche commerciali

» In fascia di rischio medio alta anche le attività relative alla compliance, alla gestione delle risorse umane, al contrasto al riciclaggio e finanziamento al terrorismo, agli aspetti di contabilità, fiscale e vigilanza

* Il macroprocesso del Credito già comprende, nelle valutazioni sottostanti, anche gli aspetti di rischio relativi ai macroprocessi di nuova introduzione (governo del credito, gestione ordinaria del credito e gestione dei crediti problematici)

» Per i macroprocessi di business, la fase di identificazione delle attività critiche ha evidenziato come prioritari i processi creditizi, compresi i prodotti del credito

» Il processo Finanza diventa rilevante a causa delle consistenti perdite rilevate negli anni pregressi

Step 2

ALTRI MACROPROCESSI (NO BUSINESS)	GIUDIZIO DI SINTESI
Politiche commerciali	ALTO
Compliance	MEDIO ALTO
Risorse umane	MEDIO ALTO
Contrasto al riciclaggio e finanziamento al terrorismo	MEDIO ALTO
Contabilità, fiscale e vigilanza	MEDIO ALTO
Risk Management	MEDIO
Rapporto con il cliente	MEDIO
Canali di contatto con la clientela	MEDIO
Immobiliare	MEDIO
Organizzazione e Demand	MEDIO BASSO
Sicurezza e Ambiente	MEDIO BASSO
Ciclo Passivo	MEDIO BASSO
Logistica e Servizi Ausiliari	MEDIO BASSO
Legale e Societario	MEDIO BASSO
Erogazione ICT	BASSO
Politiche e prassi di remunerazione e incentivazione	BASSO
Business Continuity Management	BASSO
Sviluppo ICT	BASSO
Organizzazione	BASSO
Pricing	BASSO
Pianificazione strategica	BASSO
Budget e controllo di gestione	BASSO
Revisione interna	BASSO
Prodotti	BASSO
Partecipazioni	BASSO
Comunicazione e Relazioni esterne	BASSO

Agenda

1 Linee guida AP 2017

2 *Interventi di audit 2017*

2 Interventi di audit 2017: *overview*

PROCESSI CENTRALI	» il piano di attività per il 2017 prevede **38 interventi** sui processi agiti dalla strutture centrali con focus principale sui processi creditizi » prevista un'*attività di consulting* in ambito MIFID II » incluse tutte le attività obbligatorie previste da disposizioni regolamentari » accolti gli input ECB in materia di modelli del credito (*Parametri EAD,LGD, PD*) e di *Credit Default Detection* » contemplate le attività di verifica ai fini delle 31 RA ECB con scadenza 2017
SOCIETA'	» pianificati **16 interventi** sul perimetro societario del Gruppo » specifico effort è stato rivolto all'attività in servicing vs Widiba e MP Fiduciaria » il presidio della rete di promozione finanziaria di Widiba è garantito sia a livello centrale (*Processo di controllo di II livello su PF e NF*; *Processo di programmazione comm.le e filiera distributiva*) che di interventi analitici sui singoli promotori e negozi finanziari. In ambito IT, in aggiunta all'intervento su *ethical hacking* sarà verificato il *Sistema antifrode su Home Banking* della società
IT AUDIT	» inserite a piano **12 attività** di audit a copertura dei rischi in materia di Information Technology (*in joint* con l'internal audit del Consorzio Operativo di Gruppo) » particolare focus è stato dedicato agli aspetti di ***cybersecurity,*** con interventi specialistici orientati a verificare la sicurezza dei sistemi (*Ethical Hacking, Sistema antifrode HB*) » prevista *un'attività di consulting* in ambito Data Governance
RETE TERRITORIALE	» la presenza sul territorio è ritenuta fondamentale e fattore vincente per l'acquisizione da parte delle risorse di una piena consapevolezza e rafforzamento della ***Risk Culture***. » l'effort sulla Rete prevede un nuovo approccio con interventi sulle strutture territoriali di governo (DTM), nel quadro di una visione sinottica volta a fornire assurance sulla complessiva gestione dei processi » per gli interventi sulle strutture territoriali sarà rappresentato l'impegno in FTE e solo approssimativamente il numero di attività , sensibilmente ridotto con il nuovo criterio

CREDITO

Processi centrali

» credit default detection: test effettività processo monitoraggio del credito
» revisione processo CRM (garanzie-perizie-avvaloramento)
» covered bond
» verifica su 1° livello dei controlli su filiera creditizia: qualità del credito
» processo di gestione recupero crediti (strategie ed execution)
» processo di gestione rischio anomalo
» revisione processo erogazione Grandi Gruppi

