BANCA D'ITALIA
EUROSISTEMA

INDAGINE SU RISK DATA AGGREGATION E RISK REPORTING

Dicembre 2024

BANCA D'ITALIA
EUROSISTEMA

INDAGINE SU RISK DATA AGGREGATION E RISK REPORTING

Dicembre 2024

Questo fascicolo presenta i principali risultati dell'indagine sull'aderenza ai principi BCBS239 in tema di aggregazione dei dati di rischio e di reporting da parte delle banche italiane svolta dalla Banca d'Italia nel 2023.

Il testo è stato curato da Francesco Sciamanna con il contributo di Alessandro Scognamiglio, Mirco Agalbato, Massimo Esposito, Giovanni Rumolo e Salvatore Vitiello.

Indirizzo
Via Nazionale 91
00184 Roma - Italia

Sito internet
http://www.bancaditalia.it

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia

INDICE

ELENCO DEGLI ACRONIMI IMPIEGATI

1LoD: First Line of Defense
2LoD: Second Line of Defense
BCBS: Basel Committee on Banking Supervision
DQ: Data Quality
EUC: End-user computing
IT: Information Technology
LSI: Less Significant Institution
RDARR: Risk Data Aggregation and Risk Reporting
SI: Significant Institution
SSM: Single Supervisory Mechanism

1. INTRODUZIONE

Carenze nella capacità di gestire ed aggregare efficacemente i dati sul rischio degli intermediari, sistemi ICT poco adeguati a supportare i processi decisionali e le attività di *risk management* possono compromettere la solidità del processo decisionale e l'efficacia del governo dei rischi degli intermediari.

Riconoscendo tale problematica, emersa anche in occasione della crisi finanziaria del 2008, il Comitato di Basilea per la Vigilanza Bancaria aveva pubblicato già nel 2013 i principi BCBS239, che descrivono le pratiche che le banche dovrebbero adottare per sviluppare solide ed efficaci capacità di gestione ed aggregazione dei dati di rischio[1].

Anche la vigilanza bancaria della BCE (*Single Supervisory Mechanism* – SSM) sta seguendo questo tema da tempo. Nel 2016 è stata condotta una *thematic review*[2] sull'argomento, nella quale sono state valutate la *governance*, le capacità di aggregazione e di segnalazione dei dati di rischio presso un campione di 25 banche significative europee. I risultati di questa *thematic review* avevano evidenziato carenze diffuse: nessuna delle banche del campione, infatti, aderiva pienamente ai principi del BCBS239. L'SSM ha poi identificato proprio nelle carenze nei processi di *risk data aggregation e risk reporting* (RDARR) una delle vulnerabilità da includere nelle priorità di vigilanza[3].

In tale contesto, nell'ambito delle iniziative individuate per dare attuazione alla priorità strategica di Vigilanza dedicata all'analisi dei rischi IT/Fintech nel sistema bancario e finanziario, il Dipartimento Vigilanza ha condotto nel corso del 2023 un'indagine per migliorare la conoscenza dei processi e delle prassi di aggregazione e reportistica dei dati di rischio adottati dalle banche italiane[4] a partire dai principi BCBS239 e in continuità con le principali evidenze emerse in ambito SSM. L'indagine fornisce, inoltre, un quadro di sintesi delle iniziative di miglioramento in essere presso le banche del campione.

---

1 I principi BCBS239 sono raggruppati in tre aree, riferite rispettivamente a (i) *governance* e infrastruttura IT, (ii) aggregazione dei dati di rischio, e (iii) reporting. (v. Principles for effective risk data aggregation and risk reporting).

2 Report on the Thematic Review on effective risk data aggregation and risk reporting.

3 Cfr. SSM supervisory priorities 2024-2026.

4 L'indagine, costituita da un esercizio di autovalutazione nel quale le banche sono chiamate a formulare un giudizio di aderenza dei processi e delle prassi di aggregazione e reportistica dei dati di rischio ai principi BCBS239, ha incluso tutte le banche significative (*significant institution* – SI) e un campione di banche meno significative (*less significant institution* – LSI).

