



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

Tableau de Board Internal Audit - #9

[aggiornamento al 11 gennaio 2019]

periodo 14.12.2018 – 11.01.2019

Direzione Chief Audit Executive

Agenda

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

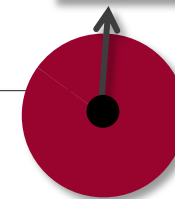
Allegati:

Focus GAP attivi in monitoraggio (rilevanza Alta) per cluster



PIANO DI
AUDIT

- » Al 11.01.2019 risulta completato il piano di audit 2018 (100% di revisioni effettuate o in fase di perfezionamento).
- » Si prevede la finalizzazione entro il 31.01 degli interventi sui processi centrali e società ancora in corso di svolgimento ad eccezione della verifica sul RAF, il cui probabile allungamento delle tempistiche è riconducibile al fatto che l'attività è direttamente collegata a quelle del Risk Management.



RISK MANAGEMENT

- » Rapp. 36/2018 - Revisione Convalida AIRB
- » Giudizio assegnato: **R1 Verde**
- » Evidenziato 1 gap a rilevanza bassa
- » La verifica, volta a valutare la funzionalità del processo di convalida AIRB, nel rispetto delle condizioni di idoneità per l'utilizzo regolamentare delle stime di rischio, non ha evidenziato criticità.

CREDITO, TESORERIA & CAPITAL MGMT

- » Rapp 65/2018 – Covered Bond
- » Giudizio assegnato: **R1 Verde**
- » Rilevati 1 gap Basso
- » L'intervento, indirizzato a valutare l'efficacia e l'efficienza del processo di emissione e gestione delle obbligazioni bancarie garantite, in coerenza con il sistema dei controlli interni e con i principi di vigilanza, ne ha evidenziato l'adeguatezza.

GESTIONE CREDITI PROBLEMATICI

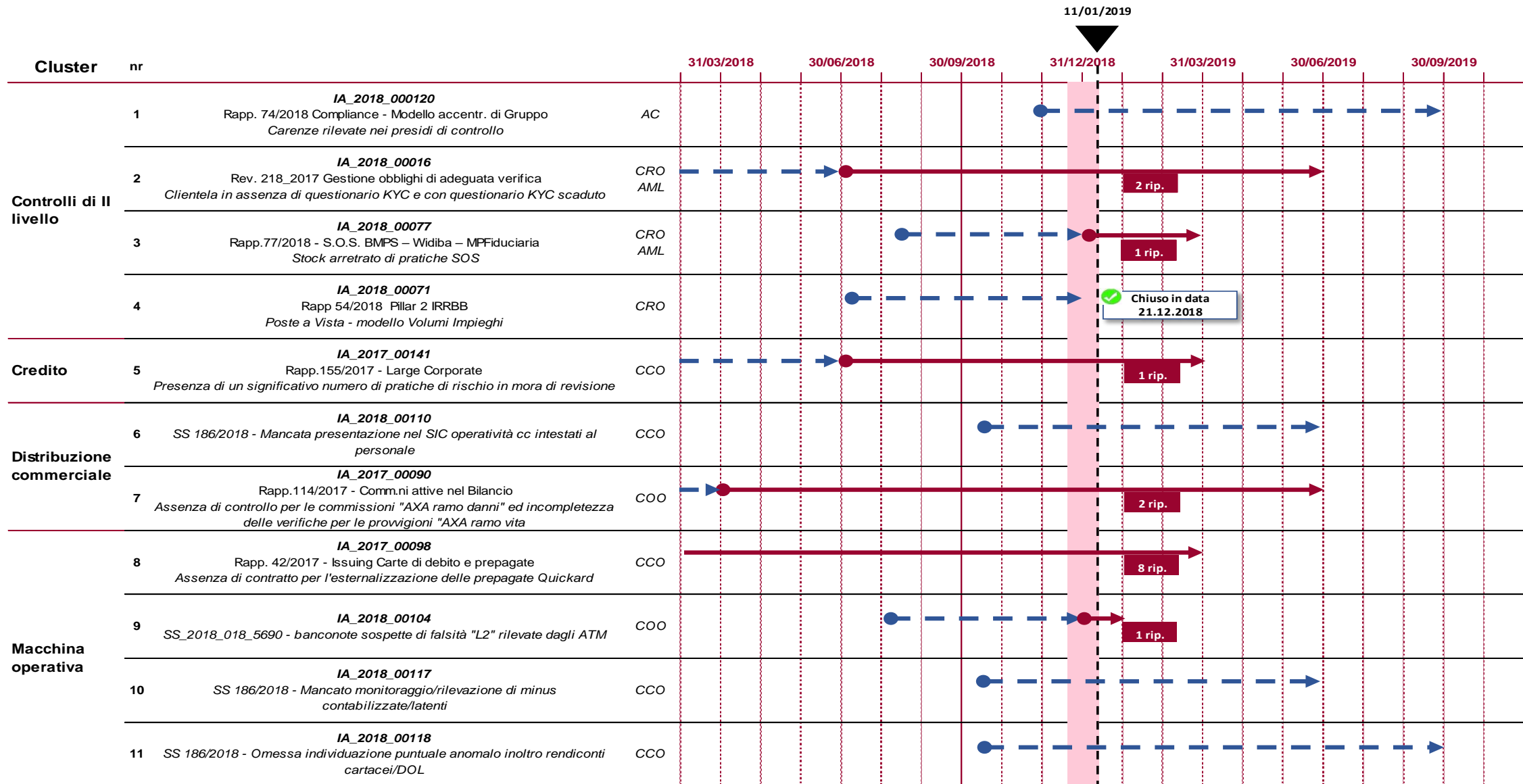
- » Rapp 71/2018 - Processo Gestione Massiva Crediti (Unlikely to Pay)
- » Giudizio assegnato: **R2 Giallo**
- » Sono stati rilevati 5 gap Medi; le principali anomalie sono relative a:
 - percorso di attribuzione automatica dei percorsi gestionali;
 - carenti controlli previsti dalla normativa sugli Organismi di Vigilanza;
 - mancata previsione di autorizzazione formale per le adesioni alle procedure concorsuali;
 - misurazione e analisi KPI;
 - controlli sulla correttezza dell'autonomia deliberativa.

ATTIVITA' DI
AUDIT NEL
PERIODO IN
ESAMEFOLLOW UP
GAP
DI AUDIT

- » Al 11.01.2019 risultano in monitoraggio **16 gap di audit a rilevanza «Alta»** di cui 8 già oggetto di almeno 1 ripianificazione della scadenza (cfr.slide successiva per rappresentazione di sintesi)
- » Rilevano nel periodo le chiusure di 3 gap a rilevanza «Alta» (Pillar 2 IRRBB; MPS Tenimenti; FEA).



