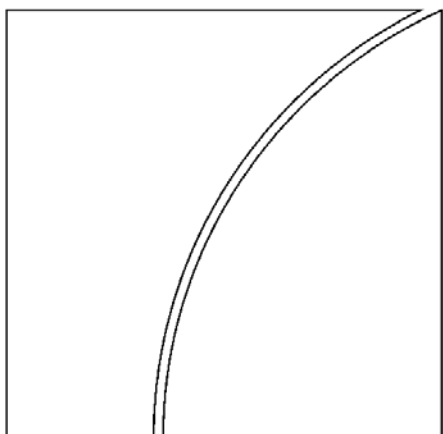


Comitato di Basilea per la vigilanza bancaria



Principi per un'efficace aggregazione e reportistica dei dati di rischio

Gennaio 2013



BANCA DEI REGOLAMENTI INTERNAZIONALI

Il presente documento è stato redatto in lingua inglese. In caso di dubbio, si rimanda alla versione originale.

La presente pubblicazione è consultabile sul sito internet della BRI (www.bis.org).

© *Banca dei Regolamenti Internazionali 2013. Tutti i diritti riservati. Sono consentite la riproduzione e la traduzione di brevi parti del testo purché sia citata la fonte.*

ISBN 92-9131-913-9 (stampa)
ISBN 92-9197-913-9 (web)

Indice

Principi per un'efficace aggregazione e reportistica dei dati di rischio	1
Introduzione	1
Definizione	3
Obiettivi.....	3
Ambito di applicazione e considerazioni preliminari	4
I. Infrastruttura e governo societario complessivi	6
II. Capacità di aggregazione dei dati di rischio	8
III. Prassi di reportistica in materia di rischio	12
IV. Verifica, strumenti e cooperazione delle autorità di vigilanza	15
V. Calendario di attuazione e disposizioni transitorie.....	17
Allegato 1 – Terminologia utilizzata nel documento	19
Allegato 2 – Sintesi dei Principi.....	21

Task force per la vigilanza sulle SIB dello Standards Implementation Group

Presidente:

Fernando Vargas, Banco de España, Madrid

Australia	Heidi Richards (APRA)	
Canada	James Dennison (OSFI)	
Cina	Zhangjun Wu (CBRC)	(da ottobre 2012)
	Xianqiu Zhang (CBRC)	(fino a settembre 2012)
Francia	Hedi Jeddi (ACP)	
Germania	Tobias Volk (Bundesbank)	
	Stefan Iwankowski (BAFIN)	
Hong Kong SAR	Sunny Yung (HKMA)	
Italia	Angelo Carriero (Bdl)	
Giappone	Mitsutoshi Adachi (BoJ)	
	Takao Miyamoto (JFSA)	(fino a giugno 2012)
	Yu Nishioki (JFSA)	(da luglio 2012)
Messico	Efrain Solorio (CNBV)	
Paesi Bassi	Truus Stadt (DNB)	(da ottobre 2012)
	Inge Veldhuis (DNB)	(fino a settembre 2012)
Spagna	Cristina Iglesias-Sarria (BdE)	
	Cecilia Lozano (BdE)	
Regno Unito	Jill Elaine Savager (FSA)	
	Ian Tower (FSA)	
Stati Uniti	Joel Anderson (OCC)	
	Stacy Coleman (FRBNY)	
	Kirk Odegard (FRB)	
Financial Stability Board	Grace Sone	
Istituto per la stabilità finanziaria	Amarendra Mohan	(da aprile 2012)
	Roland Raskopf	(fino a marzo 2012)
Segretariato	Juan Carlos Crisanto	
	Ruth Doubleday	(fino ad agosto 2012)

Principi per un'efficace aggregazione e reportistica dei dati di rischio

*Dov'è la saggezza che abbiamo perduto sapendo?
Dov'è la sapienza che abbiamo perduto nell'informazione?*

T. S. Eliot, La Rocca (1934)

Introduzione

1. Uno degli insegnamenti più significativi della crisi finanziaria globale iniziata nel 2007 è che le tecnologie informatiche e le architetture dei dati aziendali delle banche non erano adeguate a sostenere la gestione complessiva dei rischi finanziari. Molte banche non disponevano della capacità di aggregare le esposizioni al rischio e di individuare le concentrazioni in maniera rapida e accurata a livello di gruppo bancario, per le varie aree operative e fra entità giuridiche diverse. Alcune banche non erano in grado di gestire efficacemente i rischi a causa delle scarse capacità di aggregazione dei dati e di prassi di reportistica inadeguate. Questa situazione ha avuto gravi conseguenze per le banche stesse e per la stabilità del sistema finanziario nel suo complesso.

2. Alla luce di ciò, il Comitato di Basilea ha emanato nell'ambito del secondo pilastro (processo di controllo prudenziale) delle linee guida supplementari¹ volte a migliorare la capacità delle banche di individuare e gestire i rischi a livello di intero istituto. In particolare, il Comitato ha sottolineato che un solido assetto per il controllo dei rischi dovrebbe contemplare adeguati sistemi informativi per la direzione (management information system, MIS)² sia a livello di area operativa, sia a livello complessivo di banca. Inoltre, il Comitato di Basilea ha fatto riferimento all'aggregazione dei dati anche nelle linee guida relative al governo societario³.

3. Il miglioramento della capacità delle banche di aggregare i dati di rischio agevolerà la risoluzione delle crisi bancarie. In particolare, per quanto riguarda le banche di rilevanza sistemica globale (G-SIB), è essenziale che le autorità competenti per la risoluzione delle crisi abbiano accesso a dati di rischio aggregati conformi alle caratteristiche fondamentali definite dal Financial Stability Board (FSB) nel documento *Key Attributes of Effective Resolution Regimes for Financial Institutions*⁴, nonché ai principi esposti di seguito. Nel quadro di un intervento di risanamento, un sistema affidabile di gestione dei dati aiuterà le banche e le autorità di vigilanza ad anticipare i problemi. Esso consentirà inoltre di individuare più facilmente le soluzioni alternative per ripristinare la solidità finanziaria e la sostenibilità delle banche che si trovano in situazione di grave difficoltà, ad esempio migliorando le prospettive di trovare un partner compatibile per una fusione.

¹ Cfr. Comitato di Basilea, *Enhancements to the Basel II framework* (luglio 2009), consultabile all'indirizzo www.bis.org/publ/bcbs158.pdf.

² Ai fini del presente documento, per MIS si intendono i sistemi relativi alle informazioni in materia di *rischio*.

³ Cfr. Comitato di Basilea, *Principles for enhancing corporate governance* (ottobre 2010), consultabile all'indirizzo www.bis.org/publ/bcbs176.pdf.

⁴ Cfr. Financial Stability Board, *Key Attributes of Effective Resolution Regimes for Financial Institutions* (ottobre 2011), consultabile all'indirizzo www.financialstabilityboard.org/publications/r_111104dd.pdf.

4. Numerosi operatori del settore bancario⁵ riconoscono i potenziali benefici di un miglioramento delle capacità di aggregazione dei dati di rischio e stanno lavorando per raggiungere questo obiettivo. Essi ritengono in particolare che verrebbero rafforzati le capacità di giudizio e il ruolo della funzione di controllo dei rischi, con vantaggi in termini di efficienza, minore probabilità di perdite, migliore processo decisionale strategico e, in ultima istanza, maggiore redditività.

5. Le autorità di vigilanza constatano che le banche continuano a incontrare difficoltà nella realizzazione di miglioramenti per quanto riguarda le capacità di aggregazione e i processi di reportistica dei dati di rischio, e auspicano maggiori progressi, in particolare nel caso delle G-SIB. Man mano che ci si allontana dall'esperienza della crisi, inoltre, vi è il pericolo che il potenziamento delle capacità delle banche in questi ambiti non sia considerato prioritario. I sistemi informatici, le basi di dati e i processi di reportistica richiedono infatti notevoli investimenti in termini di risorse umane e finanziarie, con benefici che potrebbero concretizzarsi solo nel lungo periodo.