2. SINTESI DEI RISULTATI

Le aree che evidenziano una minore aderenza ai principi BCBS239 sono la *governance* (Principio 1), l'architettura dei dati e l'infrastruttura IT (Principio 2) (Figura 1, pannello di sinistra).

Figura 1

Aderenza ai principi BCBS239 e stato delle iniziative (a)

RDARR - Aderenza complessiva ai principi BCBS239

Tag	Principio	SI	LSI	Tutti
Tag 1 - Governance & IT	1 - Governance	2.42	2.80	2.59
	2 - Architettura dei dati e infrastruttura IT	2.67	2.60	2.64
Tag 2 - Capacità di aggregazione dei dati di rischio	3 - Accuratezza e integrità	2.67	2.30	2.50
	4 - Completezza	2.25	2.10	2.18
	5 - Tempestività	2.17	2.10	2.14
	6 - Adattabilità	2.42	2.00	2.23
	7 - Accuratezza	2.67	2.70	2.68
Tag 3 - Reporting	8 - Esaustività	1.83	1.60	1.73
	9 - Chiarezza e utilità	2.25	1.80	2.05
	10 - Periodicità	2.17	1.70	1.95
	11 - Diffusione	1.92	1.60	1.77

Stato delle attività per livello di aderenza - Tutti i principi RDARR

Maturità delle iniziative / Livello di aderenza	Iniziative in corso	Consapevole, ma nessuna iniziativa identificata	Nessuna iniziativa riportata
1 - Pienamente	0.0%	0.8%	13.6%
2 - Largamente	9.9%	6.6%	32.6%
3 - Parzialmente	16.5%	13.6%	5.8%
4 - Non raggiunto	0.0%	0.0%	0.4%

(a) Per il livello di aderenza (pannello di sinistra), il campo di variazione numerico è compreso tra 1 (massima aderenza) e 4 (minima aderenza); il colore verde indice il massimo livello di aderenza, il colore giallo un livello intermedio e il colore arancio il livello minimo di aderenza. Per lo stato delle iniziative (pannello di destra), il campo di variazione numerico è compreso tra 0% e 100%; l'intensità del colore indica una percentuale maggiore.

- Le debolezze della *governance* sono in parte più accentuate nelle LSI e riguardano prevalentemente l'assenza di adeguati requisiti di *data quality* in occasione di eventi aziendali e la mancanza di processi di validazione indipendente sulle capacità di aggregazione e reporting dei dati di rischio. Insufficienze infrastrutturali e nel disegno dell'architettura IT interessano le banche SI con frequenza maggiore rispetto alle LSI; viceversa, per le LSI le carenze si concentrano nel governo dei processi di data aggregation e reporting laddove supportati da strumenti di *end-user computing* (EUC).
- Con riferimento alle capacità di generare e aggregare dati di rischio in modo preciso, accurato e affidabile anche in caso di tensioni o crisi (Principio 3), emergono risultati sostanzialmente allineati alle aspettative. Si segnalano, tuttavia, esigenze di maggiore automazione nell'attività di riconciliazione tra dati gestionali, contabili e regolamentari, e nell'assicurare maggiore presidio del *data lineage* (presidio del dato dall'origine al punto di utilizzo).
- La reportistica costituisce il profilo di maggiore aderenza ai principi BCBS239, con alcune debolezze che emergono nell'attività di controllo dei report (Principio 7).

- In generale, al netto delle differenze sopra menzionate, il livello di aderenza ai principi BCBS239 non mostra differenze particolarmente rilevanti né rispetto alla tipologia di banca (SI o LSI) né rispetto al tipo di rischio rappresentato (di credito, di mercato, di tasso d'interesse, di liquidità e rischio operativo).
- Il grado di aderenza ai principi BCBS239 appare per le LSI inferiore a quello delle SI soltanto per la *governance*. Tale evidenza può essere giustificata in termini di proporzionalità, considerando che a dimensioni inferiori corrispondono assetti operativi, organizzativi e di controllo più snelli. Peraltro, le procedure dei fornitori di servizi di *core banking*, ai quali le LSI ricorrono frequentemente, contribuiscono a presidiare la robustezza e la qualità dei dati.
- Inoltre, laddove le banche hanno segnalato di avere intrapreso iniziative per aumentare il livello di conformità ai principi BCBS239, si evidenzia che il livello di maturità delle iniziative tende a essere proporzionale rispetto al grado di non conformità dichiarato (Figura 1, pannello di destra).