Società

» Microcredito di Solidarietà
» MPS Leasing & Factoring: valorizzazione dei crediti nel Bilancio d'esercizio

Rete territoriale

» nuove procedure di erogazione del credito
» processo di erogazione creditizia: coerenza delle delibere alle politiche creditizie
» posizioni performing in percorso di recupero estremo: efficacia ed efficienza dei processi gestionali e dei presidi di controllo
» gestione eventi operativi/parametri Linee Valore SB, PMI: efficacia ed efficienza dei processi gestionali e dei presidi di controllo
» efficienza operativa (tempi di delibera, operazioni abbandonate, etc.)
» processo di gestione delle operazioni oggetto di restrizione ipotecaria: adeguatezza presidi a supporto
» gestione recupero crediti (Settori Dipartimentali Recupero Crediti)
» gestione rischio anomalo (Settori Dipartimentali Rischio Anomalo)
» gestione documentale e processo creditizio di *origination*
» specifici su prodotti del credito: gestione operativa mutui retali, anticipi, finanziamenti specifici (credito agrario: destinazione e modalità rientro), delibere di forzatura e indici di morosità, monitoraggio mutui a SAL non in ammortamento e monitoraggio mutui retail

MACCHINA OPERATIVA

Processi centrali

- rilasci applicazioni IT
- processo formazione budget
- gestione cause legali
- governo del fornitore Fruendo
- commissioni attive nel bilancio di esercizio: composizione e rappresentazione contabile («commissioni percepite dalle società assicurative»)
- ECB RA 7 - policy contabili credito

Processi esternalizzati (Fruendo)

- pagamento fatture
- anticipi fatture COG
- gestione assegni

Società

- COG: budget spese
- COG: gestione normativa
- COG: bilancio – piano dei conti
- MPS Fiduciaria: aspetti contabili: interfacciamento della procedura contabile con la procedura gestionale
- Magazzini Generali di Mantova

FINANZA PROPRIETARIA e LIQUIDITA'

Processi centrali

» revisione del processo di contribuzione alla determinazione del parametro Euribor
» revisione sul processo di gestione della finanza proprietaria

Società

» MPS Capital Services: revisione sull'attività dell'Ufficio Government & Money Market

DISTRIBUZIONE COMMERCIALE

Processi centrali

» issuing carte di debito e prepagate
» gestione servizi POS
» revisione attività in Gestioni Patrimoniali
» programmazione commerciale e filiera distributiva BMPS

Società

» Widiba: programmazione commerciale e filiera distributiva
» MP Fiduciaria: attività dei presidi commerciali: interrelazioni con il presidio operativo

Rete territoriale e PF

» modalità di attuazione dei processi di approccio alla clientela sotto il profilo Mifid
» modello operativo Hub & Spoke: corretta e completa attuazione
» processo di gestione dei documenti contrattuali nei Centri private
» Widiba: processo di collocamento da parte dei PF e Negozi Finanziari

CONTROLLO RISCHI E CONFORMITA'

Processi centrali

- revisione adeguata verifica
- revisione operazioni personali
- revisione sul processo di trasparenza bancaria
- revisione corporate governance
- politiche e prassi di remunerazione
- segnalazioni di vigilanza prudenziale
- revisione convalida AIRB
- revisione convalida AMA
- revisione LGD
- revisione PD
- revisione EAD
- revisione processo RAF
- revisione ICAAP
- revisione ILAAP
- processo Mifid 2 (*consulting*)

Società

- MPS Fiduciaria: adempimenti in materia di antiriciclaggio e contrasto al terrorismo
- Widiba: processo di controllo di 2° livello su PF e NF (funzione di compliance)
- Integra: AML

Rete territoriale

- modalità di gestione delle Operazioni Sospette e coerenza delle valutazioni

Interventi di audit 2017 : *copertura per macroambiti*

INFORMATION TECHNOLOGY

Processi centrali

- sviluppo applicativi ARGO
- garante privacy: nuove regole di *alerting*
- usura calcolo TEG
- VISA PIN Security audit
- Data Governance (*consulting*)
- servizio anagrafe
- Ethical Hacking sistemi di Gruppo
- sistema antifrode su HB
- seguimento test BCM
- piano DR e seguimento test
- disponibilità dei sistemi e livello di servizio
- AUI
- ECB RA 12/13 - Upgrade Banche Dati con info su Collaterali

Società

- Widiba: sistema antifrode su HB
- Widiba: ethical hacking
- MP Belgio: continuità operativa