6. L'FSB ha avviato numerose iniziative a livello internazionale per assicurare che vengano compiuti ulteriori progressi nel rafforzamento delle capacità di aggregazione e delle prassi di segnalazione dei dati di rischio, che sono essenziali per favorire la stabilità finanziaria. Fra queste si segnalano:

- l'elaborazione dei *Principi per un'efficace aggregazione e reportistica dei dati di rischio* definiti nel presente documento. Questa iniziativa trae origine dalla raccomandazione contenuta nel *Progress report on implementing the recommendations on enhanced supervision* dell'FSB, pubblicato il 4 novembre 2011:

“L'FSB, in collaborazione con gli organismi di emanazione degli standard, definirà una serie di aspettative prudenziali al fine di portare le capacità di aggregazione dei dati delle società finanziarie, in particolare delle SIFI, a un livello tale da garantire alle autorità di vigilanza, alle società stesse e ad altri fruitori dei dati (ad esempio le autorità competenti per la risoluzione delle crisi) che i rapporti elaborati dai sistemi MIS forniscano una rappresentazione accurata dei rischi. Dovrebbe essere definita per tutte le SIFI una tabella di marcia per il rispetto delle aspettative prudenziali; al riguardo, il termine ultimo per le G-SIB dovrebbe essere l'inizio del 2016, data in cui comincerà l'applicazione progressiva dei requisiti addizionali di assorbimento delle perdite previsti per queste banche”;

- la definizione di un nuovo modello comune di raccolta dei dati per le istituzioni finanziarie di rilevanza sistemica globale (G-SIFI) al fine di colmare le principali lacune informative individuate nel corso della crisi, come quelle relative alle esposizioni bilaterali e alle esposizioni verso paesi/settori/strumenti. Tale iniziativa dovrebbe mettere a disposizione delle autorità un quadro di riferimento più efficace per la valutazione del rischio sistemico potenziale;
- un'iniziativa congiunta dei settori pubblico e privato per sviluppare un codice identificativo globale (Legal Entity Identifier, LEI). Il sistema LEI permetterà di identificare in maniera univoca nel mondo intero tutti i soggetti giuridici impegnati in una transazione finanziaria e costituirà un tassello fondamentale per migliorare la qualità delle informazioni finanziarie a livello mondiale.

⁵ Cfr. il rapporto *Risk IT and Operations: Strengthening capabilities* (giugno 2011) dell'Institute of International Finance.

7. Altre iniziative e requisiti in materia di dati di rischio dovranno essere attuati nei prossimi anni⁶. Il Comitato ritiene che il miglioramento delle capacità di aggregazione e delle prassi di reportistica dei dati di rischio consentirà alle banche di aderire efficacemente a tali iniziative.

Definizione

8. Ai fini del presente documento, il termine “aggregazione dei dati di rischio” indica la definizione, la raccolta e l’elaborazione dei dati di rischio in conformità ai requisiti di segnalazione di una banca al fine di consentire a quest’ultima di misurare i risultati reddituali in rapporto alla tolleranza/propensione al rischio⁷. Tale concetto comprende la classificazione, l’accorpamento e la scomposizione di serie di dati.

Obiettivi

9. Questo documento presenta una serie di principi volti a rafforzare le capacità di aggregazione e le prassi di segnalazione interna dei dati di rischio delle banche (di seguito, i “Principi”). L’attuazione efficace di tali Principi dovrebbe a sua volta consentire di migliorare la gestione dei rischi e i processi decisionali presso le banche.

10. L’adozione di questi Principi consentirà di ottenere miglioramenti fondamentali nella gestione delle banche. I Principi dovrebbero sostenere le iniziative delle banche volte a:

- migliorare l’infrastruttura per la reportistica delle informazioni più importanti, in particolare quelle utilizzate dal consiglio di amministrazione e dall’alta direzione per individuare, monitorare e gestire i rischi;
- migliorare il processo decisionale nell’intera organizzazione bancaria;
- migliorare la gestione delle informazioni presso le varie entità giuridiche, favorendo al tempo stesso una valutazione esaustiva delle esposizioni al rischio a livello consolidato globale;
- ridurre la probabilità e la gravità delle perdite legate a carenze nella gestione dei rischi;
- ridurre i tempi di predisposizione delle informazioni e quindi accelerare il processo decisionale;
- migliorare la qualità della pianificazione strategica di un’istituzione e la sua capacità di gestire i rischi inerenti a nuovi prodotti o servizi.

⁶ Ad esempio, i requisiti in materia di segnalazione dei dati previsti dalle norme di Basilea 3 e Solvency II, i piani di risanamento e risoluzione delle crisi, le modifiche agli schemi per le segnalazioni di vigilanza FINREP e COREP, nonché quelle dei principi contabili internazionali (IFRS) e del Foreign Account Tax Compliance Act (FATCA).

⁷ “La propensione al rischio è data dal livello e dal tipo di rischio che un’impresa è capace e disposta ad assumersi nel quadro delle proprie esposizioni e operazioni, dati i suoi obiettivi operativi e gli obblighi verso gli stakeholder”, come specifica il rapporto del Senior Supervisors Group *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure* (dicembre 2010).

11. Una solida capacità di gestione dei rischi costituisce parte integrante del *franchise value* di una banca. Pertanto, un'efficace attuazione dei Principi dovrebbe accrescere il valore di una banca. Il Comitato ritiene che i benefici di lungo periodo legati al miglioramento delle capacità di aggregazione dei dati di rischio e delle relative prassi di reportistica compenseranno ampiamente gli investimenti sopportati dalle banche.

12. Per quel che riguarda le autorità di vigilanza bancaria, i presenti Principi integreranno le altre iniziative tese a migliorare l'intensità e l'efficacia dell'attività di vigilanza. Per quanto concerne invece le autorità competenti per la risoluzione delle crisi, una migliore aggregazione dei dati di rischio dovrebbe permettere di intervenire sulle banche in maniera più ordinata, riducendo così il potenziale onere per i contribuenti.

Ambito di applicazione e considerazioni preliminari

13. I Principi sono destinati inizialmente alle SIB e si applicano a livello sia di gruppo bancario sia di singole entità. Per questi istituti occorrono aspettative prudenziali comuni e chiare in materia di aggregazione e reportistica dei dati di rischio. Le autorità nazionali di vigilanza bancaria potranno comunque applicare i Principi a una gamma più ampia di banche, proporzionalmente alle dimensioni, alla natura e alla complessità delle loro operazioni.

14. Le banche designate come G-SIB dall'FSB nel novembre 2011⁸ o 2012⁹ devono conformarsi a questi Principi entro il gennaio 2016; gli istituti designati come G-SIB in occasione degli aggiornamenti annuali successivi dovranno adeguarsi ai Principi entro tre anni dalla designazione¹⁰. Le G-SIB soggette alla scadenza del 2016 dovranno procedere gradualmente verso l'adozione efficace dei Principi a partire dall'inizio del 2013. Le autorità nazionali di vigilanza e il Comitato di Basilea seguiranno e valuteranno i progressi, conformemente alla sezione V del presente documento.

15. Le autorità nazionali di vigilanza sono caldamente incoraggiate ad applicare i Principi anche alle banche designate come D-SIB, a partire da tre anni dalla designazione¹¹.

16. I Principi e le aspettative prudenziali contenuti in questo documento si applicano ai dati relativi alla gestione dei rischi di una banca, inclusi i dati fondamentali per consentire alla banca di far fronte in modo efficace ai rischi in cui incorre. I dati di rischio e i relativi report dovrebbero permettere alla direzione di monitorare e seguire l'evoluzione dei rischi in relazione alla tolleranza/propensione al rischio della banca.

17. I Principi si applicano altresì a tutti i principali modelli interni di gestione dei rischi, compresi i modelli per il calcolo del patrimonio di vigilanza nell'ambito del primo pilastro (ad

⁸ Cfr. FSB, *Policy Measures to Address to Systemically Important Financial Institutions* (4 novembre 2011), consultabile all'indirizzo www.financialstabilityboard.org/publications/r_111104bb.pdf.

⁹ Cfr. FSB, *Update of group of global systemically important banks – G-SIBs* (1° novembre 2012), consultabile all'indirizzo www.financialstabilityboard.org/publications/r_121031ac.pdf.

¹⁰ Tale disposizione è in linea con il documento dell'FSB *Update of group of global systemically important banks – G-SIBs* (1° novembre 2012).

¹¹ Cfr. Comitato di Basilea, *Schema per il trattamento delle banche di rilevanza sistemica nazionale* (ottobre 2012), consultabile all'indirizzo www.bis.org/publ/bcbs233_it.pdf.

esempio, metodo basato sui rating interni per il rischio di credito e metodi avanzati di misurazione per il rischio operativo), i modelli per il calcolo del capitale economico nell'ambito del secondo pilastro e gli altri modelli più importanti per la gestione dei rischi (ad esempio i modelli di valore a rischio).

18. I Principi si applicano ai processi di gestione dei rischi adottati dai gruppi bancari. Tuttavia le banche potrebbero trarre beneficio dall'applicazione dei Principi anche ad altri processi, come quelli finanziari e operativi, nonché alle segnalazioni di vigilanza.