3. L'ADERENZA AI PRINCIPI BCBS239

Aspetti di *governance*

I principi BCBS239 individuano nella *governance* complessiva un fattore chiave e una precondizione per costituire processi efficaci di aggregazione e reporting dei dati di rischio. L'indagine, pertanto, inquadra la *governance* sotto molteplici aspetti: la struttura dei processi, le principali pratiche adottate e altri aspetti rilevanti.

Struttura dei processi

Le responsabilità per le attività di regolamentazione interna, per la supervisione dell'implementazione delle policy e linee guida interne e per la valutazione e il monitoraggio della *data quality* (DQ), sono formalmente assegnate nella maggioranza di casi (Figura 2). Tali attività risultano assegnate ad un'unità organizzativa dedicata per tutte le SI (nel 50 per cento dei casi la responsabilità ricade esclusivamente sulla 1LoD[5], nel restante 50 per cento si osserva il coinvolgimento di funzioni di 2LoD) e in poco meno di un terzo delle LSI (unicamente nel 1LoD).

Figura 2

Attribuzione formale delle attività

RDARR - Principio 1 - Governance - Attribuzione formale delle attività

	SI		LSI	
	Sì	No	Sì	No
Attività				
Emanazione di policy e linee guida	11	1	8	2
Supervisionare l'implementazione	12	0	6	4
Valutare e monitorare la qualità dei dati	11	1	7	3
Totale	34	2	21	9

Principali pratiche di *governance* e altri aspetti rilevanti

La definizione di network di *data owners*[6], la formalizzazione e la ripartizioni dei ruoli e delle responsabilità tra IT e business, il monitoraggio sulla qualità dei dati e la revisione periodica degli standard di *data quality* rappresentano tutte esempi di prassi di *governance* ampiamente adottate (Figura 3). Risulta mediamente meno diffusa la valutazione delle implicazioni su RDARR di eventi aziendali quali ad esempio le fusioni, le acquisizioni e le dismissioni, il lancio di nuovi prodotti, le innovazioni di processo o dei sistemi IT.

---

5 I sistemi di controllo interno delle banche includono tre tipologie di controlli, tra loro complementari e indipendenti: (i) controlli di linea (c.d. "controlli di primo livello", "*first line of defense*" o 1LoD) che vengono effettuati dalle stesse strutture operative e sono diretti ad assicurare il corretto svolgimento delle operazioni; (ii) controlli sui rischi e sulla conformità (c.d. "controlli di secondo livello", "*second line of defense*" o 2LoD), a cui sono preposte funzioni distinte da quelle produttive, che hanno l'obiettivo di assicurare, tra l'altro, la corretta attuazione del processo di gestione dei rischi e la conformità dell'operatività aziendale alle norme, e (iii) revisione interna (c.d. "controlli di terzo livello", "*third line of defense*" o 3LoD), volta a individuare violazioni delle procedure e della regolamentazione nonché a valutare periodicamente la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema dei controlli interni e del sistema informativo.

6 Il *data owner* rappresenta un'importante funzione nella *governance* dei dati aziendali. Tale funzione, tra l'altro, (i) sovrintende all'intero ciclo di vita dei dati di competenza, assicurandone l'accuratezza, l'integrità, la completezza e la tempestività, (ii) monitora la qualità dei dati attraverso processi codificati, (iii) assicura efficaci azioni di rimedio. (v. Guide on effective risk data aggregation and risk reporting).

I principi BCBS239 mettono in rilievo l'importanza di considerare il tema RDARR nella strategia ICT delle banche, ponendo attenzione sia agli aspetti di miglioramento connessi ad eventuali carenze, sia alla necessità di attuare le iniziative assicurando l'allocazione di risorse umane e finanziarie adeguate. L'indagine evidenzia che il tema RDARR è incluso nella *IT strategy* delle banche, sebbene in misura maggiore per le SI rispetto alle LSI.

