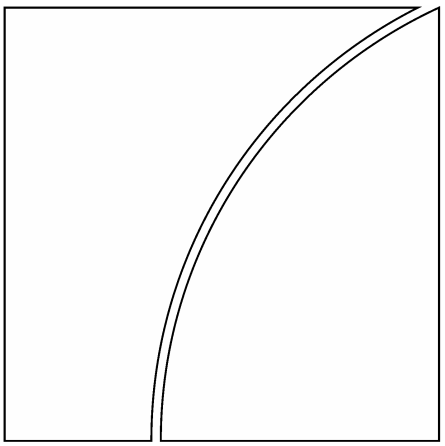
Basler Ausschuss für Bankenaufsicht



Management operationeller Risiken – Praxisempfehlungen für Banken und Bankenaufsicht

Februar 2003

BANK FÜR INTERNATIONALEN ZAHLUNGSAUSGLEICH

Bezug von Publikationen oder Aktualisierung der Versandliste:

Basler Ausschuss für Bankenaufsicht
Sekretariat
c/o Bank für Internationalen Zahlungsausgleich
CH-4002 Basel, Schweiz

E-mail: publications@bis.org

Fax: +41 61 280 9100

Diese Publikation ist auch auf der BIZ-Website verfügbar (www.bis.org).

Auch in Englisch, Französisch, Spanisch und Italienisch veröffentlicht.

Arbeitsgruppe Risikomanagement des Basler Ausschusses für Bankenaufsicht

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

Banque Nationale de Belgique, Brüssel	Dominique Gressens
Commission Bancaire et Financière, Brüssel	Jos Meuleman
Office of the Superintendent of Financial Institutions, Ottawa	Jeff Miller
Commission Bancaire, Paris	Laurent Le Mouël
Deutsche Bundesbank, Frankfurt am Main	Magdalene Heid Karin Sagner-Kaiser
Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn	Kirsten Straus
Banca d'Italia, Rom	Claudio D'Auria Fabrizio Leandri Sergio Sorrentino
Bank of Japan, Tokio	Satoshi Yamaguchi
Financial Services Agency, Tokio	Hirokazu Matsushima
Commission de Surveillance du Secteur Financier, Luxemburg	Davy Reinard
De Nederlandsche Bank, Amsterdam	Klaas Knot
Banco de España, Madrid	Guillermo Rodriguez-Garcia Juan Serrano
Finansinspektionen, Stockholm	Jan Hedquist
Sveriges Riksbank, Stockholm	Thomas Flodén
Eidgenössische Bankenkommission, Bern	Martin Sprenger
Financial Services Authority, London	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
Europäische Zentralbank, Frankfurt am Main	Panagiotis Strouzas
Europäische Kommission, Brüssel	Michel Martino Melania Savino
Sekretariat des Basler Ausschusses für Bankenaufsicht, Bank für Internationalen Zahlungsausgleich	Stephen Senior

Inhalt

Management operationeller Risiken – Praxisempfehlungen für Banken und Bankenaufsicht

Einleitung

1. Die im folgenden Papier dargelegten Grundsätze bilden ein Rahmenkonzept zur effektiven Handhabung und Beaufsichtigung operationeller Risiken, anhand dessen Banken und Aufsichtsinstanzen Strategien und Methoden zum Management operationeller Risiken bewerten können.

2. Der Basler Ausschuss für Bankenaufsicht („Ausschuss") weiss, dass der spezifische Ansatz, den eine Bank für ihr Management operationeller Risiken wählt, von vielfältigen Faktoren abhängt, u.a. ihrer Grösse und Versiertheit sowie der Art und Komplexität ihrer Tätigkeiten. Für jede Bank, gleich welcher Grösse und Reichweite, sind jedoch trotz dieser Unterschiede klare Strategien und eine Überwachung durch das oberste Verwaltungsorgan wie auch die Geschäftsleitung, eine starke Risikokultur in Bezug auf die Handhabung der operationellen Risiken[1] und die internen Kontrollen (die u.a. klar abgegrenzte Verantwortlichkeiten und Aufgabentrennung umfasst), ein effektives internes Meldewesen und Notfallpläne unverzichtbare Elemente eines Konzepts für ein wirksames Management operationeller Risiken. Der Ausschuss ist daher überzeugt, mit den hier dargelegten Grundsätzen Praxisempfehlungen zu geben, die für alle Banken relevant sind. Die aktuelle Arbeit des Ausschusses zum Thema operationelles Risiko stützt sich auf sein im September 1998 veröffentlichtes Papier *Rahmenkonzept für interne Kontrollsysteme in Bankinstituten.*

