



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

Tableau de Board Internal Audit - #5

[aggiornamento al 31 Agosto 2018]

periodo 13.07.2018 – 31.08.2018

Direzione Chief Audit Executive

Agenda

- 1 Overview interventi di audit
- 2 Interventi di processo chiusi
- 3 SAL interventi rete e canali distributivi
- 4 Interventi di processo in corso
- 5 Interventi di processo da avviare
- 6 Interventi straordinari

Allegati:

Focus interventi di processo chiusi nel periodo

Focus compito interventi di processo avviati nel periodo



1 Overview interventi di audit

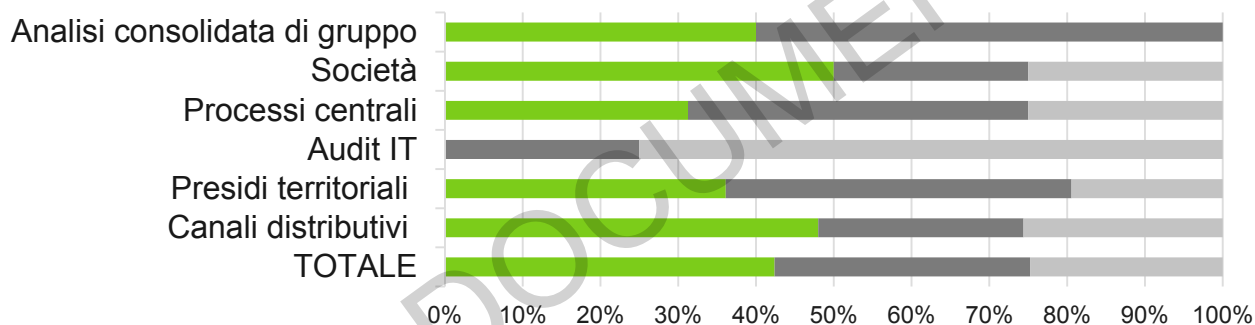
SAL Audit Plan 2018

| INTERVENTI PROCESSI STRUTTURE | IN CORSO (*) | | CHIUSI | AUDIT PLAN | Δ CHIUSI VS TDB PRECEDENTE | AVANZAMENTO RISPETTO ALL'AP (in corso + chiusi / Audit Plan) |
|---|----------------|--------------|----------------|------------|---|--|
| | IN SVOLGIMENTO | IN REPORTING | | | | |
| Analisi consolidata di gruppo | 3 | - | 2 ^a | 5 | 2 | 100.0% |
| Società | 2 | - | 4 | 9 | - | 66.7% |
| Processi centrali | 12 | 2 | 10 | 33 | 2 | 72.7% |
| Audit IT | 1 | - | - | 4 | - | 25.0% |
| Presidi territoriali | 12 | 4 | 13 | 36 | 3 | 80,6% |
| Canali distributivi (compresa Rete Promotori) | 17 | 16 | 60 | 125 | 7 | 74,4% |
| SUB TOTALE PIANIFICATI | 47 | 22 | 89 | 212 | 14 | 74,5% |
| Indagini / Servizi speciali | 18 | 2 | 20 | 60** | | |
| Interventi straordinari | 4 | - | 2 | - | | |
| TOTALE | 69 | 24 | 111 | 272 | | |

^a I 2 interventi finalizzati di tipologia «Analisi consolidata di Gruppo» sono:
 - AML (SOS) di Gruppo su BMPS, Widiba e Fiduciaria
 - Ethical Hacking di Gruppo (BMPS, NY e Widiba) - **IT Audit**

Avanzamento interventi su Audit Plan (%)

■ Chiusi da Audit Plan ■ In corso da Audit Plan ■ Da avviare



AP 2018: variazioni di perimetro

L'intervento pianificato **Credit Default Detection: efficacia e tempi di riguardo al processo di identificazione del Forboreance (Finding #6 e #7 OSI-1238 BCE)** è stato suddiviso in due accertamenti a causa delle diverse date di prevista chiusura delle attività della Banca relative ai due *finding* in oggetto. Inoltre è stata aggiunta la revisione su MPS Tenimenti, non inizialmente prevista in sede di pianificazione della DCAE, a seguito dell'accentramento della funzione IA della società.

Il numero di interventi di processo previsti in Audit Plan 2018 è stato conseguentemente incrementato di 2 unità e rivisto il perimetro di 1 intervento in corso. Di seguito le nuove revisioni a piano:

- **Revisione Finding #7 OSI-1238 - Credit Default Detection: focus non-binding parameters**
- **Revisione Finding #6 OSI-1238 - Efficacia e tempestività del processo di classificazione a maggior rischio delle posizioni oggetto di Forborne**
- **MPS Tenimenti – Aspetti amministrativo-contabili e presidio dei controlli**

(*) Si intendono «in corso» gli interventi per cui sono almeno iniziate le attività di preparazione (pianificazione, raccolta documenti ...); si considerano «in svolgimento» gli interventi in corso per cui non è stato ancora effettuato l'exit meeting e «in reporting» quelli per cui quest'ultimo risulta invece già effettuato ed è in fase di redazione il relativo rapporto.

(**) Dato stimato sulla base del trend storico degli ultimi anni



MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

2 Interventi di processo chiusi: Audit plan 2018 (1/2)

| N. RAPPORTO | DATA DI PUBBLICAZIONE | MACROPROCESSO | DESCRIZIONE INTERVENTO | GRADE ¹ | GAP ² | | | | PILASTRI SREP | | | | ORGANI DESTINATARI | | | | |
|-------------|-----------------------|--|--|--------------------|------------------|------|-------|------|-----------------|----|----|----|--------------------|----|----|----|---------|
| | | | | | ALTI | MEDI | BASSI | TOT. | BM | IG | RC | RL | Pres. CdA | AD | CS | CR | ODV 231 |
| 064/2018 | 20/03/2018 | CREDITO | Microcredito di Solidarietà | R1 | | | | | Non Applicabile | | | | | | | | |
| 073/2018 | 20/03/2018 | CONTABILITA' FISCALE E VIGILANZA | Magazzini Generali Fiduciari di Mantova Spa | R1 | | | | | Non Applicabile | | | | | | | | |
| 075/2018 | 20/03/2018 | POLITICHE E PRASSI DI REMUNERAZIONE E INCENTIVAZIONE | Politiche e prassi di remunerazione (Mandatory) | R1 | | | 2 | 2 | | X | | | X | X | X | X | |
| 095/2018 | 27/03/2018 | CONTABILITA' FISCALE E VIGILANZA | Processo fiscale sui servizi di investimento | R2 | | 3 | | 3 | | X | | | | | | | |
| 079/2018 | 27/04/2018 | SICUREZZA E AMBIENTE | Widiba-Sistema antifrode su Home Banking (IT audit) | R2 | | 4 | 4 | 8 | | X | | | | | | | |
| 091/2018 | 02/05/2018 | COMPLIANCE | Integra - Processo Carte | R1 | | | 2 | 2 | Non Applicabile | | | | | | | | |
| 096/2018 | 11/06/2018 | CONTABILITA' FISCALE E VIGILANZA | IFRS9 | R1 | | | | | | X | | | | | | | |
| 044/2018 | 11/06/2018 | RISK MANAGEMENT | Controparte e Mercato: focus su modello CCR (Credit Counterparty Risk) e modifiche market risk FRTB (Fundamental Review of Trading Book) | R2 | | | 6 | 6 | | X | X | | | | | | |
| 089/2018 | 12/06/2018 | LEGALE E SOCIETARIO | Gestione Processo Successioni | R2 | | 4 | 6 | 10 | | X | | | | | | | |

(1) Il Grade si riferisce esclusivamente all'intervento oggetto di revisione e non deve essere inteso come una valutazione direttamente correlabile al pilastro SREP di riferimento. A tal proposito, l'associazione intervento – pilastro SREP non tiene conto degli «obiettivi di controllo» comuni a tutti i processi (cd. Trasversali) e riconducibili integralmente al Pillar «Internal Governance & SCI».

(2) Riferimento allegati per evidenza gap delle revisioni chiuse nel periodo di riferimento del presente Report.



2 Interventi di processo chiusi: Audit plan 2018 (2/2)

| N. RAPPORTO | DATA DI PUBBLICAZIONE | MACROPROCESSO | DESCRIZIONE INTERVENTO | GRADE ¹ | GAP ² | | | | PILASTRI SREP | | | | ORGANI DESTINATARI | | | | |
|-------------|-----------------------|-------------------------------|--|--------------------|------------------|------|-------|------|---------------|----|----|----|--------------------|----|----|----|---------|
| | | | | | ALTI | MEDI | BASSI | TOT. | BM | IG | RC | RL | Pres. CdA | AD | CS | CR | ODV 231 |
| 072/2018 | 06/07/2018 | GESTIONE CREDITI PROBLEMATICI | Processo Gestione Crediti Ristrutturati | R2 | | 2 | | 2 | | X | X | | | | | | |
| 063/2018 | 11/07/2018 | INCASSI E PAGAMENTI | Gestione ATM | R3 | 1 | 7 | | 8 | X | X | | | X | X | X | X | |
| 054/2018 | 11/07/2018 | RISK MANAGEMENT | Evoluzione Pillar 2 con focus IRRBB | R3 | 1 | 2 | 2 | 5 | | X | X | | X | X | X | X | |
| 077/2018 | 23/07/2018 | COMPLIANCE | AML (SOS) di Gruppo su BMPS, Widiba e Fiduciaria | R3 | 2 | 6 | 1 | 9 | | X | | | X | X | X | X | X |
| 041/2018 | 31/07/2018 | RISK MANAGEMENT | Data quality di riconciliazione LGD (TRIM) | R2 | | 1 | 2 | 3 | | X | X | | | | | | |
| 070/2018 | 10/08/2018 | CREDITO | High Risk | R2 | | 2 | 1 | 3 | | X | X | | X | X | X | X | |
| 062/2018 | 16/08/2018 | SICUREZZA E AMBIENTE | Ethical Hacking di Gruppo (BMPS, NY e Widiba) | R2 | | 4 | 1 | 5 | | X | | | X | X | X | X | |

----- Interventi chiusi da Report Trimestrale Internal Audit 2Q 2018.

(1) Il Grade si riferisce esclusivamente all'intervento oggetto di revisione e non deve essere inteso come una valutazione direttamente correlabile al pilastro SREP di riferimento. A tal proposito, l'associazione intervento – pilastro SREP non tiene conto degli «obiettivi di controllo» comuni a tutti i processi (cd. Trasversali) e riconducibili integralmente al Pillar «Internal Governance & SCI».

(2) Riferimento allegati per evidenza gap delle revisioni chiuse nel periodo di riferimento del presente Report.

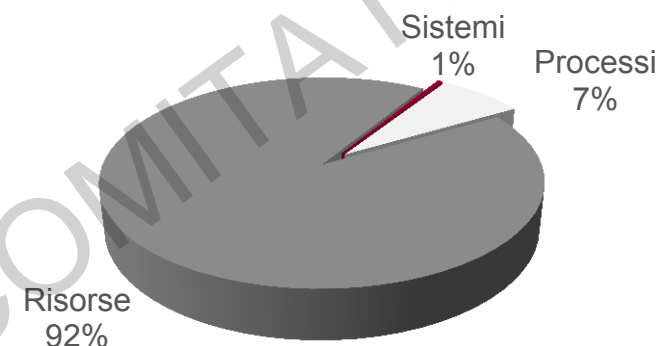


3 SAL interventi rete e canali distributivi: Audit plan 2018

Giudizi su presidi territoriali e strutture operative

| | AMBITO* | R1 | R2 | R3 | R4 |
|----------------------|---------------------------------|----|----|----|----|
| PRESIDI TERRITORIALI | Altri rischi operativi | - | 1 | 2 | - |
| | Compliance | - | - | - | - |
| | Credito | 1 | 8 | 1 | - |
| | Processi Commerciali/Gestionali | - | - | - | - |
| | Servizi di Investimento | - | - | - | - |
| STRUTTURE OPERATIVE | Altri rischi operativi | - | 16 | 4 | - |
| | Compliance | 4 | 23 | 5 | - |
| | Credito | - | 11 | 2 | - |
| | Processi Commerciali/Gestionali | 20 | 3 | 1 | - |
| | Servizi di Investimento | 7 | 6 | - | - |
| PROMOTORI FINANZIARI | Complessivo** | 6 | 9 | 3 | - |

Frequenza dei fattori causali



Anomalie di processo più comuni rilevate per ambito d'intervento

| AMBITO D'INTERVENTO | NR ANOMALIE | Δ ANOMALIE TOT VS TDB PRECEDENTE | DESCRIZIONE ANOMALIA DI PROCESSO CON MAGGIORE FREQUENZA | NR | % rilevanti/totali | Δ ANOMALIE RILEVANTI VS TDB PRECEDENTE |
|-----------------------------------|-------------|----------------------------------|--|----|--------------------|--|
| Altri rischi operativi | 122 | 9 | ELEVATA CONSISTENZA E/O FREQUENZA DI DOCUMENTI SOSPESI IN PARDO | 19 | 15,6% | 3 |
| | | | PRESENZA DI DOCUMENTI SOSPESI IN TORB | 15 | 12,3% | 2 |
| Compliance | 174 | 21 | MANCATA RIVALUTAZIONE PERIODICA DELLA CLIENTELA FINALIZZATA AL CONTROLLO COSTANTE DEL RAPPORTO CONTINUATIVO (ARTT. 18-19 D.LGS 231/2007) | 41 | 23,6% | 4 |
| | | | MANCATA O INCOMPLETA ACQUISIZIONE DEL QUESTIONARIO KYC | 38 | 21,8% | 4 |
| Credito | 53 | 0 | MANCATA/NON PUNTUALE ATTENZIONE AGLI ADEMPIMENTI AMMINISTRATIVI (RINNOVO PRATICHE, RATING, ETC.) | 7 | 13,2% | 0 |
| | | | MANCATA/NON CORRETTA FORMALIZZAZIONE DELLA DOCUMENTAZIONE DELLE LINEE DI CREDITO ACCORDATE AL CLIENTE | 6 | 11,3% | 0 |
| Processi Commerciali e Gestionali | 18 | 0 | GESTIONE SPECIMEN DI FIRMA DIPENDENTI NON CONFORME | 4 | 22,2% | 0 |
| | | | CONTI CORRENTI PRESENZA DI SALDI SCOPERTI/SCONFINATI | 3 | 16,7% | 0 |
| Servizi di Investimento | 77 | 12 | RIPROFILAZIONE MIFID ASSENTE | 16 | 20,8% | 1 |
| | | | CONSULENZA AVANZATA: INADEGUATA ATTENZIONE A "SEMAFORI ROSSI" ED ALLE ATTIVITÀ CONNESSE | 15 | 19,5% | 0 |



MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

*Il totale dei giudizi per ambito può non essere uguale al totale dei giudizi per intervento perché una revisione può evidenziare più anomalie; inoltre i giudizi e le anomalie rilevate si riferiscono ad interventi sia chiusi che in corso

** Il giudizio sui promotori finanziari viene attribuito sull'operatività complessiva degli stessi

Interventi di processo in corso: Audit plan 2018 (1/2)

| N. INCARICO | MACROPROCESSO | DESCRIZIONE INTERVENTO | DATA INIZIO | EXIT MEETING | DATA FINE PRESUNTA | PILASTRI SREP | | | | ORGANI DESTINATARI PREVISTI | | | | |
|-------------|-----------------------------------|--|-------------|--------------|--------------------|-----------------|----|----|----|-----------------------------|----|----|----|---------|
| | | | | | | BM | IG | RC | RL | Pres. CdA | AD | CS | CR | OdV 231 |
| 119/2018 | SERVIZI DI INVESTIMENTO | Gestione intermediazione in oro con aziende orafe | 10/04/2018 | 12/06/2018 | 30/09/2018* | Non Applicabile | | | | | | | | |
| 085/2018 | RAPPORTO CON IL CLIENTE | Dematerializzazione disposizioni operative e firma grafometrica | 08/05/2018 | | 30/09/2018* | Non Applicabile | | | | | | | | |
| 094/2018 | CONTABILITA' FISCALE E VIGILANZA | Business Model (focus su commissioni) | 10/05/2018 | | 30/09/2018* | X | X | | | | | | | |
| 067/2018 | CREDITO | Revisione Credit Default Detection – focus non-binding parameters - Findings #7 OSI 1238 BCE | 06/06/2018 | | 20/09/2018* | | | X | | | | X | | |
| 045/2018 | RISK MANAGEMENT | ILAAP | 14/06/2018 | | 31/10/2018 | | X | | | X | X | X | X | |
| 042/2018 | RISK MANAGEMENT | ICAAP | 19/06/2018 | | 22/09/2018* | | X | X | | X | X | X | X | |
| 093/2018 | CREDITO | Underestimation of key metrics for calculating loan loss provisions (FINDING 8 OSI 1238) | 02/07/2018 | | 28/09/2018 | | X | | | | | X | | |
| 038/2018 | FINANZA/ TESORERIA & CAPITAL MGMT | Processo di contribuzione alla determinazione dei parametri EURIBOR e EONIA | 09/07/2018 | 24/08/2018 | 15/09/2018* | Non Applicabile | | | | | | | | |
| 037/2018 | RISK MANAGEMENT | Processo convalida AMA | 13/07/2018 | | 28/09/2018 | | X | X | | X | X | X | X | |
| 040/2018 | RISK MANAGEMENT | Calcolo EAD nel nuovo modulo ECL (Finding #2 OSI 1238) | 13/07/2018 | | 15/09/2018 | Non Applicabile | | | | | | X | | |

L'associazione intervento – pilastro SREP non tiene conto degli «obiettivi di controllo» comuni a tutti i processi (cd. Trasversali) e riconducibili integralmente al Pillar «Internal Governance & SCI».



Interventi di processo in corso: Audit plan 2018 (2/2)

| N. INCARICO | MACROPROCESSO | DESCRIZIONE INTERVENTO | DATA INIZIO | EXIT MEETING | DATA FINE PRESUNTA | PILASTRI SREP | | | | ORGANI DESTINATARI PREVISTI | | | | |
|-------------|----------------------------------|--|-------------|--------------|--------------------|-----------------|----|----|----|-----------------------------|----|----|----|---------|
| | | | | | | BM | IG | RC | RL | Pres. CdA | AD | CS | CR | OdV 231 |
| 092/2018 | CICLO PASSIVO | Gestione fornitori, attività negoziali e contratti 240 | 16/07/2018 | | 30/10/2018 | Non Applicabile | | | | | | X | | X |
| 068/2018 | CREDITO | Business Plan Sofferenze (Finding #9 OSI 1238 BCE) | 17/07/2018 | | 30/09/2018 | Non Applicabile | | | | | | X | | |
| 103/2018 | PRODOTTI | Widiba - Prodotto Mutui on Line in ottica di redditività | 20/07/2018 | | 30/09/2018 | Non Applicabile | | | | | | | | |
| 090/2018 | DATA GOVERNANCE | Data Governance: struttura organizzativa, framework e strumenti a supporto | 23/07/2018 | | 12/10/2018 | | X | | | | | | | |
| 104/2018 | COMPLIANCE | MIFID II: Processo/Modello e modalità distributive/controlli di 1° livello | 31/07/2018 | | 30/11/2018 | Non Applicabile | | | | | | X | | |
| 074/2018 | COMPLIANCE | Compliance: modello accentrato di Gruppo con focus su Widiba e MPS CS (previsti specifici approfondimenti su usura) | 06/08/2018 | | 31/12/2018 | | X | | | | | X | | X |
| 071/2018 | GESTIONE CREDITI PROBLEMATICI | Processo Gestione Massiva Crediti (Unlikey to Pay) | 08/08/2018 | | 31/10/2018 | | X | | | | | | | |
| 118/2018 | GESTIONE ORDINARIA DEL CREDITO | Gestione istruttoria veloce | 17/08/2018 | | 01/10/2018 | Non Applicabile | | | | | | | | |
| 226/2018 | CREDITO | Revisione Finding #6 OSI 1238 - Efficacia e tempestività del processo di classificazione a maggior rischio delle posizioni oggetto di Forborne | 10/08/2018 | | 20/09/2018 | | X | X | | | | X | | |
| 241/2018 | CONTABILITA' FISCALE E VIGILANZA | MPS Tenimenti – Aspetti amministrativo-contabili e presidio dei controlli | 17/07/2018 | | 15/10/2018 | Non Applicabile | | | | | | | | |



Interventi di processo da avviare: Audit Plan 2018 (1/2)

| MACROPROCESSO | PROCESSO | DESCRIZIONE INTERVENTO | NOTE |
|-------------------------------------|--|--|-------------------------|
| BUSINESS CONTINUITY MANAGEMENT | Sistema di Gestione della Continuità Operativa | Business Continuity Management | Mandatory |
| BUSINESS CONTINUITY MANAGEMENT | Sistema di Gestione della Continuità Operativa | Disaster Recovery | Mandatory |
| COMPLIANCE | Gestione adempimenti prescrittivi in materia di tutela dei dati personali (d.lgs.196/2003) | Controlli Privacy | Mandatory |
| CORPORATE GOVERNANCE | Governo operativo | Corporate governance (assessment circa la conformità alle linee guida dell'EBA in materia di internal governance EBA/GL/2017/11 che entreranno in vigore dal 30.06.2018) | Collegio Sindacale |
| CREDITO | Gestione Crediti a Contenzioso | SIRIO: piattaforma gestione contenzioso | Processo esternalizzato |
| CREDITO | Gestione Garanzie Ipotecarie | Double and Multicounting Collaterals (Finding #3 OSI 1238 BCE) | BCE |
| CREDITO TESORERIA & CAPITAL MGMT | Presidio operazioni di cartolarizzazione Presidio operazioni di cartolarizzazione/cessione di attività collaterizzati | Covered Bond | Mandatory |
| DATA GOVERNANCE | Gestione IT Qualità dei Dati | Data quality LGD | |
| EROGAZIONE ICT | Governo degli ambienti IT | MP Belgio (IT audit) | |



5 Interventi di processo da avviare: Audit Plan 2018 (2/2)

| MACROPROCESSO | PROCESSO | DESCRIZIONE INTERVENTO | NOTE |
|-------------------------|---|---|-----------------------|
| FINANZA | Presidio Adempimenti contabilità | Processo di segnalazione al FITD (Fondo Interbancario di Tutela dei Depositi) della posizione aggregata per depositante | |
| PRODOTTI DEL CREDITO | PRODOTTI DEL CREDITO | Gestione Anticipi | |
| RISK MANAGEMENT | Convalida interna dei sistemi di misurazione dei rischi | Processo convalida AIRB | Mandatory |
| RISK MANAGEMENT | Presidio dei rischi | RAF | Mandatory |
| SERVIZI DI INVESTIMENTO | Gestione del servizio a supporto dei CF | Widiba - Piattaforma WISE a supporto dei servizi di investimento | |
| SERVIZI FIDUCIARI | Gestione dell'incarico fiduciario | MP Fiduciaria Mandati societari - assessment | Attività in servicing |



6 Interventi straordinari: Audit plan 2018

| INTERVENTI CHIUSI | | | | | | | | | |
|-------------------|--------------------------|-------------|--|--------------------|--------------------|----|----|----|---------|
| RICHIEDENTE | DATA RICHIESTA | N. RAPPORTO | DESCRIZIONE INTERVENTO | DATA PUBBLICAZIONE | ORGANI DESTINATARI | | | | |
| | | | | | Pres. CdA | AD | CS | CR | ODV 231 |
| AD/CS | 01/08/2017* | 120/2018 | Follow-up 228/2017 Diamanti | 20/03/2018 | x | x | x | x | |
| AD/CS | 01/08/2017* | - | Aggiornamento Rapporto 120/2018 Diamanti** | 17/04/2018 | x | x | x | x | |
| AD | 01/08/2017* | - | Consulenza forense Deloitte su operatività in diamanti** | 31/05/2018 | x | x | x | x | |
| AD | 29/03/2018 | 149/2018 | Mutui Retail erogati I trim. 2018 | 17/07/2018 | | x | x | x | |
| CdA AD | 10/05/2018 17/05/2018 | - | Consulenza forense Deloitte in relazione alla ricostruzione ** fattuale degli accadimenti e dei flussi informativi inerenti le operazioni di finanza strutturata denominate Santorini e Alexandria | - | x | x | | | |

* Data richiesta iniziale a valle della quale sono stati già effettuati e presentati agli Organi due rapporti (#228/2017 e #229/2017)

** Tali interventi non hanno dato origine a rapporti di audit trattandosi di attività di coordinamento/supporto di consulenze di tipo forensic e/o di follow up, pertanto non sono conteggiati nella tabella «SAL AP 2018» di cui alla slide n.3.

| INTERVENTI IN CORSO | | | | |
|---------------------|----------------|-------------|---|-------------|
| RICHIEDENTE | DATA RICHIESTA | N. RAPPORTO | DESCRIZIONE INTERVENTO | DATA INIZIO |
| CS/ODV 231 | 12/02/2018 | 151/2018 | Servizio Speciale: Antiriciclaggio - Trieste Piazza Borsa - accertamento gestione posizione Hotel Pasteur srl | 13/02/2018 |
| CS | 11/07/2018 | 229/2018 | Approfondimento Incidenti di sicurezza IT anno 2017 | 16/07/2018 |
| CS | 11/07/2018 | 230/2018 | Approfondimento errato calcolo del TEG riferito alla procedura sugli anticipi (usura) | 16/07/2018 |
| CR | 01/08/2018 | 237/2018 | Comitato Rischi - Richiesta di approfondimenti circa le procedure IT ad alta "manualità" | 10/08/2018 |



Allegato - Focus interventi di processo chiusi nel periodo



Revisione SOS di Gruppo (BMPS, Widiba e MP Fiduciaria) - Rapp. 77/2018 (1/6)

ANAGRAFICA INTERVENTO

Intervento: Revisione S.O.S. – Segnalazione Operazioni Sospette di BMPS - Widiba e MP Fiduciaria

Obbligatorietà: NO

Unità auditate: Funzioni AML delle rispettive società

Tipologia di intervento: Settoriale in loco

Data open meeting: 06/04/2018 BMPS 04/05 Widiba 08/05 MP Fiduciaria

Data exit meeting: 27/06/18 MPFiduciaria – 28/06/18 BMPS – 03/07/18 Widiba

ESITO INTERVENTO

GRADE COMPLESSIVO INTERVENTO



La scala di valutazione si articola su quattro livelli a criticità crescente: Rating 1 (VERDE), Rating 2 (GIALLO), Rating 3 (ARANCIONE), Rating 4 (ROSSO).

| FATTORE CAUSALE | DISTRIBUZIONE DEI GAP PER RILEVANZA | | |
|-----------------|-------------------------------------|-------|-------|
| | ALTA | MEDIA | BASSA |
| 👤 Risorse | - | 1 | - |
| 🔄 Processi | 2 | 5 | 1 |
| 🏢 Sistemi | - | - | - |
| Totale | 2 | 6 | 1 |

PRECEDENTI INTERVENTI DI REVISIONE (SE ESISTENTI)

| AMBITO INTERVENTO | PERIODO DELLA VERIFICA | N. RAPPORTO | GRADE INTERVENTO |
|---|------------------------|------------------|------------------|
| BMPS: Processo di Segnalazione operazioni sospette ai sensi D.Lgs 231/01 | 23/10/2015-22/12/2015 | 620/2015 | Parz. Favorevole |
| Widiba | | Primo intervento | |
| MP Fiduciaria – Adempimenti in materia di antiriciclaggio e contrasto al finanziamento del terrorismo | 13/4/2017 -28/6/2017 | 137/2017 | Giallo |

ORGANI DESTINATARI DEL PRESENTE AUDIT

| LEGAL ENTITY | ORGANO DESTINATARIO |
|--------------|-------------------------|
| BMPS | Presidente CdA |
| BMPS | Amministratore Delegato |
| BMPS | Collegio Sindacale |
| BMPS | Comitato Rischi |
| BMPS | OdV 231/01 |



BMPS – Analisi impatti variazioni normativa esterna

Banca MPS ha provveduto ad analizzare gli impatti dell'adeguamento al D.Lgs. 90/17. Dall'analisi sono emerse 25 prescrizioni normative riguardanti il processo di segnalazione delle operazioni sospette, delle quali 20 comportano adeguamenti nei processi/procedure della Banca al fine di conformarsi alle nuove disposizioni. È stato positivamente riscontrato che ognuna di tali prescrizioni è stata associata ad una o più attività pianificate nel Plan AML 2018, con scadenze ragionevoli rispetto alle necessità (più brevi le tempistiche per le variazioni normative, più ampie per le modifiche IT, comunque entro l'anno). Rileva la necessità di procedere ad ulteriore analisi ed eventuale adeguamento al momento dell'entrata in vigore delle nuove «Disposizioni in materia di organizzazione procedure e controlli interni in materia di AML-CFT», correlate al D.Lgs. 90/17 poste in consultazione dalla vigilanza in data 13/04/18.