1 Executive Summary - GAP in monitoraggio al 11.01.2019 (rilevanza «Alta»)* 1/2

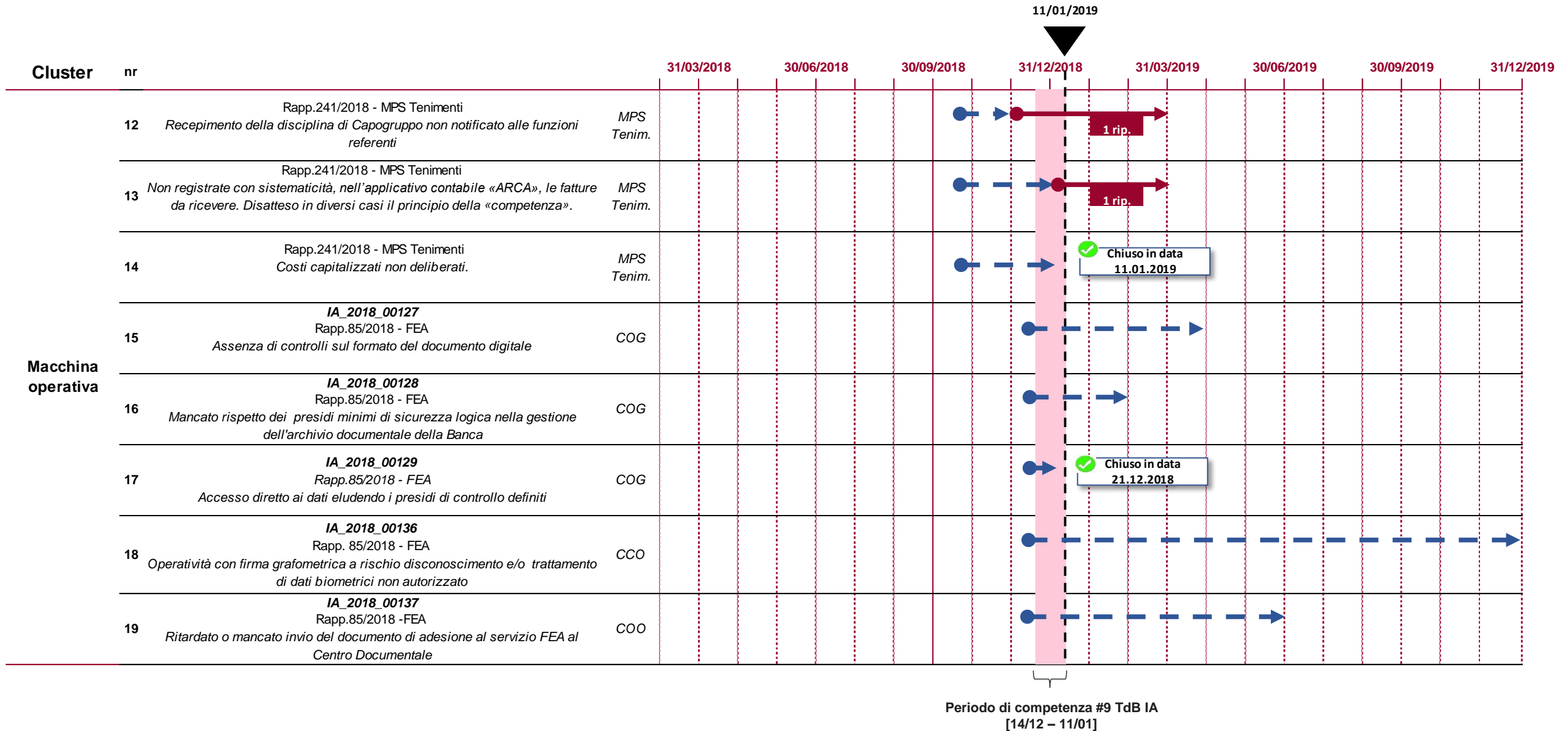


Periodo di competenza #9 TdB IA
[14/12 – 11/01]

*Cfr. Allegato



1 Executive Summary - GAP in monitoraggio al 11.01.2019 (rilevanza «Alta»)* 2/2



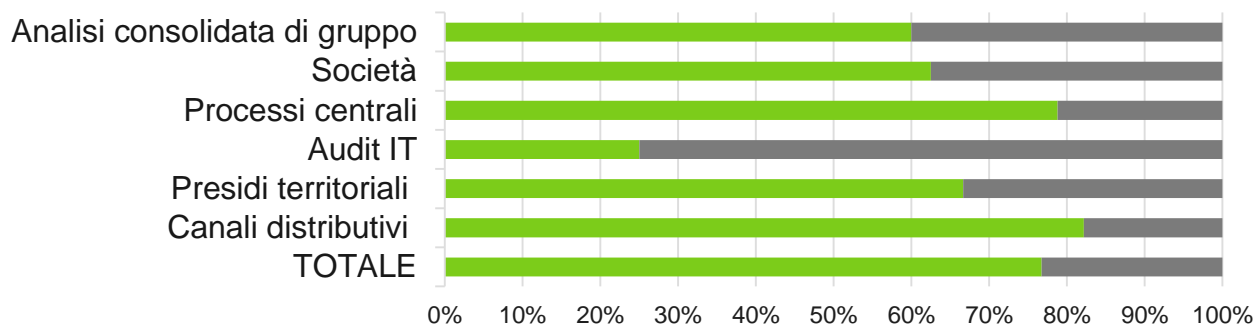
1 Overview interventi di audit

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	1	1	3 ^o	5	-	100,0%
Società	3	-	5	8	-	100,0%
Processi centrali	5	2	26	33	3	100,0%
Audit IT	2	1	1	4	-	100,0%
Presidi territoriali	6	6	24	36	-	100,0%
Canali distributivi (compresa Rete Promotori)	8	15	106	127 ^b	10	101,6%
SUB TOTALE PIANIFICATI	25	25	165	213	13	100,9%
Indagini / Servizi speciali	26	-	40	60**		
Interventi straordinari	1	0	7	3		
TOTALE	52	25	212	276		

Avanzamento interventi su Audit Plan (%)

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



^a I 3 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**
- Compliance di Gruppo (BMPS, Widiba e MPS CS)


(*) 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

3 Interventi di processo chiusi: Audit Plan 2018 (1/4)

N. RAPPORTO	DATA DI PUBBLICAZIONE	MACROPROCESSO	DESCRIZIONE INTERVENTO	GRADE ¹	GAP ²				CONTROLLI SSM ³				ORGANI DESTINATARI BMPS				
					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 	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							
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	

(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 – controlli SSM 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) Legenda controlli SSM (Single Supervisory Mechanism : BM Business Model - 1° Pillar; IG Internal Governance - 2° Pillar; RC Risk to Capital - 3° Pillar; RL Risk to Liquidity - 4° Pillar.



3 Interventi di processo chiusi: Audit Plan 2018 (2/4)

N. RAPPORTO	DATA DI PUBBLICAZIONE	MACROPROCESSO	DESCRIZIONE INTERVENTO	GRADE ¹	GAP ²				CONTROLLI SSM ³				ORGANI DESTINATARI BMPS				
					ALTI	MEDI	BASSI	TOT.	BM	IG	RC	RL	Pres. CdA	AD	CS	CR	ODV 231
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 [OdV 231] Ⓞ														
			- BMPS	R3	1	2		3		X			X	X	X	X	X
			- MP Fiduciaria	R3	1	2		3					*				
			- Widiba	R2		2	1	3									
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) Ⓞ														
			- BMPS	R2		2	1	3		X			X	X	X	X	
			- Widiba	R2		2		2					*				
			- Filiale NY 🔒	R2									X	X	X	X	
038/2018	13/09/2018	FINANZA/ TESORERIA & CAPITAL MGMT	Processo di contribuzione alla determinazione dei parametri EURIBOR e EONIA	R1					Non Applicabile								

* Gli estratti relativi alle legal entity sono stati inviati ai rispettivi organi aziendali

(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 – controlli SSM 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) Legenda controlli SSM (Single Supervisory Mechanism : BM Business Model - 1° Pillar; IG Internal Governance - 2° Pillar; RC Risk to Capital - 3° Pillar; RL Risk to Liquidity - 4° Pillar.



3 Interventi di processo chiusi: Audit Plan 2018 (3/4)

N. RAPPORTO	DATA DI PUBBLICAZIONE	MACROPROCESSO	DESCRIZIONE INTERVENTO	GRADE	GAP				CONTROLLI SSM				ORGANI DESTINATARI BMPS				
					ALTI	MEDI	BASSI	TOT.	BM	IG	RC	RL	Pres. CdA	AD	CS	CR	ODV 231
119/2018	25/09/2018	CREDITO	Gestione intermediazione in oro con aziende orafe	R2					Non Applicabile								
094/2018	04/10/2018	PIANIFICAZIONE STRATEGICA/CONTABILITA'	Business Model (focus su commissioni)	R2		2	2	4	X	X				X	X		
037/2018	04/10/2018	RISK MANAGEMENT	Processo convalida AMA 	R1						X	X		X	X	X	X	
042/2018	04/10/2018	RISK MANAGEMENT	ICAAP 	R1						X	X		X	X	X	X	
040/2018	09/10/2018	RISK MANAGEMENT	Calcolo EAD nel nuovo modulo ECL (Finding #2 OSI 1238)	R2					Non Applicabile				X	X	X	X	
093/2018	09/10/2018	CREDITO	Underestimation of key metrics for calculating loan loss provisions (FINDING 8 OSI 1238)	R1						X			X	X	X	X	
226/2018	11/10/2018	CREDITO	Efficacia e tempestività del processo di classificazione a maggior rischio delle posizioni oggetto di Forborne (Finding #6 OSI-1238)	R1						X	X		X	X	X	X	
067/2018	11/10/2018	CREDITO	Revisione Credit Default Detection – focus non binding parameters (Finding #7 OSI-1238)	R1							X		X	X	X	X	
068/2018	11/10/2018	CREDITO	Business Plan Sofferenze (Finding #9 OSI-1238)	R2			1	1			X		X	X	X	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 – controlli SSM 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) Legenda controlli SSM (Single Supervisory Mechanism : BM Business Model - 1° Pillar; IG Internal Governance - 2° Pillar; RC Risk to Capital - 3° Pillar; RL Risk to Liquidity - 4° Pillar).



