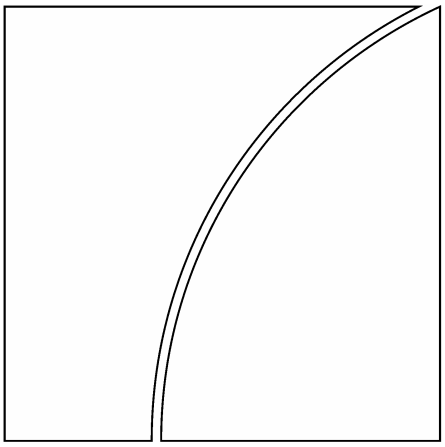
Comitato di Basilea per la vigilanza bancaria



Prassi corrette per la gestione e il controllo del rischio operativo

Febbraio 2003

BANCA DEI REGOLAMENTI INTERNAZIONALI

Le richieste di copie della pubblicazione vanno inviate a:

Segretariato del
Comitato di Basilea per la vigilanza bancaria
c/o Banca dei Regolamenti Internazionali
CH-4002 Basilea, Svizzera

E-mail: publications@bis.org

Fax: +41 61 280 9100

Questa pubblicazione è disponibile sul sito Internet della BRI (www.bis.org).

Pubblicata anche in francese, inglese, spagnolo e tedesco.

Risk Management Group
del Comitato di Basilea per la vigilanza bancaria

Presidente:
Roger Cole – Federal Reserve Board, Washington, D.C.

Banque Nationale de Belgique, Bruxelles	Dominique Gressens
Commission Bancaire et Financière, Bruxelles	Jos Meuleman
Office of the Superintendent of Financial Institutions, Ottawa	Jeff Miller
Commission Bancaire, Parigi	Laurent Le Mouël
Deutsche Bundesbank, Francoforte sul Meno	Magdalene Heid Karin Sagner-Kaiser
Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn	Kirsten Straus
Banca d'Italia, Roma	Claudio D'Auria Fabrizio Leandri Sergio Sorrentino
Bank of Japan, Tokyo	Satoshi Yamaguchi
Financial Services Agency, Tokyo	Hirokazu Matsushima
Commission de Surveillance du Secteur Financier, Lussemburgo	Davy Reinard
De Nederlandsche Bank, Amsterdam	Klaas Knot
Banco de España, Madrid	Guillermo Rodriguez-Garcia Juan Serrano
Finansinspektionen, Stoccolma	Jan Hedquist
Sveriges Riksbank, Stoccolma	Thomas Flodén
Commissione federale delle banche, Berna	Martin Sprenger
Financial Services Authority, Londra	Helmut Bauer Victor Dowd
Federal Deposit Insurance Corporation, Washington, D.C.	Mark Schmidt
Federal Reserve Bank of New York	Beverly Hirtle Stefan Walter
Federal Reserve Board, Washington, D.C.	Kirk Odegard
Office of the Comptroller of the Currency, Washington, D.C.	Kevin Bailey Tanya Smith
Banca centrale europea, Francoforte sul Meno	Panagiotis Strouzas
Commissione europea, Bruxelles	Michel Martino Melania Savino
Segretariato del Comitato di Basilea per la vigilanza bancaria, Banca dei Regolamenti Internazionali	Stephen Senior

Indice

Introduzione 1
Premessa 1
Tendenze e prassi nel settore bancario 2
Prassi corrette 3
Creazione di un appropriato contesto di gestione del rischio 5
Gestione del rischio: individuazione, valutazione, monitoraggio e controllo/mitigazione 6
Ruolo delle autorità di vigilanza 10
Ruolo dell'informativa esterna 11

Introduzione

1. Il presente documento enuncia una serie di principi guida per un'efficace gestione e supervisione del rischio operativo, cui dovrebbero fare riferimento le banche e le autorità di vigilanza nel valutare le politiche e le prassi applicate in tale ambito.

2. Il Comitato di Basilea per la vigilanza bancaria ("il Comitato") riconosce che l'approccio specifico adottato dalla singola banca per la gestione del rischio operativo può dipendere da una serie di fattori, tra cui la dimensione e il grado di sofisticatezza dell'istituzione, nonché la natura e la complessità delle sue operazioni. Tuttavia, malgrado tali differenze, la definizione di chiare strategie e la sorveglianza da parte del consiglio di amministrazione e dell'alta direzione, un'affermata cultura interna del rischio operativo[1] e dei controlli (fondata, tra l'altro, su esplicite linee di responsabilità e sulla separatezza delle mansioni), un efficiente sistema di reporting interno e l'apprestamento di piani di emergenza sono tutti elementi essenziali di un efficace sistema di gestione del rischio operativo per le banche di ogni tipo e dimensione. Il Comitato ritiene pertanto che i principi qui delineati stabiliscano prassi corrette applicabili da tutte le banche. L'attuale lavoro del Comitato nell'ambito del rischio operativo si rifà al suo precedente documento *Schema per i sistemi di controllo interno nelle organizzazioni bancarie* (settembre 1998).

Premessa

3. La deregolamentazione e la globalizzazione dei servizi finanziari, unitamente al progressivo affinamento della tecnologia finanziaria, stanno rendendo più complessa l'attività delle banche e, quindi, il loro profilo di rischio (ossia, il livello di rischiosità fra le varie operazioni e/o categorie di rischio di un'istituzione). L'evoluzione delle prassi bancarie induce a ritenere che i rischi diversi da quelli di credito, di tasso di interesse e di mercato possano essere sostanziali. Qui di seguito sono indicati alcuni esempi di questi nuovi e sempre più importanti fattori di rischio.

- In assenza di adeguati controlli, il crescente impiego di tecnologie altamente automatizzate può trasformare il rischio di errori manuali di trattamento dei dati in rischio di disfunzioni sistemiche, dato il sempre maggiore ricorso a sistemi globalmente integrati.
- L'espansione del commercio elettronico comporta rischi potenziali (ad esempio, frodi interne ed esterne, sicurezza dei sistemi) di cui non si ha ancora piena padronanza.
- Operazioni di acquisizione, fusione, scorporo e consolidamento di notevole entità mettono alla prova la funzionalità dei sistemi nuovi o di quelli di recente integrazione.
- La comparsa di banche operanti come prestatrici di servizi su vasta scala rende necessario il costante mantenimento di controlli interni e di sistemi di backup di alto livello.
- L'utilizzo da parte delle banche di strumenti per la mitigazione del rischio (ad esempio, garanzie collaterali, derivati su crediti, accordi di compensazione, cartolarizzazione, ecc.) al fine di ottimizzare l'esposizione ai rischi di credito e di mercato potrebbe a sua volta originare altre tipologie di rischio (ad esempio, rischio legale).
- Il crescente ricorso ad accordi di esternalizzazione e la partecipazione a sistemi di compensazione e regolamento da parte delle banche possono ridurre taluni rischi, ma comportarne altri di notevole portata.