L'indagine evidenzia, inoltre, la consapevolezza dei Board of Directors e del Senior Management delle limitazioni della reportistica interna in termini di carenze tecniche e copertura del perimetro. Per quanto attiene alla misurazione della qualità dei dati, i report sono sottoposti al Board of Directors nel 42,9 per cento dei casi (63,6 per cento delle SI, 20 per cento delle LSI) e al Senior Management nel 15,2 per cento dei casi (23,6 per cento delle SI, 6 per cento delle LSI)[7].

In sintesi, le prassi di *governance* delle SI risultano per lo più aderenti ai principi BCBS239. Per le LSI emergono, invece, maggiori carenze: l'80 per cento del campione di LSI non ha formalizzato ruoli e distinto responsabilità tra IT e business nel contesto dei processi di RDARR né ha previsto di sottoporre le proprie capacità RDARR a validazione indipendente.

Figura 3

Pratiche di *governance* e altri aspetti

RDARR - Principio 1 - Governance - Principali pratiche di governance

	SI		LSI	
	Sì	No	Sì	No
Pratica				
Un network di data owners è definito in 1LoD ed è responsabile delle procedure di controllo dei dati	12	0	5	5
I ruoli e le responsabilità tra business e IT sono definiti e formalizzati per i processi RDARR	12	0	2	8
I processi di reporting della qualità dei dati sono implementati e monitorati	11	1	6	4
Gli standard di qualità dei dati sono regolarmente rivisti	9	3	4	6
I processi di gestione del cambiamento garantiscono i requisiti di qualità dei dati	6	6	6	4
Totale	50	10	23	27

RDARR - Principio 1 - Governance - Altri aspetti di governance

	SI		LSI	
	Sì	No	Sì	No
Aspetto				
RDARR è incluso nella strategia IT comprendendo i requisiti di budget	11	1	4	6
Il consiglio di amministrazione e l'alta direzione sono consapevoli delle limitazioni della reportistica	10	2	6	4
Le capacità RDARR sono assoggettate a validazione indipendente	7	5	2	8
Totale	28	8	12	18

Architettura dei dati e infrastruttura IT

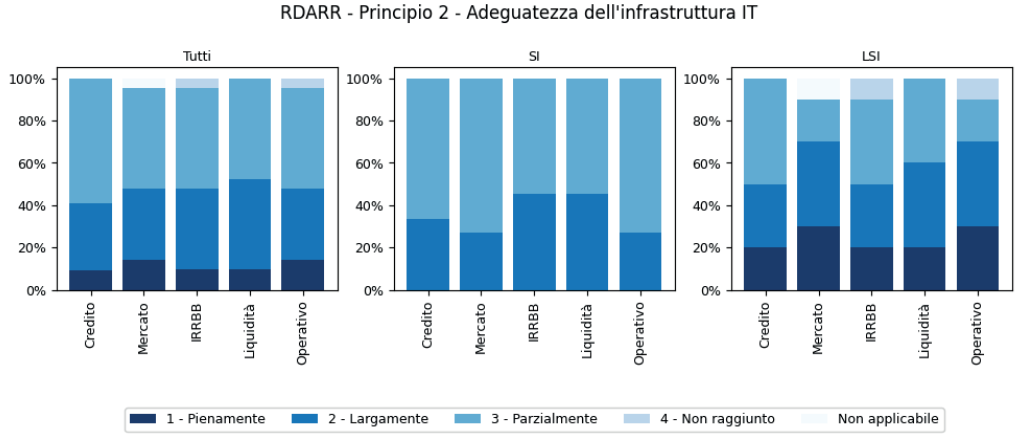
La robustezza dell'architettura dei dati di rischio e l'affidabilità dell'infrastruttura tecnologica rappresentano imprescindibili requisiti di un'efficace funzione di aggregazione e reportistica delle informazioni di rischio. I principi BCBS239 sottolineano il ruolo che l'automazione riveste nell'assicurare i necessari controlli sulla qualità dei dati e sulle elaborazioni per la reportistica.