2 Interventi di processo chiusi: Audit Plan 2018 (4/4)

N. RAPPORTO	DATA DI PUBBLICAZIONE	MACROPROCESSO	DESCRIZIONE INTERVENTO	GRADE ¹	GAP ²				CONTROLLI SSM ³				ORGANI DESTINATARI BMPS				
					ALTI	MEDI	BASSI	TOT.	BM	IG	RC	RL	Pres. CdA	AD	CS	CR	ODV 231
241/2018	26/10/2018	CONTABILITA' FISCALE E VIGILANZA	MPS Tenimenti – Aspetti amministrativo-contabili e presidio dei controlli	R3	3	6		9	Non Applicabile					X	X		
045/2018	26/10/2018	RISK MANAGEMENT	ILAAP 	R1						X			X	X	X	X	
074/2018	30/11/2018	COMPLIANCE	Compliance: modello accentrato di Gruppo con focus su Widiba e MPS CS (previsti specifici approfondimenti su usura)  [OdV 231]	R3	1	4	1	6		X			X	X	X	X	X
085/2018	12/12/2018	RAPPORTO CON IL CLIENTE	Dematerializzazione disposizioni operative e firma grafometrica	R4	5	3	4	12	Non Applicabile				X	X	X	X	
083/2018	12/12/2018	BCM	Disaster Recovery 	R1						X							
039/2018	13/12/2018	FINANZA	Processo di segnalazione al FITD (Fondo Interbancario di Tutela dei Depositi) della posizione aggregata per depositante 	R1					Non Applicabile				X	X	X	X	
036/2018	20/12/2018	RISK MANAGEMENT	Processo convalida AIRB 	R1			1	1		X	X						
071/2018	07/01/2019	GESTIONE CREDITI PROBLEMATICI	Processo Gestione Massiva Crediti (Unlikely to Pay)	R2		5		5		X							
065/2018	07/01/2019	CREDITO TESORERIA & CAPITAL MGMT	Covered Bond 	R1			2	2		X	X	X					

— Nuovi interventi avviati post TdB #8.

(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.

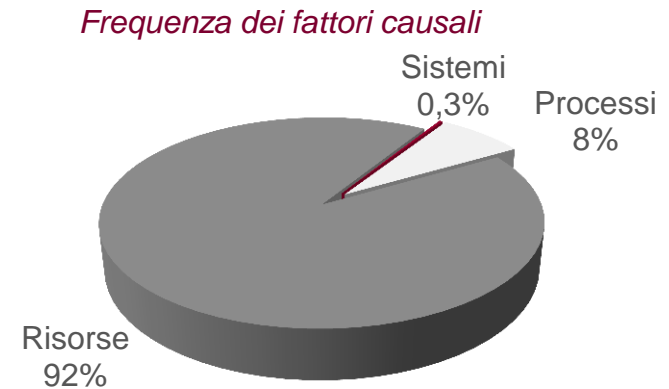
(3) Legenda controlli SSM (Single Supervisory Mechanism : BM Business Model - 1° Pillar; IG Internal Governance - 2° Pillar; RC Risk to Capital - 3° Pillar; RL Risk to Liquidity - 4° Pillar).



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	-	2	-	-
	Credito	4	9	1	-
	Processi Commerciali/Gestionali	-	-	-	-
	Servizi di Investimento	-	1	-	-
STRUTTURE OPERATIVE	Altri rischi operativi	1	22	6	-
	Compliance	5	29	5	-
	Credito	-	15	6	-
	Processi Commerciali/Gestionali	25	5	1	-
	Servizi di Investimento	10	27	1	-
PROMOTORI FINANZIARI	Complessivo**	15	19	6	-



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	164	1	ELEVATA CONSISTENZA E/O FREQUENZA DI DOCUMENTI SOSPESI IN PARDO	27	16,5%	0
			PRESENZA DI DOCUMENTI SOSPESI IN TORB	20	12,2%	0
Compliance	240	9	MANCATA RIVALUTAZIONE PERIODICA DELLA CLIENTELA FINALIZZATA AL CONTROLLO COSTANTE DEL RAPPORTO CONTINUATIVO (ARTT. 18-19 D.LGS 231/2007)	62	25,8%	1
			MANCATA O INCOMPLETA ACQUISIZIONE DEL QUESTIONARIO KYC	51	21,3%	0
Credito	85	7	MANCATA/NON CORRETTA FORMALIZZAZIONE DELLA DOCUMENTAZIONE DELLE LINEE DI CREDITO ACCORDATE AL CLIENTE	12	14,1%	1
			MANCATA/NON PUNTUALE ATTENZIONE AGLI ADEMPIMENTI AMMINISTRATIVI (RINNOVO PRATICHE, RATING, ETC.)	10	11,8%	0
Processi Commerciali e Gestionali	27	-1	GESTIONE SPECIMEN DI FIRMA DIPENDENTI NON CONFORME	5	18,5%	0
			MANCATO RAGGIUNGIMENTO DEGLI OBIETTIVI COMMERCIALI	4	14,8%	0
Servizi di Investimento	153	5	RIPROFILAZIONE MIFID ASSENTE	21	13,7%	0
			CONSULENZA AVANZATA: INADEGUATA ATTENZIONE A "SEMAFORI ROSSI" ED ALLE ATTIVITÀ CONNESSE	21	13,7%	1






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

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

N. INCARICO	MACROPROCESSO	DESCRIZIONE INTERVENTO	DATA INIZIO	EXIT MEETING	DATA FINE PRESUNTA	CONTROLLI SSM				ORGANI DESTINATARI BMPS PREVISTI				
						BM	IG	RC	RL	Pres. CdA	AD	CS	CR	OdV 231
076/2018	CORPORATE GOVERNANCE	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)	19/10/2018		31/01/2019*		X					X		
092/2018	CICLO PASSIVO	Gestione fornitori, attività negoziali e contratti [CS e OdV 231] 	16/07/2018	24/12/2018	31/01/2019*		X					X		X
103/2018	PRODOTTI	Widiba - Prodotto Mutui on Line in ottica di redditività	20/07/2018		20/01/2019*	Non Applicabile								
090/2018	DATA GOVERNANCE	Data Governance: struttura organizzativa, framework e strumenti a supporto	23/07/2018		31/01/2019*		X							
104/2018	COMPLIANCE	MIFID II: Processo/Modello e modalità distributive/controlli di 1° livello a livello Gruppo [CS] 	31/07/2018		31/01/2019*	Non Applicabile						X		
118/2018	GESTIONE ORDINARIA DEL CREDITO	Gestione istruttoria veloce	17/08/2018		14/01/2019*	Non Applicabile								
046/2018	RISK MANAGEMENT	RAF 	04/10/2018		31/01/2019*		X							



Per data inizio.

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

* Le date segnalate hanno subito degli slittamenti rispetto a quanto indicato nel Tableau de Board #8 per varie motivazioni tra le quali l'ampliamento dei perimetri delle revisioni e/o sopraggiunte richieste di altre attività straordinarie.