4. Le diverse forme di rischio sopra elencate possono essere raggruppate sotto la denominazione di "rischio operativo", che il Comitato ha definito come "il rischio di perdite … derivanti da disfunzioni a livello di procedure, personale e sistemi interni, oppure da eventi esogeni[2]". Questa definizione comprende il rischio legale, ma non quelli di posizionamento strategico e di reputazione.

---

[1] Per *cultura interna del rischio operativo* si intende l'insieme di valori, atteggiamenti, competenze e comportamenti a livello individuale o collettivo che determinano l'impegno e lo stile adottati dall'impresa nella gestione del rischio operativo.

[2] La definizione è stata adottata dal settore nel quadro del lavoro del Comitato per la definizione di un requisito patrimoniale minimo a fronte del rischio operativo. Sebbene il presente documento non faccia formalmente parte dell'Accordo sul capitale, il Comitato auspica tuttavia che i principi basilari per un sano sistema di gestione del rischio operativo in esso

5. Il Comitato riconosce che il rischio operativo è un termine che può assumere significati diversi all'interno del settore bancario. Di conseguenza, a fini interni (nonché per l'applicazione del documento sulle Prassi corrette) le banche possono adottare la definizione ritenuta più confacente. Nondimeno, quale che sia il significato letterale, per assicurare un'efficace gestione e supervisione del rischio operativo è essenziale che le banche abbiano una chiara cognizione di quello che si intende con questa tipologia di rischio. È altresì importante che la definizione consideri l'intera gamma dei rischi operativi rilevanti cui la banca è esposta, nonché le più importanti cause di gravi perdite operative. Le principali fattispecie di rischio operativo che il Comitato – in collaborazione con gli operatori del settore – ha individuato come potenziale causa di perdite sostanziali sono:

- ***frode interna*** - esempi: alterazione intenzionale di dati, sottrazione di beni e valori, operazioni in proprio basate su informazioni riservate;
- ***frode esterna*** - esempi: furto, contraffazione, falsificazione, emissione di assegni a vuoto, pirateria informatica;
- ***rapporto di impiego e sicurezza sul posto di lavoro*** - esempi: risarcimenti richiesti da dipendenti, violazione delle norme a tutela della salute e sicurezza del personale, attività sindacale, pratiche discriminatorie, responsabilità civile;
- ***pratiche connesse con la clientela, i prodotti e l'attività*** - esempi: violazione del rapporto fiduciario, abuso di informazioni confidenziali, transazioni indebite effettuate per conto della banca, riciclaggio di denaro di provenienza illecita, vendita di prodotti non autorizzati;
- ***danni a beni materiali*** - esempi: atti di terrorismo e vandalismo, terremoti, incendi, inondazioni;
- ***disfunzioni e avarie di natura tecnica*** - esempi: anomalie di infrastrutture e applicazioni informatiche, problemi di telecomunicazione, interruzioni nell'erogazione di utenze;
- ***conformità esecutiva e procedurale*** - esempi: errata immissione di dati, gestione inadeguata delle garanzie, documentazione legale incompleta, indebito accesso consentito a conti di clienti, inadempimenti di controparti non clienti, controversie legali con fornitori.

Tendenze e prassi nel settore bancario

6. Nel suo lavoro sulla supervisione del rischio operativo, il Comitato ha voluto acquisire una conoscenza più approfondita delle tendenze e prassi in atto nel settore per quanto concerne la gestione di tale tipologia di rischio. Ciò ha comportato numerose riunioni con organizzazioni bancarie, indagini sulle metodologie in uso e analisi dei risultati. Grazie a tali sforzi, il Comitato ritiene di possedere una buona cognizione sia delle varie pratiche correnti nel settore bancario sia delle iniziative degli operatori volte a perfezionare i sistemi di gestione del rischio operativo.

7. Il Comitato è consapevole del fatto che la gestione di specifici rischi operativi non costituisce una novità per le banche; essa è sempre stata importante al fine di impedire le frodi, preservare l'integrità dei controlli interni, ridurre gli errori nel trattamento delle operazioni e così via. Relativamente nuova è invece la sua concezione come approccio integrale, comparabile in linea di principio – anche se non sempre nella forma – alla gestione dei rischi di credito e di mercato. Le tendenze indicate nell'introduzione del documento, congiuntamente al crescente numero di ingenti perdite per disfunzioni operative registrate in varie parti del mondo, hanno indotto le banche e le autorità di vigilanza a considerare la gestione del rischio operativo come una disciplina a se stante, analogamente a quanto già avvenuto in molti altri settori economici.

8. Per gestire il rischio operativo, le banche in passato si sono basate quasi esclusivamente sui meccanismi di controllo esistenti all'interno delle singole aree di attività, integrati dalla funzione di revisione. Sebbene tali meccanismi rimangano importanti, di recente è emersa la tendenza a istituire strutture e procedimenti mirati espressamente alla gestione del rischio operativo. A tale proposito, un numero crescente di banche è giunto alla conclusione che sistemi di questo tipo accrescono la

---

enunciati informino le aspettative dalle autorità di vigilanza nel valutare l'adeguatezza patrimoniale delle banche, ad esempio nell'ambito del processo prudenziale.

sicurezza e la solidità dell'istituzione, e sta pertanto muovendosi in direzione del trattamento del rischio operativo come categoria distinta di rischio, in analogia a quanto avviene per i rischi di credito e di mercato. Il Comitato ritiene essenziale un attivo scambio di idee fra organi di vigilanza e operatori al fine di elaborare appropriate linee guida per la gestione delle esposizioni a fronte del rischio operativo.

9. Il presente documento si articola nelle seguenti sezioni: creazione di un appropriato contesto per la gestione del rischio; gestione del rischio: individuazione, valutazione, monitoraggio e controllo/mitigazione; ruolo delle autorità di vigilanza; ruolo dell'informativa esterna.