Hintergrund

3. Die Deregulierung und Globalisierung der Finanzdienstleistungen, gepaart mit zunehmend anspruchsvollen Finanzierungstechniken, haben eine höhere Komplexität der Bankgeschäfte und somit auch der Risikoprofile der Banken (d.h. der Höhe des Risikos in jeder Tätigkeit und/oder Risikokategorie eines Instituts) zur Folge. Neu aufkommende Praktiken im Bankgeschäft könnten neben dem Kreditrisiko, dem Zinsänderungsrisiko und dem Marktrisiko erhebliche andere Risiken mit sich bringen. Für diese neuen und wachsenden Risiken des Bankgeschäfts seien folgende Beispiele genannt:

- Die zunehmende Automatisierung hat bei unzureichender Kontrolle das Potenzial, Risiken der fehlerhaften manuellen Bearbeitung in Risiken des Systemausfalls zu verwandeln, da sich die Banken vermehrt auf global integrierte Systeme stützen
- Das Wachstum des elektronischen Handels birgt potenzielle Risiken (z.B. im Zusammenhang mit internen und externen betrügerischen Handlungen und der Systemsicherheit), die noch nicht vollständig geklärt sind
- Grosse Übernahmen, Fusionen, Ausgliederungen und Konsolidierungen stellen die Tragfähigkeit neuer oder neu integrierter Systeme auf die Probe
- Die Entwicklung von Banken zu Dienstleistern mit grossen Volumina macht eine kontinuierliche Aufrechterhaltung leistungsfähiger interner Kontrollen und Sicherungssysteme erforderlich
- Banken können Techniken zur Risikominderung einsetzen (z.B. Sicherheiten, Kreditderivate, Netting und Verbriefung), um ihre Markt- und Kreditrisiken zu optimieren, doch diese können ihrerseits Risiken in anderer Form mit sich bringen (z.B. Rechtsrisiken)

[1] *Die interne Risikokultur in Bezug auf die operationellen Risiken* wird hier als die Gesamtheit der individuellen und kollektiven Werte, Einstellungen, Kompetenzen und Verhaltensweisen verstanden, die das Engagement eines Unternehmens für das Management operationeller Risiken und den Stil dieses Risikomanagements bestimmen.

- Die zunehmende Auslagerung („Outsourcing“) und die Teilnahme an Clearing- und Abwicklungssystemen können einige Risiken mindern, die Banken aber auch erheblichen anderen Risiken aussetzen

4. Die vielfältigen oben aufgeführten Risiken lassen sich unter dem Begriff „operationelles Risiko“ zusammenfassen, das der Ausschuss als „die Gefahr von unmittelbaren oder mittelbaren Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder von externen Ereignissen eintreten“, definiert hat.[2] Diese Definition schliesst Rechtsrisiken ein, nicht jedoch strategische Risiken oder Reputationsrisiken.

5. Der Ausschuss weiss, dass der Begriff „operationelles Risiko“ innerhalb des Bankensektors unterschiedliche Bedeutungen hat und dass Banken deshalb für interne Zwecke (einschl. der Umsetzung der Praxisempfehlungen in diesem Papier) eigene Definitionen des operationellen Risikos verwenden. Doch unabhängig von der genauen Definition ist es für eine wirksame Handhabung und Kontrolle dieser Risikokategorie unabdingbar, dass die Banken klar verstehen, was mit dem Begriff „operationelles Risiko“ gemeint ist. Wichtig ist darüber hinaus, dass die Definition das gesamte Spektrum nennenswerter operationeller Risiken für die jeweilige Bank berücksichtigt und die wichtigsten Ursachen grosser operationeller Verluste erfasst. Zu den operationellen Risikoereignissen, die der Ausschuss in Zusammenarbeit mit dem Bankensektor als mögliche Verursacher grosser Verluste identifiziert hat, zählen:

- ***interne betrügerische Handlungen***, z.B. absichtlich falsche Angabe von Positionen, Diebstahl durch Mitarbeiter und Insidergeschäfte auf eigene Rechnung von Mitarbeitern
- ***externe betrügerische Handlungen***, z.B. Raub, Fälschung, Scheckbetrug und Schäden durch Computerhacker
- ***Einstellungspraktiken und Sicherheit am Arbeitsplatz***, z.B. Haftungsansprüche von Mitarbeitern, Verstoss gegen Vorschriften der Arbeitsmedizin und der Sicherheit, gewerkschaftliche Aktivitäten, Diskriminierungsklagen, allgemeine Haftung
- ***Kunden, Produkte und Geschäftspraxis***, z.B. Verletzung von Treuhänderpflichten, Missbrauch vertraulicher Kundeninformationen, unsaubere Handelspraktiken auf Rechnung der Bank, Geldwäsche und Verkauf nicht genehmigter Produkte
- ***Schäden am Sachvermögen***, z.B. Terrorismus, Vandalismus, Erdbeben, Brände und Überschwemmungen
- ***Geschäftsunterbrechungen und Systemausfälle***, z.B. Hardware- und Softwarepannen, Telekommunikationsprobleme, Stromausfälle
- ***Ausführung, Lieferung und Prozessmanagement***, z.B. fehlerhafte Dateneingabe, fehlerhafte Verwaltung von Sicherheiten, unvollständige rechtliche Dokumentation, nicht genehmigter Zugang zu Kundenkonten, Fehlverhalten von Kontrahenten (nicht Kunden) und Auseinandersetzungen mit Zulieferern