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

N. INCARICO	MACROPROCESSO	DESCRIZIONE INTERVENTO	DATA INIZIO	EXIT MEETING	DATA FINE PRESUNTA	CONTROLLI SSM				ORGANI DESTINATARI B;MPS PREVISTI				
						BM	IG	RC	RL	Pres. CdA	AD	CS	CR	OdV 231
084/2018	BUSINESS CONTINUITY MANAGEMENT	Business Continuity Management 	04/10/2018	18/12/2018	31/01/2019*		X							
082/2018	DATA GOVERNANCE	Data quality LGD	08/10/2018		15/01/2019*		X							
117/2018	PRODOTTI DEL CREDITO	Gestione Anticipi	31/10/2018	05/12/2018	15/01/2019*	Non Applicabile								
086/2018	COMPLIANCE	Controlli Privacy 	30/10/2018	20/12/2018	31/01/2019*		X							
035/2018	SERVIZI FIDUCIARI	MP Fiduciaria Mandati societari – assessment	14/11/2018		31/01/2019*	Non Applicabile								
069/2018	CREDITO	SIRIO: piattaforma gestione contenzioso	14/11/2018		31/01/2019^		X	X						
102/2018	SERVIZI DI INVESTIMENTO	Widiba - Piattaforma WISE a supporto dei servizi di investimento	15/11/2018		31/01/2019*	Non Applicabile								
066/2018	CREDITO	Double and Multicounting Collaterals (Finding #3 OSI 1238 BCE)	26/11/2018		31/01/2019	Non Applicabile								

* Le date segnalate hanno subito degli slittamenti rispetto a quanto indicato nel Tableau de Board #8 per varie motivazioni tra le quali l'ampliamento dei perimetri delle revisioni e/o sopraggiunte richieste di altre attività straordinarie.



5 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 forensic 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			
CS	11/07/2018	230/2018	Approfondimento errato calcolo del TEG riferito alla procedura sugli anticipi (usura)	20/09/2018			x		
BANKITALIA	07/09/2018	-	Approfondimento Project Ice Deloitte Forensic (terza fase)**	27/09/2018	x	x	x		
CS	11/07/2018	229/2018	Approfondimento Incidenti di sicurezza IT anno 2017	30/10/2018			x		
CS/ODV 231	12/02/2018	151/2018	Servizio Speciale: Antiriciclaggio - Trieste Piazza Borsa - accertamento gestione posizione Hotel Pasteur srl	14/11/2018	x	x	X		x
CR	01/08/2018	237/2018	Comitato Rischi - Richiesta di approfondimenti circa le procedure IT ad alta "manualità"	26/11/2018				X	
ECB Guidance on Leveraged Transactions	16/05/2017	280/2018	Revisione Leveraged Transactions	04/12/2018	X	X	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.6.

INTERVENTI IN CORSO				
RICHIEDENTE	DATA RICHIESTA	N. RAPPORTO	DESCRIZIONE INTERVENTO	DATA INIZIO
CS	26/09/2019	284/2018	Servizio Speciale: accertamento gestione processo usura	05/10/2018



Allegato - Focus GAP attivi in monitoraggio (rilevanza «Alta») per cluster



Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») – Controlli di II livello 1/2

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig.	# Rip.	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
1	74/2018 del 30/11/2018	<p><u>IA 2018_00120</u> <u>Compliance: modello accentrato di Gruppo con focus su Widiba e MPS CS</u></p> <p>Carenze rilevate nei presidi di controllo, in particolare:</p> <ul style="list-style-type: none"> la pianificazione di dettaglio dei controlli da svolgere sulla Piattaforma Compliance risulta incompleta, anche a fronte di controlli eventualmente svolti; la valutazione di conformità in casi specifici è riferibile ad «analisi e supporto svolto nel continuo» per assenza di controlli specifici pianificati/documentati, sia riguardo a materie della Capogruppo caratterizzate da valutazione «parzialmente conforme» (es. anticorruzione), sia riguardo a 10 materie (su 12) oggetto di valutazione da parte di Widiba. Si fa altresì presente che in Widiba, la valutazione di conformità è ancora assente per numerose materie, ne' risultano pianificati/documentati controlli su tali materie da parte del Settore Compliance Widiba, mentre è stata appena avviata la pianificazione/svolgimento controlli su quelle non valutate ma oggetto di sinergia con Capogruppo (perimetro IT, Gestione Patrimonio). Infine su MPSCS, la valutazione di conformità non è ancora stata emessa per alcune materie, anche in presenza di controlli avviati (es. «esternalizzazioni»); le attività di controllo sull'operato dei Presidi Specialistici delle controllate, unitamente ad eventuali controlli «in autonomia» da parte della Funzione Compliance sulle materie da essi presidiate, non risultano pianificati; limiti nella «tracciatura» dell'attività di seguimiento dei controlli inerenti le Aree Normativa usura e Trasparenza che non permettono di comprendere con chiarezza lo «stato di avanzamento» nella risoluzione delle problematiche riscontrate. Tale «stato di avanzamento» deve risultare opportunamente «memorizzato» nella procedura informatica di riferimento («Piattaforma di Compliance» e/o RIGAM). Occorre, inoltre, stabilire nella normativa aziendale o in quella interna alla Funzione di Compliance, i discriminanti che implicano, nel caso di esiti «non positivi» dei controlli, il censimento dei «gap» in RIGAM. 	<p>Rafforzare l'attività di controllo sulle materie presidiate tramite le seguenti azioni:</p> <p>a) pianificare ed inserire in Piattaforma Compliance il dettaglio dei controlli da effettuare nel corso dell'anno ad integrazione del Compliance Plan;</p> <p>b) prevedere lo svolgimento di controlli, in ottica risk based, su tutte le materie oggetto di valutazione sia per quanto attiene la Capogruppo che per le controllate, motivando eventuali valutazioni basate solo su «analisi e supporto svolto nel continuo»;</p> <p>c) pianificare annualmente in dettaglio specifiche attività di controllo sull'operato dei Presidi Specialistici della Capogruppo e delle controllate unitamente ad eventuali controlli «in autonomia» da parte della Funzione Compliance;</p> <p>d) ottimizzare la «tracciatura» dell'attività di seguimiento dei controlli aventi esito «parzialmente conforme» o «non conforme». In particolare, lo «stato di avanzamento» nella risoluzione delle problematiche riscontrate deve risultare opportunamente «memorizzato» nella procedura informatica di riferimento. La normativa aziendale / interna alla Funzione Compliance deve prevedere i discriminanti che implicano, nel caso di esiti «non positivi» dei controlli, il censimento dei «gap» in RIGAM.</p>	0%	30/09/19	-	-	Funzione di Compliance di Capogruppo	<p><i>La Funzione ha definito un Remediation Plan articolato per la risoluzione delle problematiche monitorando nel tempo lo stato di avanzamento. Le evidenze fornite confermano che l'attività sta procedendo in linea con le scadenze previste. In ottica prudenziale, considerata l'articolazione dell'attività (ed il ridotto stato di avanzamento medio dei singoli interventi) si mantiene una valutazione del SAL complessivo minima.</i></p>



Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») – Controlli di II livello 2/2