19. Tutti i Principi contenuti in questo documento sono applicabili anche ai processi esternalizzati a terzi.

20. I Principi coprono quattro ambiti strettamente collegati:

- infrastruttura e governo societario complessivi;
- capacità di aggregazione dei dati di rischio;
- prassi di reportistica in materia di rischio;
- verifica, strumenti e cooperazione delle autorità di vigilanza.

21. Le capacità di aggregazione dei dati di rischio e le relative prassi di reportistica vengono trattate separatamente in questo documento, sebbene siano chiaramente collegate fra loro e non possano sussistere autonomamente. La qualità della reportistica per la gestione dei rischi dipende dalle capacità di aggregazione dei dati, e i relativi flussi di informazioni dalla presenza di solide infrastrutture e meccanismi di governo societario.

22. Le banche dovrebbero rispettare tutti i Principi in materia di aggregazione e di reportistica dei dati di rischio simultaneamente. Tuttavia, in circostanze eccezionali potrebbero essere accettati compromessi fra Principi diversi, ad esempio nel caso di richieste urgenti o puntuali di informazioni su aree di rischio nuove o poco note. Tali compromessi non dovrebbero in alcun caso avere conseguenze rilevanti sulle decisioni in materia di gestione dei rischi. Gli organi decisionali delle banche, in particolare il consiglio di amministrazione e l'alta direzione, dovrebbero essere a conoscenza di tali compromessi e dei limiti o delle carenze che comportano.

Le autorità di vigilanza si attendono che le banche si dotino di politiche e processi per l'adozione di soluzioni di compromesso di questo tipo. Le banche dovrebbero essere in grado di spiegare le conseguenze di tali scelte sul loro processo decisionale mediante relazioni qualitative e, per quanto possibile, misure quantitative.

23. Il concetto di rilevanza utilizzato in questo documento significa che i dati e i report in materia di rischio potranno eccezionalmente omettere determinate informazioni solo nel caso in cui ciò non influisca sul processo decisionale di una banca (ovvero solo nel caso in cui gli organi decisionali, in particolare il consiglio di amministrazione e l'alta direzione, non possano essere influenzati dalle informazioni omesse oppure non esprimerebbero valutazioni diverse qualora fossero a conoscenza di tutte le informazioni).

Nell'applicazione del concetto di rilevanza le banche dovranno tenere conto di considerazioni che vanno oltre il numero o l'entità delle esposizioni non segnalate, come ad esempio il tipo di rischio oppure l'evoluzione dinamica tipica dell'attività bancaria. Le banche dovrebbero inoltre tenere conto del potenziale impatto futuro delle informazioni omesse sul processo decisionale. Le autorità di vigilanza si attendono che le banche siano in grado di giustificare le eventuali omissioni effettuate sulla base del concetto di rilevanza.

24. Le banche dovrebbero sviluppare la capacità di produrre report prospettici in grado di fornire indicazioni precoci sulle violazioni dei limiti di rischio potenzialmente eccedenti la

propensione/tolleranza al rischio della banca. Tale capacità dovrebbe parimenti consentire alle banche di effettuare prove di stress flessibili ed efficaci, in grado di fornire una valutazione prospettica dei rischi. Le autorità di vigilanza si attendono che la reportistica relativa alla gestione dei rischi consenta alle banche di anticipare i problemi e fornisca una valutazione prospettica del rischio.

25. È possibile che in caso di incompletezza dei dati si ricorra occasionalmente alla valutazione di esperti per agevolare il processo di aggregazione, nonché l'interpretazione dei risultati nell'ambito del processo di reportistica dei rischi. Il ricorso al giudizio di un esperto anziché a dati completi e accurati dovrebbe avvenire solo in via eccezionale, e non dovrebbe esercitare un impatto rilevante sul rispetto dei Principi da parte della banca. In caso di ricorso a un esperto, le autorità di vigilanza si attendono che ciò avvenga in maniera trasparente e chiaramente documentata, in modo da consentire una verifica indipendente dell'iter seguito e dei criteri utilizzati nel processo decisionale.

I. Infrastruttura e governo societario complessivi

26. Le banche dovrebbero disporre di un solido sistema di governo societario, una robusta architettura dei dati di rischio e un'affidabile infrastruttura informatica. Questi elementi sono indispensabili per assicurare il rispetto degli altri Principi enunciati nel presente documento. In particolare, il consiglio di amministrazione della banca dovrebbe vigilare sulla responsabilità dell'alta direzione di applicare tutti i principi relativi all'aggregazione e alle procedure di reportistica dei dati di rischio, nonché sulla strategia adottata per soddisfare tali Principi nei tempi concordati con le autorità di vigilanza.

Principio 1

Governo societario – Le capacità di aggregazione dei dati di rischio e le relative prassi di reportistica di una banca dovrebbero essere sottoposte a solidi dispositivi di governance, coerenti con gli altri principi e orientamenti emanati dal Comitato di Basilea¹².

27. Il consiglio di amministrazione e l'alta direzione dovrebbero promuovere l'individuazione, la valutazione e la gestione dei rischi relativi alla qualità dei dati nell'ambito del quadro complessivo per la gestione dei rischi. Quest'ultimo dovrebbe contemplare accordi sui livelli di servizio per i processi sia esternalizzati sia interni relativi ai dati di rischio, politiche aziendali in materia di riservatezza, integrità e disponibilità dei dati, nonché politiche di gestione dei rischi.

28. Il consiglio di amministrazione e l'alta direzione dovrebbero esaminare e approvare il quadro di riferimento per l'aggregazione e la reportistica dei dati di rischio a livello di gruppo bancario e assicurarsi che vengano impiegate risorse adeguate.

29. Le capacità di aggregazione dei dati di rischio e le relative prassi di reportistica di una banca dovrebbero:

¹² Ad esempio quelli contenuti nei documenti *Principles for Enhancing Corporate Governance* (ottobre 2010) e *Enhancements to the Basel II framework* (luglio 2009) del Comitato di Basilea.

- a) essere pienamente documentate e soddisfare elevati standard di convalida. Il processo di convalida dovrebbe essere indipendente e verificare l'osservanza da parte della banca dei Principi enunciati nel presente documento. Lo scopo principale della convalida indipendente è garantire che i processi di aggregazione e reportistica dei dati di rischio funzionino correttamente e siano adeguati al profilo di rischio della banca. Le attività di convalida indipendente dovrebbero essere allineate e integrate con le altre attività di verifica indipendente nel quadro del programma di gestione dei rischi della banca¹³ e riguardare tutte le componenti dei processi di aggregazione e reportistica dei dati di rischio. Secondo le prassi comuni, la convalida indipendente dei suddetti processi dovrebbe essere condotta avvalendosi di personale con competenze specifiche in materia di informatica, elaborazione e segnalazione dei dati¹⁴.
- b) essere considerate parte integrante di ogni nuova iniziativa, comprese acquisizioni e/o dismissioni, sviluppo di nuovi prodotti, nonché iniziative più generali di cambiamento dei processi o dei sistemi informatici. Nel valutare l'opportunità di un'acquisizione rilevante, il processo di dovuta diligenza della banca dovrebbe considerare la capacità di aggregazione dei dati di rischio e le relative prassi di reportistica dell'entità oggetto di acquisizione, nonché l'impatto che l'operazione avrebbe sulle proprie capacità e procedure in materia. Le conseguenze per l'aggregazione dei dati di rischio dovrebbero essere considerate esplicitamente dal consiglio di amministrazione e rientrare nella decisione di procedere con l'operazione. La banca dovrebbe definire il periodo entro il quale integrare e allineare nell'ambito della propria struttura le capacità di aggregazione dei dati di rischio e le relative prassi di reportistica dell'entità acquisita;
- c) non risentire della struttura del gruppo bancario. La struttura del gruppo non dovrebbe ostacolare le capacità di aggregazione dei dati di rischio né a livello consolidato né a qualsiasi livello rilevante nell'ambito dell'organizzazione (ad esempio, livello sub-consolidato, di giurisdizione od operativo). In particolare, le capacità di aggregazione dei dati di rischio non dovrebbero dipendere dalle scelte effettuate dalla banca relativamente alla struttura giuridica o alla presenza geografica¹⁵.