Trends und Praktiken im Bankgeschäft

6. In seiner Arbeit zur Beaufsichtigung operationeller Risiken war der Ausschuss bestrebt, sein Verständnis aktueller Trends und Praktiken im Management operationeller Risiken des Bankgeschäfts zu vertiefen. Diese Bemühungen umfassten zahlreiche Gespräche mit Bankenorganisationen, Erhebungen über Praktiken des Bankgewerbes sowie die Analyse der Ergebnisse. Dank diesen Bemühungen ist der Ausschuss seiner Ansicht nach nun gut informiert über das Spektrum der derzeitigen

[2] Diese Definition wurde im Zuge der Arbeit des Ausschusses zur Entwicklung einer aufsichtlichen Eigenkapitalanforderung für das operationelle Risiko vom Bankensektor übernommen. Obwohl dieses Papier formell kein Bestandteil der Eigenkapitalvereinbarung ist, geht der Ausschuss davon aus, dass die hier dargelegten Grundelemente eines Rahmenkonzepts für sachgerechtes Management operationeller Risiken massgebend dafür sein werden, was die Aufsichtsinstanzen bei der Prüfung der Eigenkapitalausstattung der Banken, z.B. im Rahmen des aufsichtlichen Überprüfungsverfahrens, erwarten werden.

Praktiken im Bankgewerbe und über dessen Bestrebungen, Methoden für das Management operationeller Risiken zu entwickeln.

7. Der Ausschuss ist sich bewusst, dass das Management spezifischer operationeller Risiken keine Neuheit ist; für Banken war es von jeher wichtig, nach Möglichkeit Betrug zu verhindern, die Integrität interner Kontrollen zu wahren, Fehler bei der Transaktionsverarbeitung zu verringern usw. Relativ neu ist allerdings, dass das Risikomanagement in Bezug auf die operationellen Risiken als eine umfassende Praxis angesehen wird, die grundsätzlich – wenn auch nicht immer formell – mit dem Kredit- und Marktrisikomanagement vergleichbar ist. Angesichts der in der Einleitung dieses Papiers genannten Trends und gleichzeitig einer steigenden Zahl spektakulärer, operationell bedingter Verluste sehen Banken und Aufsichtsinstanzen das Management operationeller Risiken zunehmend als eine für das gesamte Unternehmen notwendige Disziplin an, wie es in vielen anderen Branchen längst der Fall ist.

8. Bisher beschränkten sich die Banken bei der Handhabung des operationellen Risikos fast vollständig auf interne Kontrollmechanismen innerhalb der Geschäftsbereiche, ergänzt durch die Revision. Diese Mechanismen bleiben zwar wichtig, doch in jüngster Zeit wurden spezifische Strukturen und Verfahren für die Handhabung operationeller Risiken entwickelt. In diesem Zusammenhang sind immer mehr Banken zu dem Schluss gelangt, dass ein Risikomanagement-Konzept für die operationellen Risiken der Sicherheit und finanziellen Gesundheit einer Bank dient, und sie behandeln das operationelle Risiko mit zunehmendem Erfolg als eigene Risikokategorie, ähnlich wie das Kredit- und das Marktrisiko. Der Ausschuss ist überzeugt, dass ein aktiver Gedankenaustausch zwischen den Aufsichtsinstanzen und dem Bankensektor für die weitere Entwicklung geeigneter Leitlinien für das Management operationeller Risiken entscheidend ist.

9. Dieses Papier gliedert sich wie folgt: Entwicklung eines geeigneten Umfelds für das Risikomanagement; Risikomanagement: Erkennung, Bewertung, Überwachung und Begrenzung/Minderung; Rolle der Bankenaufsicht; Rolle der Offenlegung.

Praxisempfehlungen

10. Bei der Erarbeitung dieser Praxisempfehlungen konnte sich der Ausschuss auf seine früheren Arbeiten über das Management anderer wichtiger Risiken des Bankgeschäfts wie das Kreditrisiko, das Zinsänderungsrisiko und das Liquiditätsrisiko stützen, und er ist der Ansicht, dass operationelle Risiken ein ebenso konsequentes Risikomanagement erfordern. Dennoch ist klar, dass sich operationelle Risiken von anderen Risiken des Bankgeschäfts unterscheiden, da sie in der Regel nicht direkt für einen erwarteten Ertrag eingegangen werden, sondern Bestandteil des Tagesgeschäfts sind, und dass sich dies auf den Risikomanagement-Prozess auswirkt.[3] Gleichzeitig kann eine unzureichende Handhabung operationeller Risiken zu einer falschen Darstellung des Risikoprofils einer Bank führen und diese erheblichen Verlusten aussetzen. Um der Andersartigkeit des operationellen Risikos gerecht zu werden, wird „Management“ operationeller Risiken für die Zwecke dieses Papiers – im Gegensatz zu der Definition in früheren Arbeiten des Ausschusses über das Risikomanagement („Erkennung, Messung, Überwachung und Begrenzung“) – als „Erkennung, Bewertung, Überwachung und Begrenzung/Minderung“ dieser Risiken definiert. Wie schon in seinen Arbeiten zu anderen Risiken des Bankgeschäfts hat der Ausschuss diese Praxisempfehlungen auf eine Reihe von Grundsätzen aufgebaut. Sie lauten:

[3] Der Ausschuss räumt jedoch ein, dass die Entscheidung einer Bank, ein operationelles Risiko einzugehen oder ihre Effizienz bei der Handhabung und Bewertung dieses Risikos für den Wettbewerb zu nutzen, in manchen Geschäftsbereichen mit sehr geringem Kredit- oder Marktrisiko (z.B. Vermögensverwaltung, Zahlungsverkehr und Abwicklung) ein fester Bestandteil ihrer Berechnung des Risiko/Ertrags-Verhältnisses ist.

Die Entwicklung geeigneter Rahmenbedingungen für das Risikomanagement

Grundsatz 1: Das oberste Verwaltungsorgan[4] sollte die wichtigsten Aspekte des operationellen Risikos der Bank als eigene Risikokategorie erkennen, die es zu handhaben gilt; ihm fällt die Aufgabe zu, das Risikomanagement-Konzept der Bank für die operationellen Risiken zu genehmigen und periodisch zu überprüfen. Dieses Konzept sollte eine für die gesamte Bank gültige Definition des operationellen Risikos beinhalten und die Grundsätze für seine Erkennung, Bewertung, Überwachung und Begrenzung/Minderung festlegen.

Grundsatz 2: Das oberste Verwaltungsorgan hat dafür zu sorgen, dass das Risikomanagement-Konzept der Bank für die operationellen Risiken einer effektiven und umfassenden internen Revision durch operationell unabhängige, angemessen ausgebildete und kompetente Mitarbeiter unterzogen wird. Die interne Revision sollte nicht direkt für das Management operationeller Risiken zuständig sein.

Grundsatz 3: Der Geschäftsleitung fällt die Aufgabe zu, das vom obersten Verwaltungsorgan genehmigte Risikomanagement-Konzept für die operationellen Risiken umzusetzen. Dieses Konzept sollte in der gesamten Bank einheitlich umgesetzt werden, und die Mitarbeiter aller Ebenen sollten ihre Verantwortlichkeiten im Hinblick auf das Management operationeller Risiken kennen. Darüber hinaus obliegt es der Geschäftsleitung, Strategien, Verfahren und Praktiken zur Handhabung des operationellen Risikos bei allen wichtigen Produkten, Tätigkeiten, Prozessen und Systemen der Bank zu entwickeln.

Risikomanagement: Erkennung, Bewertung, Überwachung und Minderung/Begrenzung

Grundsatz 4: Die Banken sollten die operationellen Risiken aller wichtigen Produkte, Tätigkeiten, Verfahren und Systeme identifizieren und bewerten. Des Weiteren sollten sie sicherstellen, dass Produkte, Tätigkeiten, Verfahren und Systeme vor ihrer Einführung mithilfe angemessener Bewertungsverfahren auf ihr operationelles Risiko hin geprüft werden.

Grundsatz 5: Die Banken sollten ein Verfahren zur regelmässigen Überwachung ihres operationellen Risikoprofils und der Risiken erheblicher Verluste einführen. Relevante Informationen sind der Geschäftsleitung und dem obersten Verwaltungsorgan regelmässig vorzulegen, um ein proaktives Management operationeller Risiken zu unterstützen.

Grundsatz 6: Die Banken sollten über Strategien, Verfahren und Praktiken zur Steuerung erheblicher operationeller Risiken verfügen. Sie sollten ihre Strategien zur Risikobegrenzung und -minderung periodisch revidieren und ihr operationelles Risikoprofil mithilfe geeigneter Strategien auf ihre gesamte Risikobereitschaft und ihr gesamtes Risikoprofil abstimmen.

Grundsatz 7: Die Banken sollten über Notfallpläne und Vorkehrungen zur Fortführung der Geschäfte verfügen, um die Kontinuität ihrer Tätigkeit und die Schadensbegrenzung im Falle einer schwerwiegenden Geschäftsunterbrechung zu gewährleisten.

Die Rolle der Bankenaufsicht

Grundsatz 8: Die Bankenaufsicht sollte von den Banken unabhängig von deren Grösse verlangen, dass sie als Bestandteil ihres generellen Risikomanagements ein wirksames System zur Erkennung, Bewertung, Überwachung und Begrenzung/Minderung erheblicher operationeller Risiken einrichten.