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig.	# Rip.	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
2	218/2017 del 02/02/2018	<p>IA 2018 00016</p> <p>Gestione obblighi di adeguata verifica della clientela in materia di AML-CFT</p> <p>Clientela in assenza di questionario KYC e con questionario KYC scaduto. Il 23% della clientela (dati aggiornati a dicembre 2017) risulta ancora privo di almeno un questionario KYC (circa 1,2mln) e ciò non consente alla Banca di poter pienamente dimostrare un'adeguata verifica della propria clientela, posto comunque che il 99% dei quali ha un profilo di rischio basso o irrilevante, sebbene assegnato in automatico dalla procedura sulla base delle informazioni presenti nei sistemi. Tale situazione è peraltro appesantita dalla presenza di 1mln ulteriore di clienti in possesso di un questionario KYC scaduto.</p>	<p>Proseguire, anche in collaborazione con la Funzione di Controllo di I livello, con le implementazioni di attività specifiche in grado di ridurre considerevolmente il numero di clienti sprovvisti di KYC (e quindi non adeguatamente conosciuti) e con KYC scaduto. Ciò agendo, in primis, sul recupero dei questionari (tenendo presente che oltre il 40% dei clienti senza KYC è concentrato nell'Area Territoriale Sud e Sicilia - 5076) ed affiancando azioni mirate in grado di identificare efficacemente ulteriori macrocasistiche che compongono il perimetro dei clienti attivi ai fini AML, eventualmente ripulendola base dati. A tal fine, rivalutare anche l'efficacia del monitoraggio periodico in essere condotto sui conti correnti tecnici delle carte prepagate estinte al fine di eliminare possibili «falsi positivi» dal novero dei clienti attivi AML (es: NDC101573801, 115650855, 18634444, 98015812, 1142785). In subordine, qualora le precedenti attività non dovessero sortire gli effetti desiderati, i rapporti che residueranno saranno da estinguere.</p>	80%	30/06/18	2	30/06/19	AML	<p>DONE</p> <p>Il tasso di copertura KYC ha raggiunto circa il 94% mentre la quota di clienti con KYC scaduto è diminuita da circa 1mln di inizio 2018 agli attuali 760mila.</p> <p>TO DO</p> <p>Continuano le attività finalizzate alla rivalutazione della clientela con KYC scaduto (BR 77272 - Ispezione BI_KYC automatico su clienti con pdr alto e KYC scaduto - FASE 2).</p> <p>La ripianificazione del gap al 30.06.2019 è allineata agli accordi presi dalla Funzione AML/CFT con Banca d'Italia</p>
3	77/2018 del 23/07/2018	<p>2. IA 2018 00077</p> <p>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 di gennaio/ settembre 2015 alle 2,4 registrate ad aprile/ maggio 2018), tuttavia permane una quota consistente di pratiche riferite all'anno 2017 (948 al 31/05/2018).</p>	<p>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 ripianificazione per 5 volte del precedente gap (IA2014_ 189) emesso nel corso della revisione conclusasi al termine del 2014.</p>	80%	31/12/18	1	31/03/19	AML	<p>DONE</p> <p>Progressiva riduzione dell'ammontare di pratiche SOS in stock. (ca. 1400 pratiche residue a dicembre 2018 – stabile rispetto a novembre).</p> <p>TO DO</p> <p>Procede lo smaltimento dello stock pratiche SOS. In linea con il piano di smaltimento concordato tra la Funzione AML/CFT e Banca d'Italia il fenomeno dovrebbe dimensionarsi entro fine marzo 2019 ad un livello sostenibile.</p>
4	54/2018 del 11/07/2018	<p>IA 2018 00071</p> <p>Evoluzione Pillar 2 con focus IRRBB</p> <p>Poste a Vista - modello Volumi Impieghi</p> <p>L'assunzione alla base del modello statistico non è rispettata per i cluster KC, PMI, PRIVATE e SB, che rappresentano il 95% dei volumi complessivi degli Impieghi (di cui SB incide per circa il 43%).</p>	<p>Per i cluster degli Impieghi per cui le assunzioni alla base del modello non sono rispettate si richiede di individuare metodologie statistiche consistenti e robuste.</p>	100%	31/12/18	-	31/12/18	CRO	<p>DONE</p> <ul style="list-style-type: none"> Analisi delle serie storiche inglobando dinamiche creditizie; applicazione del modello attuale alla luce delle dinamiche creditizie; stima degli impatti sulle misure IRRBB; stima degli impatti sull'impairment dei crediti; adeguamento Framework e manuali metodologici

✓ Chiuso in data
21.12.2018



Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») - Credito

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig.	# Rip.	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
5	155/2017 del 15/11/2017	<u>IA 2017 00141</u> <u>Revisione Large Corporate</u> Presenza di un significativo numero di pratiche di rischio in mora di revisione. Alla data del 31/08/2017 su un portafoglio di 447 controparti affidate, pari ad un accordato di €mld 11,4, risulta un arretrato di 279 posizioni, pari ad un accordato di €mld 6,8 e corrispondente al 62% ca. del totale del portafoglio affidato.	Finalizzare il piano operativo già avviato per la riduzione dell'arretrato sulla base di priorità «risk based» (rating, classificazione amministrativa e gestionale, anzianità ultimo rinnovo...).	40%	30/06/18	1	01/04/19	CCO	DONE <i>Lo stock di pratiche scadute alla data del 30.11.2018 era di 228 pari al 61%. Di queste, 35 sono in corso di delibera da parte della Direzione Crediti Performing e dell'Area Ristrutturazioni. Il perfezionamento di tali istruttorie porterebbe l'arretrato al 52,51%.</i> TO DO <i>Incrementare l'attività di revisione delle pratiche giungendo ad un livello fisiologico di arretrato al 01/04/2019.</i>



Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») – Distribuzione commerciale

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig.	# Rip.	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
6	SS 186/2018 Del 16/10/2018	IA_2018_00110 Mancata presentazione nel SIC 1017 - operatività cc intestati al personale - delle operazioni affluite sui cc (cat. 109) eseguite da pdl aperti con la matricola di operatori diversi dall'intestatario del rapporto	Estensione del perimetro delle operazioni soggette a controllo.	20%	Studio di prefattib. 31/12/18	-	30/06/19	CCO	Completato lo studio di prefattibilità e avviate le attività implementative
7	114/2017 del 29/06/2017	IA_2017_00090 Comm.ni attive nel Bilancio d'esercizio – composizione e rappr.ne contabile (commissioni percepite da Soc. Ass.) Assenza di controllo per le commissioni "AXA ramo danni" ed incompletezza delle verifiche per le provvigioni "AXA ramo vita" Assenza di controlli per le commissioni di retrocessione riferite al "ramo danni", la cui incidenza sulla totalità delle provvigioni contabilizzate nel 2016 è pari al 17,90% (€/mgl. 29.444 su complessive € mgl. 164.422).Presenti, inoltre disallineamenti nelle commissioni del "ramo vita" tra il calcolo elaborato dall'applicativo Syfe e quanto determinato dalla Compagnia Assicuratrice, per €/mgl. 2.063 in valore assoluto (€/mgl. 1.120 in termini di somma algebrica).	Sistemazione delle differenze relative alle commissioni del "ramo vita" e del "ramo danni" presenti tra i flussi "AXA" ed i calcoli elaborati dall'applicativo Syfe. Definire, nell'ambito di una strutturata e regolare attività di controllo, azioni dirette ad individuare le differenze più rilevanti, alle quali dovrà provvedere il Settore Banca Collocatrice. In particolare per le tariffe del "ramo vita", dovranno essere intrapresi interventi per la sostanziale riduzione delle differenze rilevate. Per le commissioni del "ramo danni", dovrà essere avviata una puntuale attività di verifica, finalizzata alla progressiva riduzione dei disallineamenti che emergeranno.	50%	31/03/18	2	30/06/19	COO	DONE Completate le attività relative al ramo vita e ultimate le analisi inerenti gli interventi procedurali riferiti al ramo danni. Al fine di assicurare il rispetto della nuova data di scadenza fissata (30.06.19) l'Area Operations Finanza ha proceduto secondo tre linee di intervento: - rafforzare il team interno dedicato ai controlli e alla definizione dei requisiti funzionali di rimozione dei disallineamenti; - acquisire dalle funzioni IT del Consorzio l'impegno al supporto e realizzazione dei rilasci determinanti al rispetto della data di mitigazione; - prevedere un'iniziativa ad hoc lato AXA (aggiornamento del motore di calcolo). TO DO Previste realizzazioni informatiche strutturate da parte del COG e dell'AXA Danni. La scadenza è stata ripianificata al 30.06.2019 per la realizzazione degli interventi procedurali preventivati da parte delle funzione/società sopra citate



Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») – Macchina operativa 1/7

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig.	# Rip.	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
8	42/2017 del 09/08/2017	<u>IA 2017_00098</u> <u>Issuing carte di debito e prepagate</u> Assenza di contratto per l'esternalizzazione delle prepagate Quickard. Basilichi Spa eroga il servizio solo sulla base dell'accettazione di un'offerta economica, in assenza di un contratto che regoli diritti ed obblighi delle parti con livelli di servizio formalizzati. Non sono stati inoltre svolti gli adempimenti in materia di privacy, per quanto riguarda il trattamento dei dati personali dei clienti da parte di terzi. In aggiunta, Basilichi Spa ha a sua volta subappaltato il processo di «prevenzione frodi» e «gestione reclami sulle carte» a Fruendo Srl, senza il preventivo accordo della Banca.	Redigere un contratto con Basilichi Spa, nel rispetto di quanto previsto dalla Circ. 285/13. Provvedere a mettere in atto gli adempimenti necessari in materia di privacy. Regularizzare il subappalto.	95%	31/12/17	8	31/03/19	CCO	DONE <i>Finalizzata la bozza del contratto con Nexi/Basilichi.</i> TO DO <i>Ripianificato nuovamente in quanto sono ancora in corso da parte della Funzione Commerciale valutazioni strategiche che impattano sul complessivo comparto della Monetica ivi comprese le carte Quickard.</i>
9	Serv Spec. SS_2018_018_5690 del 16/10/2018	<u>IA 2018_00104</u> <u>Servizio Speciale SS_2018_018_5690</u> L'esecuzione degli adempimenti previsti per le banconote versate nell'impianto ATM e da questo scartate poiché "sospette di falsità – L2" (che necessitano del verbale di rilevazione e trasmissione a Bankit tramite l'applicativo SIMEC), non è attualmente monitorata da altre Funzioni della Filiale e/o da Strutture esterne alla stessa. L'esecuzione di tali attività è lasciata alla sola autonoma iniziativa dell'operatore con il rischio che le stesse non vengano poste in essere ovvero siano realizzate con tempistiche diverse da quanto richiesto.	Predisposizione di un "alert" da indirizzare nella MyFace - Cruscotto Filiale accessibile a tutti gli operatori dell'U.O. di gestione dell'impianto, con la specifica scadenza degli adempimenti da porre in essere. Segnalazione che rimarrà attiva per il corrispondente arco temporale di 5 gg. Predisposizione di un nuovo controllo SIC da attribuire al Reparto Controlli di AT con il quale evidenziare a tale Struttura la lista delle filiali interessate alla gestione delle banconote "L2".	90%	31/12/18	1	31/01/19	COO	DONE <i>Le esigenze sono state definite e le Funzioni IT coinvolte (Monetica, Sportello e Reporting). Completati i test UAT con esito positivo.</i> TO DO <i>In attesa del passaggio in produzione da parte del COG.</i>
10	SS 186/2018 Del 16/10/2018	<u>IA 2018_00117</u> Mancato monitoraggio/rilevazione di minus contabilizzate/latenti	Periodica rilevazione delle posizioni che hanno accumulato minus rilevanti	20%	Studio di prefattib. 31/01/19	-	30/06/19	CCO	<i>Completato lo studio di prefattibilità e avviate le attività implementative</i>
11	SS 186/2018 Del 16/10/2018	<u>IA 2018_00118</u> Omessa individuazione puntuale anomalo inoltro rendiconti cartacei/DOL	Divieto di recapito su Strutture BMPS e acquisizione manleva per disallineamento residenza anagrafica e recapito postale. Verifiche periodiche per richieste DOL.	20%	Studio di prefattib. 31/12/18	-	30/09/19	CCO	<i>Completato lo studio di prefattibilità e avviate le attività implementative</i>



Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») – Macchina operativa 2/7

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig.	# Rip.	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
12	241/2018 del 24/10/2018	<p>MPS Tenimenti SpA - Aspetti amministrativo-contabili e presidio dei controlli</p> <p>Recepimento della disciplina di Capogruppo non notificato alle funzioni referenti e assenza di una declinazione normativa adeguata alle specificità dell'azienda.</p> <p>In relazione agli ambiti esaminati nella presente revisione, non risultano notificati alle funzioni referenti i documenti normativi indicati nell'allegato n. 3.</p> <p>Per le direttive/policy di maggior significatività e nei casi in cui la normativa di Capogruppo non è adeguata alle specificità dell'azienda, la relativa disciplina dovrà essere riformulata coerentemente alle caratteristiche della Società.</p>	<p>Formulazione del recepimento normativa e adeguamento alla gestione caratteristica dell'azienda</p> <p>Relativamente ai documenti indicati nell'allegato n. 3 provvedere a notificare il relativo recepimento nei confronti delle funzioni referenti e a redigere una normativa interna, nei casi espressamente indicati (all.to n3/4).</p> <p>In particolare si ravvisa la necessità di regolamentare adeguatamente il processo deliberativo di «gestione della spesa», nel rispetto delle direttive/policy di Capogruppo.</p> <p>Per esigenze di correttezza operativa, è possibile differenziare il processo autorizzativo in relazione alla natura del costo, distinguendo tra:</p> <ul style="list-style-type: none"> • <u>Spese obbligatorie</u> (fase autorizzativa assolta con l'approvazione dell'apposito stanziamento a budget – cfr. D. 144 «Gestione della spesa» par. 4.1.1 – vers. 16 del 18.1.2018); • <u>Spese discrezionali</u> (soggette a preventiva autorizzazione); • <u>Spese discrezionali</u> per contratto a tacito rinnovo (fase autorizzativa assolta con l'approvazione dell'apposito stanziamento a budget); • <u>Commissioni/interessi passivi</u> (non soggetto ad autorizzazione); • <u>Utenze/cartelle esattoriali</u> (non soggette ad autorizzazioni). <p>La normativa in argomento dovrà, inoltre, prevedere la rendicontazione trimestrale nei confronti della Capogruppo per le imputazioni di importo rilevante effettuate direttamente a sistema (c.d. «spese secche») - cfr. D 839 «Direttiva di Gruppo in materia di gestione della spesa e gestione dei fornitori par. 5.6 – vers. 18 del 21.3.2018. Infine, per regolamentare i controlli di 1° e 2° livello riferiti ad adempimenti di routine e/o inerenti l'attività caratteristica, può ritenersi sufficiente la predisposizione di Ordini di Direzione (OdD).</p>	50%	30/11/18	1	31/03/19	MPS Tenimenti	<p>DONE</p> <p><i>L'impegno di notificare il recepimento delle direttive di gruppo alle varie funzioni referenti è stato eseguito nei tempi e modalità convenute.</i></p> <p>TO DO</p> <p><i>La Società sta predisponendo, in collaborazione con le competenti funzioni della Capogruppo, l'adeguamento delle direttive/policy della Capogruppo calibrandola sulla realtà aziendale.</i></p> <p><i>E' stata predisposta una bozza di riferimento che dovrà essere completata entro la data del 31.03.2019. Inoltre sono stati già predisposti alcuni ordini di direzione mirati al controllo della gestione della spesa e dei fornitori.</i></p>



Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») – Macchina operativa 3/7

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig.	# Rip.	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
13	241/2018 del 24/10/2018	<p><u>MPS Tenimenti SpA - Aspetti amministrativo-contabili e presidio dei controlli</u></p> <p>Non registrate con sistematicità, nell'applicativo contabile «ARCA», le fatture da ricevere. Disatteso in diversi casi il principio della «competenza».</p> <p>Carente la gestione delle fatture da ricevere, non sistematicamente registrate nell'applicativo contabile «ARCA».</p> <p>Presenza in bilancio di sopravvenienze passive di significativo importo per omesse registrazioni degli ordini di acquisto disposti, contabilizzati al ricevimento della fattura (principio di cassa).</p>	<p>Regolamentare il processo di contabilizzazione delle fatture da ricevere, nel rispetto dei principi di redazione del bilancio</p> <p>Disciplinare, con disposizioni interne (OdD), le tempistiche e le corrette modalità di registrazione delle fatture</p>	50%	31/12/18	1	31/03/19	MPS Tenimenti	<p>DONE</p> <p>Relativamente a quanto richiesto sulle fatture da ricevere, ovvero al rispetto del principio di competenza, le nuove regole rientreranno nella policy sulla gestione della spesa.</p> <p>Sono stati emessi nel frattempo gli ordini di direzione n. 1 e 2 che regolamentano le ordinazioni delle merci, la gestione della ricezione della merce e delle bolle, oltre alle tempistiche per la registrazione in contabilità, per rispettare il principio di competenza anche nelle fatture da ricevere</p> <p>TO DO</p> <p>Finalizzare la normativa interna per regolamentare in maniera strutturata la contabilizzazione delle fatture da ricevere</p> <p>Considerate le specificità dell'azienda e al fine di modulare adeguatamente la normativa dedicata, è stata convenuta una ripianificazione al 31.03.019.</p>
14		<p><u>MPS Tenimenti SpA - Aspetti amministrativo-contabili e presidio dei controlli</u></p> <p>Costi capitalizzati non deliberati.</p> <p>Non sistematicamente deliberati dal CdA i costi oggetto di capitalizzazione</p>	<p>Delibera dei costi capitalizzati.</p> <p>Sottoporre a delibera del CdA i costi che saranno capitalizzati nel corso dell'esercizio, preventivamente alla stesura del bilancio</p>	100%	31/12/18	-	31/12/18	MPS Tenimenti	<p>DONE</p> <p>Nella seduta consiliare del 18 gennaio 2019 verrà portata a ratifica una relazione con le capitalizzazioni effettuate nel 2018. Per il 2019 verrà impostato il budget e tutte le capitalizzazioni saranno preventivamente autorizzate dal Consiglio stesso.</p>

✓ **Chiuso in data
11.01.2019**



Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») - Macchina operativa 4/7

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig.	# Rip .	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
15	85/2018 del 12/12/2018	<p><u>IA 2018 00127</u></p> <p><u>Dematerializzazione disposizioni operative e firma grafometrica</u></p> <p>Assenza di controlli sul formato del documento digitale</p> <p>Il DPCM del 22 febbraio 2013 «<i>Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali</i>» include tra i requisiti della soluzione di Firma Elettronica Avanzata (FEA):</p> <ul style="list-style-type: none"> «l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati»; «la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma». <p>Allo scopo di rispettare tali requisiti, la soluzione FEA implementata dalla Banca prevede l'adozione del formato standard internazionale ISO 19005-1:2005, PDF/A*, per i documenti a firma grafometrica.</p> <p>Si osserva tuttavia che non sono presenti controlli atti a garantire che i documenti prodotti dalle diverse applicazioni bancarie e sottoposti alla firma del cliente siano conformi al suddetto formato.</p> <p>Questa carenza ha consentito la sottoscrizione di documenti ab origine non conformi al formato PDF/A, circostanza questa che ne ha determinato l'alterazione del contenuto che ad oggi risulta illeggibile. I documenti della specie risultano pertanto privi di qualsiasi validità.</p> <p>A tal proposito, con riferimento alla sottoscrizione di operazioni su Fondi Anima si osserva che:</p> <ul style="list-style-type: none"> in data 12/06 sono stati rilasciati in produzione 5 modelli non conformi che hanno determinato l'archiviazione di 165 documenti illeggibili su un totale di 429 sottoscritti. In data 28/06 sono stati rilasciati in produzione 2 modelli non conformi che hanno determinato l'archiviazione di 18 documenti illeggibili su un totale di 41 sottoscritti. <p>(*) Standard ISO 19005-1:2005, Document management -- Electronic document file format for long-term preservation, https://www.iso.org/standard/38920.html</p>	<p>Implementare controlli per verificare la consistenza del documento digitale al formato PDF/A</p> <p>Allo scopo di garantire l'aderenza ai requisiti regolamentari definiti per la Firma Elettronica Avanzata, implementare controlli che consentano di accertare la conformità al formato PDF/A, del documento elettronico sottoposto alla firma del cliente.</p> <p>Assicurare la conformità al suddetto formato anche in uscita dal sistema di acquisizione della firma cliente.</p>	50%	30/04/2019	-	-	COG	<p>DONE</p> <p>Predisposizione istruzioni per la funzione Cash Management ai fini della corretta predisposizione dei template:</p> <ul style="list-style-type: none"> Blocco della pubblicazione template eseguito Processo per la pubblicazione informatica dei template Manuale utente per la corretta implementazione dei template consegnato Normativa <p>Testato, su un campione significativo di documenti il tool automatico selezionato per la verifica di conformità sia dei template che dei singoli documenti.</p> <p>TO DO</p> <p>Introdurre controlli automatici preventivi sui template prodotti dalla funzione di Business Responsabile</p> <p>Eseguire un test di correttezza dei template esistenti e bloccare i template non conformi alle regole.</p> <p>Introdurre un controllo a monte dell'invio di un documento alla firma: controllare che non vi siano errori di natura tipografica o di composizione. In caso affermativo: bloccare il processo e invocare firma cartacea(**):</p> <ul style="list-style-type: none"> Test Piano di avvio in produzione definito (Sarà introdotto anche un controllo di correttezza formale a valle della apposizione delle firme (rif GAP 8 – IA_2018_00132)



Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») – Macchina operativa 5/7

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig.	# Rip.	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
16	85/2018 del 12/12/2018	<p><u>IA 2018_00128</u></p> <p><u>Dematerializzazione disposizioni operative e firma grafometrica</u></p> <p>Mancato rispetto dei presidi minimi di sicurezza logica nella gestione dell'archivio documentale della Banca, IBM Content Manager (CM)</p> <p>a) Il governo e la gestione delle utenze applicative che accedono al CM nonché dei relativi profili abilitativi vengono condotti difformemente dalle policy aziendali in materia*. Si rileva altresì che non è possibile, allo stato attuale, ricostruire l'associazione delle utenze ai corrispondenti asset di riferimento e strutture responsabili dell'utilizzo.</p> <p>b) Con riferimento alle modalità di accesso agli strumenti nativi a supporto del CM**, si osserva che:</p> <ul style="list-style-type: none"> le applicazioni non sono integrate con il sistema di autenticazione <i>Single Sign-On</i> (SSO) e non risultano implementati i processi di gestione centralizzati delle credenziali e dei profili abilitativi*; la consolle di amministrazione, utilizzata anche per il censimento delle utenze, è accessibile esclusivamente tramite un'utenza generica (<i>icmadmin</i>) condivisa tra più risorse afferenti a strutture consortili diverse; l'applicazione web per l'accesso diretto ai contenuti del CM è acceduta da risorse della Banca e del Consorzio utilizzando le utenze applicative. <p>c) Gli strumenti a supporto del CM non sono auditabili non essendo disponibili né log degli accessi né delle operazioni effettuate. Non è pertanto possibile ricostruire a posteriori l'operatività degli utenti.</p> <p>(*) D 02026 «Regole in materia di Gestione e Controllo Accessi: Accesso ad Applicazioni e Sistemi ICT» D 00150 «Processo Gestione Accessi Logici» del Consorzio</p> <p>(**) <i>IBM System Administration Client</i>, consolle di amministrazione del CM <i>IBM Content Navigator</i>, applicazione web per l'accesso diretto ai contenuti del CM</p>	<p>Ricondurre la gestione del CM alle Policy di sicurezza logica</p> <p>a) Ricondurre la gestione delle utenze applicative e dei relativi profili abilitativi nell'ambito delle policy aziendali in materia. Eseguito un assessment sulle utenze applicative attualmente censite finalizzato a ricondurre ciascuna utenza al proprio asset di riferimento, affinché sia sempre chiaramente identificabile la Struttura responsabile del loro corretto utilizzo.</p> <p>b) Implementare i corretti presidi di sicurezza per l'accesso agli strumenti a supporto del CM:</p> <ul style="list-style-type: none"> valutare l'opportunità di integrare gli strumenti a supporto del CM nell'ambito del sistema di autenticazione SSO. Da subito, ricondurre le richieste di accesso logico nell'ambito del processo di Gruppo; creare le necessarie utenze nominative di tipo gestionale da assegnare agli utenti della consolle di amministrazione del CM, disattivando contestualmente l'utenza generica; inibire l'utilizzo interattivo delle utenze applicative tramite Content Navigator. Implementare inoltre le necessarie modifiche affinché la parte segreta delle credenziali (password) sia gestita in modo sicuro. <p>c) Implementare per gli strumenti a supporto del CM un sistema di tracciatura degli accessi e dell'operatività svolta in modo da garantirne la verificabilità.</p>	60%	28/02/19	-	-	COG	<p>DONE</p> <p>Riconduzione utenza Amministrativa a LDAP: <i>completato, controllato via CyberArk, applicazione standard COG.</i></p> <p>Bloccato l'accesso diretto ai contenuti via applicazione web.</p> <p>Attivazione della tracciatura degli accessi e delle attività di amministrazione mediante CyberArk.</p> <p>TO DO</p> <p>Riconduzione utenze tecniche a LDAP.</p> <p>Riconduzione utenze applicative a LDAP e modifica relative applicazioni per utilizzo nuove utenze secondo le policy di utilizzo standard.</p>



Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») – Macchina operativa 6/7

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig.	# Rip.	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
17	85/2018 del 12/12/2018	<p><u>IA_2018_00129</u></p> <p>Dematerializzazione disposizioni operative e firma <u>grafometrica</u></p> <p>Accesso diretto ai dati eludendo i presidi di controllo definiti</p> <p>Nel corso delle verifiche è stato accertato l'utilizzo, diffuso e trasversale nell'ambito del Consorzio, dell'applicativo "Gestione Tabellare" per condurre attività di accesso diretto in modifica ai dati operativi, eludendo tutti i presidi di controllo ad oggi implementati per garantire il rispetto delle policy di sicurezza logica di Gruppo.</p> <p>Tale situazione espone a elevati rischi, non presidiati, d'integrità, riservatezza e disponibilità dei dati aziendali.</p> <p>Si osserva infine che tutte le modifiche condotte direttamente sui dati tramite Gestione Tabellare non sono state, fino ad oggi, oggetto di monitoraggio e rilevazione. Questo pertanto può aver indotto anche a valutazioni non corrette del rischio informatico sottostante le singole applicazioni interessate.</p>	<p>Ricondurre l'accesso diretto ai dati nell'ambito delle Policy di Gruppo</p> <p>Circoscrivere l'utilizzo dell'applicativo alle sole tabelle di dominio, escludendo pertanto tutte le tabelle operative contenenti dati di business e/o informazioni riconducibili ai clienti.</p> <p>Ricondurre la gestione dei profili abilitativi e della tracciatura delle operazioni svolte a quanto previsto dalle policy aziendali (panieri abilitativi/Log Unico).</p> <p>Nelle more, adottare i necessari presidi a mitigazione dei rischi individuati.</p>	100%	31/12/18	-	-	COG	<div>  Chiuso in data 21.12.2018 </div>

Focus GAP attivi in monitoraggio al 11.01.2019 (rilevanza «Alta») - Macchina operativa 7/7

Nr	Rapporto	Nome Intervento Descrizione del GAP	Soluzione proposta	% SAL	Data Mitig. Orig	# Rip.	Data Ultima Mitig.	FO	Aggiornamento SAL 11.01.2019
18	85/2018 del 12/12/2018	<p><u>IA 2018 00136</u></p> <p><u>Dematerializzazione disposizioni operative e firma grafometrica</u></p> <p>Operatività con firma grafometrica a rischio disconoscimento e/o trattamento di dati biometrici non autorizzato</p> <p>Prima dell'accentramento obbligatorio (dicembre 2015) le istruzioni operative prevedevano la conservazione in filiale dell' adesione al servizio di FEA (circa 1,3M di documenti).</p> <p>Questa condizione espone ad una minore certezza di recupero della documentazione e non ne garantisce la correttezza formale (es. presenza delle firma). Quanto detto è stato confermato da una ricognizione compiuta presso un campione di filiali, i cui esiti hanno rilevato un'elevata percentuale (99% in un caso e 65% nell'altro) di documentazione non firmata e/o archiviata in maniera non appropriata.</p> <p>Quanto sopra non tutela efficacemente dal rischio di disconoscimento di operazioni sottoscritte grafometricamente da un cliente senza preventiva adesione al Servizio di FEA, né dal rischio di non conformità per il trattamento non autorizzato di dati biometrici con possibili sanzioni amministrative.</p>	<p>Recupero documentazione presente in filiale.</p> <p>Recuperare tale documentazione riconfigurando un Piano di accentramento sul modello dell'iniziativa 2017 che ha centralizzato solo 12.102 documenti.</p> <p>Per quanto non immediatamente recuperabile, inibire ai clienti l'operatività mediante firma grafometrica.</p>	30%	31/12/19	-	-	<p>Dir Rete</p> <p>con il contributo del</p> <p>Servizio Organization Partner COO e Digital Center e Servizio Controlli, Conformità e Operations</p>	<p>TO DO</p> <p><i>Proseguire nell'azione di recupero dei contratti ante 2016 presenti in filiale</i></p> <p>DONE</p> <p><i>Avviata duplice azione di recupero. In primis è stata coinvolta direttamente la rete per ricercare i contratti di circa 70.000 posizioni considerate maggiormente a rischio. Successivamente è stata creata una task force per recuperare i contratti presenti in un campione di 165 filiali.</i></p>
19	85/2018 del 12/12/2018	<p><u>IA 2018 00137</u></p> <p><u>Dematerializzazione disposizioni operative e firma grafometrica</u></p> <p>Ritardato o mancato invio del documento di adesione al servizio FEA al Centro Documentale</p> <p>Gli accertamenti hanno riguardato quei clienti per i quali le Filiali/Centri Specialistici non hanno trasmesso al Centro Documentale il documento di adesione al Servizio di FEA tramite procedura PARDO:</p> <ul style="list-style-type: none"> documenti "sospesi" (n. 9.671 al 30/04/18, su un totale di 1.360.697 prodotti). L'analisi sui suddetti documenti ha rilevato sospesi datati (il 60% originato ante 2018) e giustificativi per la sospensione in gran parte vaghi, assenti o che confermano la mancata firma del cliente; documenti "annullati" (n. 16.839 al 30/04/18). Per questi è stato verificato su un campione di 30 unità che fosse stata inibita l'operatività con firma grafometrica o in caso contrario non vi fossero altri documenti Pardo collegati. Il test è fallito per tutti i casi analizzati. <p>Sospendere o annullare la pratica PARDO non esclude l'operatività con firma grafometrica del cliente e, al contempo, non consente l'effettuazione dei controlli da parte del Centro Documentale (presenza firma e completezza della documentazione di adesione). Come rappresentato nel gap precedente anche questa condizione espone al rischio di disconoscimento di operazioni sottoscritte grafometricamente da un cliente e al rischio di non conformità per il trattamento non autorizzato di dati biometrici.</p>	<p>Limitare l'incidenza di documentazione sospesa/annullata in PARDO</p> <p>Al fine di limitare i rischi indotti da «documentazione sospesa/annullata», prevedere una serie di misure di controllo per limitarne la proliferazione, richiamando la Rete alla sistemazione di quanto non regolarizzato.</p>	30%	30/06/19	-	-	<p>Servizio Organization Partner COO e Digital Center</p> <p>con il contributo del</p> <p>Servizio Controlli, Conformità e Operations</p>	<p>TO DO</p> <p><i>Rilasciare il BR volto a rafforzare i controlli sul processo di adesione alla FEA prevedendo una nuova funzionalità di annullamento che esegua in automatico i controlli di operatività e di pardo non accentrato.</i></p> <p><i>Rafforzare inoltre le misure di monitoraggio sui sospesi.</i></p> <p>DONE</p> <p><i>Implementata soluzione tattica che consente l'annullamento del documento Pardo solo al titolare. Pubblicato aggiornamento normativo.</i></p> <p><i>Attivato BR per soluzione target.</i></p>