30. L'alta direzione della banca dovrebbe avere piena consapevolezza e comprensione dei limiti che impediscono una completa aggregazione dei dati di rischio, come limiti in termini di copertura (rischi non rilevati o affiliate non considerate), limiti tecnici (indicatori della performance dei modelli o ricorso a procedure manuali) o limiti legali (ostacoli di natura giuridica alla condivisione di dati fra giurisdizioni). L'alta direzione dovrebbe garantire che la strategia informatica della banca prevede modalità atte a perfezionare le capacità di aggregazione e la reportistica dei dati di rischio e a colmare eventuali carenze rispetto ai Principi qui enunciati, tenendo conto delle mutevoli esigenze aziendali. L'alta direzione dovrebbe inoltre stabilire, nell'ambito del processo di pianificazione strategica informatica, quali siano i dati fondamentali per le iniziative di aggregazione e per gli interventi

¹³ In particolare la cosiddetta "seconda linea di difesa" nell'ambito del sistema di controllo interno della banca.

¹⁴ Inoltre, la convalida dovrebbe essere separata dall'attività di revisione al fine di garantire la piena osservanza della distinzione tra la seconda e la terza *linea di difesa* nell'ambito del sistema di controllo interno della banca. Cfr., fra gli altri, i Principi 2 e 13 del documento *Internal Audit Function in Banks* del Comitato di Basilea (giugno 2012).

¹⁵ Tenuto conto di eventuali ostacoli di natura giuridica allo scambio di dati tra paesi.

sull'infrastruttura informatica, e assecondare questi interventi mediante l'allocazione di risorse umane e finanziarie adeguate.

31. Il consiglio di amministrazione ha la responsabilità di definire le proprie esigenze in termini di reportistica, e dovrebbe essere consapevole dei limiti che impediscono una completa aggregazione dei dati di rischio all'interno dei report ricevuti. Il consiglio di amministrazione dovrebbe inoltre essere al corrente dell'attuazione e del rispetto nel tempo, da parte della banca, dei Principi qui enunciati.

Principio 2

Architettura dei dati e infrastruttura informatica – Una banca dovrebbe progettare, realizzare e mantenere un'architettura dei dati e un'infrastruttura informatica in grado di sostenere appieno le capacità di aggregazione dei dati di rischio e le prassi di reportistica non solo in condizioni normali, ma anche in situazioni di tensione o di crisi, nel rispetto degli altri Principi.

32. Le capacità di aggregazione dei dati di rischio e le relative prassi di reportistica dovrebbero essere esplicitamente considerate nei processi di pianificazione della continuità operativa della banca ed essere sottoposte a un'analisi di impatto aziendale.

33. Le banche dovrebbero definire tassonomie e un'architettura di dati integrate¹⁶ per l'intero gruppo, comprendenti informazioni sulle caratteristiche dei dati stessi (metadati), nonché l'impiego di identificativi unici e/o di denominazioni convenzionali unificate per contrassegnare dati come entità giuridiche, controparti, clienti e conti.

34. Andrebbero istituiti ruoli e competenze specifiche relativamente alla "proprietà" (ownership) e alla qualità dei dati e delle informazioni di rischio sia per le funzioni operative sia per quelle informatiche. Gli owner (le funzioni operative e informatiche), in collaborazione con i gestori dei rischi, dovrebbero garantire la presenza di controlli adeguati lungo l'intero ciclo di vita dei dati e per tutti gli aspetti dell'infrastruttura tecnologica. Gli owner delle funzioni operative devono in particolare assicurarsi che i dati vengano correttamente inseriti dall'unità di front office pertinente, siano aggiornati e allineati alle definizioni previste, e che le capacità di aggregazione dei dati di rischio e le relative prassi di reportistica siano coerenti con le politiche della banca.

II. Capacità di aggregazione dei dati di rischio

35. Le banche dovrebbero sviluppare e mantenere solide capacità di aggregazione dei dati di rischio al fine di garantire che i relativi report forniscano un'affidabile rappresentazione dei rischi (il soddisfacimento delle aspettative in materia di aggregazione dei dati è condizione necessaria per il soddisfacimento delle aspettative in materia di reportistica). Il rispetto di un Principio non dovrebbe avvenire a scapito del rispetto di un altro Principio. Le capacità di aggregazione dei dati di rischio dovrebbero soddisfare tutti i Principi simultaneamente, in conformità al paragrafo 22 del presente documento.

¹⁶ Le banche non devono necessariamente impiegare un solo modello di dati, bensì dotarsi di solide procedure di raccordo automatizzato qualora si avvalgano di più modelli.

Principio 3

Accuratezza e integrità – Le banche dovrebbero essere in grado di generare dati di rischio precisi e affidabili, al fine di soddisfare i requisiti di accuratezza della reportistica sia in condizioni normali, sia in caso di tensione/crisi. L'aggregazione dei dati dovrebbe essere ampiamente automatizzata, così da ridurre al minimo la probabilità di errori.

36. Le banche dovrebbero aggregare i dati di rischio in modo accurato e affidabile.
- a) I controlli relativi ai dati di rischio dovrebbero essere altrettanto rigorosi di quelli applicabili ai dati contabili.
 - b) Qualora una banca faccia ricorso a procedure manuali e applicazioni informatiche desktop (ad esempio fogli di calcolo e database) e disponga di specifiche unità di rischio che utilizzano tali applicazioni per sviluppare software, la banca dovrebbe predisporre efficaci strumenti di attenuazione del rischio (ad esempio procedure e politiche in materia di end-user computing) e altri controlli efficaci da applicare uniformemente a tutti i processi della banca.
 - c) Al fine di garantirne l'accuratezza, i dati di rischio devono essere raccordati con le fonti della banca, inclusi ove opportuno i dati contabili¹⁷.
 - d) Le banche dovrebbero cercare di attingere a un'unica fonte autorevole di dati per ciascun tipo di rischio.
 - e) Gli addetti alle funzioni di controllo dei rischi dovrebbero disporre di un accesso sufficiente ai dati di rischio, che consenta loro di aggregare, convalidare e raccordare adeguatamente tali dati ai fini della reportistica.
37. Quale presupposto per il soddisfacimento di questo Principio, le banche dovrebbero dotarsi di un "glossario" dei concetti utilizzati, di modo che i dati ricevano la medesima definizione nell'intera organizzazione.
38. Vi dovrebbe essere il giusto equilibrio fra sistemi automatizzati e sistemi manuali. Nei casi che necessitano l'applicazione del giudizio professionale, un intervento manuale potrebbe risultare appropriato, mentre per molti altri processi è auspicabile un maggiore livello di automazione al fine di ridurre il rischio di errori.
39. Le autorità di vigilanza si attendono che le banche documentino e illustrino tutti i processi di aggregazione dei dati, sia automatizzati sia manuali (basati sul giudizio professionale o di altro tipo). La documentazione dovrebbe fra l'altro spiegare l'opportunità delle soluzioni alternative manuali eventualmente adottate in caso di problemi ai sistemi informatici, la loro rilevanza per l'accuratezza dell'aggregazione dei dati di rischio e le misure proposte per ridurre l'impatto.
40. Le autorità di vigilanza si attendono che le banche misurino e monitorino l'accuratezza dei dati e predispongano appropriati canali affinché le questioni rilevanti siano portate all'attenzione dei livelli gerarchici opportuni, nonché piani operativi per ovviare a una scarsa qualità dei dati.

¹⁷ Ai fini di questo documento, il termine "raccordo" indica il processo di raffronto tra voci o risultati e la spiegazione delle discrepanze.

Principio 4

Completezza – Le banche dovrebbero essere in grado di individuare e aggregare tutti i dati sui rischi rilevanti dell'intero gruppo bancario. Tali dati dovrebbero essere disponibili per ciascuna linea operativa, entità giuridica, tipo di attività, settore economico, area geografica e altre categorie, come opportuno a seconda del rischio in questione, in modo da permettere l'individuazione e la reportistica delle posizioni di rischio, delle concentrazioni e dei rischi emergenti.

41. Le capacità di aggregazione dei dati di una banca dovrebbero includere tutte le posizioni di rischio rilevanti, comprese quelle fuori bilancio.

42. Non è necessario che un'organizzazione bancaria esprima tutte le forme di rischio con un'unica misura o su una base comune, tuttavia le capacità di aggregazione dei dati di rischio dovrebbero essere le stesse a prescindere dalla scelta dei sistemi di aggregazione utilizzati. Nondimeno, ogni sistema dovrebbe indicare chiaramente l'approccio specifico impiegato per aggregare le posizioni relative a ciascuna misura di rischio, al fine di consentire al consiglio di amministrazione e all'alta direzione di valutare correttamente i risultati.