Widiba - Analisi impatti variazioni normativa esterna

Riscontrata la redazione della gap analysis sugli impatti del D.Lgs. 90/17 per tener conto delle proprie specificità bancarie. Per ogni innovazione normativa la Funzione AML ha delineato azioni specifiche di adeguamento e tale analisi viene costantemente aggiornata ed implementata con le attività in corso. Sono previsti ulteriori adeguamenti dal II semestre 2018 per allineare i processi interni alle nuove Disposizioni di Banca d'Italia attualmente in fase di consultazione, all'emanazione delle istruzioni sulle «comunicazioni oggettive» da parte dell'UIF ed in seguito agli aggiornamenti normativi pubblicati dalla Capogruppo. In tale ambito sono state analizzate le delibere di nomina del Resp. Funzione AML, Delegato SOS e per gli obblighi rafforzati di adeguata verifica sia in relazione alla normativa esterna vigente che al Provvedimento di Banca d'Italia su organizzazione e controlli in materia di AML in consultazione.

MP Fiduciaria - Analisi impatti variazioni normativa esterna

Il D.Lgs. 90/2017 è stato oggetto di analisi autonoma, rispetto a quella di Capogruppo, da parte del Responsabile dell'Ufficio Legale e Antiriciclaggio di M.P. Fiduciaria. Da tale analisi è emerso che gli impatti di maggiore rilevanza per la Controllata sono relativi alla potenziale abolizione dell'archivio unico informatico (al momento mantenuto in attesa di indicazioni specifiche della Capogruppo e di possibili ulteriori evoluzioni normative dettate da Banca d'Italia) ed alle tempistiche di invio delle segnalazioni di operazioni sospette (in mancanza di specifiche di Banca d'Italia M.P. Fiduciaria ha optato per effettuare la segnalazione prima dell'apertura del rapporto o dell'esecuzione dell'operazione). Eventuali integrazioni della normativa della Controllata, comunque, circoscritte, potranno essere effettuate considerando i n. 2 provvedimenti esecutivi di Banca d'Italia in materia di antiriciclaggio in fase di consultazione a partire dal 30 aprile 2018 e, quindi, gli orientamenti della Capogruppo.

Con riferimento agli impatti sul processo di segnalazione delle operazioni sospette, non si rilevano per gli aspetti relativi alla riservatezza delle persone che effettuano la segnalazione o che forniscono informazioni integrative dell'operazione su specifica richiesta dell'U.I.F., necessità particolari di migliorie dato il numero ristretto di Personale coinvolto e la sostanziale continuità di presenza in ruolo. Relativamente, invece, agli aspetti concernenti la generazione dei flussi periodici da inviare all'U.I.F., agli scambi informativi con altri intermediari finanziari ed agli obblighi di astensione di esecuzione dell'operazione, si è in attesa di specifiche legislative che saranno, verosimilmente, contenute nei n. 2 provvedimenti esecutivi precedentemente citati.

BMPS - Esame stato problematiche riscontrate da PWC e in precedenti revisioni

L'esito dell'assessment ha individuato 44 azioni correttive complessive, di cui 20 attinenti al processo SOS o alla «governance» ma con riflessi sul medesimo processo: tra di esse, 15 sono interventi di mitigazione, mentre 5 suggerimenti. Si è osservato positivamente come tutti gli interventi di mitigazione trovino corrispondenza in una o più attività pianificate nel Plan AML 2018: tra di esse sono previsti anche interventi straordinari volti a sanare la problematica relativa allo stock di pratiche in arretrato, sul quale peraltro insiste un gap di audit (IA_2014_189) risalente a verifica svolta nel 2014 e ri-pianificato 5 volte. Permane, infatti, un ritardo nella lavorazione delle pratiche SOS da parte della Funzione AML sebbene lo stock si sia fortemente ridotto e la capacità pro-capite di lavorazione sia cresciuta. E' opportuno quindi proseguire nelle attività adottando per tempo iniziative operative non a carattere straordinario utili ad evitare il riformarsi dello stesso ed a mantenere tempistiche di lavorazione delle singole pratiche coerenti con i dettami normativi (cfr. gap 1 alto Banca MPS - cod. SREP: IG.2.6).

Widiba - Accertamento valenza dei limiti di processo osservati da PWC per la Capogruppo anche per Widiba

Il sistema dei controlli di I e II livello non risulta ancora assestato: pianificata dal 2016 e progressivamente sviluppata una piattaforma (Dashboard) da condividere tra la Funzione AML ed una Struttura che esegua i controlli di I° livello, da costituire all'interno della Digital Branch (DB) in quanto le responsabilità attribuite da Reg. 1 alla DB non sono ottimali per il rispetto dei criteri di riservatezza previsti da normativa – in specie lato IT. L'intervento IT in oggetto è stato schedato entro la fine dell'anno con tempi di rilascio della piattaforma Dashboard per il 2019. Il dimensionamento qualitativo e quantitativo della struttura di AML è stato pianificato dal 2016, ma non è ancora completato.

MPFiduciaria - Accertamento valenza dei limiti di processo osservati da PWC per la Capogruppo anche per MP Fiduciaria

Si sono esaminati, congiuntamente al Responsabile dell'Ufficio Legale e Antiriciclaggio di M.P. Fiduciaria, i "gap" emersi a seguito dell'assessment A.M.L. – C.F.T. condotto da P.W.C. sulla Capogruppo, per accertarne la valenza anche per la Controllata.

In questo senso, non si rilevano, per M.P. Fiduciaria, criticità particolari relativamente agli aspetti di formazione del personale, di chiarezza nella definizione dei ruoli e delle responsabilità degli Uffici interessati al processo delle segnalazioni delle operazioni sospette di riciclaggio, alla formalizzazione delle comunicazioni fra gestori di rete e gli Uffici di Direzione ed alla eccessiva manualità del processo.

Resta, viceversa, ancora aperto il "gap" relativo al dimensionamento quali-quantitativo della Funzione Antiriciclaggio, già evidenziato dalla Controllata nella sua Relazione Annuale A.M.L. 2017 e nell'A.M.L. Plan 2018 e sottolineato, anche, nella Relazione Annuale di Audit 2017.

Con riferimento alle tematiche inerenti lo "stock" delle operazioni ritenute "a rischio" ancora da esaminare, all'articolazione dei controlli di primo e secondo livello ed alla relativa reportistica, si consideri quanto riportato nel sottostante paragrafo concernente il monitoraggio, la gestione ed il controllo delle operazioni sospette.

In merito ai limiti di "circularizzazione" della reportistica verso le Strutture di Capogruppo, rileva, quanto sintetizzato nel sottostante paragrafo inerente all'analisi della reportistica.

BMPS - Gestione Monitoraggio e controllo Operazioni Rischiose

Il contemporaneo incremento della capacità produttiva (10,5 FTE tra task force temporanea – 5,5 – e neo immessi in ruolo – 5 -) e l'applicazione generalizzata del nuovo metodo di lavorazione («sprint») hanno portato ad una notevole crescita della produttività media pro-capite (passata dalle 0,7 pratiche pro-capite medie del gennaio/settembre 2015, alle 1,4 registrate al 31/12/17 fino alle 2,4 registrate ad aprile/maggio 2018) e ad un forte calo dello stock di pratiche arretrate, passato dalle 3.881 pratiche del 31/12/15, alle 3.620 del 31/12/17 fino alle 1.742 del 31/05/18, ormai concentrato su di un solo polo territoriale: emerge il limite dell'attuale sistema delle deleghe territoriali in corso di aggiornamento, che impedisce una redistribuzione dei carichi di lavoro. Le attività svolte dal polo di Siena risultano da normare, come previsto dal Plan 2018, con riguardo particolare all'interscambio informativo verso i poli territoriali dedicati alla lavorazione delle pratiche Gianos nonché alla capacità di tracciatura e rappresentazione dell'attività di propria competenza svolta. Il sistema dei controlli in essere non è risultato adatto a fornire una view processuale congruente, con giudizi sistematicamente sul limite inferiore del range di valutazione senza che siano definite strategie efficaci di mitigazione. Le limitate sinergie tra controlli di primo e di secondo livello, specie a riguardo delle pratiche non valutate rendono incompleto il buon presidio sulla completezza dell'operatività del primo livello di segnalazione rilevato (cfr. gap medio 2 Banca MPS – cod. SREP: IG.6.3).

Widiba - Gestione Monitoraggio e controllo Operazioni Rischiose

La capacità di lavorazione del 1° livello risulta non adeguata: con riferimento 2017-2018 risulta in diminuzione il numero di pratiche dichiarate in arretrato (13%) mentre è significativa la percentuale di pratiche non lavorate dal 1° livello riferita al 2015-2016 (cfr. gap 2 medio – cod. SREP: IG 2.6). Permane un rischio per mancate lavorazioni di SOS su extragianos (veicolate ancora per mail o Sisifo) non presidiato da controlli, parzialmente mitigato da recenti modifiche di processo – indirizzamento delle segnalazioni dei CF direttamente alla Funzione AML. La criticità rilevata sulla logistica della Funzione AML (open space privo del requisito di riservatezza) è stata rimossa a fine giugno 2018 per input della stessa Funzione. I controlli di II livello sono da ridefinire e vengono svolti ancora senza regolarità anche per il mantenimento in carico, da parte della Funzione AML, di attività di controllo in supplenza del 1° livello (cfr. gap 1 medio – cod. SREP: IG 1.2 e 6.3).

MP Fiduciaria - Gestione Monitoraggio e controllo Operazioni Rischiose

Dall'esame dei procedimenti sanzionatori "ex-art. 41" ("mancata segnalazione di operazioni sospette di riciclaggio"), delle richieste di informazioni o di sequestro cautelativo del patrimonio di clienti provenienti dall'Autorità Giudiziaria, delle richieste di adeguata verifica rafforzata trasmesse dal Responsabile dell'Ufficio Gestione Mandati al Responsabile dell'Ufficio Legale e Riciclaggio non si sono rilevati limiti funzionali concernenti il processo di segnalazione delle operazioni sospette di riciclaggio.

Tuttavia, dall'analisi degli "inattesi Weanti" (ossia delle operazioni definite dall'applicativo WEANTI potenzialmente a "rischio di riciclaggio"), si rileva la necessità di efficientare i controlli di 1° livello considerando, nel rispetto dei dettami di "compliance", l'ipotesi di rivedere le modalità di determinazione degli "inattesi", al fine di renderli maggiormente "mirati", e di ottimizzare la tempestività degli accertamenti (cfr. gap n. 1 medio – cod. SREP: IG.6.3). Non sono risultati, inoltre, completi e "tracciati" i controlli di 2° livello da parte dell'Ufficio Legale ed Antiriciclaggio: tali controlli hanno rilevanza particolare per le transazioni con maggiore "punteggio di rischio" inserite nella "fascia di rischio" alta. In questo senso, si osserva la necessità di un "mirato" adeguamento "quali-quantitativo" dell'Ufficio da perseguire nel rispetto degli obiettivi di redditività previsti a "budget" ("crescita sostenibile") (cfr. gap n. 2 medio – cod. SREP: IG.2.6).

Dall'analisi dello stato di aggiornamento dell'adeguata verifica della clientela, si è rilevato, infine, con riferimento al 31/3/2018, che per n. 180 clienti il modulo WEANTI è risultato "non popolato" delle informazioni relative all'adeguata verifica, mentre per n. 585 clienti (di cui n. 154 definiti dall'applicativo WEANTI con profilo di "rischio alto" e n. 431 con "profilo di rischio" medio), l'adeguata verifica è risultata scaduta e non aggiornata. Di tale problematica il Direttore Generale ha opportunamente informato il C.d.A. della Controllata. Dato quanto osservato, si ritiene necessario monitorare con frequenza almeno mensile la situazione dei clienti con adeguata verifica assente o scaduta rendicontando in maniera sistematica gli Organi Apicali di M.P. Fiduciaria. Quindi, considerando gli esiti dell'attività di monitoraggio e raccordandosi, come da accordi stipulati, con la Capogruppo e Widiba, occorrerà identificare eventuali limiti nelle singole fasi del processo di aggiornamento per superarli (cfr. gap n. 1 alto – codice SREP: IG.2.12).

Revisione SOS di Gruppo (BMPS, Widiba e MP Fiduciaria) - Rapp.77/2018 (5/6)

ANALISI DELLA
REPORTISTICA
PERIODICA
PRODotta PER
I VERTICI
AZIENDALI E
PER GLI
ORGANISMI DI
CONTROLLO

BMPS - Analisi della normativa interna e accertamento della funzionalità del processo relativo alla produzione della reportistica aziendale

Nel documento D 01915 sui Flussi Informativi si prevede la predisposizione di una Relazione e di un Piano di Attività annuali da inviare. È inoltre contemplata la trasmissione di una informativa trimestrale sul tema dell'Antiriciclaggio nella quale si dettaglia, tra le altre, le contestazioni ricevute dal MEF nonché il numero di segnalazioni sospette inoltrate e archiviate.

Gli esiti delle verifiche hanno condotto ad appurare l'effettivo invio della reportistica come sopra descritto. Inoltre, si è potuto riscontrare lo scambio informatizzato del profilo di rischio tra le Società del Gruppo assumendo il livello più alto tra quelli presenti. Viceversa, risulta migliorabile il flusso informatizzato fra la Capogruppo e MP Fiduciaria, delle informazioni relative ai clienti condivisi oggetto di segnalazione di operazione sospetta di riciclaggio (cfr. **gap 3 medio Banca MPS - cod. SREP: IG.2.11**).

Widiba - Analisi della reportistica per i Vertici Aziendali e degli scambi informativi da / verso la Capogruppo

Verificata la presenza della mappatura dei flussi informativi SCI - verticali, orizzontali, verso l'esterno - allegata alla Policy SCI di WIDIBA (D.10 v. del 2015). Riscontrata la redazione e l'invio agli organi di Vertice – anche per il tramite di altre Funzioni Aziendali – dei flussi obbligatori previsti dalle disposizioni di Banca d'Italia. Prodotta e condivisa anche la reportistica trimestrale.

Da rivalutare l'attualità e l'utilità a fini di presidio della materia di taluni flussi informativi, sia verticali che orizzontali, poiché risultano censiti ma non prodotti e, in caso di necessari adeguamenti al mutato contesto, sottoporli all'approvazione del CdA; infine necessaria alla base una condivisione con Capogruppo dei criteri di rendicontazione al fine di fornire una visione omogenea a livello di Gruppo (cfr. **gap 3 basso – cod. SREP: IG 2.11**).