7 Per le LSI, in particolare, non esistono linee di riporto sui report della qualità dei dati nel 42 per cento dei casi.

Sotto questo profilo, le banche valutano la propria architettura dei dati e infrastruttura IT parzialmente aderenti ai principi BCBS239. In particolare, per le SI emergono maggiormente insufficienze infrastrutturali e di disegno dell'architettura IT, mentre per le LSI si evidenziano debolezze nei processi di data aggregation e reporting supportati da strumenti di *end-user computing* (EUC).

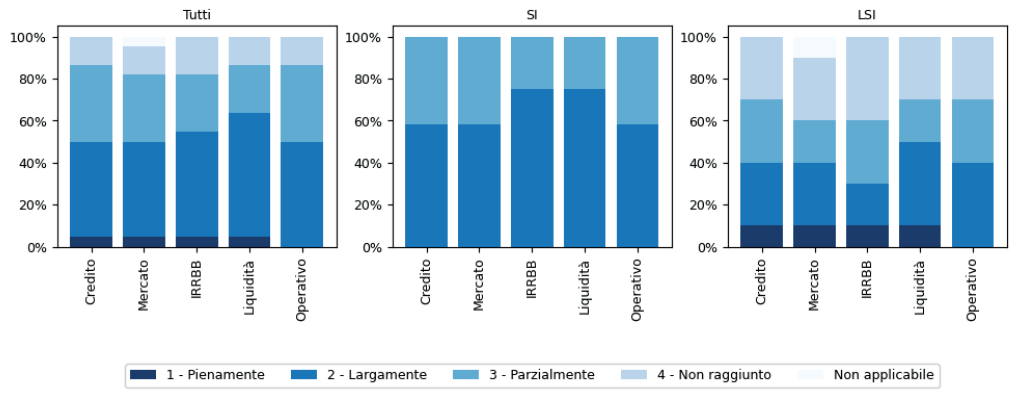
Nel 47,2 per cento dei casi l'infrastruttura IT è ritenuta completamente o largamente adeguata nel supportare un'efficace aggregazione dei dati di rischio (35,8 per cento SI, 60 per cento LSI); tale capacità è solo parziale nel 49,9 per cento dei casi (Figura 4).

Figura 4



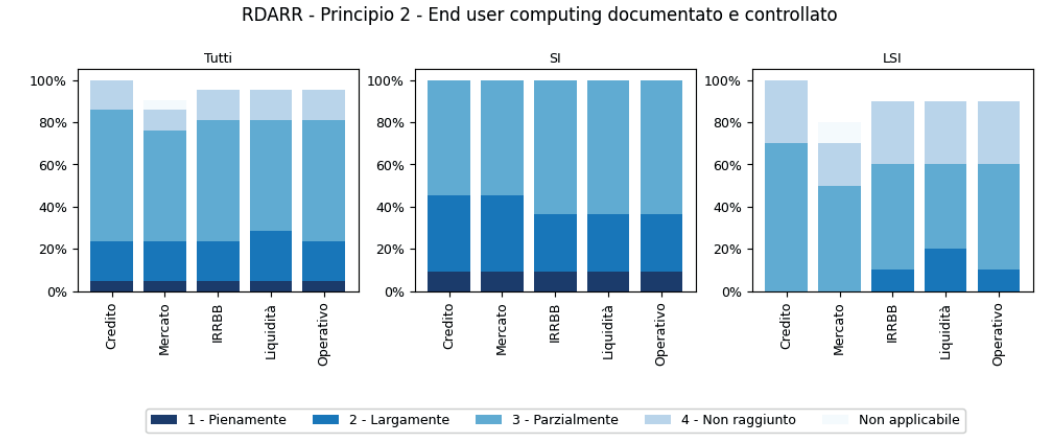
La qualità dei dati di rischio è sottoposta a procedure di controllo strutturate, comprensive di processi di *escalation* per le rettifiche, completamente o largamente soddisfacenti per il 53,6 per cento del campione (65 per cento SI, 40 per cento LSI) (Figura 5).