Prassi corrette

10. Nell'elaborare queste prassi corrette il Comitato si è rifatto a suoi precedenti lavori sulla gestione di altri importanti rischi bancari – come quelli di credito, di tasso di interesse e di liquidità –, e ritiene che un analogo rigore vada applicato nel gestire il rischio operativo. Nondimeno, è chiaro che quest'ultimo differisce dagli altri rischi bancari in quanto di norma non viene assunto direttamente in vista di un profitto, ma è connaturato nello svolgimento dell'attività aziendale, e ciò influisce quindi sulle sue modalità di gestione[3]. Al tempo stesso, l'inadeguata gestione del rischio operativo può tradursi in un'immagine distorta del profilo di rischio dell'istituzione, ed esporla a pesanti perdite. Data la particolare natura del rischio operativo, ai fini di questo documento con "gestione" si intende "individuazione, valutazione, monitoraggio e controllo/mitigazione" del rischio stesso; tale definizione differisce da quella di "individuazione, misurazione, monitoraggio e controllo" adottata dal Comitato in precedenti documenti sulla gestione del rischio. Sulla falsariga dei lavori concernenti altri rischi bancari, il Comitato ha articolato questo documento in una serie di principi, enunciati qui di seguito.

Creazione di un appropriato contesto di gestione del rischio

Principio 1: Il consiglio di amministrazione[4] dovrebbe essere consapevole dei principali aspetti del rischio operativo della banca in quanto distinta categoria di rischio da gestire, e dovrebbe approvare e riesaminare periodicamente il sistema di gestione del rischio operativo. Il sistema dovrebbe fornire una definizione a livello aziendale di tale rischio e stabilire i criteri in base ai quali esso deve essere individuato, valutato, monitorato e controllato/mitigato.

Principio 2: Il consiglio di amministrazione dovrebbe assicurarsi che il sistema di gestione del rischio operativo sia sottoposto a un rigoroso e compiuto processo di auditing interno da parte di personale funzionalmente indipendente, adeguatamente formato e competente. La funzione di audit interno non dovrebbe essere direttamente responsabile della gestione del rischio operativo.

Principio 3: L'alta direzione dovrebbe avere la responsabilità di attuare il sistema di gestione del rischio operativo approvato dal consiglio di amministrazione. Il sistema dovrebbe essere costantemente applicato all'intera organizzazione bancaria, e il personale di ogni livello dovrebbe essere consapevole delle proprie responsabilità in ordine alla gestione del rischio operativo. L'alta direzione dovrebbe inoltre avere la responsabilità di definire politiche, processi e procedure aziendali per la gestione del rischio operativo in ogni prodotto, attività, processo e sistema rilevante della banca.

---

[3] Il Comitato riconosce tuttavia che in alcune aree di attività con rischio di credito o di mercato minimo (ad esempio, gestione di patrimoni, servizi di pagamento e regolamento), la decisione di assumere rischi operativi – o di competere sulla base della propria capacità di gestire e "prezzare" efficacemente tali rischi – costituisce parte integrante della strategia di rischio/rendimento adottata dalla banca.

[4] Questo documento fa riferimento a una struttura decisionale costituita da consiglio di amministrazione e alta direzione. Il Comitato è consapevole delle notevoli differenze legali e regolamentari esistenti fra i vari paesi per quanto concerne le funzioni di tali organi. In alcuni paesi il consiglio di amministrazione ha il compito principale – se non esclusivo – di sovrintendere all'operato dell'organo esecutivo (alta direzione o direzione generale) per assicurare che questo assolva i suoi compiti. Per tale motivo, in alcuni casi tale organo è designato come "supervisory board". In altri paesi il consiglio ha competenze più estese, in quanto definisce le linee generali della gestione aziendale. Alla luce di tali differenze, in questo documento i termini "consiglio di amministrazione" e "alta direzione" non individuano entità legalmente definite, ma semplicemente i due organi decisionali operanti in una banca.

Gestione del rischio: individuazione, valutazione, monitoraggio e controllo/mitigazione

Principio 4: Le banche dovrebbero individuare e valutare il rischio operativo insito in ogni prodotto, attività, processo e sistema rilevante. Esse dovrebbero inoltre assicurarsi che prima di introdurre nuovi prodotti, processi e sistemi o di intraprendere nuove attività, il connesso rischio operativo sia sottoposto ad adeguate procedure di valutazione.

Principio 5: Le banche dovrebbero istituire un processo di regolare monitoraggio dei profili di rischio operativo e delle esposizioni a perdite rilevanti. Dovrebbe essere operante una regolare segnalazione delle informazioni pertinenti all'alta direzione e al consiglio di amministrazione, che promuova un'attiva gestione del rischio operativo.

Principio 6: Le banche dovrebbero disporre di politiche, processi e procedure per controllare e/o mitigare i rischi operativi rilevanti. Esse dovrebbero valutare periodicamente le strategie per il controllo e la riduzione del rischio, nonché conformare – mediante appropriate strategie – il loro profilo di rischio operativo alla propensione al rischio e al profilo di rischio complessivi.

Principio 7: Le banche dovrebbero predisporre piani di emergenza e di continuità operativa per assicurare la prosecuzione dell'attività e minimizzare le perdite in caso di gravi disfunzioni operative.

Ruolo delle autorità di vigilanza

Principio 8: Le autorità di vigilanza bancaria dovrebbero richiedere che tutte le banche, a prescindere dalla loro dimensione, dispongano di un efficace sistema per individuare, valutare, monitorare e controllare/mitigare i rischi operativi, e che esso sia inquadrato in un approccio complessivo alla gestione del rischio.

Principio 9: Le autorità di vigilanza dovrebbero condurre, in modo diretto o indiretto, regolari valutazioni indipendenti delle politiche, procedure e prassi applicate dalla banca nella gestione del rischio operativo. Esse dovrebbero inoltre assicurarsi che sussistano adeguati meccanismi di segnalazione che permettano loro di tenersi informate sugli sviluppi intervenuti nelle banche.

Ruolo dell'informativa esterna

Principio 10: Le banche dovrebbero fornire e pubblicare informazioni in modo da consentire al mercato di valutare il loro approccio alla gestione del rischio operativo.