MP Fiduciaria - Analisi della reportistica per i Vertici Aziendali e degli scambi informativi da / verso la Capogruppo

La Relazione Annuale ed il Piano Annuale sono state trasmesse alla Funzione Antiriciclaggio della Capogruppo per la condivisione finale in data 22/2/2018 e sono state approvate dal C.d.A. della Capogruppo nella seduta del 27/2/2018. Le Comunicazioni trimestrali sono risultate opportunamente inviate a B.M.P.S. e compilate in conformità agli "standard" previsti dalla Capogruppo.

Dall'esame della realtà operativa, si è potuto riscontrare che è attivo uno scambio informatizzato, da / verso B.M.P.S e le altre Società del Gruppo, finalizzato alla omogeneizzazione al livello più alto del "profilo di rischio" dei clienti condivisi. Si rileva, tuttavia, la necessità di ottimizzare lo scambio informatizzato avente lo scopo di condividere, a livello di Gruppo, anche la clientela già oggetto di segnalazione di operazione sospetta da parte di una singola Società (ambito di miglioramento).



BMPS - Focus D.Lgs. 231/01 in ambito Segnalazione Operazioni Sospette

Il Modello 231 connesso al processo di gestione delle SOS, redatto nel 2015 ed attualmente in vigore, è risultato coerente come strutturazione (assegnazione delle fasi di processo, dei rischi sottostanti e dei presidi atti a mitigarli). La revisione del catalogo dei controlli di II livello, così da fornire una visione più accurata del processo / rischi sottostanti, e lo smaltimento dell'arretrato di lavorazione delle pratiche oggetto di segnalazione avranno esito di rafforzare ulteriormente il Modello.

Widiba - Focus D.Lgs. 231/01 in ambito Segnalazione Operazioni Sospette

Stante gli esiti delle verifiche condotte, si ritiene che i presidi a mitigazione dei rischi 231/01 connessi alle fasi di processo SOS nella responsabilità della Direzione AML & Risk siano parzialmente da rafforzare. L'efficacia del sistema dei controlli e del Modello Organizzativo 231 di WIDIBA risulterà rinforzato con la attuazione delle attività, al momento in corso, finalizzate ad una migliore strutturazione dei controlli di I livello e, conseguentemente, di II livello. Per una maggiore efficacia del sistema dei controlli interni si reputa quindi utile la prevista condivisione con il I livello della dashboard, la predisposizione di flussi informativi sugli esiti dei controlli svolti dalla Digital Branch, rivalutando l'utilità e l'attualità di quelli attualmente censiti nella Policy SCI di Widiba (anno 2015).

MP Fiduciaria - Focus D.Lgs. 231/01 in ambito Segnalazione Operazioni Sospette

Dall'esame dei verbali dell'Organismo di Vigilanza "ex – D.Lgs. 231/01" non sono emersi elementi di rilievo.

Si è riscontrato, inoltre, per le attività relative alle segnalazioni di operazioni sospette di riciclaggio, che la Funzione Compliance (esternalizzata in Capogruppo) ha elaborato, a seguito di un "self-assessment" da cui non sono emersi elementi di rischio rilevante, opportuni "protocolli di controllo" in cui si dettagliano per le Strutture Aziendali interessate (Ufficio Gestione Mandati e Ufficio Legale e Antiriciclaggio) gli strumenti di controllo ("set" di norme interne e controlli specifici) atti a prevenire la commissione di reati "ex – D.Lgs. 231/01" (reato ex-art. 2638 c.c. – Ostacolo all'esercizio delle funzioni delle autorità pubbliche di Vigilanza).

Gli accertamenti eseguiti durante la revisione hanno permesso di riscontrare la funzionalità di tali strumenti di controllo.

La Funzione Formazione della Capogruppo ha confermato che i corsi di formazione obbligatoria, in tema di "Responsabilità Amministrativa delle Società – D.Lgs. 231/2001", sono stati completati da ciascuna risorsa di M.P. Fiduciaria.

Revisione SOS di Gruppo - Rapp.77/2018 - BMPS audit finding

| N. | PROCESSO | GAP | RILEVANZA (A/M/B) | FATTORE CAUSALE | RACCOMANDAZIONE | STRUTTURA OWNER | SCADENZA (GG/MM/AA) |
|----|--|--|----------------------|--------------------|--|------------------------|------------------------|
| 1 | Gestione obblighi di segnalazione operazioni sospette di riciclaggio | Stock arretrato di pratiche SOS Ritardo nella lavorazione delle pratiche SOS da parte del II livello di valutazione: lo stock di pratiche arretrate è stato ridotto (passando dalle 3.881 pratiche del 31/12/15 alle 1.742 del 31/05/18) e la capacità pro-capite di lavorazione cresciuta (passando dalle 0,7 pratiche pro-capite medie del gennaio/settembre 2015 alle 2,4 registrate ad aprile/maggio 2018), tuttavia permane una quota consistente di pratiche riferite all'anno 2017 (948 al 31 maggio 2018). | A | ↔ | Proseguire nell'attività volta ad eliminare l'arretrato di lavorazione adottando per tempo iniziative operative non a carattere straordinario (gestione del turnover previsto, flessibilità delle modalità di lavoro) utili ad evitare il riformarsi dello stesso ed a mantenere tempistiche di lavorazione delle singole pratiche coerenti con i dettami normativi. Ciò in considerazione del periodico riaccumularsi di pratiche che ha comportato la ri-pianificazione per 5 volte del precedente gap (IA2014_ 189) emesso nel corso della revisione conclusasi al termine del 2014. | F. AML | 31.12.18 |
| 2 | Gestione obblighi di segnalazione operazioni sospette di riciclaggio | Controlli non adatti a fornire una visione di processo La struttura dei controlli risulta da rafforzare, ciò allo scopo di fornire una visione più accurata e puntuale del processo e dei rischi sottostanti: i controlli attuali sono mirati ad intercettare fenomeni negativi su basi non statistiche e con metodologie in alcuni casi da revisionare (si veda ad esempio le mancate risposte in tempo utile da parte delle strutture sui nominativi campionati: sono considerati errori anziché esser escluse dai calcoli), restituendo valutazioni (92% dei 50 controlli mensili in 10 mesi riportano vulnerabilità «molto significativa») non rappresentative del processo. | M | ↔ | Revisionare il catalogo dei controlli di secondo livello: <ul style="list-style-type: none">da un punto di vista metodologico (scelta dei fenomeni di rischio da sottoporre a controllo, capacità di fornire una view di processo tramite una valutazione statistica, definizione di una strategia di mitigazione del rischio che si è deciso di controllare, seguimiento delle problematiche);dal punto di vista del perimetro da presidiare, intercettando aspetti attualmente non coperti (operatività della struttura VOS, efficacia controlli 1° livello su pratiche non valutate dalle filiali, specie se extragianos). | F. AML | 31.12.18 |
| 3 | Gestione obblighi di segnalazione operazioni sospette di riciclaggio | Limiti nello scambio fra la Capogruppo e M.P. Fiduciaria relativamente all'informativa relativa ai clienti condivisi oggetto di segnalazione di operazione sospetta di riciclaggio Si rilevano carenze nello scambio delle informazioni relative ai clienti condivisi oggetto di segnalazione di operazione sospetta di riciclaggio. | M | ↔ | Occorre rendere pienamente operativo lo scambio informatizzato, non automatizzato a causa dei differenti sistemi informativi, fra la Capogruppo e MP Fiduciaria, dei clienti condivisi oggetto di segnalazione di operazione sospetta di riciclaggio e in generale rafforzare tale flusso su tutte le controllate. | F.AML | 31.07.18 |
| | | | | | | CHIUSURA 08.08.2018 | |

📁 Sistemi ↔ Processi 👤 Risorse



Revisione SOS di Gruppo - Rapp.77/2018 - Widiba audit finding

| N. | PROCESSO | GAP | RILEVANZA (A/M/B) | FATTORE CAUSALE | RACCOMANDAZIONE | STRUTTURA OWNER | SCADENZA (GG/MM/AA) |
|----|--|-----|----------------------|--------------------|--|--------------------|------------------------|
| 1 | Gestione obblighi di segnalazione operazioni sospette di riciclaggio Controlli di 1° e 2° livello Impostazione del sistema dei controlli di 1° e 2° livello da rafforzare. La Funzione di 2° livello svolge attività di 1° livello supplendo alla struttura deputata da Regolamento n. 1 (Digital Branch – responsabile anche della lavorazione). Tale situazione limita il perimetro delle verifiche nella sua estensione e la regolarità della frequenza con la quale vengono svolte quelle attualmente previste. | | M | ⇔ | Rimodulare il sistema dei controlli nel seguente modo: 1) completare gli interventi previsti dal piano AML per la costituzione di un'efficace struttura che si occupi della lavorazione delle pratiche SOS e dei controlli di 1° livello; 2) delegare alla neocostituita struttura i controlli di 1° livello; 3) ridefinire il catalogo dei controlli in carico alla Funzione AML e svolgere con tempistiche congrue i controlli sulla completezza dell'attività operativa del 1° livello, sulle abilitazioni agli applicativi (Gianos e Dashboard), sulla possibile mancata lavorazione di extragianos segnalate da addetti/ CF (per ciascuna categoria non abilitata al Gianos) e sull'andamento delle fasi di lavorazione (tempistiche e carichi di lavoro). | F. AML Widiba | 31.12.18 |
| 2 | Gestione obblighi di segnalazione operazioni sospette di riciclaggio Monitoraggio attività di lavorazione pratiche Digital Branch La lavorazione delle pratiche da parte della Digital Branch, sulla cui completezza è previsto un controllo di secondo livello (MTR 01), risulta non presidiata da un'attività di controllo adeguata a rilevare e mantenere le tempistiche di lavorazione entro termini ragionevoli: continua a mantenersi alta la quota di pratiche Gianos Inattesi non valutate (13% da luglio 2017 a maggio 2018). | | M | ⇔ | Proseguire con l'attività di regolarizzazione delle pratiche non esitate richiesta alla struttura di primo livello, finalizzandola a sanare l'arretrato in tempi brevi. Assicurare e documentare uno stretto presidio dell'operatività di lavorazione della Digital Branch, definendo in normativa le tempistiche massime di lavorazione per le singole tipologie di pratiche e monitorandone l'effettivo rispetto. | F. AML Widiba | 31.12.18 |
| 3 | Gestione obblighi di segnalazione operazioni sospette di riciclaggio Flussi informativi e criteri per l'elaborazione dei dati a) Flussi informativi non redatti. In particolare, n. 2 flussi orizzontali (mensili e trimestrali) mappati dalla Policy SCI di WIDIBA non sono redatti (1 con owner la Funzione AML verso la Direzione People & Finance e n. 1 con owner Digital Branch verso AML); b) i criteri utilizzati per l'elaborazione dei dati rendicontati a Capogruppo e ai Vertici Aziendali sono differenti da quelli in uso presso la Capogruppo stessa. | | B | ⇔ | Rivalutare l'attualità e l'utilità dei flussi attualmente disciplinati dalla Policy SCI di Widiba (anno 2015) ai fini del presidio dell'ambito SOS e della disciplina AML nel suo complesso. Condividere con la Capogruppo, i criteri di elaborazione dei dati rendicontati in modo da permetterne il raccordo a livello di Gruppo (Es. pratiche Gianos vs protocolli UIF). | F. AML Widiba | 31.12.18 |

📁 Sistemi ⇔ ⚙️ Processi 📌 Risorse



Revisione SOS - Rapp.77/2018 - MP Fiduciaria audit finding

| N. | PROCESSO | GAP | RILEVANZA (A/M/B) | FATTORE CAUSALE | RACCOMANDAZIONE | STRUTTURA OWNER | SCADENZA (GG/MM/AA) |
|----|--|---|----------------------|-----------------|--|--------------------------|------------------------|
| 1 | Gestione adempimenti operativi per il contrasto al riciclaggio e al finanziamento del terrorismo | Limiti nell'attività di aggiornamento dell'adeguata verifica del cliente. Analizzando la "base-dati" di WEANTI al 31/03/2018, si è riscontrata, per n. 180 dei n. 2182 clienti attivi, l'assenza delle informazioni relative all'adeguata verifica, mentre per n. 585 clienti (di cui n. 154 con "profilo di rischio" alto e n. 431 con "profilo di rischio" medio) l'adeguata verifica è risultata scaduta e non aggiornata. | A | ↔ | Occorre rendere pienamente operativo un processo di monitoraggio almeno mensile dell'attività di aggiornamento dell'adeguata verifica. Tale monitoraggio dovrà permettere di accertare tempestivamente eventuali limiti delle singole fasi del processo ("colli di bottiglia") per facilitare il loro rapido superamento. Gli esiti dell'attività di monitoraggio dovranno essere rendicontati in maniera sistematica agli Organi Apicali della Società. | Ufficio Gestione Mandati | 31.12.18 |
| 2 | Gestione adempimenti operativi per il contrasto al riciclaggio e al finanziamento del terrorismo | Limiti nella tempestività dei controlli 1° livello sugli "inattesi - WEANTI". Relativamente al periodo 1/2/2018 – 31/3/2018, per gli "inattesi - WEANTI", i controlli di 1° livello, di competenza dell'Ufficio Gestione Mandati, sono stati limitati a n. 152 dei n. 1.104 casi complessivi (data di esecuzione degli accertamenti: 18/5/18). | M | ↔ | Ottimizzare la tempestività delle verifiche, considerando, anche, l'ipotesi di rivedere, nel rispetto dei dettami di "compliance", le modalità di determinazione degli "inattesi" al fine di renderli maggiormente "mirati". | Ufficio Gestione Mandati | 31.12.18 |
| 3 | Gestione adempimenti operativi per il contrasto al riciclaggio e al finanziamento del terrorismo | Limiti nell'esecuzione dei controlli di 2° livello sugli "inattesi - WEANTI". Relativamente al periodo 1/1/2017 – 31/3/2018, i controlli di 2° livello dell'Ufficio Legale ed Antiriciclaggio sugli "inattesi - WEANTI" non sono risultati completi ed opportunamente "tracciati". Tali controlli sono di particolare rilevanza per le transazioni con "maggiore punteggio di rischio" inserite nella "fascia di rischio" alta. | M | 👤 | L'attuale dimensionamento "quali-quantitativo" dell'Ufficio Legale ed Antiriciclaggio impone di definire delle priorità di azione che conducono a dedicare le risorse disponibili alle attività operative sottraendole a quelle di controllo. Si rileva, quindi, la necessità di un "mirato" adeguamento della Struttura, da perseguire nel rispetto degli obiettivi di redditività previsti a "budget" ("crescita sostenibile"), al fine di potere opportunamente rafforzare l'attività di controllo di 2° livello. | Ufficio Antiriciclaggio | 30.09.18 |