---

[4] In diesem Papier wird von einer Geschäftsführungsstruktur ausgegangen, die sich aus einem obersten Verwaltungsorgan und einer Geschäftsleitung zusammensetzt. Der Ausschuss weiss, dass die rechtlichen und sonstigen Rahmenbedingungen in den einzelnen Ländern sehr unterschiedlich sind, was die Funktion des obersten Verwaltungsorgans und der Geschäftsleitung betrifft. In einigen Ländern besteht die Hauptaufgabe, wenn nicht sogar die einzige Aufgabe des Verwaltungsorgans darin, das geschäftsführende Organ (Geschäftsleitung, Generaldirektion, Direktorium) zu beaufsichtigen, um sicherzustellen, dass dieses seine Aufgaben erfüllt. Aus diesem Grund wird das Verwaltungsorgan in einigen Ländern auch als „Aufsichtsrat" bezeichnet, d.h. es hat in diesem Fall keine geschäftsführenden Funktionen. In anderen Ländern dagegen sind die Aufgaben des „Verwaltungsrats" breiter gefächert, d.h. er legt die allgemeinen geschäftspolitischen Richtlinien der Bank fest. Angesichts dieser Unterschiede werden in diesem Papier mit „oberstem Verwaltungsorgan" und „Geschäftsleitung" nicht rechtliche Konstrukte bezeichnet, sondern zwei entscheidungstragende Funktionen innerhalb der Bank.

Grundsatz 9: Die Bankenaufsicht sollte direkt oder indirekt regelmässige, unabhängige Prüfungen der Strategien, Verfahren und Praktiken einer Bank im Hinblick auf ihre operationellen Risiken durchführen. Die Aufsichtsinstanzen sollten sicherstellen, dass geeignete Mechanismen vorhanden sind, damit sie über die Entwicklungen in den Banken auf dem Laufenden sind.

Die Rolle der Offenlegung

Grundsatz 10: Die Banken sollten genügend Informationen offen legen, damit Marktteilnehmer sich ein Urteil über ihren Ansatz beim Management der operationellen Risiken bilden können.

Die Entwicklung geeigneter Rahmenbedingungen für das Risikomanagement

11. Fehlendes Verständnis und unzulängliche Handhabung operationeller Risiken, die bei praktisch allen Transaktionen und Tätigkeiten einer Bank vorhanden sind, kann die Wahrscheinlichkeit stark erhöhen, dass einige von ihnen unerkannt und unkontrolliert bleiben. Sowohl das oberste Verwaltungsorgan als auch die Geschäftsleitung sind für die Schaffung einer Unternehmenskultur verantwortlich, die dem wirksamen Management operationeller Risiken und sachgerechten internen Kontrollen eine hohe Priorität einräumt. Das Risikomanagement für operationelle Risiken ist am wirksamsten, wenn die Kultur einer Bank Wert auf hohe moralische Standards für die Mitarbeiter aller Ebenen legt. Das oberste Verwaltungsorgan und die Geschäftsleitung sollten eine Unternehmenskultur fördern, die mit Taten wie mit Worten die Erwartung etabliert, dass alle Mitarbeiter bei den Geschäften der Bank Integrität walten lassen.

Grundsatz 1: Das oberste Verwaltungsorgan sollte die wichtigsten Aspekte des operationellen Risikos der Bank als eigene Risikokategorie erkennen, die es zu handhaben gilt; ihm fällt die Aufgabe zu, das Risikomanagement-Konzept der Bank für die operationellen Risiken zu genehmigen und periodisch zu überprüfen. Dieses Konzept sollte eine für die gesamte Bank gültige Definition des operationellen Risikos beinhalten und die Grundsätze für seine Erkennung, Bewertung, Überwachung und Begrenzung/Minderung festlegen.

12. Dem obersten Verwaltungsorgan obliegt es, ein bankweites Konzept zum gezielten Management operationeller Risiken als eigener Risikokategorie für die Sicherheit und Solidität der Bank zu genehmigen. Das oberste Verwaltungsorgan muss der Geschäftsleitung klare Leitlinien und Ziele hinsichtlich der Grundsätze des Konzepts vorgeben und die von der Geschäftsleitung dementsprechend entwickelten Strategien genehmigen.

13. Ein Konzept für das Management operationeller Risiken sollte sich auf eine angemessene Definition stützen, die klar formuliert, was in der jeweiligen Bank ein operationelles Risiko darstellt. Das Konzept sollte auf die operationelle Risikobereitschaft und -toleranz der Bank abgestimmt sein, spezifiziert anhand von Managementstrategien für diese Risiken und von Prioritäten für Massnahmen zu ihrer Handhabung (einschl. des Ausmasses und der Form ihrer Externalisierung). Des Weiteren sollte es Strategien beinhalten, die den Ansatz der Bank zur Erkennung, Bewertung, Überwachung und Begrenzung/Minderung operationeller Risiken erkennbar machen. Der Grad der Formalisierung und Ausdifferenzierung des Konzepts für das Management operationeller Risiken sollte dem Risikoprofil der Bank entsprechen.