Creazione di un appropriato contesto di gestione del rischio

11. Una conoscenza e una gestione inadeguate del rischio operativo – una tipologia di rischio presente nella quasi totalità delle operazioni e attività bancarie – aumentano fortemente la probabilità che taluni rischi sfuggano all'individuazione e al controllo. Il consiglio di amministrazione e l'alta direzione hanno entrambi la responsabilità di creare una cultura organizzativa che assegni un'elevata priorità all'efficace gestione del rischio operativo e all'osservanza di rigorosi controlli sull'operatività. La gestione del rischio operativo è più efficace laddove la cultura aziendale pone l'accento su elevati standard deontologici a tutti i livelli dell'istituzione. Il consiglio di amministrazione e l'alta direzione dovrebbero promuovere una cultura organizzativa che esalti, nelle parole e nei fatti, l'integrità morale di ogni dipendente nel condurre gli affari della banca.

Principio 1: Il consiglio di amministrazione dovrebbe essere consapevole dei principali aspetti del rischio operativo della banca in quanto distinta categoria di rischio da gestire, e dovrebbe approvare e riesaminare periodicamente il sistema di gestione del rischio operativo. Il sistema dovrebbe fornire una definizione a livello aziendale di tale rischio e stabilire i criteri in base ai quali esso deve essere individuato, valutato, monitorato e controllato/mitigato.

12. Il consiglio di amministrazione dovrebbe approvare l'attuazione a livello aziendale di un sistema esplicitamente inteso a gestire il rischio operativo in quanto distinta tipologia di rischio per la sicurezza e la solidità della banca. Il consiglio dovrebbe fornire all'alta direzione chiari orientamenti e direttive circa i principi su cui si basa tale sistema, nonché autorizzare le corrispondenti politiche definite dalla direzione stessa.

13. Il sistema di gestione del rischio operativo deve basarsi su un'appropriata definizione che specifichi chiaramente ciò che costituisce rischio operativo per la banca. Il sistema dovrebbe considerare la propensione e la tolleranza della banca verso il rischio operativo, come precisato nelle direttive e nelle priorità stabilite dall'istituzione nella gestione di tale rischio, nonché la misura e il modo in cui esso viene trasferito all'esterno. Il sistema dovrebbe anche comprendere le politiche che definiscono l'approccio della banca nell'individuare, valutare, monitorare e controllare/mitigare le esposizioni. Il grado di formalizzazione e di tecnicità del sistema dovrebbe essere commisurato al profilo di rischio della banca.

14. Il consiglio di amministrazione ha la responsabilità di istituire una struttura direzionale in grado di far applicare il sistema di gestione del rischio operativo adottato dalla banca. Poiché un aspetto rilevante della gestione di tale rischio concerne l'esistenza di rigorosi controlli interni, è particolarmente importante che il consiglio istituisca chiare linee di competenza, di responsabilità e di reporting. Occorre inoltre assicurare la separazione tra le funzioni di controllo e quelle operative, e fornire loro sostegno al fine di evitare conflitti di interesse. Il sistema dovrebbe altresì specificare i processi fondamentali che la banca deve porre in atto per gestire il rischio operativo.

15. Il consiglio di amministrazione dovrebbe riesaminare periodicamente il sistema per assicurarsi che la banca stia gestendo i rischi operativi derivanti da cambiamenti delle condizioni del mercato e da altri fattori esterni, o dall'introduzione di nuovi prodotti, attività e sistemi. Tale riesame dovrebbe anche mirare a integrare quelle innovazioni nella gestione del rischio operativo che risultino appropriate per l'attività, i sistemi operativi e le procedure della banca. Se necessario, il consiglio dovrebbe assicurarsi che il sistema di gestione del rischio operativo venga modificato alla luce di tale analisi, affinché esso possa cogliere tutti i rischi sostanziali.

Principio 2: Il consiglio di amministrazione dovrebbe assicurarsi che il sistema di gestione del rischio operativo sia sottoposto a un rigoroso e compiuto processo di auditing interno da parte di personale funzionalmente indipendente, adeguatamente formato e competente. La funzione di audit interno non dovrebbe essere direttamente responsabile della gestione del rischio operativo.

16. Le banche dovrebbero avere in funzione un adeguato processo di audit interno per verificare che le politiche e le procedure operative siano dovutamente applicate[5]. Il consiglio (sia direttamente sia per mezzo del proprio comitato di revisione) dovrebbe assicurarsi che la portata e la frequenza di

[5] Il documento *Internal Audit in Banks and the Supervisor's Relationship with Auditors*, edito dal Comitato nell'agosto 2001, descrive il ruolo dell'audit interno ed esterno.

tali verifiche siano appropriate all'esposizione al rischio. La funzione di auditing dovrebbe attestare periodicamente che il sistema di gestione del rischio operativo della banca venga applicato in modo corretto in tutta l'azienda.

17. Qualora la funzione di auditing sia coinvolta nella sorveglianza del sistema di gestione del rischio operativo, il consiglio dovrebbe assicurarsi che venga preservata la sua indipendenza. Questa potrebbe essere compromessa da una partecipazione diretta al processo di gestione del rischio operativo. La funzione di auditing può fornire preziose indicazioni ai quadri preposti alla gestione del rischio, ma non dovrebbe avere responsabilità dirette in questo ambito. Il Comitato riconosce che, nella pratica, la funzione di auditing può avere in talune banche (specie quelle di minori dimensioni) una responsabilità iniziale nella definizione di un programma di gestione del rischio operativo. In questi casi, le banche dovrebbero far sì che la responsabilità della gestione corrente di tale rischio sia assegnata quanto prima ad altre funzioni.

Principio 3: L'alta direzione dovrebbe avere la responsabilità di attuare il sistema di gestione del rischio operativo approvato dal consiglio di amministrazione. Il sistema dovrebbe essere costantemente applicato all'intera organizzazione bancaria, e il personale di ogni livello dovrebbe essere consapevole delle proprie responsabilità in ordine alla gestione del rischio operativo. L'alta direzione dovrebbe inoltre avere la responsabilità di definire politiche, processi e procedure aziendali per la gestione del rischio operativo in ogni prodotto, attività, processo e sistema rilevante della banca.

18. L'alta direzione dovrebbe tradurre i principi del sistema di gestione del rischio operativo stabiliti dal consiglio di amministrazione in specifiche politiche, procedure e processi attuabili e verificabili nell'ambito delle diverse unità operative della banca. Anche se ogni livello di management è responsabile dell'appropriatezza e dell'efficacia di politiche, processi, procedure e controlli nella sfera di propria competenza, l'alta direzione dovrebbe stabilire chiare linee gerarchiche, funzionali e di reporting che incoraggino queste responsabilità, assicurandosi altresì che siano disponibili congrue risorse per gestire il rischio operativo in modo efficace. Inoltre, l'alta direzione dovrebbe valutare l'adeguatezza del processo di sorveglianza in relazione ai rischi insiti nelle attività delle varie unità.