📁 Sistemi ↔️ Processi 👤 Risorse



Revisione LGD – Data Quality TRIM – Rapp. 41/2018 (1/3)

ANAGRAFICA INTERVENTO

Intervento: Revisione LGD – Data Quality

Obbligatorietà: NO

Unità auditate: - Servizio Credit Risk Models/Area Lending Risk Officer/Direzione CRO
- Servizio Data Governance e Reporting Management/Area Pianificazione, CDG e Data Governance/Direzione CFO
- Servizio Applicazioni Bilancio e Rischi/Area Applicazioni Governo/COG
- Servizio Gestione Portafoglio Creditizio/Area Credi Portfolio Governance/ Direzione CLO
- Servizio Gestione Recupero Crediti /Area Recupero Crediti/Direzione Crediti non performing/Direzione CLO

Tipologia di intervento: Settoriale

Data open meeting: 26/03/2018

Data exit meeting: 11/07/2018

ESITO INTERVENTO

GRADE COMPLESSIVO INTERVENTO

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

La scala di valutazione si articola su quattro livelli a criticità crescente: Rating 1 (VERDE), Rating 2 (GIALLO), Rating 3 (ARANCIONE), Rating 4 (ROSSO).

| FATTORE CAUSALE | DISTRIBUZIONE DEI GAP PER RILEVANZA | | |
|-----------------|-------------------------------------|-------|-------|
| | ALTA | MEDIA | BASSA |
| Risorse | 1 | | |
| Processi | 2 | 1 | 2 |
| Sistemi | 2 | | |
| Totale | | 1 | 2 |

PRECEDENTI INTERVENTI DI REVISIONE (SE ESISTENTI)

ORGANI DESTINATARI DEL PRESENTE AUDIT

| AMBITO INTERVENTO | PERIODO DELLA VERIFICA | N. RAPPORTO | GRADE INTERVENTO |
|-------------------|------------------------|-------------|------------------|
|-------------------|------------------------|-------------|------------------|

| LEGAL ENTITY | ORGANO DESTINATARIO |
|--------------|---------------------|
|--------------|---------------------|



GOVERNANCE

Chiaro assetto organizzativo, adeguata cultura del rischio ed informazioni strategiche condivise

I ruoli e le responsabilità risultano adeguatamente delineati sia nelle direttive interne inerenti il Sistema di Gestione della Data Governance sia nella documentazione relativa alle progettualità (BR 60265 e 41766). È attualmente in corso l'aggiornamento della normativa interna nelle sezioni Elenco Funzioni e Ruoli Interessati poiché il quadro di raccordo tra Funzioni/Ruoli e Strutture/Organi citato in normativa non risulta aggiornato rispetto all'attuale struttura organizzativa.

Nell'ambito del Regolamento n. 1 sono adeguatamente definite le linee di riporto gerarchico e risulta ben individuabile il collocamento dei ruoli in ambito di Sistema di Gestione della Data Governance. Dai frequenti aggiornamenti del Regolamento n. 1 in merito alle funzioni Governo e Supporto Data Governance – intercorsi anche durante la revisione – si evince che il processo di definizione del Sistema di Gestione della Data Governance non è ancora concluso.

Sulla base delle informazioni fornite dai responsabili delle strutture auditate si apprezza un congruo livello di cultura del rischio da parte delle risorse, sviluppato attraverso la partecipazione a corsi di Risk Management ed eventi di riversamento interno, nonché un'adeguata condivisione delle informazioni strategiche, incluse quelle relative alla gestione del rischio.

REPORTING

Adeguati flussi informativi

Rileva la presenza di un adeguato flusso informativo tra la Funzione Supporto Data Governance e la Funzione di Business responsabile per l'output rilevante LGD, nel rispetto delle prescrizioni previste dalla normativa interna relativa allo Standard Documentale di Data Governance. Sono stati riscontrati, inoltre, adeguati e strutturati flussi informativi, sia verticali che orizzontali. Ai fini del passaggio in produzione dei controlli di Data Quality sulla piattaforma di data quality IrionDQ, si apprezza il fatto che sia stato opportunamente attivato un flusso informativo tra Business Data Steward e Technical Data Steward in modo da gestire le anomalie storiche (ovvero quelle emerse nelle serie storiche e non oggetto di trattamento in IrionDQ).

DATA LINEAGE E DOCUMENTAZIONE TECNICA

Documentazione tecnica disallineata e non completa che comporta la mancata replicabilità

L'analisi della documentazione tecnica ha fatto **emergere alcuni elementi di criticità legati alla non coerenza fra i diversi documenti prodotti e il mancato allineamento di questi alle procedure attualmente in produzione. Questo non rende possibile ricostruire l'intero processo senza ricorrere ai testi delle query utilizzate (GAP 1)**. Le anomalie riscontrate sono state comunicate già alla struttura owner e, pertanto, si richiede la tempestiva conclusione delle attività di analisi di quanto segnalato e la conseguente revisione della documentazione tecnica.

In particolare la maggiore criticità emersa dalle analisi di data lineage riguarda l'indicazione della tabella relativa ai movimenti utilizzata per la costruzione della base dati finale. Dai documenti, infatti, questa risulta essere la FY3009E_KZ_MOVIMENTI ma gli approfondimenti condotti hanno permesso di appurare, invece, l'utilizzo della FY3015E_KZ_MOVIMENTI_VAL che differisce dalla precedente in quanto viene costruita considerando come campo chiave la data valuta che, nella prima tabella, non viene utilizzata.

Dagli approfondimenti con la Funzione Risk Management emerge inoltre che è in corso una revisione del documento metodologico ai fini di un suo allineamento alle procedure utilizzate.

CONTROLLI

Parziale tracciabilità dei controlli svolti dalla funzione RM

Le dimensioni di Data Quality previste dalle direttive interne risultano solo parzialmente coperte dai controlli definiti dal Business Data Steward in relazione all'output rilevante LGD, avendo verificato che risultano coperte soltanto "Accuratezza", "Completezza" e "Correttezza".

I controlli risultano concentrati sulla fase di alimentazione dei dati e non nella procedura di calcolo del parametro LGD. Pertanto, **si richiede il completamento, all'interno della progettualità in corso (BR 72440), dell'inserimento dei controlli riguardanti gli importi su esposizioni/movimenti/spese indirette. Per quanto concerne il controllo sulle garanzie, viste le difficoltà nelle implementazioni, si richiede che questo venga effettuato al di fuori dell'applicativo IrionDQ ma che venga, comunque, tracciato in termini di esito, anomalie e soluzioni (Gap 2).**

PROCESSO ELABORATIVO BASE DATI

Coerenza delle informazioni tra le diverse basi dati

L'attività di ricostruzione delle basi dati utilizzate al fine del calcolo del parametro LGD ha consentito di individuare le tabelle del DWHC a partire dalle quali vengono estratte le principali informazioni. Le analisi delle query di elaborazione, ed in particolare il confronto delle informazioni tra i diversi data base, non ha evidenziato differenze significative. La Funzione Risk Management ha confermato la coerenza funzionale dell'assegnazione degli attributi.

Tuttavia sono emersi sia dei disallineamenti dei dati relativi alle garanzie ipotecarie tra gli applicativi gestionali sia la presenza di un numero anomalo di garanzie ipotecarie dello stesso importo e dello stesso garante. Pertanto, si richiede di individuare tali casistiche e di valutare, nel caso in cui non sia possibile ricostruire la veridicità del dato, la necessità e la fattibilità di interventi correttivi sulla base dati (Gap 3).

Revisione LGD – Data Quality TRIM - *Rapp. 41/2018 - Audit finding*

| N. | PROCESSO | GAP | RILEVANZA (A/M/B) | FATTORE CAUSALE | RACCOMANDAZIONE | STRUTTURA OWNER | SCADENZA (GG/MM/AA) |
|----|-------------------------------|--|----------------------|--------------------|---|---|------------------------|
| 1 | Governance Rischio Credito | Documentazione tecnica non coerente, non allineata alla procedura in uso. Data lineage frammentario. | M | ↔ | Rivedere la documentazione tecnica | COG - Servizio Applicazioni Bilancio e Rischi | 30/09/2018 |
| 2 | Rischio di Credito | Controlli di Risk Management non inseriti nei progetti di implementazione su IrionDQ. | B | ↔ | Completare l'inserimento dei controlli nel BR 72440 e tracciare i controlli svolti extra-IrionDQ. | BMPS - Servizio Credit Risk Models | 31/12/2018 |
| 3 | Rischio di Credito | Presenza di valori anomali sulle garanzie ipotecarie | B | ↔ | Valutare interventi correttivi sulla base dati | BMPS - Servizio Credit Risk Models | 31/03/2019 |

 Sistemi
  Processi
  Risorse



Revisione High Risk – Rapp. 70/2018 (1/3)

ANAGRAFICA INTERVENTO

Intervento: Revisione High Risk
Obbligatorietà: NO
Unità auditata/e: Direzione CLO – Area High Risk
Tipologia di intervento: revisione ordinaria
Data open meeting: [11/04/2018]
Data exit meeting: [26/07/2018]

ESITO INTERVENTO

| GRADE COMPLESSIVO INTERVENTO | | | |
|------------------------------|----------------------|-------------------------|---------------------|
| Rating 1 (VERDE) | Rating 2 (GIALLO) | Rating 3 (ARANCIONE) | Rating 4 (ROSSO) |

La scala di valutazione si articola su quattro livelli a criticità crescente: Rating 1 (VERDE), Rating 2 (GIALLO), Rating 3 (ARANCIONE), Rating 4 (ROSSO).

| FATTORE CAUSALE | DISTRIBUZIONE DEI GAP PER RILEVANZA | | |
|-----------------|-------------------------------------|-------|-------|
| | ALTA | MEDIA | BASSA |
| 👤 Risorse | - | 1 | 1 |
| 🔄 Processi | - | 1 | - |
| 🏠 Sistemi | - | - | - |
| Totale | - | 2 | 1 |

PRECEDENTI INTERVENTI DI REVISIONE (SE ESISTENTI)

| AMBITO INTERVENTO | PERIODO DELLA VERIFICA | N. RAPPORTO | GRADE INTERVENTO |
|-------------------|------------------------|-------------|------------------|
| NA | NA | NA | NA |

ORGANI DESTINATARI DEL PRESENTE AUDIT

| LEGAL ENTITY | ORGANO DESTINATARIO |
|--------------|-------------------------|
| BMPS | Presidente del CdA |
| BMPS | Amministratore Delegato |
| BMPS | Collegio Sindacale |
| BMPS | Comitato Rischi |



Revisione High Risk – Rapp. 70/2018 (2/3)

OVERVIEW

Il Roll-Out del progetto High Risk si è concluso a Luglio 2017 con l'attivazione di un modello operativo specialistico, sia a livello Centrale che Territoriale, dedicato alla gestione del portafoglio creditizio contraddistinto dalla presenza di elementi di rischio (c.d criteri di ingresso). La filiera HR a livello Centrale è gestita dall'Area HR che si articola in 2 strutture, il Servizio Delibere HR, la cui mission è quella di presidiare la corretta classificazione del proprio portafoglio di riferimento, valutando e deliberando le proposte di classificazione e di rimodulazione degli affidamenti, e svolgendo attività di advisory all'Area Credito Territoriale e il Servizio Qualità Processo Creditizio (SQPC), al quale è affidato il presidio della qualità del portafoglio crediti High Risk e Low Risk per tutti i Mds della Banca, mediante la prevenzione e la gestione dei fenomeni di deterioramento, fornendo assistenza e consulenza alle ACT, tramite gli Uffici Qualità Monitoraggio (UQM). Nel momento in cui si verificano contemporaneamente le caratteristiche indicate come criteri di uscita, le controparti restano nel perimetro HR per 4 mesi, rimanendo in stato di monitoraggio. La classificazione a IPRA, Sofferenza o l'avvio di una ristrutturazione comporta la perdita dell'attributo HR. Al 30/03/2018 il portafoglio High Risk era costituito da 150.022 ndc, pari a un utilizzato complessivo di €Mln 6.064, di cui 76,17% in stato amministrativo Performing.

DINAMICHE PORTAFOGLIO HR

Al 30/03/18 le cause principali di ingresso nel perimetro HR sono «Performing con almeno un Forborne» e «Performing con sconfinamenti >45 gg» (€Mln 2.297). I flussi di uscita dal portafoglio HR, nel periodo Gennaio 2018 - Maggio 2018, sono rappresentati per oltre il 69% da posizioni ritornate nel perimetro Low Risk. Tuttavia nello stesso arco temporale si assiste ad una dinamica del numero di ingressi in HR frequentemente superiore alle uscite. Emerge, quindi, la necessità di rafforzare le misure atte alla prevenzione del deterioramento del merito creditizio in quelle posizioni Low Risk che presentano maggiori criticità. La normativa aziendale prevede fattispecie esclusivamente automatiche di targatura in HR e riconduzione in Low Risk delle posizioni, ciò nonostante dal 01/01/2018 al 07/06/2018, 45 controparti sono state interessate da modifiche manuali, di cui 6 con «stargatura» HR (esenzione da HR e riconduzione in LR) ancora in corso e 39 con periodo di esenzione terminato. La «targatura» manuale di ingresso in HR ha interessato 5 controparti. Tali fattispecie rivestono carattere di eccezionalità e sono frutto di condivisione tra più livelli gerarchici delle filiere HR e LR. Viene richiesto, quindi, alle funzioni owner di normare tale processo elencando le casistiche in cui è ammesso il procedimento manuale a correzione dell'automatismo e predisporre idonea attività di rendicontazione (Cfr. Gap n. 1).