43. Le autorità di vigilanza si attendono che le banche producano dati di rischio completi e che misurino e monitorino la completezza dei dati. L'eventuale presenza di lacune nei dati di rischio non dovrebbe pregiudicare la capacità della banca di gestire i rischi efficacemente. Le autorità di vigilanza si aspettano che i dati delle banche siano sostanzialmente completi, e che le eventuali eccezioni vengano individuate e motivate.

Principio 5

Tempestività – Le banche dovrebbero essere in grado di generare in tempi brevi dati di rischio aggregati e aggiornati, rispettando al tempo stesso i principi di accuratezza e integrità, completezza e adattabilità. I tempi esatti dipenderanno dalla natura e dalla potenziale volatilità dei rischi oggetto di misurazione, nonché dalla loro rilevanza per il profilo di rischio complessivo della banca. Essi dipenderanno altresì dai requisiti in termini di periodicità della reportistica per la gestione dei rischi, sia in situazione normale sia in caso di tensione/crisi, definiti in base alle caratteristiche e al profilo di rischio complessivo delle singole banche.

44. Le capacità di aggregazione dei dati di rischio di una banca dovrebbero essere tali da garantire che essa possa produrre informazioni di rischio aggregate in tempi brevi, così da rispettare tutti i requisiti previsti per la reportistica per la gestione dei rischi.

45. Il Comitato di Basilea riconosce che le diverse tipologie di dati dovranno essere disponibili in tempi diversi, a seconda del tipo di rischio, e che alcuni dati potrebbero rendersi necessari più rapidamente in situazione di tensione/crisi. Le banche devono strutturare i loro sistemi in modo tale da consentire che in situazione di tensione/crisi vengano prodotti tempestivamente dati aggregati su tutti i rischi fondamentali.

46. Fra i dati sui rischi fondamentali figurano:

a) l'esposizione creditizia aggregata verso un importante cliente societario. A titolo di confronto, i gruppi di esposizioni al dettaglio potrebbero non variare in modo altrettanto rilevante in tempi brevi, ma potrebbero comunque presentare notevoli concentrazioni;

- b) le esposizioni al rischio di credito di controparte, ad esempio per operazioni in derivati;
- c) le esposizioni, le posizioni, i limiti operativi e le concentrazioni di mercato per settori e per regioni in relazione all'attività di negoziazione;
- d) gli indicatori del rischio di liquidità, come i flussi/regolamenti monetari e la provvista;
- e) gli indicatori urgenti del rischio operativo (ad esempio disponibilità dei sistemi, accesso non autorizzato).

47. Le autorità di vigilanza verificheranno che i requisiti delle singole banche in termini di periodicità, sia per le situazioni normali sia per i casi di tensione/crisi, consentano di generare in tempi brevi dati di rischio aggregati e aggiornati.

Principio 6

Adattabilità – Le banche dovrebbero essere in grado di generare dati aggregati per soddisfare un'ampia gamma di richieste puntuali, ad hoc, di informazioni sui rischi, comprese le richieste in situazioni di tensione/crisi, nonché quelle formulate in relazione all'evoluzione delle esigenze interne o per rispondere a quesiti delle autorità di vigilanza.

48. Le capacità di aggregazione dei dati di rischio delle banche dovrebbero essere flessibili e adattabili per soddisfare all'occorrenza richieste ad hoc di informazioni e per valutare i rischi emergenti. Questa adattabilità consentirà alle banche di migliorare la gestione dei rischi, in particolare per quanto riguarda i dati previsionali, nonché di agevolare la conduzione di prove di stress e analisi di scenario.

49. L'adattabilità presuppone:

- a) processi flessibili di aggregazione che consentano di aggregare i dati di rischio per effettuare valutazioni e assumere decisioni in tempi rapidi;
- b) la possibilità di adattare i dati alle esigenze degli utenti (ad esempio creando dashboard, o evidenziando i punti salienti e le anomalie), ottenere il grado di dettaglio ricercato e produrre rapidamente report di sintesi;
- c) la capacità di integrare i nuovi sviluppi relativi all'organizzazione aziendale e/o fattori esterni che influenzano il profilo di rischio della banca;
- d) la capacità di integrare le modifiche del quadro normativo.

50. Le autorità di vigilanza si attendono che le banche siano in grado di generare sottoinsiemi di dati in base agli scenari richiesti oppure a seguito di particolari eventi economici. Ad esempio, le banche dovrebbero poter aggregare rapidamente i dati di rischio sulle esposizioni creditizie per paesi¹⁸ a una data specifica per un elenco di paesi, nonché i dati sulle esposizioni creditizie per settori economici a una data specifica per un elenco di settori, e ciò per tutte le linee operative e le aree geografiche.

¹⁸ Ad esempio, le esposizioni verso prenditori sovrani, banche, imprese e clientela al dettaglio.

III. Prassi di reportistica in materia di rischio

51. Dati accurati, completi e tempestivi rappresentano le fondamenta di una gestione efficace dei rischi. Tuttavia, essi non garantiscono da soli che il consiglio di amministrazione e l'alta direzione ricevano informazioni adeguate per assumere decisioni efficaci in materia di rischio. Ai fini di una corretta gestione dei rischi è necessario che le informazioni appropriate siano presentate alle persone giuste al momento opportuno. La reportistica basata sui dati di rischio dovrebbe essere accurata, chiara e completa. Il suo contenuto dovrebbe essere corretto e presentato agli organi decisionali appropriati in tempi tali da consentire una risposta adeguata. Per risultare efficaci, i report di rischio dovrebbero soddisfare i principi illustrati di seguito. Il rispetto di un Principio non dovrebbe avvenire a scapito del rispetto di un altro Principio, in conformità al paragrafo 22 di questo documento.

Principio 7

Accuratezza – La reportistica sui rischi dovrebbe veicolare i dati aggregati in maniera accurata e precisa, e fornire una fedele rappresentazione dei rischi. Essa dovrebbe inoltre essere oggetto di raccordo e convalida.

52. La reportistica sui rischi dovrebbe essere accurata e precisa, al fine di garantire che il consiglio di amministrazione e l'alta direzione possano fare affidamento sulle informazioni aggregate per assumere decisioni rilevanti in materia di rischio.

53. Al fine di garantire l'accuratezza della reportistica, le banche dovrebbero dotarsi come minimo dei seguenti elementi:

- a) requisiti e processi definiti per il raccordo della reportistica con i dati di rischio;
- b) verifica delle modifiche automatiche e manuali e controlli di ragionevolezza, compreso un inventario delle regole di convalida applicate alle informazioni quantitative. L'inventario dovrebbe includere la spiegazione delle convenzioni utilizzate per descrivere eventuali relazioni logiche o matematiche da sottoporre a verifica attraverso le convalide e i controlli;
- c) procedure integrate per individuare, segnalare e spiegare gli errori o le carenze nell'integrità dei dati attraverso la segnalazione di valori anomali (exception report).

54. Le approssimazioni costituiscono parte integrante della reportistica e della gestione dei rischi. I risultati ricavati da modelli, analisi di scenario e prove di stress sono esempi di approssimazioni che forniscono informazioni fondamentali per la gestione dei rischi. Sebbene le aspettative in materia di approssimazioni possano differire rispetto a quelle relative ad altre tipologie di reportistica, le banche dovrebbero seguire i principi di segnalazione contenuti in questo documento e stabilire aspettative in termini di affidabilità delle approssimazioni (accuratezza, tempestività, ecc.) al fine di garantire che la direzione possa fare affidamento sulle informazioni ricevute per assumere decisioni rilevanti in materia di rischio. Tali aspettative dovrebbero riguardare anche i dati utilizzati per ottenere le approssimazioni.

55. Le autorità di vigilanza si attendono che l'alta direzione della banca stabilisca requisiti di accuratezza e precisione sia per la reportistica abituale, sia per quella in situazione di tensione/crisi, comprese le informazioni relative posizioni ed esposizioni critiche. Tali requisiti dovrebbero essere commisurati all'importanza delle decisioni che si baseranno sulle informazioni in parola.

56. Le autorità di vigilanza si attendono che, ai fini dei requisiti di accuratezza, le banche adottino un approccio analogo a quello della rilevanza contabile. Ad esempio, potrebbe essere ritenuta rilevante un'omissione o un'inesattezza suscettibile di influenzare le decisioni in materia di rischio da parte dei fruitori dei dati. Le banche dovrebbero essere in grado di motivare i requisiti di accuratezza. Le autorità di vigilanza si attendono che le banche considerino la possibilità di applicare requisiti di precisione a seconda dei processi e dei risultati di convalide, verifiche e operazioni di raccordo.