19. L'alta direzione dovrebbe assicurarsi che le attività della banca vengano svolte da personale qualificato – che disponga di adeguata esperienza e capacità tecnica, nonché delle necessarie risorse – e che i quadri cui spettano funzioni di monitoraggio e verifica della conformità delle politiche aziendali siano funzionalmente indipendenti dalle unità da essi controllate. La direzione dovrebbe assicurarsi che la politica di gestione del rischio operativo della banca sia stata comunicata con chiarezza al personale di ogni livello nelle unità in cui vi siano rischi operativi rilevanti.

20. L'alta direzione dovrebbe assicurarsi che il personale con responsabilità di gestione del rischio operativo comunichi in modo efficace con quello preposto ai rischi di credito, di mercato e di altro tipo, nonché con le funzioni addette all'acquisto di servizi esterni, quali quelli assicurativi e di outsourcing. La mancanza di un'adeguata comunicazione può originare importanti omissioni o sovrapposizioni nel sistema aziendale di gestione del rischio.

21. L'alta direzione dovrebbe inoltre assicurarsi che le politiche di retribuzione seguite dalla banca siano coerenti con la sua propensione al rischio. I sistemi retributivi che di fatto incentivano lo staff a discostarsi dalle strategie della banca (ad esempio, superando i limiti di esposizione) indeboliscono i processi di gestione del rischio.

22. Cura speciale dovrebbe essere prestata alla qualità dei controlli documentali e alle modalità di trattamento delle operazioni. Politiche, procedure e processi collegati a tecnologie avanzate a sostegno di alti volumi di transazioni, in particolare, dovrebbero essere ben documentati e resi noti a tutto il personale interessato.

Gestione del rischio: individuazione, valutazione, monitoraggio e controllo/mitigazione

Principio 4: Le banche dovrebbero individuare e valutare il rischio operativo insito in ogni prodotto, attività, processo e sistema rilevante. Esse dovrebbero inoltre assicurarsi che prima di introdurre nuovi prodotti, processi e sistemi o di intraprendere nuove attività, il connesso rischio operativo sia sottoposto ad adeguate procedure di valutazione.

23. L'individuazione dei rischi è di importanza cruciale per la successiva definizione di un efficace processo di monitoraggio e controllo del rischio operativo. Per una corretta individuazione dei rischi devono essere considerati sia i fattori interni (quali struttura della banca, natura delle attività

svolte, qualità del personale, modifiche organizzative, rotazione dell'organico) sia quelli esterni (ad esempio, evoluzione del settore bancario, progressi tecnologici) che potrebbero incidere negativamente sugli obiettivi aziendali.

24. Oltre a individuare i rischi potenzialmente più gravi, le banche dovrebbero valutare la propria vulnerabilità a tali rischi. Una corretta valutazione consente alla banca di conoscere meglio il suo profilo di rischio e di allocare in modo più efficiente le risorse per la gestione dei rischi.

25. Le banche impiegano vari strumenti per individuare e valutare il rischio operativo, fra i quali:

- auto-diagnosi: analisi delle operazioni e delle attività della banca a fronte di un ventaglio di potenziali vulnerabilità al rischio operativo. Questo metodo è di natura endogena e si avvale spesso di liste di controllo e/o gruppi di lavoro per individuare i punti di forza e di debolezza del contesto di rischio operativo dell'istituzione. Le matrici valutative ("scorecard"), ad esempio, costituiscono uno strumento per tradurre giudizi qualitativi in parametri quantitativi in base ai quali viene assegnata una graduazione ai diversi tipi di esposizione al rischio operativo. Talune matrici possono riferirsi a rischi peculiari di una determinata area operativa e altre ricomprendere rischi che attraversano trasversalmente vari ambiti di attività. Esse possono riguardare, oltre ai fattori di rischio, anche le corrispondenti tecniche di mitigazione. Le "scorecard" sono impiegabili per allocare capitale economico alle diverse linee operative in relazione ai risultati ottenuti nel gestire e controllare i vari aspetti del rischio operativo;
- mappatura dei rischi: classificazione di unità operative, funzioni organizzative e flussi di processi in base alla tipologia di rischio. L'esercizio può rivelare eventuali aree critiche e facilitare così la definizione delle priorità per i successivi interventi della direzione;
- indicatori di rischio: grandezze statistiche e/o numeriche, spesso di carattere finanziario, in grado di fornire utili elementi conoscitivi sulla posizione di rischio di una banca. Essi vengono generalmente sottoposti a un riesame periodico (ad esempio, con cadenza mensile o trimestrale) allo scopo di sollecitare l'attenzione della banca sulla possibile insorgenza di aree critiche. Esempi di indicatori di rischio sono il numero delle transazioni mancate, i tassi di rotazione del personale, la frequenza e/o la gravità di errori e omissioni;
- misurazione: alcune banche hanno iniziato a quantificare l'esposizione al rischio operativo ricorrendo a vari metodi. Ad esempio, i dati storici sulle perdite subite dalla banca possono fornire utili informazioni per valutare l'esposizione e definire politiche di controllo/mitigazione. Affinché tali dati possano essere validamente impiegati, è necessario istituire uno schema che rilevi sistematicamente la frequenza, la gravità e altri aspetti rilevanti dei singoli eventi generatori di perdita. Alcune banche integrano inoltre tali dati con analoghi riscontri di altre imprese del settore, analisi di scenari e fattori di valutazione del rischio.

Principio 5: Le banche dovrebbero istituire un processo di regolare monitoraggio dei profili di rischio operativo e delle esposizioni a perdite rilevanti. Dovrebbe essere operante una regolare segnalazione delle informazioni pertinenti all'alta direzione e al consiglio di amministrazione, che promuova un'attiva gestione del rischio operativo.

26. Per poter gestire in modo adeguato il rischio operativo è essenziale un efficace processo di monitoraggio. Il regolare monitoraggio facilita la pronta individuazione e correzione di eventuali carenze relative a politiche, processi e procedure in materia di gestione del rischio operativo. A sua volta, ciò può ridurre considerevolmente la potenziale frequenza e/o gravità degli eventi di perdita.