ANALISI CAMPIONE DI DELIBERE

Le verifiche hanno riguardato un campione di 54 delibere, assunte dalle strutture centrali, su posizioni HR nel periodo 01/01/2018-31/03/2018 corrispondenti ad totale deliberato di €Mln 237,3, pari al 79% per controparti e al 77% dei volumi complessivi delle delibere di periodo. Gli esiti sull'adeguatezza dell'istruttoria non evidenziano significative criticità, con il 98% di evidenze positive. Corretta anche la valutazione del patrimonio responsabile e la scelta della forma tecnica in relazione alle esigenze finanziarie del cliente ed alla sua rischiosità. Coerentemente con quanto riportato in normativa, le delibere campionate rientrano tutte in Area Riqualificazione e non prevedono concessioni di nuova finanza. Relativamente alla correttezza della gestione operativa della pratica di rischio il 76% del campione analizzato ha dato esito positivo, 3 delle 4 pratiche in mora di revisione, al momento delle analisi, sono state rinnovate nel corso dell'intervento di Audit. La quarta pratica è stata classificata UTP. In 6 casi (Cfr. Gap n. 2) le garanzie non risultavano correttamente perfezionate (di queste, una è stata regolarizzata in corso di revisione). In 6 occasioni il rispetto delle condizioni di delibera è parso non soddisfatto/controllato. Per la posizione ANGELANTONI LIFE SCIENCE S.R.L. – NDC 213375692, si ritiene opportuna la riconduzione nel perimetro High Risk al fine di procedere ad una valutazione complessiva sulla classificazione del gruppo Angelantoni, in considerazione delle forti perdite e delle dinamiche reddituali e patrimoniali negative che il bilancio consolidato di gruppo riporta (Cfr. Gap n. 3).



Il Processo di monitoraggio e presidio della qualità del portafoglio creditizio della Banca è il risultato delle interazioni tra più Funzioni, il Servizio Qualità Processo Creditizio, gli Uffici Qualità e Monitoraggio di Area Territoriale e i gestori delle relazioni in rete. Il dato di partenza di tale attività è rappresentato dall'analisi dei KPI, elaborati dal Servizio Credit Control Unit, che formano la base per poi sviluppare ed attuare il piano di azione correttive dei fenomeni di rischio individuati.

Tali indicatori, nei primi 5 mesi del 2018, non mostrano un trend costante bensì risultati discontinui in particolare per i KPI «incidenza nuovi sconfinamenti >30 gg delle esposizioni Forborne PE» e «tasso di cura delle esposizioni Forborne NPE».

Gli obiettivi gestionali previsti sono stati raggiunti e/o superati per i KPI «tasso di mora di revisione HR» e «incidenza sconfinamenti >30 gg delle esposizioni Forborne PE». Relativamente ai KPI «tasso di cura delle esposizioni forborne NPE» e «tasso regolarizzazione sconfinamenti 20-90», il budget, invece, non è stato conseguito: per quest'ultimo indice si denota comunque un trend positivo di riduzione degli sconfinamenti.

Le analisi condotte sugli esiti delle campagne esaminate (periodo gennaio-aprile 2018) evidenziano una bassa percentuale di obiettivi intermedi presenti al termine del primo ciclo operativo. Le riduzioni di sconfinamenti Forborne 1-24 gg e 25-89 gg si attestano rispettivamente al 39% e 55%.

Nell'attuale organigramma del CLO il SQPC fa parte dell'Area High Risk pur svolgendo attività di monitoraggio e indirizzo anche per le posizioni rientranti nel perimetro Low Risk e ha autorità funzionale ma non gerarchica sugli UQM di AT. A oggi, quindi, nonostante le molteplici iniziative intraprese dal Servizio SPQC, la risposta della Rete risulta da rafforzare. Tale soluzione organizzativa si estrinseca in una non sempre efficace unità nella filiera di gestione e indirizzo tra le strutture centrali e gli uffici periferici di Area Territoriale, la cui reattività e incisività nell'azione di monitoraggio e risoluzione delle anomalie/sconfinamenti presenta margini di miglioramento. A tal proposito è stata interessata la Direzione Rete al fine di condividere la necessità di sottolineare l'importanza della partecipazione attiva delle strutture territoriali al fine di ottenere una più efficace finalizzazione dell'attività di controllo di primo livello, anche nell'ottica dell'ottimizzazione della sinergia con le strutture del CLO.

Revisione High Risk – Rapp. 70/2018 – Audit finding

| N. | PROCESSO | GAP | RILEVANZA (A/M/B) | FATTORE CAUSALE | RACCOMANDAZIONE | STRUTTURA OWNER | SCADENZA (GG/MM/AA) | CODICE OB SREP |
|----|----------|---|----------------------|-----------------|--|--------------------|------------------------|-------------------|
| 1 | Credito | Carenze nell'impianto normativo di processo Nel periodo di analisi (01/01/2018 al 07/06/2018) sono stati rilevate modifiche manuali di ingresso/uscita dal perimetro High Risk. | M | ⇔ | Declinare nella normativa, D02226 «Regole generali in materia di Gestione e Monitoraggio operativo del credito», i casi in cui è ammesso il procedimento manuale a correzione dell'automatismo ingresso/uscita dal perimetro High Risk e predisporre idonea attività di rendicontazione periodica. | Area High Risk | 31/12/18 | IG.1.2 |
| 2 | Credito | Mancato perfezionamento delle garanzie Al 18/07/2018 risultavano le seguenti anomalie su 5 posizioni campionate: • non perfezionate in AGAR le garanzie collegate alle seguenti pratiche di rischio: | M | 👤 | Procedere all'acquisizione delle garanzie indicate. | Area High Risk | 31/12/18 | R.C.1.22 |
| 3 | Credito | Criticità su pratiche campionate Rilevati elementi di criticità sulla posizione ANGELANTONI LIFE SCIENCE S.R.L. – NDC 213375692 : | B | 👤 | Ricondurre nel perimetro High Risk la pratica al fine di valutare l'intero gruppo di relazione | Area High Risk | 31/12/18 | N.A. |

 Sistemi
  Processi
  Risorse



Revisione Ethical Hacking di Gruppo (BMPS, Widiba e Filiale di NY) - Rapp. 62/2018 (1/4)

ANAGRAFICA INTERVENTO

Intervento: Ethical Hacking di Gruppo (BMPS, Widiba e Filiale di NY)

Obbligatorietà: NO per BMPS e Widiba, SI per Filiale di NY

Unità auditata/e: Consorzio Operativo MPS, Widiba e Filiale di N.Y.

Tipologia di intervento: Revisione Settoriale Ordinaria a distanza

Data open meeting: Non previsto (intervento avviato il 14/05/18)

Data exit meeting: 18/07/18 BMPS - 18/07/18 Widiba – 16/07/18 NY

Condivisione con Area Sicurezza Integrata: 25/07/2018

Condivisione con Area Digital e Physical Banking: 26/07/2018

ESITO INTERVENTO

GRADE COMPLESSIVO INTERVENTO

| | | | |
|---------------------|-----------------------------------|-------------------------|---------------------|
| Rating 1 (VERDE) | Rating 2 BMPS Widiba/Fil NY | Rating 3 (ARANCIONE) | Rating 4 (ROSSO) |
|---------------------|-----------------------------------|-------------------------|---------------------|

La scala di valutazione si articola su quattro livelli a criticità crescente: Rating 1 (VERDE), Rating 2 (GIALLO), Rating 3 (ARANCIONE), Rating 4 (ROSSO).

| FATTORE CAUSALE | DISTRIBUZIONE DEI GAP PER RILEVANZA | | |
|-----------------|-------------------------------------|-------|-------|
| | ALTA | MEDIA | BASSA |
| 👤 Risorse | - | - | - |
| ↔ Processi | - | - | - |
| 🖥 Sistemi | - | 4 | 1 |
| Totale | 0 | 4 | 1 |

PRECEDENTI INTERVENTI DI REVISIONE (SE ESISTENTI)

| AMBITO INTERVENTO | PERIODO DELLA VERIFICA | N. RAPPORTO | GRADE INTERVENTO |
|---|------------------------|-------------|-----------------------|
| Attività di Ethical Hacking su Digital Banking | 29/05/2017 31/08/2017 | 102_2017 | Rating 3 ARANCIONE |
| Attività di Ethical Hacking sulla Filiale di New York | 29/05/2017 31/08/2017 | 164_2017 | Rating 2 GIALLO |
| Attività di Ethical Hacking su Widiba | 03/10/2016 30/11/2016 | 417_2016 | Rating 3 ARANCIONE |
| Attività di Ethical Hacking sulla Filiale di New York | 03/10/2016 15/12/2016 | 416_2016 | Rating 1 VERDE |

ORGANI DESTINATARI DEL PRESENTE AUDIT

| LEGAL ENTITY | ORGANO DESTINATARIO |
|--------------|-------------------------|
| BMPS | Presidente del CdA |
| BMPS | Amministratore Delegato |
| BMPS | Collegio Sindacale |
| BMPS | Comitato Rischi |



Revisione Ethical Hacking di Gruppo (BMPS, Widiba e Filiale NY) - Rapp. 62/2018 (2/4)

DIFESA PERIMETRALI

BMPS Digital Banking - Difese Perimetrali: Monitoraggio per rilevazione attacchi da Internet, svolto dal Security Operation Center, estremamente migliorato ma ancora perfezionabile

La verifica ha avuto come principale obiettivo la verifica del corretto funzionamento dell'infrastruttura tecnologica del SOC (Security Operation Center) e, nello specifico, degli strumenti di difesa perimetrale, quali l'Intrusion Detection e Prevention System, dedicati alla pronta identificazione e prevenzione degli attacchi provenienti dalla rete Internet.

Le difese perimetrali sono risultate estremamente migliorate rispetto a quanto riscontrato nel 2017, grazie soprattutto all'installazione di nuovi sistemi di difesa (Palo Alto). L'Intrusion Prevention System ha bloccato molti dei tentativi di scansione condotti nel corso dell'attività. Tuttavia, il fatto che alcune tipologie di attacco (condotte anche con metodi automatici) verso l'applicazione web non siano state intercettate suggerisce la necessità di intervenire con ulteriori controlli allo scopo di aumentare il perimetro delle tipologie di attacco rilevabili (cfr. gap basso 3 Banca MPS – cod. SREP: IG.6.3).

Widiba Banca On Line - Difese Perimetrali: Monitoraggio per rilevazione attacchi da Internet adeguato ma poco scalabile con l'aumento della clientela

Uno degli obiettivi dell'attività è stato quello di verificare il corretto funzionamento dell'infrastruttura tecnologica e, nello specifico, degli strumenti di difesa perimetrale, quali Intrusion Detection e Prevention System, dedicati alla pronta identificazione e prevenzione degli attacchi provenienti dalla rete Internet.

Gli apparati installati presso Widiba hanno correttamente bloccato tutte le scansioni automatiche eseguite nel corso dell'attività. Altri tentativi di attacco, non bloccati automaticamente, sono stati comunque intercettati dagli strumenti di monitoraggio interni e, nei casi reputati di effettivo rischio, sono state attuate le necessarie misure di contenimento per le minacce rilevate (ad esempio disattivazione dell'utenza con cui venivano condotti i tentativi di attacco). Tale sistema di difesa perimetrale, che si basa su verifiche manuali svolte dagli addetti alla sicurezza, risulta poco scalabile con l'aumento della clientela e dovrà pertanto evolvere nel tempo.

VERIFICA INFRASTRUTTURALE

New York – Verifica Infrastrutturale: Nuove vulnerabilità rilevate su sistemi locati presso la filiale, prontamente risolte

La verifica viene svolta annualmente su specifica richiesta dalla Federal Reserve System (FED) con l'obiettivo di valutare il livello di sicurezza dei sistemi IT presenti presso la Filiale di New York.

L'attività di quest'anno ha inizialmente rilevato un grado di sicurezza complessivamente non adeguato. La maggior parte delle problematiche a rischio più elevato sono state riscontrate su 3 sistemi di recente installazione. Tali sistemi sono stati installati senza seguire le policy internazionali di sicurezza, introducendo nuove vulnerabilità all'interno della infrastruttura di sistema della Filiale. È opportuno evidenziare che tali sistemi sono risultati essere gruppi statici di continuità (sistemi UPS), non particolarmente critici in quanto, per loro natura, non contengono informazioni sensibili.

Da segnalare peraltro che le vulnerabilità riscontrate appartengono alle stesse macro-categorie rilevate negli anni passati, ovvero mancanza di aggiornamenti del software ed errate configurazioni dei sistemi.

Si fa però presente che i rischi operativi sottesi sono in parte mitigati dal fatto che le vulnerabilità rilevate risultano sfruttabili esclusivamente da un attaccante collegato alla rete interna della Banca e con il proprio computer abilitato all'accesso. In considerazione di ciò è stato richiesto alla filiale di New York di intervenire obbligatoriamente per quanto riguarda le vulnerabilità con impatto critico e alto; sarà comunque data indicazione affinché valutino anche le restanti vulnerabilità presenti nel report redatto da Mind Security (prevalentemente relative a problemi di configurazione e crittografia) e provvedano a ottimizzare, laddove ritenuto opportuno, i parametri di sicurezza non configurati correttamente.

Come già segnalato sopra, la filiale di New York, una volta informata delle risultanze dell'attività, si è immediatamente attivata per la risoluzione delle vulnerabilità a rischio più elevato (cfr. slide n. 6). Nel presente rapporto non sono quindi stati sollevati gap.



Revisione Ethical Hacking di Gruppo (BMPS, Widiba e Filiale NY) - Rapp. 62/2018 (3/4)

APPLICAZIONE WEB

BMPS Digital Banking - Applicazione Web: *Grado di sicurezza migliorato ma ancora non totalmente adeguato agli standard di sicurezza*

Migliorato rispetto al 2017 il complessivo livello di sicurezza dell'applicazione web Digital Banking. Le vulnerabilità individuate, nessuna di livello critico, risultano sfruttabili solo in associazione ad attacchi di phishing¹ o di social engineering².

Emerge quindi un trend positivo che va perseguito con le attività da mettere in campo per la risoluzione delle problematiche che sono state individuate (cfr. gap medio 1 Banca MPS – cod. SREP: IG.6.3). Tra queste rileva la possibilità, previa autenticazione all'applicazione di Digital Banking come cliente della Banca, di automatizzare la ricerca di numeri di cellulare appartenenti ad altri utenti.

Da segnalare che la maggior parte delle vulnerabilità individuate, alcune riscontrate anche nell'attività svolta l'anno precedente, sono principalmente riconducibili al processo di sviluppo del software, ancora non sufficientemente presidiato e solo parzialmente adeguato agli standard de-facto internazionali in materia di sicurezza.

Sono state identificate anche alcune vulnerabilità a minore impatto, che concorrono comunque a diminuire il livello di sicurezza complessivo associato alla piattaforma applicativa.