14. Das oberste Verwaltungsorgan ist dafür verantwortlich, eine Führungsstruktur zu schaffen, die die Umsetzung des Konzepts zum Management operationeller Risiken ermöglicht. Da starke interne Kontrollen ein wesentlicher Aspekt des Managements operationeller Risiken sind, ist es besonders wichtig, dass das oberste Verwaltungsorgan klare Zuständigkeiten, Verantwortlichkeiten und Berichtslinien festlegt. Darüber hinaus sollte es für eine Trennung der Aufgaben und Berichtslinien zwischen der Kontrolle operationeller Risiken, den Geschäftsbereichen und den Supportfunktionen sorgen, um Interessenkonflikte zu vermeiden. Ausserdem sollte das Konzept eine klare Formulierung der wichtigsten Verfahren enthalten, die die Bank für das Management operationeller Risiken benötigt.

15. Das oberste Verwaltungsorgan sollte das Konzept regelmässig überprüfen, um zu gewährleisten, dass die Bank die operationellen Risiken handhabt, die sich aus Veränderungen am Markt bzw. anderen Faktoren des wirtschaftlichen Umfelds oder aus neuen Produkten, Tätigkeiten oder Systemen ergeben. Diese Überprüfung sollte auch dazu dienen, die bestmögliche Praxis für das Management operationeller Risiken zu ermitteln, die den Tätigkeiten, Systemen und Verfahren der Bank entspricht. Falls notwendig, sollte das oberste Verwaltungsorgan dafür Sorge tragen, dass das Konzept für das Management operationeller Risiken im Licht dieser Analyse so revidiert wird, dass es erhebliche operationelle Risiken erfasst.

Grundsatz 2: Das oberste Verwaltungsorgan hat dafür zu sorgen, dass das Risikomanagement-Konzept der Bank für die operationellen Risiken einer effektiven und umfassenden internen Revision durch operationell unabhängige, angemessen ausgebildete und kompetente Mitarbeiter unterzogen wird. Die interne Revision sollte nicht direkt für das Management operationeller Risiken zuständig sein.

16. Die Banken sollten über eine angemessene interne Revision verfügen, um zu verifizieren, dass operative Strategien und Verfahren effektiv umgesetzt worden sind.[5] Das oberste Verwaltungsorgan sollte (entweder direkt oder indirekt durch seinen Geschäftsprüfungsausschuss) sicherstellen, dass der Erfassungsbereich und die Häufigkeit der durchgeführten Revisionen den bestehenden Risiken gerecht werden. Die Revision sollte regelmässig verifizieren, dass das Risikomanagement-Konzept der Bank für die operationellen Risiken in der gesamten Bank wirksam umgesetzt wird.

17. Entsprechend der Aufsichtsfunktion der Revision über das Management operationeller Risiken sollte das oberste Verwaltungsorgan für die Unabhängigkeit der Revisionsfunktion sorgen. Diese Unabhängigkeit kann gefährdet werden, wenn die Revision direkt am Risikomanagement beteiligt ist. Die Revision kann den Risikomanagement-Verantwortlichen wertvolle Rückmeldungen liefern, sollte hier jedoch selbst keine direkte Verantwortung tragen. Der Ausschuss räumt ein, dass die Revision in der Praxis in einigen Banken, insbesondere kleineren, anfänglich dafür zuständig sein kann, ein Konzept für das Management der operationellen Risiken zu entwickeln. Wo dies der Fall ist, sollte die Bank dafür sorgen, dass die Verantwortung für die tägliche Handhabung der operationellen Risiken möglichst bald auf andere übertragen wird.

Grundsatz 3: Der Geschäftsleitung fällt die Aufgabe zu, das vom obersten Verwaltungsorgan genehmigte Risikomanagement-Konzept für die operationellen Risiken umzusetzen. Dieses Konzept sollte in der gesamten Bank einheitlich umgesetzt werden, und die Mitarbeiter aller Ebenen sollten ihre Verantwortlichkeiten im Hinblick auf das Management operationeller Risiken kennen. Darüber hinaus obliegt es der Geschäftsleitung, Strategien, Verfahren und Praktiken zur Handhabung des operationellen Risikos bei allen wichtigen Produkten, Tätigkeiten, Prozessen und Systemen der Bank zu entwickeln.