27. Oltre a monitorare gli eventi di perdita, le banche dovrebbero definire indicatori atti a segnalare anticipatamente l'accentuarsi dei rischi di perdite future. Tali indicatori (definiti spesso "indicatori chiave di rischio" o "indicatori di early warning") dovrebbero pertanto essere prospettici, e potrebbero considerare potenziali fonti di rischio operativo quali la rapida espansione dell'attività, l'introduzione di nuovi prodotti, la rotazione del personale, blocchi operativi, tempi di fermo dei sistemi e così via. Allorché a tali indicatori sono direttamente collegati determinati valori-soglia, il processo di monitoraggio può contribuire efficacemente a individuare i rischi sostanziali in modo trasparente, consentendo alla banca di reagire in maniera adeguata.

28. La frequenza del monitoraggio dovrebbe rispecchiare i rischi incorsi, nonché la frequenza e la natura dei cambiamenti nel contesto operativo. Il monitoraggio dovrebbe costituire parte integrante dell'attività della banca. I risultati di questa attività dovrebbero entrare a far parte dei rendiconti trasmessi alla direzione e al consiglio di amministrazione, così come le analisi di conformità redatte dalle funzioni di auditing interno e/o di gestione del rischio. Anche le eventuali valutazioni espresse

dall'autorità di vigilanza (e/o a questa destinate) potrebbero informare l'attività di monitoraggio, e dovrebbero parimenti essere oggetto di comunicazione interna all'alta direzione e al consiglio di amministrazione, ove necessario.

29. L'alta direzione dovrebbe ricevere regolari rapporti dalle aree competenti, come ad esempio unità operative, gruppi di lavoro, strutture di gestione del rischio operativo, audit interno. Tali rapporti dovrebbero contenere dati finanziari, operativi e di riscontro di origine interna, nonché informazioni esterne di mercato su fatti e circostanze rilevanti ai fini del processo decisionale. Essi dovrebbero essere distribuiti agli appropriati livelli di direzione e alle unità della banca potenzialmente esposte all'impatto di fattori critici, e analizzare compiutamente le eventuali aree problematiche, sollecitando pronte misure correttive. Affinché tali segnalazioni siano utili e affidabili, la direzione dovrebbe regolarmente verificare la tempestività, l'accuratezza e la rilevanza dei sistemi di reporting e dei controlli interni più in generale. Per valutare l'utilità e l'affidabilità dei rapporti interni, la direzione può anche avvalersi di rendiconti prodotti da soggetti esterni (società di revisione, organi di vigilanza). L'informativa in materia di rischio dovrebbe essere analizzata nell'ottica di migliorare la performance della gestione del rischio, nonché di definire nuove politiche, procedure e prassi in questo ambito.

30. In generale, il consiglio di amministrazione dovrebbe ricevere sufficienti informazioni di alto livello che gli permettano di avere una chiara cognizione del profilo di rischio complessivo della banca e di valutarne le implicazioni sul piano gestionale e strategico.

Principio 6: Le banche dovrebbero disporre di politiche, processi e procedure per controllare e/o mitigare i rischi operativi rilevanti. Esse dovrebbero valutare periodicamente le strategie per il controllo e la riduzione del rischio, nonché conformare – mediante appropriate strategie – il loro profilo di rischio operativo alla propensione al rischio e al profilo di rischio complessivi.

31. Le attività di controllo mirano ad affrontare i rischi operativi individuati dalla banca[6]. Per i rischi controllabili, questa dovrebbe decidere se desideri impiegare procedure di controllo e altre tecniche appropriate, ovvero assumere i rischi stessi. Per quelli non controllabili, la banca dovrebbe decidere se accollarseli, ridurre la portata dell'attività in questione ovvero dismetterla in toto. Oltre a stabilire i processi e le procedure di controllo, le banche dovrebbero disporre di uno schema che assicuri l'osservanza di un insieme documentato di politiche interne concernenti il sistema di gestione del rischio. Tale sistema potrebbe contemplare:

- esami dei progressi realizzati nel conseguimento degli obiettivi stabiliti, da effettuarsi a cura dei vertici della banca;
- verifica della conformità con i controlli di direzione;
- politiche, processi e procedure concernenti l'esame, il trattamento e la risoluzione di casi di non conformità;
- un sistema di approvazioni e autorizzazioni documentate per garantire il rispetto di appropriate linee di responsabilità.

32. Pur rivestendo di per sé un'importanza cruciale, un sistema di politiche e procedure formalizzate e documentate deve essere integrato da una solida cultura del controllo, che promuova comportamenti corretti nella gestione del rischio. Spetta al consiglio di amministrazione e all'alta direzione la responsabilità di introdurre tale cultura, che deve costituire parte integrante delle normali attività della banca. I controlli consentono di reagire prontamente al mutare delle condizioni, evitando di incorrere in costi superflui.

33. Un efficace sistema di controllo interno presuppone inoltre che vi sia un'appropriata separatezza delle funzioni e che al personale non vengano attribuite responsabilità suscettibili di creare conflitti di interesse. L'assegnazione di compiti confliggenti a singoli individui o gruppi può consentire loro di celare perdite, errori o azioni discutibili. Pertanto, le aree che comportano un potenziale conflitto di interesse dovrebbero essere individuate, ridotte al minimo e sottoposte ad attento monitoraggio e controllo indipendente.

---

[6] Per maggiori dettagli, si veda *Schema per i sistemi di controllo interno nelle organizzazioni bancarie*, Comitato di Basilea per la vigilanza bancaria, settembre 1998.

34. Oltre alla separazione dei compiti, le banche dovrebbero assicurare di disporre di ulteriori prassi interne per controllare il rischio operativo. Fra tali prassi figurano:

- un rigoroso monitoraggio del rispetto dei limiti o delle soglie di esposizione al rischio;
- il mantenimento di presidi a protezione dell'accesso ai locali della banca e dell'utilizzo di beni e documenti;
- l'accertamento dei requisiti di competenza e formazione professionale dei dipendenti;
- l'individuazione di linee di attività o di prodotto la cui redditività sembra discostarsi da quella ragionevolmente attesa (ad esempio, nell'ipotesi in cui un'attività di negoziazione a rischio contenuto e a basso margine produca rendimenti tali da indurre il sospetto che questi siano stati conseguiti violando i controlli interni);
- la regolare verifica e riconciliazione delle transazioni e dei conti.

Negli anni recenti la mancata adozione di tali prassi si è tradotta per alcune banche in ingenti perdite operative.