Per proseguire sulla strada del continuo miglioramento, appare pertanto necessario individuare le misure a rimedio delle macro-categorie di vulnerabilità ancora presenti e renderle parte integrante del processo di sviluppo del software, come da indicazione dei principali standard internazionali in termini di sicurezza. In tale contesto si evidenzia, inoltre, la necessità di eseguire specifici test di sicurezza e garantire una continua review del codice sorgente dell'applicazione, finalizzata ad individuare eventuali nuovi errori di programmazione, i cui esiti devono essere vincolanti all'effettivo rilascio in produzione.

¹ il phishing è un tipo di frode ideato per indurre gli utenti a rivelare – con l'inganno – informazioni personali o finanziarie attraverso un'email o un sito web, ma sempre più spesso anche tramite messaggi in arrivo da applicazioni molto usate come Whatsapp o Facebook.

² per social engineering si intende quell'insieme di tecniche, non necessariamente informatiche, che possono indurre la vittima ad eseguire azioni desiderate dall'attaccante, solitamente con l'obiettivo di ottenere informazioni necessarie a perpetrare azioni fraudolente.

Widiba Banca On Line - Applicazione Web: *Grado di sicurezza complessivamente adeguato ma perfettibile*

Il livello di sicurezza dell'applicazione web Banca On Line è complessivamente in linea con gli standard di sicurezza attesi. Le vulnerabilità individuate, tutte di livello medio e basso, risultano sfruttabili solo in associazione ad attacchi di phishing o di social engineering.

Da segnalare che molte delle vulnerabilità attualmente presenti, principalmente riconducibili alla mancanza di controlli di validazione dei dati inseriti dall'utente, erano state individuate anche a seguito di analoghe attività di verifica condotte negli anni passati; per queste però Banca Widiba non aveva apportato correttivi assumendosene il rischio residuo. Considerato il buon livello complessivo di sicurezza raggiunto, è necessario proseguire sulla strada del continuo miglioramento (cfr. gap medio 1 Widiba – cod. SREP: IG.6.3), rafforzando ulteriormente il processo di sviluppo del software, introducendo specifici controlli sulla validazione dei dati (di input e output) così da limitare la probabilità di introdurre nuove criticità. In tale contesto si evidenzia l'opportunità di garantire una continua review del codice sorgente dell'applicazione, finalizzata ad individuare eventuali nuovi errori di programmazione, i cui esiti devono essere vincolanti all'effettivo rilascio in produzione.



Revisione Ethical Hacking di Gruppo (BMPS, Widiba e Filiale NY - Rapp. 62/2018 (4/4)

APPLICAZIONI PER DISPOSITIVI MOBILI

BMPS Digital Banking – Applicazioni per Dispositivi Mobili: Grado di sicurezza complessivamente adeguato ma perfettibile

Sia sulla piattaforma Android (smartphone o tablet di tipo “Samsung”) che su quella iOS (dispositivi “Apple”) è stato riscontrato un grado di sicurezza migliorato rispetto al 2017, che tuttavia non rispetta ancora tutte le principali best practice internazionali.

Per entrambe le piattaforme sono infatti state rilevate vulnerabilità di media rilevanza (cfr. gap medio 2 Banca MPS – cod. SREP: IG.6.3) relative in particolare a problemi di configurazione e di «information disclosure» (i.e. fuga di informazioni utili al fine di un attacco).

Widiba Banca On Line - Applicazioni per Dispositivi Mobili: Grado di sicurezza complessivamente adeguato ma perfettibile

E' stato riscontrato un grado di sicurezza complessivamente adeguato ma ancora migliorabile sia sulla piattaforma Android (smartphone o tablet di tipo “Samsung”) che su quella iOS (dispositivi “Apple”).

Per entrambe le piattaforme sono infatti state rilevate vulnerabilità di media rilevanza (cfr. gap medio 2 Widiba – cod. SREP: IG.6.3) relative in particolare a problemi di configurazione delle applicazioni.

DATI DI SINTESI

BMPS Digital Banking - Dati di Sintesi

La società Minded Security, che ha condotto le verifiche, ha rilevato complessivamente 24 vulnerabilità. In dettaglio: 17 risultato della verifica sull'applicazione web Digital Banking (2 a rilevanza alta, 8 media e 7 bassa), 7 risultato della verifica sulle applicazioni mobili Digital Banking (tutte a rilevanza media).

Widiba Banca On Line - Dati di Sintesi

La società Minded Security, che ha condotto le verifiche, ha rilevato complessivamente 16 vulnerabilità. In dettaglio: 12 risultato della verifica sull'applicazione web Digital Banking (6 a rilevanza media e 6 bassa), 4 risultato della verifica sulle applicazioni mobili Digital Banking (tutte a rilevanza media).

Da segnalare che in seguito a verifiche successive 3 vulnerabilità sono risultate falsi positivi (1 a rilevanza media e 2 a rilevanza bassa), inoltre una a rilevanza media è stata prontamente risolta in data 19 luglio.

Filiale di New York – Dati di Sintesi




La società Minded Security, che ha condotto le verifiche, ha rilevato complessivamente 19 vulnerabilità infrastrutturali, di cui 3 a rilevanza critica, 6 alta, 8 media e 2 bassa.

Da segnalare che la filiale di New York, non appena informata delle risultanze dell'attività, si è immediatamente attivata per la risoluzione delle vulnerabilità più rischiose, risolvendo la totalità di quelle a rilevanza critica e alta, ed alcune di quelle ad impatto minore. In considerazione di ciò non sono stati sollevati gap.

Le verifiche effettuate hanno riscontrato la corretta risoluzione delle vulnerabilità individuate con l'attività effettuata nel 2017.






Revisione Ethical Hacking di Gruppo - Rapp. 62/2018 - BMPS audit finding

| N. | PROCESSO | GAP | RILEVANZA (A/M/B) | FATTORE CAUSALE | RACCOMANDAZIONE | STRUTTURA OWNER | SCADENZA (GG/MM/AA) | CODICE OB SREP |
|----|---|--|----------------------|---|--|--|------------------------|-------------------|
| 1 | Gestione dei processi operativi di sicurezza logica | <p>Applicazione WEB: livello di sicurezza dell'applicazione web migliorabile</p> <p>Il livello di sicurezza complessivo dell'applicazione web sviluppata per la piattaforma Digital Banking è risultato migliorato ma ancora non del tutto adeguato agli standard de-facto internazionali in materia di sicurezza delle informazioni; sono state infatti rilevate varie problematiche, legate soprattutto alla non corretta gestione dell'input degli utenti, alcune delle quali presenti anche nei risultati dell'attività svolta lo scorso anno. Nello specifico, l'attività condotta ha evidenziato come l'applicazione presenti n.17 vulnerabilità di cui n. 2 di criticità¹ alta, n. 8 di criticità media e n. 7 di criticità bassa.</p> <p>A titolo esemplificativo ma non esaustivo dei rischi cui l'applicazione è potenzialmente soggetta, si rappresenta come, da posizione privilegiata², sia possibile enumerare i numeri di telefono di altri utenti che hanno il servizio Digital Banking.</p> <p>¹ Valutazione del livello di criticità assegnato dalla società di consulenza tra quattro possibili - critico, alto, medio, basso - calcolato come prodotto della probabilità di accadimento per l'impatto.</p> <p>² Dopo inserimento delle credenziali (utenza, password e OTP)</p> | M |  | <p>Sanare le vulnerabilità applicative rilevate e implementare un ciclo di sviluppo sicuro del codice</p> <p>Implementare gli opportuni controlli e configurazioni al fine di sanare le vulnerabilità applicative riscontrate così come dettagliate nel report tecnico «Monte dei Paschi di Siena Digital: WAPT/MAPT report», allegato alla presente.</p> <p>In considerazione anche del buon livello di maturità già raggiunto, proseguire con il rafforzamento del processo di sviluppo del software allineandolo ai principali standard internazionali in termini di sicurezza (es. OWASP «The ten most critical web application security risks»). Rafforzare, inoltre, verifiche di conformità ai criteri di sicurezza adottati (ad esempio code review del software), i cui esiti devono essere vincolanti all'effettivo rilascio in produzione.</p> | Consorzio Servizio Self Banking | 31/03/19 | IG.6.3 |
| 2 | Gestione dei processi operativi di sicurezza logica | <p>Applicazioni mobili: livello di sicurezza delle applicazioni mobile migliorabile</p> <p>L'attività di penetration test svolta sulle applicazioni mobili sviluppate per dispositivi Android e iOS ha evidenziato un livello di sicurezza migliorato ma ancora non del tutto adeguato agli standard de-facto internazionali in materia di sicurezza delle informazioni.</p> <p>Nel dettaglio, le verifiche condotte hanno portato alla luce n.7 vulnerabilità di criticità media, alcune delle quali presenti anche nei risultati dell'attività svolta lo scorso anno, che espongono le applicazioni a rischi inerenti la confidenzialità delle informazioni.</p> | M |  | <p>Sanare le vulnerabilità rilevate</p> <p>Implementare gli opportuni controlli e configurazioni al fine di sanare le vulnerabilità applicative riscontrate così come dettagliate nel report tecnico «Monte dei Paschi di Siena Digital: WAPT/MAPT report», allegato alla presente.</p> | Consorzio Servizio Self Banking | 31/03/19 | IG.6.3 |
| 3 | Gestione dei processi operativi di sicurezza logica | <p>Sistema di difesa perimetrale sull'applicazione Digital Banking ottimizzabile</p> <p>I sistemi di difesa perimetrale hanno correttamente bloccato le scansioni eseguite con tool automatici come nmap, Nessus e Burp. Si segnala tuttavia l'assenza di controlli accentrati volti ad individuare tentativi di attacco automatizzati (ad esempio numero elevato di richieste eseguite in tempi estraneamente ridotti provenienti dallo stesso ip ed indirizzati sulla stessa pagina).</p> | B |  | <p>Efficientare gli strumenti di intercettazione delle intrusioni</p> <p>Verificare la possibilità di implementare controlli mirati ad intercettare, già a livello di difesa perimetrale, eventuali tentativi di attacco automatizzati (ad esempio attivando controlli sul SIEM).</p> | Consorzio Servizio Sicurezza Informatica e BCM | 15/12/18 | IG.6.3 |



Revisione Ethical Hacking di Gruppo - Rapp. 62/2018 - Widiba audit finding

| N. | PROCESSO | GAP | RILEVANZA (A/M/B) | FATTORE CAUSALE | RACCOMANDAZIONE | STRUTTURA OWNER | SCADENZA (GG/MM/AA) | CODICE OB SREP |
|----|---|---|----------------------|---|---|---|------------------------|-------------------|
| 1 | Gestione dei processi operativi di sicurezza logica | <p>Applicazione WEB: livello di sicurezza dell'applicazione web migliorabile</p> <p>Il livello di sicurezza complessivo dell'applicazione web sviluppata per la piattaforma Banca On Line di Widiba è risultato migliorato ma ancora non del tutto adeguato agli standard de-facto internazionali in materia di sicurezza delle informazioni; sono state infatti rilevate varie problematiche, legate soprattutto alla non corretta gestione dell'input degli utenti, generalmente presenti anche nei risultati dell'attività svolta gli scorsi anni. Nello specifico, l'attività condotta ha evidenziato come l'applicazione presenti n.12 vulnerabilità di cui n. 6 di criticità¹ media e 6 bassa.</p> <p>¹ Valutazione del livello di criticità assegnato dalla società di consulenza tra quattro possibili - critico, alto, medio, basso - calcolato come prodotto della probabilità di accadimento per l'impatto.</p> | M |  | <p>Sanare le vulnerabilità applicative rilevate e rafforzare il processo di sviluppo sicuro del codice</p> <p>Implementare gli opportuni controlli e configurazioni al fine di sanare le vulnerabilità applicative riscontrate così come dettagliate nel report tecnico «Widiba Application: WAPT/MAPT report», allegato alla presente.</p> <p>In considerazione anche del buon livello di maturità già raggiunto, si ritiene auspicabile proseguire con il rafforzamento del processo di sviluppo del software allineandolo ai principali standard internazionali in termini di sicurezza (es. OWASP «The ten most critical web application security risks»). Introdurre, inoltre, verifiche di conformità ai criteri di sicurezza adottati (ad esempio code review del software), i cui esiti devono essere vincolanti all'effettivo rilascio in produzione.</p> | Widiba Direzione IT e Innovazione Digitale | 31/12/18 | IG.6.3 |
| 2 | Gestione dei processi operativi di sicurezza logica | <p>Applicazioni mobili: criticità minori nella gestione della configurazione</p> <p>L'attività di penetration test svolta sulle applicazioni mobili sviluppate per dispositivi Android e iOS ha evidenziato un livello di sicurezza migliorato ma ancora non del tutto adeguato agli standard de-facto internazionali in materia di sicurezza delle informazioni.</p> <p>Nel dettaglio, le verifiche condotte hanno portato alla luce n.4 vulnerabilità di criticità media, alcune delle quali presenti anche nei risultati dell'attività svolta gli scorsi anni, che espongono le applicazioni a rischi inerenti la confidenzialità delle informazioni.</p> | M |  | <p>Sanare le vulnerabilità rilevate</p> <p>Implementare gli opportuni controlli e configurazioni al fine di sanare le vulnerabilità applicative riscontrate così come dettagliate nel report tecnico «Widiba Application: WAPT/MAPT report», allegato alla presente.</p> | Widiba Direzione IT e Innovazione Digitale | 31/12/18 | IG.6.3 |

 Sistemi ↔  Processi  Risorse



Allegato - Focus compito interventi di processo avviati nel periodo



INTERVENTO

- » Intervento: Gestione fornitori, attività negoziale e contratti
- » Unità auditata: Area Acquisti, Cost Management e Logistica/Servizio Acquisti di Gruppo e Gestione Fornitori (Salzano Antonio); eventuali Centri di Spesa individuati sulla base del campione selezionato

Ambito

Le attività di negoziazione per l'individuazione del fornitore, la formalizzazione dell'impegno economico e la gestione accentrata dei fornitori sia per quanto riguarda le singole assegnazioni sia per gli accordi quadro.

Obiettivi

1. Valutare l'adeguatezza dei processi operativi e l'efficacia del sistema dei controlli, anche con riferimento alle disposizioni previste per le aziende a partecipazione pubblica.
2. Accertare la conformità delle prassi agite alla normativa interna in materia.
3. Accertare il rispetto delle linee guida di condotta ai fini "231".
4. Valutare la rispondenza dei processi agli obiettivi SREP.

Limiti

L'intervento riguarderà le negoziazioni di maggior rilievo che prevedono una gestione accentrata da parte della Funzione Acquisti.

Non sono comprese nel perimetro le verifiche di natura ICT sugli applicativi a supporto del processo.