Principio 8

Esaustività – La reportistica sui rischi dovrebbe coprire tutte le aree di rischio rilevanti all'interno dell'organizzazione. Essa dovrebbe avere un livello di approfondimento e di copertura commisurato alle dimensioni e alla complessità delle operazioni e del profilo di rischio della banca, nonché ai requisiti dei destinatari.

57. La reportistica sui rischi dovrebbe segnalare le informazioni sulle esposizioni e sulle posizioni relative a tutte le aree di rischio significative (ad esempio, rischio di credito, rischi di mercato, rischio di liquidità, rischio operativo) e a tutte le loro componenti significative (ad esempio, singolo prenditore, paese e settore di attività per quanto riguarda il rischio di credito). Essa dovrebbe parimenti contenere informazioni sulle grandezze collegate al rischio (ad esempio patrimonio di vigilanza e capitale economico).

58. La reportistica dovrebbe rilevare le concentrazioni di rischio emergenti, fornire informazioni nel contesto dei limiti e della propensione/tolleranza al rischio e, ove opportuno, formulare raccomandazioni per eventuali interventi. Essa dovrebbe descrivere lo stato di attuazione delle misure approvate dal consiglio di amministrazione o dall'alta direzione per ridurre il rischio o affrontare specifiche situazioni di rischio. La reportistica dovrebbe consentire di monitorare le tendenze emergenti attraverso previsioni e prove di stress prospettiche.

59. Le autorità di vigilanza si aspettano che le banche determinino, in materia di reportistica, i requisiti che meglio si addicono ai rispettivi modelli operativi e profili di rischio. Le autorità di vigilanza dovranno ritenere soddisfacenti le scelte effettuate dalle banche in termini di copertura dei rischi, analisi e interpretazione, scalabilità e comparabilità fra entità del gruppo bancario. Ad esempio, un report sui dati di rischio aggregati dovrebbe contenere quantomeno le seguenti informazioni: adeguatezza patrimoniale, patrimonio di vigilanza, proiezioni sui coefficienti patrimoniali e di liquidità, rischio di credito, rischi di mercato, rischio operativo, rischio di liquidità, risultati delle prove di stress, concentrazioni all'interno di una stessa categoria di rischio o fra categorie diverse, posizioni e piani di finanziamento.

60. Le autorità di vigilanza si aspettano che la reportistica sui rischi destinata al consiglio di amministrazione e all'alta direzione fornisca una valutazione prospettica dei rischi e non si basi soltanto sui dati correnti e pregressi. Essa dovrebbe contenere previsioni o scenari relativi alle principali variabili di mercato e agli effetti sulla banca, in modo da informare il consiglio di amministrazione e l'alta direzione del probabile andamento futuro della capitalizzazione e del profilo di rischio della banca.

Principio 9

Chiarezza e utilità – La reportistica sui rischi dovrebbe segnalare le informazioni in maniera chiara e concisa. Essa dovrebbe essere di facile comprensione e al tempo stesso esauriente, così da favorire un processo decisionale informato. I singoli report dovrebbero contenere informazioni significative adattate alle esigenze dei destinatari.

61. La reportistica sui rischi dovrebbe favorire una corretta gestione dei rischi e facilitare il processo decisionale dei destinatari, in particolare il consiglio di amministrazione e l'alta direzione. Essa dovrebbe garantire che le informazioni siano pertinenti e adattate alle necessità dei destinatari.

62. La reportistica dovrebbe presentare il giusto equilibrio fra dati di rischio, analisi e interpretazioni, e spiegazioni qualitative. L'equilibrio tra informazioni quantitative e qualitative varierà a seconda dei livelli dell'organizzazione, nonché del grado di aggregazione applicato. Ai livelli più elevati dell'organizzazione, l'aggregazione sarà presumibilmente maggiore, e si renderà pertanto necessario un maggiore grado di interpretazione qualitativa.

63. Le politiche e le procedure di reportistica dovrebbero recepire le differenti esigenze informative del consiglio di amministrazione, dell'alta direzione e degli altri livelli dell'organizzazione (ad esempio i comitati di rischio).

64. Il consiglio di amministrazione, essendo uno dei principali destinatari della reportistica sui rischi, è responsabile di definire le proprie esigenze in materia e di osservare i propri obblighi verso gli azionisti e le altre parti interessate. Il consiglio di amministrazione dovrebbe assicurarsi di richiedere e di ricevere le informazioni opportune, che gli consentano di adempiere il proprio mandato nei confronti della banca e dei rischi ai quali è esposta. Ciò permetterà al consiglio stesso di garantire che il proprio operato avviene nel rispetto dei limiti di tolleranza/propensione al rischio prefissati.

65. Il consiglio di amministrazione dovrebbe avvisare l'alta direzione qualora la reportistica sui rischi non risponda ai requisiti da esso definiti e non fornisca il livello o il tipo di informazioni adeguato per determinare la tolleranza/propensione al rischio della banca e controllare che venga rispettata. Il consiglio di amministrazione dovrebbe indicare se i report ricevuti siano sufficientemente accurati e presentino il giusto equilibrio tra informazioni qualitative e quantitative.

66. Anche l'alta direzione figura fra i principali destinatari della reportistica sui rischi ed è responsabile di definire le proprie esigenze al riguardo. Essa dovrebbe assicurarsi di ricevere le informazioni opportune, che le consentano di adempiere il proprio mandato nei confronti della banca e dei rischi ai quali è esposta.

67. Le banche dovrebbero stilare un inventario e una classificazione dei dati di rischio che facciano riferimento ai concetti utilizzati per elaborare la reportistica.

68. Le autorità di vigilanza si aspettano che la reportistica sui rischi sia chiara e utile. I singoli report dovrebbero presentare il giusto equilibrio tra dati dettagliati, analisi qualitative, interpretazioni e raccomandazioni conclusive. L'interpretazione e la spiegazione dei dati, incluse le tendenze osservate, dovrebbero essere chiare.

69. Le autorità di vigilanza si attendono che le banche verifichino periodicamente con i destinatari che le informazioni aggregate e riportate siano pertinenti e appropriate, in termini sia quantitativi sia qualitativi, ai fini del governo societario e del processo decisionale.

Principio 10

Periodicità – Il consiglio di amministrazione e l'alta direzione (o altri destinatari, se del caso) dovrebbero definire la frequenza della produzione e della distribuzione della reportistica sui rischi. I requisiti di periodicità dovrebbero riflettere le esigenze dei destinatari, la natura dei rischi segnalati, la rapidità della loro evoluzione, nonché l'importanza della reportistica stessa ai fini di una corretta gestione dei rischi e di un

processo decisionale efficace ed efficiente nell'intera banca. La frequenza della reportistica dovrebbe aumentare nei periodi di tensione/crisi.

70. La frequenza della reportistica varierà a seconda della tipologia di rischio, degli obiettivi e dei destinatari. Le banche dovrebbero valutare periodicamente l'obiettivo di ciascun tipo di report e stabilire i tempi entro i quali i report vadano prodotti in situazioni normali e in caso di tensione/crisi. Le banche dovrebbero verificare regolarmente la propria capacità di produrre report accurati nei tempi stabiliti, in particolare in situazione di tensione/crisi.

71. Le autorità di vigilanza si aspettano che nei periodi di tensione/crisi tutta la reportistica pertinente e rilevante relativa alle posizioni/esposizioni ai rischi di credito, di mercato e di liquidità sia disponibile in tempi assai brevi, per consentire di reagire efficacemente all'evoluzione dei rischi. Al riguardo, alcune informazioni su posizioni/esposizioni specifiche potrebbero rendersi necessarie immediatamente (in giornata).

Principio 11

Diffusione – La reportistica sui rischi dovrebbe essere distribuita alle parti interessate nel rispetto degli obblighi di riservatezza.

72. Dovrebbero essere messe in atto procedure volte a consentire che i dati di rischio vengano raccolti e analizzati rapidamente e i relativi report pervengano tempestivamente a tutti i destinatari del caso. Tale esigenza va soppesata con la necessità di garantire l'opportuna riservatezza.

73. Le autorità di vigilanza si aspettano che una banca confermi periodicamente che i destinatari del caso ricevono report tempestivi.

IV. Verifica, strumenti e cooperazione delle autorità di vigilanza

74. Le autorità di vigilanza avranno un importante ruolo da svolgere nell'incentivare e monitorare l'attuazione e il rispetto dei Principi da parte delle banche. Esse dovranno inoltre verificare l'osservanza dei Principi presso le diverse banche per accertare che i Principi stessi stiano producendo gli esiti desiderati e valutare l'opportunità di ulteriori miglioramenti.