Figura 5



D'altra parte, tra le procedure informatiche in uso presso le banche per finalità di reportistica, quelle realizzate autonomamente dalle funzioni di business (c.d. *end-user computing* – EUC) possono presentare criticità qualora sprovviste di adeguati presidi strutturati di controllo. L'indagine evidenzia una carenza nella gestione dei processi supportati da strumenti di *end user computing* (EUC), più accentuata nel sottocampione LSI, in termini di classificazione per complessità e rilevanza delle procedure EUC in essere e gestione delle modifiche manuali dei dati (Figura 6).

Figura 6



I sistemi IT e i processi di business a supporto delle attività di aggregazione dei dati di rischio e di reporting sono completamente o largamente inclusi nei piani di *business continuity* nella maggioranza dei casi (75,3 per cento del campione).

Infine, in tema di *data architecture*, nell'81,9 per cento del campione le procedure informatiche sono ritenute completamente o largamente idonee a garantire la massima granularità dei dati, mentre la definizione di una tassonomia dei dati omogenea e integrata è maggiormente presente nelle SI (66 per cento) rispetto alle LSI (20 per cento).

Capacità di aggregazione dei dati di rischio

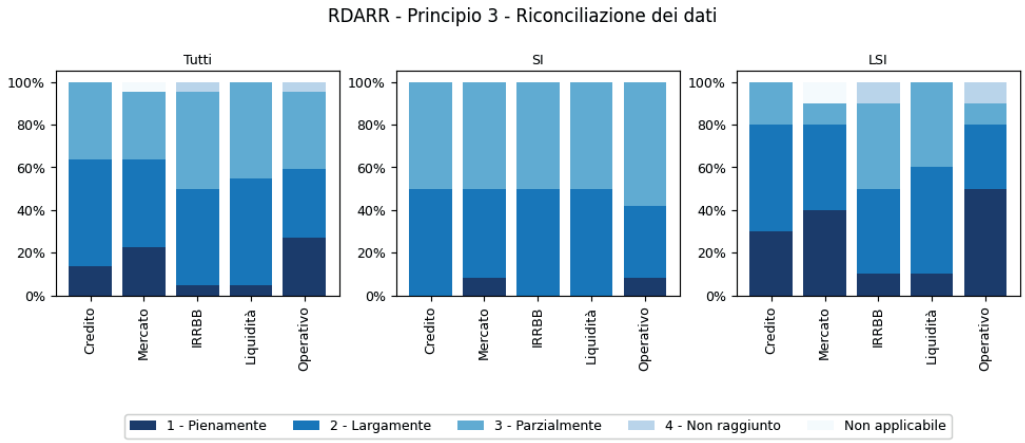
Una solida capacità di aggregazione dei dati di rischio a partire dai dati elementari costituisce una condizione necessaria affinché i report possano fornire una rappresentazione affidabile e tempestiva dei rischi. I principi BCBS239 qualificano questo aspetto in termini di accuratezza e integrità delle elaborazioni dei dati elementari, completezza delle fonti informative, tempestività rispetto ai requisiti di reporting, e adattabilità al cambiamento dei fabbisogni informativi degli stakeholder rilevanti.

Nel complesso, risultano completamente o largamente adeguate le procedure di riconciliazione dei dati[8] nel 58,1 per cento del campione (48,3 per cento SI, 50

8 Si tratta della riconciliazione dei dati contabili con quelli prudenziali e di rischio.

per cento LSI). Inoltre, il 49 per cento del campione (42,7 per cento SI, 56 per cento LSI) possiede strumenti per tracciare l'intero ciclo di vita dei dati di rischio (c.d. *data lineage*) dalle fonti dei dati elementari fino alla predisposizione dei report (Figura 7).

Figura 7



In termini di completezza del perimetro dei dati, nell'82,7 per cento del campione la capacità nell'aggregare tutti i dati di rischio rilevanti è ritenuta completamente o largamente soddisfacente, includendo voci fuori bilancio, dati relativi alle componenti del gruppo e alle linee di business.