Rapp. 68/2018 - Business Plan Sofferenze (Finding #9 OSI-1238 BCE): *focus compito*

INTERVENTO

- Intervento: Verifica aggiornamento previsioni di recupero e adeguatezza degli accantonamenti sulle posizioni con BP scaduto. - Realizzazione di quanto richiesto da ECB nel Finding 9 della OSI 1238
- Unità auditate: **Area Credit Portfolio Governance**/Servizio Gestione Portafoglio Creditizio - **Area Recupero Crediti**/ Servizio Presidio performance e Interfaccia Piattaforma - Servizio Recupero Crediti

Ambito

In ordine al progetto «Argo 3: Riepilogo dei 9 Finding della OSI 1238 e connesse attività di audit pianificate – p. 9 Tempestività aggiornamento Business Plan e adeguatezza accantonamenti sulle posizioni con Business Plan scaduto», la presente revisione si focalizzerà sul completamento delle previsioni di recupero e la valutazione degli accantonamenti (dubbi esiti), alla data del 30/06/2018, relativamente al portafoglio classificato a contenzioso con GBV > € Mgl 500.

Obiettivi

L'obiettivo dell'accertamento sarà quello di:

- ✓ verificare l'aggiornamento delle policies per assicurare una applicazione consistente del tempo di recupero a tutte le esposizioni deteriorate;
- ✓ fornire *assurance* ai Vertici Aziendali in ordine a quanto finalizzato nell'ambito del progetto "ARGO 3" sulle azioni correttive poste in essere per il completamento, alla data del 30/06/2018, delle previsioni dei recuperi attesi sul portafoglio in «Gestione Diretta e su quello assegnato al Servicer Esterno con GBV > € Mgl 500, attraverso un SAL della lavorazione dei Business Plan.
- ✓ Valutare gli obiettivi di controllo in ambito SREP (Supervisory Review and Evaluation Process) associati ai processi esaminati.

Limiti

Con riferimento ai sistemi informativi non saranno condotte verifiche specialistiche di tipo "IT" e, relativamente ai sistemi contabili, le verifiche saranno dirette ad accertare la regolarità degli aspetti gestionali e operativi posti in essere con esclusione delle modalità informatiche con cui tali dati vengono trattati nei diversi sistemi e contabilizzati in Bilancio della Banca.



Rapp. 103/2018 - Revisione sul processo di Istruttoria ed Erogazione del Prodotto «Mutui Widiba»: *focus compito*

INTERVENTO

- » Intervento: *Istruttoria ed Erogazione dei «Mutui Widiba»*
- » Unità auditata/e: : *Ufficio Crediti - Direzione Operations & Gestione Immobiliare*

Ambito

Processo di concessione del mutuo e in particolare:

- Generazione della domanda
- Istruttoria reddituale
- Analisi reddituale
- Analisi tecnico legale
- Stipula e Perfezionamento

Obiettivi

Accertare le modalità di gestione e presidio sul portafoglio Mutui Widiba della Banca mediante la valutazione della consistenza e composizione del portafoglio mutui, la sua concentrazione, redditività e gestione delle posizioni problematiche.

Limiti

La verifica, nell'ambito del mercato e della rete di distribuzione di Banca Widiba, sarà condotta in riferimento al prodotto «Mutui Widiba».

Non si entrerà nel 'merito' della discrezionalità della concessione del mutuo



Rapp. 90/2018 - Data Governance: struttura organizzativa, framework e strumenti a supporto: *focus compito*

INTERVENTO

- » Intervento: Data Governance: Struttura Organizzativa, Framework e Strumenti a Supporto
- » Unità auditate: "Servizio Data Governance e Reporting Management"; "Servizio DWH e Reporting" del COG; eventuali altre Funzioni individuate in corso di intervento.

| Ambito | Obiettivi | Limiti |
|--|--|---|
| <ul style="list-style-type: none">» Data Governance: Struttura Organizzativa, Framework e Strumenti a Supporto | <ol style="list-style-type: none">1. Valutare la rispondenza del modello alle best practice di settore ed ai requisiti esterni.2. Esaminare gli aspetti di conformità dei processi definiti e delle prassi agite rispetto alla normativa interna in materia.3. Valutare l'efficacia e l'adeguatezza del sistema dei controlli, tramite verifiche sulle singole fasi.4. Valutare gli strumenti predisposti a supporto dei processi anche tramite verifiche a campione sugli output prodotti5. Valutare la rispondenza dei processi agli obiettivi SREP. | <p>Non saranno ricomprese nel perimetro verifiche di Data Quality che sarà oggetto di uno specifico intervento già previsto in Audit Plan per il corrente anno.</p> |



Rapp. 104/2018 - Misure individuate dal Gruppo MPS per conformarsi alle prescrizioni della normativa di matrice MiFID II: *focus compito*

INTERVENTO

- » Intervento: *Misure individuate dal Gruppo (MPS, MP Capital Services e Widiba) per conformarsi alle prescrizioni della normativa di matrice MiFID II*
- » Unità auditata/e: *Direzione Chief Commercial Officer; Direzione Chief Operating Officer; Area Compliance; Direzione Chief Risk Officer.*

Ambito

Recepimento nuove prescrizioni MiFID II in riferimento ai profili richiamati dalla Consob con comunicazione n. 0056318 dell'1-3-2018.

Gli accertamenti saranno condotti a distanza e con accessi presso le strutture aziendali specificamente coinvolte nella definizione ed attuazione dei processi adottati dal Gruppo per uniformarsi alle novità normative di matrice MiFID II ed introdotte con decorrenza 2 gennaio 2018

Obiettivi

Accertare le modalità operative con le quali il Gruppo si è conformato alle novità regolamentari di matrice MiFID II, ivi compresa la ricostruzione delle attività progettuali, nonché, limitatamente alla Banca MPS, verificare le prime risultanze degli impatti commerciali intesi come adeguatezza dei supporti organizzativi forniti alla rete commerciale (norme, procedure, aspetti info – formativi).

Limiti

La verifica sarà condotta in riferimento ai profili di attenzione richiamati dalla Consob con comunicazione n. 0056318 dell'1-3-2018:

- processo di product governance;
- Consulenza in materi di investimenti;
- Valutazione di adeguatezza e appropriatezza;
- Prodotti complessi ed execution only;
- Informativa alla clientela (costi e oneri);
- Pratiche di vendita abbinata;
- Best execution (solo per MPS Capital Services);
- Conflitti di interesse;
- Incentivi;
- Requisiti di conoscenza e competenza del personale degli intermediari

Gli aspetti comportamentali saranno oggetto di revisione ad hoc.



Rapp. 74/2018 - Compliance – Modello accentrato di Gruppo - focus Widiba e MPS Capital Services : *focus compito*

INTERVENTO

- Intervento: Compliance – Modello accentrato di Gruppo con “focus” su Widiba e M.P.S. Capital Services.
- Unità auditata: Area Compliance di Banca M.P.S.

Ambito

- Efficacia e l'efficienza del Modello Accentrato di Gruppo adottato per la gestione del rischio di non conformità (cfr. Ispezione JST - OSI-2015-ITMPS-32-33 FINDING #4).
- Controlli finalizzati a presidiare - limitatamente a Banca Monte dei Paschi, a Widiba e MPS Capital Services - le specifiche “Aree Normative” relative al contrasto all'usura, alla trasparenza dei servizi e prodotti bancari ed alla trasparenza dei servizi e prodotti di finanziamento.
- Aggiornamento del “Modello Organizzativo 231/2001” programmate per il corrente anno.

Obiettivi

- Analisi della “messa a regime” del Modello Accentrato di Gruppo per la gestione della Compliance (nuovo assetto organizzativo deliberato e comunicato a J.S.T. nel settembre 2017).
- Verifica dell'esecuzione delle attività poste in essere dalla Funzione Compliance di Capogruppo nei confronti delle Controllate Widiba e M.P.S. Capital Services.
- In relazione al contrasto all'usura, esame dei controlli di I e II livello e dei flussi informativi tra le Funzioni Aziendali e nei confronti dei Vertici.
- In relazione alla trasparenza dei servizi e prodotti bancari e dei servizi e prodotti di finanziamento, esame dei controlli di II livello ed analisi dello stato di avanzamento del Piano Interventi predisposto nell'ottobre 2017 per la risoluzione delle criticità rilevate da Banca d'Italia durante l'ispezione del 2016.
- Analisi dello stato di evoluzione del Progetto di revisione biennale del “Modello Organizzativo 231/2001” (limitatamente a Banca Monte dei Paschi ed alle Controllate Widiba ed M.P.S. Capital Services).

Limiti

Nell'esame della “messa a regime” del Modello Accentrato della Funzione Compliance non sarà compresa l'analisi delle 2 aree normative “Tax Compliance” e “Salute e Sicurezza sul Lavoro e Tutela Ambientale”, fatto salvo per le attività svolte in tale campo da parte della Funzione Compliance. Gli accertamenti verteranno, sostanzialmente, sulla corretta esecuzione delle attività di controllo previste: non saranno, conseguentemente, effettuate analisi sistematiche di merito sulle valutazioni formulate dalla Funzione Compliance. L'ambito delle verifiche escluderà l'esame degli aspetti I.T. degli applicativi in uso.



Rapp. 71/2018 - Processo gestione massiva crediti problematici classificati a Inadempienza Probabile Rischio Anomalo (IPRA): *focus compito*

INTERVENTO

- » Intervento: Audit sulla gestione massiva dei crediti Problematici classificati a Inadempienza Probabile Rischio Anomalo
- » Unità auditata/e: Servizio Gestione Massiva Crediti Problematici/Direzione Crediti Non Performing

Ambito

Processo: Gestione Massiva Crediti Problematici – Inadempienza Probabile Rischio Anomalo (IPRA)

Fase: Acquisizione posizioni IPRA massivo;

Fase: Gestione posizioni IPRA massivo;

Fase: Gestione e monitoraggio attività con Società di recupero esterne (SRES);

Sistema dei Controlli Interni a presidio dei rischi connessi al processo di gestione delle posizioni classificate a contenzioso.

Obiettivi

Saranno verificate:

- le modalità di lavorazione dei nuovi flussi di pratiche targate «recupero massivo»;
- le modalità di gestione delle posizioni assegnate ai settori competenti (Micro, Small, Specialized), con focus sul seguimiento dei processi legali (procedure concorsuali, cause passive, azioni esecutive, ecc.), delle proposte transattive, della gestione delle spese connesse all'attività IPRA massivo;
- Le attività di monitoraggio e controlli eseguiti dalla Struttura sulle attività realizzate dalle SRES
- la funzionalità e l'adeguatezza del Sistema dei Controlli Interni.

Limiti

Attività svolta sulla base delle informazioni disponibili nei sistemi informativi della Banca integrata da eventuali altre evidenze da acquisire nell'ambito della visita presso il Servizio Gestione Massiva Crediti Problematici della Direzione Crediti Non Performing, anche con visite in loco presso i Settori External Collection e/o Operation.



Rapp. 118/2018 - Processo di Gestione scoperti/sconfinamenti : «Istruttoria Veloce» - aspetti gestionali, di monitoraggio e di controllo): *focus compito*

INTERVENTO

- » Accertamenti sul Processo di “Gestione scoperti/sconfinamenti: Istruttoria Veloce”
- » Unità auditate/coinvolute: Servizio Standard e Politiche Creditizie e Servizio Qualità del Processo Creditizio della Direzione CLO; Servizio Controlli, Conformità e Operations e Strutture di Rete campionate della Direzione CCO

| Ambito | Obiettivi | Limiti |
|---|--|--|
| Processo di gestione scoperti/sconfinamenti derivanti dall'esecuzione di Istruttorie Veloci e connesso Sistema dei Controlli Interni a presidio dei rischi. | Valutare l'adeguatezza dei seguenti ambiti: <ol style="list-style-type: none">1. gestionale/operativa, con riguardo all'attività della Rete nelle varie fasi del processo;2. controlli e monitoraggi - a livello di Strutture Centrali e di Rete - a presidio dei rischi insiti nel processo auditato, avendo a riguardo anche gli strumenti e i flussi informativi. | Sono stati escluse dall'analisi le posizioni classificate a «rischio anomalo» e «in ristrutturazione», in relazione alla gestione di tali fattispecie da parte di filiera specialistica di DG. |



Rapp. 226/2018 - Revisione finding #6 OSI 1238 – Efficacia e tempestività del processo di classificazione a maggior rischio delle posizioni oggetto di forborne: *focus compito*

INTERVENTO

- » Intervento: Revisione Finding #6 OSI 1238 - Efficacia e tempestività del processo di classificazione a maggior rischio delle posizioni oggetto di forborne
- » Unità auditate: Direzione CLO - Area Credit Portfolio Governance; Area High Risk.

Ambito

- Aggiornamento del D1991, "Policy di Gruppo in materia di classificazione e valutazione del credito". sulla base delle indicazioni di ECB di cui all'OSI 1238
- Analisi del disegno dei processi e dei relativi controlli di I e II livello, tesi ad evitare una errata classificazione delle posizioni forborne

Obiettivi

- Valutare le attività poste in essere per il rafforzamento dei controlli di I e II livello per l'individuazione e corretta classificazione delle posizioni forborne che presentano segnali di deterioramento.
- Valutare la coerenza delle modifiche apportate al D1991 con quanto indicato da ECB nella follow-up letter relativa all'On Site Inspection 1238.
- Analisi dei processi di «classificazione forzata» predisposti nelle more dell'integrazione degli automatismi sulla riclassificazione nei sistemi informativi della Banca
- Valutazione degli obiettivi di controllo in ambito SREP (Supervisory Review and Evaluation Process) associati ai processi esaminati.

Limiti

Il perimetro dell'attività da svolgere è stato definito nel paragrafo relativo agli Ambiti della revisione



Rapp. 241/2018 - Revisione MPS Tenimenti SpA - Aspetti amministrativo-contabili e presidio dei controlli: *focus compito*

INTERVENTO

- » Intervento: *Aspetti amministrativo-contabili e presidio dei controlli*
- » Unità auditate: MPS Tenimenti SpA

Ambito

- Aspetti amministrativo-contabili inerenti la gestione della Società ed analisi degli adempimenti più rilevanti nella redazione del bilancio d'esercizio. In tale ambito sarà oggetto di verifica il processo di valutazione del patrimonio immobiliare.
- Presidio dei controlli nelle attività di natura gestionale e contabile.

Obiettivi

Adeguatezza delle strutture amministrativo-contabile e del presidio relativo alle attività di controllo.

Limiti

Nessun limite previsto.