35. Il rischio operativo può risultare accentuato nelle banche che hanno avviato nuove attività o linee di prodotto (specie se queste non sono in linea con le strategie seguite per il core business), hanno fatto ingresso in mercati poco familiari o si sono impegnate in operazioni geograficamente distanti dalla propria sede. Si aggiunga che, nella gran parte di questi casi, le banche non provvedono ad adeguare l'infrastruttura per la gestione e il controllo del rischio all'espansione dell'attività operativa. Alcune delle perdite più rilevanti registrate negli ultimi anni hanno riguardato aziende in cui era presente almeno una delle circostanze suddette. Di conseguenza, è fondamentale che nelle banche in cui ricorrono siffatte circostanze venga prestata particolare attenzione ai processi interni di controllo.

36. Taluni rischi operativi hanno una bassa probabilità statistica ma un fortissimo impatto potenziale in termini finanziari. Inoltre, non tutti i fattori di rischio possono essere controllati (vedi le calamità naturali). Per ridurre l'esposizione a questi eventi, oppure la loro frequenza e/o gravità, possono essere impiegati strumenti o programmi di mitigazione del rischio. Ad esempio, mediante coperture assicurative – in particolare quelle che prevedono clausole di pronto e certo risarcimento – è possibile esternalizzare il rischio di perdite "a bassa frequenza ed elevato impatto" causate da eventi quali il pagamento di danni a terzi per errori, omissioni, smarrimento di valori, frodi di dipendenti o di parti terze e calamità naturali.

37. Tuttavia, le banche dovrebbero considerare gli strumenti di mitigazione non tanto come un sostituto, quanto il complemento di un rigoroso sistema di controllo interno del rischio operativo. L'esistenza di meccanismi in grado di rilevare e correggere prontamente eventuali errori nella gestione del rischio può ridurre considerevolmente le esposizioni. Si dovrà inoltre valutare attentamente la misura in cui strumenti di mitigazione quali le assicurazioni attenuino realmente i rischi, o non li trasferiscano invece ad altri settori e aree, o non ne creino addirittura di nuovi (ad esempio, rischio giuridico o di controparte).

38. Parimenti importanti per la mitigazione del rischio sono gli investimenti in tecnologie operative e di sicurezza informatica appropriate. Tuttavia, le banche devono essere consapevoli del fatto che un'accresciuta automazione può trasformare le perdite ad alta frequenza e basso impatto in altre a bassa frequenza ed elevato impatto. Queste ultime possono derivare da un blocco o da un'estesa disfunzione del servizio dovuta a motivi interni o a fattori non controllabili direttamente dalla banca (ad esempio, eventi esterni). Tali problemi possono causare gravi difficoltà all'istituzione e mettere a repentaglio la sua capacità di svolgere le attività fondamentali. Come indicato nel Principio 7, le banche dovrebbero predisporre piani di emergenza e di continuità operativa che affrontino questo rischio.

39. Le banche dovrebbero altresì definire politiche per gestire i rischi connessi con l'outsourcing. L'esternalizzazione di attività può abbassare il profilo di rischio trasferendo certe funzioni a soggetti esterni dotati di maggiori competenze e capacità specialistiche per controllare i rischi connessi. Tuttavia, il ricorso a parti terze non diminuisce la responsabilità del consiglio di amministrazione e dell'alta direzione di assicurare che tali funzioni siano svolte in modo sicuro e corretto, e nel rispetto della normativa vigente. L'outsourcing dovrebbe basarsi su rigorose convenzioni e/o accordi contrattuali che stabiliscano una chiara suddivisione delle responsabilità fra prestatori esterni dei servizi e banca utente. Inoltre, è necessario che vengano gestiti i relativi rischi residuali, fra cui la possibilità di disfunzioni nell'erogazione dei servizi stessi.

40. A seconda dell'importanza e della natura dell'attività, la banca dovrebbe conoscere le potenziali ricadute sulla propria operatività e sulla clientela derivanti da possibili anomalie nei servizi prestati da fornitori esterni, terzi o gestori intragruppo, siano esse dovute a disfunzioni tecniche o a problemi gestionali dei prestatori di servizi. Il consiglio di amministrazione e la direzione dovrebbero assicurarsi che i diritti e gli obblighi dei contraenti siano chiaramente definiti, compresi e giuridicamente efficaci. Nel quadro della valutazione del rischio dovrebbe essere considerata esplicitamente la responsabilità legale e la capacità finanziaria delle parti terze di indennizzare la banca a seguito di errori, negligenze e altre disfunzioni operative. Le banche dovrebbero effettuare test preliminari di "dovuta diligenza" e monitorare l'operato dei fornitori di servizi, specie di quelli che difettano di esperienza nel contesto regolamentato dell'attività bancaria. Per le funzioni di importanza critica, la banca può ritenere necessario predisporre piani di emergenza che considerino la disponibilità di fornitori alternativi, nonché i costi e le risorse connessi con l'eventuale ricorso a questi ultimi, anche a brevissimo termine.

41. In certi casi, la banca può decidere di mantenere un dato livello di rischio operativo, ovvero di autotutelarsi contro tale rischio. In questi casi, e se il rischio è sostanziale, la decisione dovrebbe essere trasparente all'interno dell'istituzione e conforme alla strategia operativa e alla propensione al rischio adottate a livello aziendale.

Principio 7: Le banche dovrebbero predisporre piani di emergenza e di continuità operativa per assicurare la prosecuzione dell'attività e minimizzare le perdite in caso di gravi disfunzioni operative.

42. Per ragioni che possono essere al di fuori del controllo della banca, in seguito a un grave evento questa può trovarsi nell'impossibilità di assolvere in tutto o in parte le proprie obbligazioni, specie se le sue infrastrutture logistiche, telecomunicative o informatiche sono state danneggiate o rese inaccessibili. A sua volta, ciò può provocare ingenti perdite finanziarie per la banca stessa, come pure disfunzioni di più ampia portata nel sistema finanziario, per esempio attraverso il canale del sistema dei pagamenti. Questa possibilità rende necessario l'apprestamento di piani di continuità operativa e di emergenza ("disaster recovery") che considerino vari scenari plausibili cui la banca potrebbe trovarsi esposta, tenuto conto della dimensione e della complessità delle sue operazioni.