Principio 12

Verifica – Le autorità di vigilanza dovrebbero verificare e valutare periodicamente il rispetto degli undici Principi sopraelencati da parte delle banche.

75. Le autorità di vigilanza dovrebbero verificare l'osservanza da parte delle banche dei Principi enunciati nelle sezioni precedenti. Le verifiche dovrebbero avvenire nel quadro del regolare programma di controlli prudenziali e potrebbero essere integrate da analisi tematiche presso varie banche rispetto a uno o più temi specifici. Le autorità potrebbero verificare l'osservanza dei Principi da parte di un istituto attraverso richieste occasionali di informazioni su particolari aspetti di rischio (ad esempio, l'esposizione verso determinati fattori di rischio), da soddisfare in tempi brevi, mettendo così alla prova la capacità di una banca di aggregare rapidamente i dati e produrre i report. Al fine di svolgere questa verifica, le autorità di vigilanza dovrebbero avere accesso alla reportistica del caso.

76. In sede di valutazione del rispetto dei Principi, le autorità di vigilanza dovrebbero attingere alle verifiche condotte da revisori interni o esterni. Le autorità di vigilanza potrebbero richiedere il contributo della funzione di audit interno di una banca oppure di esperti indipendenti. Le autorità devono avere accesso a tutti i documenti del caso, come relazioni dei revisori e rapporti di convalida interni, e, ove necessario, essere in grado di incontrare i revisori esterni o gli esperti indipendenti per discutere delle capacità di aggregazione dei dati di rischio.

77. Le autorità di vigilanza dovrebbero verificare la capacità delle banche di aggregare i dati e produrre report sia in un contesto di stabilità, sia in situazione di tensione/crisi, compresa l'eventualità di un repentino aumento dei volumi di attività.

Principio 13

Interventi correttivi e misure prudenziali – Le autorità di vigilanza dovrebbero disporre e fare uso delle risorse e degli strumenti idonei per esigere dalle banche interventi correttivi efficaci e tempestivi volti a colmare le carenze riscontrate nelle capacità di aggregazione dei dati di rischio e nelle relative prassi di reportistica. Le autorità di vigilanza dovrebbero essere in grado di ricorrere a una serie di strumenti, incluso al secondo pilastro.

78. Le autorità di vigilanza dovrebbero esigere dalle banche interventi correttivi efficaci e tempestivi al fine di colmare le eventuali carenze riscontrate nelle capacità di aggregazione dei dati di rischio e nelle relative prassi di reportistica, nonché nei controlli interni.

79. Le autorità di vigilanza dovrebbero disporre di una serie di strumenti per colmare le carenze rilevanti eventualmente riscontrate nelle capacità di aggregazione dei dati di rischio e di reportistica, fra cui ad esempio: la richiesta di interventi correttivi da parte delle banche; una maggiore intensità della vigilanza; la richiesta di una verifica indipendente da parte di terzi, come revisori esterni; l'applicazione di maggiorazioni patrimoniali, sia come strumenti di attenuazione del rischio sia come incentivo nel quadro del secondo pilastro¹⁹.

80. Qualora ritengano che le carenze riscontrate nell'aggregazione dei dati di rischio e nella relativa reportistica siano all'origine di debolezze significative nella gestione dei rischi, le autorità di vigilanza dovrebbero essere in grado di porre un limite ai rischi assunti da una banca oppure alla crescita delle sue operazioni.

81. In caso di nuove iniziative imprenditoriali le autorità di vigilanza hanno la facoltà di richiedere, prima di autorizzare una nuova operazione o un'acquisizione, che i piani di attuazione delle banche garantiscano la possibilità di una corretta aggregazione dei dati di rischio.

82. Laddove richieda a una banca di effettuare un intervento correttivo, l'autorità di vigilanza dovrà stabilire un calendario per il completamento dell'intervento stesso. Le autorità di vigilanza dovrebbero disporre di procedure di escalation per richiedere interventi correttivi più severi o rapidi nell'eventualità che la banca non affronti adeguatamente le carenze riscontrate, ovvero nel caso in cui le autorità stesse ritengano opportune ulteriori misure.

¹⁹ Cfr. Comitato di Basilea, *Enhancements to the Basel II framework* (luglio 2009).

Principio 14

Cooperazione tra autorità del paese di origine e del paese ospitante – Le autorità di vigilanza dovrebbero cooperare con le corrispondenti autorità di altre giurisdizioni ai fini della sorveglianza e della verifica del rispetto dei Principi e, se del caso, ai fini dell’attuazione di eventuali interventi correttivi.

83. L’efficace cooperazione e un adeguato scambio di informazioni tra le autorità di vigilanza del paese di origine e del paese ospitante dovrebbero concorrere a irrobustire le prassi di gestione dei rischi della banca per l’insieme delle operazioni da questa condotte in più giurisdizioni. Ove possibile, le autorità di vigilanza dovrebbero evitare di svolgere verifiche ridondanti e non coordinate sull’aggregazione dei dati di rischio e la relativa reportistica.

84. La cooperazione può assumere la forma dello scambio di informazioni nel rispetto delle norme applicabili, nonché di consultazioni bilaterali o multilaterali (ad esempio attraverso i collegi di supervisor), anche periodiche. Le comunicazioni mediante teleconferenza e posta elettronica possono rivelarsi particolarmente utili per seguire l’evoluzione degli interventi correttivi. La cooperazione in seno ai collegi dei supervisor dovrebbe conformarsi ai principi delineati in materia dal Comitato di Basilea²⁰.

85. Le autorità di vigilanza dovrebbero mettere a confronto le rispettive esperienze riguardo alle capacità di aggregazione dei dati di rischio e alle relative prassi di reportistica nelle varie entità di un gruppo bancario. Tale confronto dovrebbe riguardare anche gli eventuali ostacoli all’aggregazione dei dati di rischio e alla relativa reportistica legati all’attività transfrontaliera, e verificare che i dati di rischio siano distribuiti adeguatamente nell’intero gruppo. Questi scambi consentiranno alle autorità di vigilanza di individuare precocemente i problemi più rilevanti e di reagire in maniera pronta ed efficace.

V. Calendario di attuazione e disposizioni transitorie

86. Le autorità di vigilanza si attendono che nei prossimi anni l’infrastruttura informatica e di gestione dei dati di cui dispongono le banche sia potenziata al fine di garantire che le capacità di aggregazione dei dati di rischio e le relative prassi di reportistica diventino sufficientemente robuste e al tempo stesso flessibili per soddisfare le esigenze delle banche sia in situazione normale, sia, in particolare, nei periodi di tensione/crisi.

87. Agli inizi del 2013 le autorità nazionali di vigilanza bancaria cominceranno a discutere dell’attuazione dei Principi con i vertici delle G-SIB. Ciò garantirà che le banche elaborino una strategia per ottemperare ai Principi entro il 2016.

88. Affinché le G-SIB possano rispettare la scadenza del 2016, le autorità nazionali di vigilanza bancaria esamineranno con i vertici aziendali i risultati della valutazione effettuata dalle banche stesse sulle capacità di aggregazione dei dati di rischio e concorderanno un calendario per apportare gli eventuali miglioramenti necessari. Le autorità di vigilanza potranno verosimilmente richiedere alle G-SIB di condurre agli inizi del 2013 un’autovalutazione basata sulle presenti aspettative, con l’obiettivo di colmare eventuali

²⁰ Cfr. Comitato di Basilea, *Good practice principles on supervisory colleges* (ottobre 2010), consultabile all’indirizzo www.bis.org/publ/bcbs177.pdf.

lacune significative entro il 2016. Le autorità di vigilanza potrebbero inoltre ricorrere alla collaborazione di esperti tecnici per valutare i piani delle banche rispetto alla scadenza del 2016²¹.

89. A partire dal 2013 il Comitato di Basilea, per il tramite dello Standards Implementation Group (SIG), seguirà i progressi delle G-SIB verso l'osservanza dei Principi. In tale contesto verrà valutata anche l'efficacia dei Principi stessi, nonché l'opportunità di apportarvi miglioramenti o emendamenti. Il Comitato di Basilea comunicherà i risultati di queste analisi all'FSB almeno una volta l'anno a partire dalla fine del 2013.

²¹ Il Comitato di Basilea riconosce che in circostanze molto specifiche ed eccezionali le autorità nazionali di vigilanza potrebbero dover ricorrere a un certo grado di flessibilità nell'applicazione della scadenza del 2016. Ad esempio, il rispetto di tale scadenza potrebbe risentire della scelta di esternalizzare determinati processi a terzi nei casi in cui i contratti di appalto prevedano scadenze successive al 2016.