In risposta ad esigenze di efficienza ed economicità dei processi di reporting interni, le banche possono applicare soglie di materialità (*materiality thresholds*) nella elaborazione dei dati di rischio, in modo da trascurare porzioni di dati che non porterebbero informazione rilevante. Affinché questa modalità di aggregazione dei dati non introduca distorsioni informative, è necessario che le soglie di materialità siano presidiate e periodicamente riviste. Nel complesso, il 90,5 per cento del campione evidenzia comportamenti coerenti con i principi BCBS239: nel 61,9 per cento dei casi non vengono applicate soglie di materialità per selezionare i dati di rischio rilevanti, e nel 28,6 per cento dei casi le soglie di materialità sono soggette a revisione; pertanto soltanto in una quota minoritaria di casi, le soglie di materialità una volta introdotte non vengono periodicamente riviste.

La tempestività nell'aggregare i dati di rischio può incidere sulla rapidità e sull'efficacia con cui vengono prese le decisioni. Nel complesso, non si evidenziano specifiche criticità in questa capacità. Le banche risultano nel complesso capaci di assicurare dati tempestivi e corretti anche in occasione di eventi di crisi.

Infine, per il 67,2 per cento del campione risultano completamente o largamente soddisfacenti le capacità di adattare i processi di aggregazione dei dati di rischio nel corrispondere ad esigenze informative estemporanee.

Reporting

La reportistica delle informazioni sui rischi rappresenta il necessario compimento della capacità di aggregazione dei dati di rischio. I principi BCBS239 qualificano questo profilo sia dal punto di vista del merito, in termini di accuratezza, esaustività e chiarezza dei report, sia di processo, in termini di frequenza e modalità di distribuzione della reportistica. I principi legati alle prassi di reportistica presentano elementi strutturali di relativa minore complessità, che rendono la loro attuazione da parte delle banche meno dispendiosa.

Nel complesso, le prassi di reportistica risultano essere quelle maggiormente aderenti ai principi BCBS239; tuttavia, non mancano alcune diffuse difficoltà nella capacità di assicurare l'accuratezza dei report. In particolare:

- nel 99,1 per cento dei casi il report è sottoposto a controlli prima della sua distribuzione, che includono, sempre dei passaggi manuali; nel 18,2 per cento del campione i controlli sono interamente manuali (6,7 per cento delle SI, 32 per cento delle LSI);
- nel 77 per cento dei casi non sono definiti in modo formale requisiti di accuratezza dei dati inclusi nei report.

I restanti aspetti legati alle prassi di reportistica sui dati di rischio non evidenziano, nel complesso, specifici elementi di criticità. In particolare:

- Esaustività:
  - i report includono informazioni sull'esposizione e le posizioni per tutti i dati di rischio e tutti gli elementi rilevanti (es. paese, settore industriale, ecc.) nel 95,5 per cento dei casi;
  - i report consentono l'individuazione delle concentrazioni di rischi emergenti nel 89,5 per cento dei casi;
  - l'informazione contenuta nei report tiene conto della propensione al rischio e fornisce indicazioni sull'evoluzione più probabile dei fenomeni e sulle conseguenze sul profilo di rischio interessato nel 100 per cento dei casi.
- Chiarezza:
  - esistono processi di feedback dai destinatari della reportistica nel 92,7 per cento dei casi;
  - i concetti rappresentati nei report di rischio sono formalmente definiti all'interno di un repertorio aziendale nel 73,6 per cento dei casi.
- Frequenza:
  - durante periodi di stress o crisi i report rilevanti sono disponibili con maggiore frequenza nell'87,6 per cento dei casi.
- Distribuzione:
  - vengono adottate procedure per la distribuzione tempestiva e sicura dei report ai destinatari rilevanti nel 94,5 per cento dei casi.

4. ATTIVITÀ DELLE BANCHE IN RELAZIONE ALL'ADERENZA AI PRINCIPI BCBS239

L'indagine evidenzia da un lato un articolato insieme di iniziative poste in essere dalle banche del campione per colmare le proprie carenze e dall'altro un diffuso grado di consapevolezza anche laddove iniziative concrete non siano state poste in essere. Inoltre, sono presenti iniziative di miglioramento anche in casi di non conformità lieve, volte principalmente al consolidamento di soluzioni o sistemi già esistenti.