18. Die Geschäftsleitung hat das vom obersten Verwaltungsorgan erstellte Konzept für das Management operationeller Risiken in spezifische Strategien, Verfahren und Praktiken umzusetzen, die in den verschiedenen Geschäftsbereichen eingeführt und verifiziert werden können. Während jede Führungsebene für die Zweckmässigkeit und Wirksamkeit der Strategien, Verfahren, Praktiken und Kontrollen innerhalb ihres Zuständigkeitsbereichs verantwortlich ist, sollte die Geschäftsleitung Weisungsbefugnisse, Zuständigkeiten und Berichtslinien eindeutig zuordnen, um diese Verantwortlichkeit zu fördern und zu bewahren, und dafür sorgen, dass die notwendigen Ressourcen zur Verfügung stehen, um operationellen Risiken wirksam zu begegnen. Darüber hinaus sollte die Geschäftsleitung prüfen, ob ihre Überwachung in Bezug auf die Risiken, die der jeweiligen Strategie einer Geschäftseinheit eigen sind, sachgerecht ist.

19. Die Geschäftsleitung hat dafür Sorge zu tragen, dass die verschiedenen Tätigkeiten der Bank von qualifizierten Mitarbeitern mit der nötigen Erfahrung, dem nötigen Fachwissen und Zugang zu den nötigen Ressourcen ausgeübt werden, und dass die Mitarbeiter, welche die Risikopolitik der Bank überwachen und ihre Einhaltung durchsetzen, unabhängig von den Einheiten sind, die sie beaufsichtigen. Die Geschäftsleitung sollte sicherstellen, dass die Strategie der Bank für das Management operationeller Risiken in Einheiten mit erheblichen solchen Risiken den Mitarbeitern aller Ebenen klar vermittelt worden ist.

20. Die Geschäftsleitung sorgt für eine effektive Kommunikation zwischen den Verantwortlichen für das Management der operationellen Risiken und den Verantwortlichen für das Management der Kredit-, Markt- und sonstigen Risiken, aber auch mit den Verantwortlichen für die Beschaffung externer Dienstleistungen (z.B. Abschluss von Versicherungen und Outsourcing). Andernfalls könnten erhebliche Lücken oder Überschneidungen im gesamten Risikomanagement der Bank die Folge sein.

21. Darüber hinaus sollte die Geschäftsleitung sicherstellen, dass die Vergütungsstrategien der Bank auf ihre Risikobereitschaft abgestimmt sind. Vergütungsstrategien, die ein von der Geschäftspolitik abweichendes Verhalten (z.B. die Überschreitung festgesetzter Limits) belohnen, schwächen das Risikomanagement einer Bank.

22. Besondere Beachtung sollte der Qualität der Dokumentationskontrollen und der Transaktionsverarbeitung geschenkt werden. Vor allem Strategien, Verfahren und Praktiken, die mit hoch-

[5] Das vom Ausschuss herausgegebene Papier *Internal Revision in Banks and the Supervisor's Relationship with Auditors* (August 2001) beschreibt die Rolle der internen und der externen Revision.

entwickelter Technik und hohen Transaktionsvolumina verbunden sind, sollten gut dokumentiert und allen damit befassten Mitarbeitern vermittelt werden.

Risikomanagement: Erkennung, Bewertung, Überwachung und Minderung/Begrenzung

Grundsatz 4: Die Banken sollten die operationellen Risiken aller wichtigen Produkte, Tätigkeiten, Verfahren und Systeme identifizieren und bewerten. Des Weiteren sollten sie sicherstellen, dass Produkte, Tätigkeiten, Verfahren und Systeme vor ihrer Einführung mithilfe angemessener Bewertungsverfahren auf ihr operationelles Risiko hin geprüft werden.

23. Risikoerkennung ist von höchster Bedeutung für die darauf basierende Entwicklung eines tragfähigen Systems zur Überwachung und Kontrolle operationeller Risiken. Damit sie wirksam ist, berücksichtigt sie sowohl interne Faktoren (z.B. Struktur der Bank, Art ihrer Geschäfte, Qualität ihrer Humanressourcen, Veränderungen ihrer Organisation und Personalfluktuation) als auch externe Faktoren (z.B. Veränderungen im Bankgeschäft und technische Fortschritte), die einer Bank bei der Erreichung ihrer Ziele hinderlich werden könnten.

24. Nach der Ermittlung der Risiken mit dem höchsten Schadenspotenzial sollte eine Bank einschätzen, wie anfällig sie gegenüber diesen Risiken ist. Eine effektive Risikobewertung ermöglicht es der Bank, ihr Risikoprofil besser zu verstehen und ihre Ressourcen für das Risikomanagement am wirksamsten einzusetzen.