Allegato 1

Terminologia utilizzata nel documento

Accuratezza	Concordanza tra una misurazione, registrazione o rappresentazione e il valore misurato, registrato o riprodotto. Questa definizione si applica sia all'aggregazione dei dati sia alla reportistica sui rischi.
Adattabilità	Attitudine delle capacità di aggregazione dei dati di rischio a modificarsi (o a essere modificate) in risposta all'evoluzione delle circostanze (interne o esterne).
Aggregazione dei dati di rischio	Definizione, raccolta ed elaborazione dei dati di rischio in conformità ai requisiti di segnalazione della banca, al fine di consentire a quest'ultima di misurare i risultati reddituali in rapporto alla tolleranza/propensione al rischio. Comprende la classificazione, l'accorpamento e la scomposizione di serie di dati.
Approssimazione	Risultato non necessariamente esatto, ma accettabile per un determinato scopo.
Chiarezza	Facilità di comprensione e assenza di indeterminatezza o ambiguità nella reportistica sui rischi.
Completezza	Disponibilità dei pertinenti dati di rischio aggregati per tutte le unità costitutive di una impresa (come entità giuridiche, linee operative, aree geografiche).
Convalida	Processo di verifica e quantificazione della correttezza di input, elaborazioni e output.
Distribuzione	Trasmissione appropriata dei report sui rischi ai soggetti e agli organi pertinenti.
Esaustività	Caratteristica della reportistica sui rischi che copre o tratta tutti i rischi significativi per l'impresa.
Integrità	Caratteristica dei dati di rischio che non hanno subito alterazioni o manipolazioni non autorizzate in grado di comprometterne l'accuratezza, la completezza e l'affidabilità.
Periodicità	Frequenza alla quale è prodotta la reportistica sui rischi.
Precisione	Concordanza tra indicazioni o valori quantitativi misurati, ottenuti reiterando la misurazione sullo stesso oggetto o su oggetti simili, nel rispetto di determinate condizioni.
Raccordo	Processo di raffronto tra voci o risultati, e spiegazione delle eventuali discrepanze.
Soluzioni alternative manuali	Impiego di processi e strumenti manuali per trasferire, manipolare o alterare i dati da aggregare o da segnalare.

Tempestività	Disponibilità dei dati di rischio aggregati in tempi tali da consentire alla banca di produrre la reportistica sui rischi alla frequenza prevista.
Tolleranza/propensione al rischio	Livello e tipo di rischio che un'impresa è capace e disposta ad assumersi nel quadro delle proprie esposizioni e operazioni, alla luce della sua attività e degli obblighi verso gli stakeholder. Viene generalmente espressa mediante indicatori sia quantitativi sia qualitativi.

Allegato 2

Sintesi dei Principi

I Principi coprono quattro ambiti strettamente collegati:

- i) infrastruttura e governo societario complessivi;
- ii) capacità di aggregazione dei dati di rischio;
- iii) prassi di reportistica in materia di rischio;
- iv) verifica, strumenti e cooperazione delle autorità di vigilanza.

I. Infrastruttura e governo societario complessivi

Principio 1

Governo societario – Le capacità di aggregazione dei dati di rischio e le relative prassi di reportistica di una banca dovrebbero essere sottoposte a solidi dispositivi di governance, coerenti con gli altri principi e orientamenti emanati dal Comitato di Basilea²².

Principio 2

Architettura dei dati e infrastruttura informatica – Una banca dovrebbe progettare, realizzare e mantenere un'architettura dei dati e un'infrastruttura informatica in grado di sostenere appieno le capacità di aggregazione dei dati di rischio e le prassi di reportistica non solo in condizioni normali, ma anche in situazioni di tensione o di crisi, nel rispetto degli altri Principi.

II. Capacità di aggregazione dei dati di rischio

Principio 3

Accuratezza e integrità – Le banche dovrebbero essere in grado di generare dati di rischio precisi e affidabili, al fine di soddisfare i requisiti di accuratezza della reportistica sia in condizioni normali, sia in caso di tensione/crisi. L'aggregazione dei dati dovrebbe essere ampiamente automatizzata, così da ridurre al minimo la probabilità di errori.

Principio 4

Completezza – Le banche dovrebbero essere in grado di individuare e aggregare tutti i dati sui rischi rilevanti dell'intero gruppo bancario. Tali dati dovrebbero essere disponibili per ciascuna linea operativa, entità giuridica, tipo di attività, settore economico, area geografica e

²² Cfr. ad esempio *Principles for Enhancing Corporate Governance* (ottobre 2010) e *Enhancements to the Basel II framework* (luglio 2009) pubblicati dal Comitato di Basilea.

altre categorie, come opportuno a seconda del rischio in questione, in modo da permettere l'individuazione e la reportistica delle posizioni di rischio, delle concentrazioni e dei rischi emergenti.

Principio 5

Tempestività – Le banche dovrebbero essere in grado di generare in tempi brevi dati di rischio aggregati e aggiornati, rispettando al tempo stesso i principi di accuratezza e integrità, completezza e adattabilità. I tempi esatti dipenderanno dalla natura e dalla potenziale volatilità dei rischi oggetto di misurazione, nonché dalla loro rilevanza per il profilo di rischio complessivo della banca. Essi dipenderanno altresì dai requisiti in termini di periodicità della reportistica per la gestione dei rischi, sia in situazione normale sia in caso di tensione/crisi, definiti in base alle caratteristiche e al profilo di rischio complessivo delle singole banche.

Principio 6

Adattabilità – Le banche dovrebbero essere in grado di generare dati aggregati per soddisfare un'ampia gamma di richieste puntuali, ad hoc, di informazioni sui rischi, comprese le richieste in situazioni di tensione/crisi, nonché quelle formulate in relazione all'evoluzione delle esigenze interne o per rispondere a quesiti delle autorità di vigilanza.

III. Prassi di reportistica del rischio

Principio 7

Accuratezza – La reportistica sui rischi dovrebbe veicolare i dati aggregati in maniera accurata e precisa, e fornire una fedele rappresentazione dei rischi. Essa dovrebbe inoltre essere oggetto di raccordo e convalida.

Principio 8

Esaustività – La reportistica sui rischi dovrebbe coprire tutte le aree di rischio rilevanti all'interno dell'organizzazione. Essa dovrebbe avere un livello di approfondimento e di copertura commisurato alle dimensioni e alla complessità delle operazioni e del profilo di rischio della banca, nonché ai requisiti dei destinatari.

Principio 9

Chiarezza e utilità – La reportistica sui rischi dovrebbe segnalare le informazioni in maniera chiara e concisa. Essa dovrebbe essere di facile comprensione e al tempo stesso esauriente, così da favorire un processo decisionale informato. I singoli report dovrebbero contenere informazioni significative adattate alle esigenze dei destinatari.

Principio 10

Periodicità – Il consiglio di amministrazione e l'alta direzione (o altri destinatari, se del caso) dovrebbero definire la frequenza della produzione e della distribuzione della reportistica sui rischi. I requisiti di periodicità dovrebbero riflettere le esigenze dei destinatari, la natura dei rischi segnalati, la rapidità della loro evoluzione, nonché l'importanza della reportistica stessa ai fini di una corretta gestione dei rischi e di un processo decisionale efficace ed efficiente.

nell'intera banca. La frequenza della reportistica dovrebbe aumentare nei periodi di tensione/crisi.

Principio 11

Diffusione – La reportistica sui rischi dovrebbe essere distribuita alle parti interessate nel rispetto degli obblighi di riservatezza.

IV. Verifica, strumenti e cooperazione delle autorità di vigilanza

Principio 12

Verifica – Le autorità di vigilanza dovrebbero verificare e valutare periodicamente il rispetto degli undici Principi sopraelencati da parte delle banche.

Principio 13

Interventi correttivi e misure prudenziali – Le autorità di vigilanza dovrebbero disporre e fare uso delle risorse e degli strumenti idonei per esigere dalle banche interventi correttivi efficaci e tempestivi volti a colmare le carenze riscontrate nelle capacità di aggregazione dei dati di rischio e nelle relative prassi di reportistica. Le autorità di vigilanza dovrebbero essere in grado di ricorrere a una serie di strumenti, incluso al secondo pilastro.

Principio 14

Cooperazione tra autorità del paese di origine e del paese ospitante – Le autorità di vigilanza dovrebbero cooperare con le corrispondenti autorità di altre giurisdizioni ai fini della sorveglianza e della verifica del rispetto dei Principi e, se del caso, ai fini dell'attuazione di eventuali interventi correttivi.