Nel complesso, il grado di attenzione e l'intensità delle iniziative sono correlati al livello di non aderenza ai principi. Permangono, d'altra parte, alcuni casi in cui, a fronte di significativi discostamenti, non risultano iniziative in essere. Le tavole sottostanti mostrano le distribuzioni di intensità della risposta delle banche incluse nel campione congiuntamente al livello di aderenza con i principi, raggruppate per le tre macro-aree dei principi BCBS239 (Figura 8).

Figura 8

Stato delle attività per livello di aderenza - Tag 1 - Governance e infrastruttura IT

Maturità delle iniziative / Livello di aderenza	Iniziative in corso	Consapevole, ma nessuna iniziativa identificata	Nessuna iniziativa riportata
1 - Pienamente	0.0%	0.0%	0.0%
2 - Largamente	15.9%	9.1%	15.9%
3 - Parzialmente	34.1%	15.9%	6.8%
4 - Non raggiunto	0.0%	0.0%	2.3%

Stato delle attività per livello di aderenza - Tag 2 - Capacità di aggregazione dei dati di rischio

Maturità delle iniziative / Livello di aderenza	Iniziative in corso	Consapevole, ma nessuna iniziativa identificata	Nessuna iniziativa riportata
1 - Pienamente	0.0%	2.3%	9.1%
2 - Largamente	8.0%	6.8%	36.4%
3 - Parzialmente	17.0%	17.0%	3.4%
4 - Non raggiunto	0.0%	0.0%	0.0%

Stato delle attività per livello di aderenza - Tag 3 - Reporting

Maturità delle iniziative / Livello di aderenza	Iniziative in corso	Consapevole, ma nessuna iniziativa identificata	Nessuna iniziativa riportata
1 - Pienamente	0.0%	0.0%	22.7%
2 - Largamente	9.1%	5.5%	36.4%
3 - Parzialmente	9.1%	10.0%	7.3%
4 - Non raggiunto	0.0%	0.0%	0.0%

In particolare, si evidenzia che per gli aspetti di *governance* e infrastruttura IT (Tag 1 – Principi 1 e 2) il 34,1 per cento delle risposte evidenzia l'esistenza di

iniziative in corso a fronte di processi o strumenti parzialmente aderenti ai principi BCBS239, mentre il 15,9 per cento, pur manifestando consapevolezza delle proprie carenze, non ha riportato l'esistenza di iniziative concrete. Inoltre, con riferimento alle capacità di aggregazione dei dati rischio (Tag 2 – Principi 3, 4, 5 e 6), il 17 per cento delle risposte presenta iniziative in corso a fronte di un livello di aderenza parziale, mentre per un ulteriore 17 per cento la banca è a conoscenza delle proprie carenze ma non ha indicato iniziative concrete di miglioramento.

NOTA METODOLOGICA

L'indagine è stata svolta a partire da questionari individuali di autovalutazione riferiti ad un campione di banche italiane, costituito dalle *Significant Institution* con sede della capogruppo in Italia e da dieci *Less Significant Institution*. Il contenuto del questionario è stato disegnato a partire dagli strumenti in uso presso l'SSM e tenendo conto dell'evoluzione delle attività SSM sul tema RDARR.

Al fine di poter fornire una visione orizzontale, sintetica e quanto più possibile quantitativa e granulare del livello di aderenza delle banche ai principi BCBS239, sono stati definiti dei punteggi per graduare le risposte. La scelta è ricaduta sull'adozione di criteri di *scoring* analoghi a quelli già in uso presso il Comitato di Basilea per la Vigilanza Bancaria nell'ambito della propria attività istituzionale sul *risk data aggregation and risk reporting*. In particolare, tale metrica, riportata nella tabella sottostante, quantifica il livello di aderenza in ragione dell'entità dei cambiamenti necessari rispetto ai processi e agli strumenti in essere.

Criteri di punteggio	
Punteggio	Definizione
1 – Pienamente	I criteri di valutazione sono pienamente raggiunti nell'ambito dell'architettura e dei processi esistenti
2 – Largamente	I criteri di valutazione sono ampiamente raggiunti: sono necessari solo interventi minori
3 – Parzialmente	I criteri di valutazione sono parzialmente raggiunti: sono necessarie azioni significative
4 – Non raggiunto	I criteri di valutazione non sono raggiunti