43. Le banche dovrebbero individuare i processi di importanza critica, compresi quelli dipendenti da fornitori esterni o da altre parti terze, per i quali sarebbe prioritario un rapido ripristino della funzionalità. Per questi processi dovrebbero essere individuati meccanismi alternativi che consentano di riattivare il servizio in caso di avaria. Particolare attenzione dovrebbe essere prestata alla capacità di recuperare i supporti documentali – fisici o elettronici – necessari per la prosecuzione dell'attività. Qualora il sistema di backup sia situato in locali esterni alla banca, oppure l'attività di quest'ultima debba essere trasferita in altra sede, è importante che le strutture di emergenza siano collocate a un'adeguata distanza da quelle principali, affinché sia ridotto al minimo il rischio che esse diventino parimenti inservibili in caso di sinistro.

44. Le banche dovrebbero riesaminare regolarmente i piani di continuità operativa e di emergenza al fine di assicurarne la coerenza con le attività e le strategie gestionali correnti. Inoltre, tali piani dovrebbero essere sottoposti a test periodici per accertarne l'effettiva applicabilità anche nell'improbabile ipotesi di una grave turbativa all'operatività della banca.

Ruolo delle autorità di vigilanza

Principio 8: Le autorità di vigilanza bancaria dovrebbero richiedere che tutte le banche, a prescindere dalla loro dimensione, dispongano di un efficace sistema per individuare, valutare, monitorare e controllare/mitigare i rischi operativi, e che esso sia inquadrato in un approccio complessivo alla gestione del rischio.

45. Le autorità di vigilanza dovrebbero richiedere alle banche di mettere a punto sistemi di gestione del rischio operativo conformi alle linee guida enunciate in questo documento e commisurati alla dimensione, alla complessità e al profilo di rischio dell'azienda. Nella misura in cui i rischi operativi intaccano la sicurezza e la solidità delle banche, gli organi di vigilanza hanno il compito di incoraggiare queste ultime a elaborare e impiegare tecniche più perfezionate per la gestione di tali rischi.

Principio 9: Le autorità di vigilanza dovrebbero condurre, in modo diretto o indiretto, regolari valutazioni indipendenti delle politiche, procedure e prassi applicate dalla banca nella gestione del rischio operativo. Esse dovrebbero inoltre assicurarsi che sussistano adeguati meccanismi

di segnalazione che permettano loro di tenersi informate sugli sviluppi intervenuti nelle banche.

46. La valutazione indipendente dell'autorità di vigilanza in merito alla gestione del rischio operativo in una banca dovrebbe considerare, fra gli altri, i seguenti elementi:

- l'efficacia del processo di gestione dei rischi e dell'intero sistema dei meccanismi di controllo;
- i metodi per monitorare e segnalare il profilo di rischio, compresi i dati sulle perdite operative e altri indicatori di rischio potenziale;
- le procedure per affrontare in modo tempestivo ed efficace gli eventi critici e le vulnerabilità;
- i sistemi interni di controllo, analisi e revisione volti ad assicurare l'integrità del processo complessivo di gestione del rischio;
- l'efficacia degli strumenti di mitigazione del rischio, come l'impiego di coperture assicurative;
- la qualità e l'esaustività dei piani di continuità operativa e di emergenza ("disaster recovery");
- i procedimenti applicati per valutare l'adeguatezza patrimoniale complessiva in relazione al profilo di rischio operativo e, ove appropriato, agli obiettivi interni di allocazione del capitale.

47. Qualora la banca faccia parte di un gruppo finanziario, le autorità di vigilanza dovrebbero inoltre assicurarsi che siano in funzione procedure atte a garantire che il rischio operativo viene gestito in modo adeguato e integrato a livello di gruppo. Tale valutazione può richiedere la collaborazione e lo scambio di informazioni con altri organi prudenziali, sulla base di procedure prestabilite. Le autorità di vigilanza possono eventualmente decidere di farsi assistere da revisori esterni in tale processo.

48. Le carenze accertate durante il processo di controllo prudenziale possono essere affrontate mediante varie modalità di azione. Le autorità dovrebbero impiegare gli strumenti più confacenti alla particolare situazione della banca e al suo contesto operativo. Al fine di essere costantemente informate sul rischio operativo, esse possono richiedere che vengano istituiti meccanismi di segnalazione diretta con la banca e i revisori esterni (ad esempio, potrebbe essere instaurata la prassi di trasmettere all'autorità di vigilanza i rapporti interni sulla gestione del rischio operativo destinati alla direzione della banca).

49. Essendo generalmente riconosciuto che i sistemi integrali di gestione del rischio operativo sono tuttora in fase evolutiva presso molti istituti, le autorità di vigilanza dovrebbero assumere un ruolo attivo nell'incoraggiare le iniziative assunte dalle banche, seguendo e valutando i progressi recenti e i piani di sviluppo futuro. Queste iniziative possono così essere poste a confronto con quelle attuate da altre istituzioni, allo scopo di fornire alle banche stesse utili riscontri sullo stato dei lavori intrapresi. Inoltre, nella misura in cui si conoscono le ragioni per cui alcuni tentativi si sono rivelati inefficaci, tali informazioni potrebbero essere diffuse – al livello di dettaglio ritenuto opportuno – per facilitare il processo di programmazione. Le autorità di vigilanza dovrebbero parimenti valutare la misura in cui la gestione del rischio operativo di una banca è stata integrata a livello dell'intera organizzazione, e ciò per assicurare un efficace controllo di tale rischio in seno alle diverse aree di attività, istituire chiare linee di comunicazione e di responsabilità, nonché incoraggiare una costante auto-diagnosi delle prassi in atto e la ricerca di eventuali nuovi strumenti di attenuazione del rischio.

Ruolo dell'informativa esterna

Principio 10: Le banche dovrebbero fornire e pubblicare informazioni in modo da consentire al mercato di valutare il loro approccio alla gestione del rischio operativo.

50. Il Comitato ritiene che la frequente pubblicazione di informazioni aggiornate e rilevanti da parte delle banche possa condurre a una migliore disciplina di mercato e, quindi, a una più efficace gestione del rischio. La portata dell'informativa dovrebbe essere commisurata al volume, al profilo di rischio e alla complessità delle operazioni della banca.

51. L'area dell'informativa sul rischio operativo non è ancora ben definita, soprattutto a causa del fatto che le banche stanno tuttora elaborando tecniche di valutazione per questo tipo di rischio. Nell'opinione del Comitato, peraltro, una banca dovrebbe pubblicare informazioni sul proprio sistema di gestione del rischio operativo in misura tale da consentire agli investitori e alle controparti di determinare se essa sia in grado di individuare, valutare, monitorare e controllare/mitigare la sua esposizione a questa tipologia di rischio.