25. Zur Erkennung und Bewertung operationeller Risiken können die Banken folgende Instrumente einsetzen:

- ***Selbst- oder Risikoeinschätzung***: Eine Bank überprüft ihre Operationen und Tätigkeitsbereiche auf ihre Anfälligkeit gegenüber einer Palette potenzieller operationeller Risiken. Dieser Prozess ist intern und umfasst häufig Checklisten und/oder Workshops, mit deren Hilfe die Stärken und Schwächen des operationellen Risikoumfelds ermittelt werden. Mit „Score-Karten" (Klassifizierungen) lassen sich z.B. qualitative Einschätzungen in quantitative Messgrössen umwandeln, die eine Rangordnung der verschiedenen operationellen Risiken ergeben. Manche Klassifizierungen können sich auf Risiken beziehen, denen nur ganz bestimmte Geschäftsbereiche ausgesetzt sind, andere ergeben eine Rangordnung von Risiken, die alle Geschäftsbereiche betreffen. Klassifizierungen können sich auf inhärente Risiken, aber auch auf die Kontrollen zur Risikominderung beziehen. Darüber hinaus kann eine Bank Score-Karten verwenden, um den Geschäftsbereichen ökonomisches Kapital entsprechend ihrer Leistung bei der Handhabung und Kontrolle verschiedener Aspekte des operationellen Risikos zuzuteilen.
- ***Risikobestandsaufnahme***: In diesem Verfahren wird für die verschiedenen Geschäftseinheiten, Funktionen oder Abläufe der Organisation eine Bestandsaufnahme nach Risikotyp vorgenommen. Es kann Schwachstellen aufdecken und dazu beitragen, Prioritäten für Massnahmen der Geschäftsleitung zu setzen.
- ***Risikoindikatoren***: Risikoindikatoren sind (häufig finanzielle) Statistiken und/oder Kennzahlen, die Aufschluss über die Risikoposition einer Bank geben können. Diese Indikatoren werden meist periodisch geprüft, z.B. monatlich oder vierteljährlich, um die Bank auf Veränderungen aufmerksam zu machen, die Anzeichen für Risikoprobleme sein könnten. Solche Indikatoren können u.a. die Anzahl der gescheiterten Transaktionen, die Personalfluktuation und die Häufigkeit und/oder Schwere von Fehlern und Versäumnissen sein.
- ***Messung***: Einige Banken haben begonnen, ihre Anfälligkeit für operationelle Risiken mit unterschiedlichen Methoden zu messen. Daten über frühere Verluste einer Bank könnten ihr z.B. aufschlussreiche Informationen liefern, um zu beurteilen, in welchem Masse sie welchen operationellen Risiken ausgesetzt ist, und um eine Strategie für deren Steuerung zu entwickeln. Eine wirksame Methode, diese Informationen gut zu nutzen, ist die systematische Erfassung der Häufigkeit, Schwere und anderer relevanter Aspekte der einzelnen Schadensfälle. Einige Banken haben darüber hinaus interne Verlustdaten mit externen Verlustdaten, Szenarioanalysen und Risikobewertungsfaktoren kombiniert.

Grundsatz 5: Die Banken sollten ein Verfahren zur regelmässigen Überwachung ihres operationellen Risikoprofils und der Risiken erheblicher Verluste einführen. Relevante Informationen

sind der Geschäftsleitung und dem obersten Verwaltungsorgan regelmässig vorzulegen, um ein proaktives Management operationeller Risiken zu unterstützen.

26. Eine wirksame Überwachung ist Voraussetzung für ein sachgerechtes Management operationeller Risiken. Regelmässige Überwachung kann den Vorteil bringen, Mängel bei den Strategien, Verfahren und Praktiken zum Management operationeller Risiken rasch aufdecken und korrigieren zu können. Eine rasche Aufdeckung und Korrektur solcher Mängel kann die potenzielle Häufigkeit und/oder Schwere von Schadensfällen erheblich verringern.

27. Zusätzlich zur Überwachung operationeller Schadensfälle sollten die Banken geeignete Indikatoren zur Früherkennung eines gestiegenen Verlustrisikos identifizieren. Solche Indikatoren (oft als zentrale Risikoindikatoren oder Frühwarnindikatoren bezeichnet) sollten zukunftsbezogen sein und könnten potenzielle Ursachen operationeller Risiken anzeigen, z.B. rasches Wachstum, die Einführung neuer Produkte, Personalfluktuation, Transaktionsunterbrechungen, Systemausfälle usw. Wenn diese Indikatoren direkt mit Schwellenwerten verknüpft sind, kann ein wirksames Überwachungsverfahren dazu beitragen, die wichtigsten Risiken in transparenter Weise zu erkennen, und die Bank in die Lage versetzen, diesen Risiken angemessen zu begegnen.

28. Der Rhythmus der Überwachung sollte auf die vorhandenen Risiken sowie auf die Häufigkeit und Art von Veränderungen im Geschäftsumfeld abgestimmt sein. Die Risikoüberwachung sollte ein fester Bestandteil des Tagesgeschäfts einer Bank sein. Ihre Erkenntnisse sollten Bestandteil der regelmässigen Berichterstattung an die Geschäftsleitung und das oberste Verwaltungsorgan sein; das Gleiche gilt für Compliance-Prüfungen, die von der internen Revision und/oder dem Risikomanagement durchgeführt werden. Berichte von (und/oder für) Aufsichtsinstanzen können ebenfalls in diese Überwachung einfliessen, und auch sie sind, wo es angebracht ist, intern der Geschäftsleitung und dem obersten Verwaltungsorgan vorzulegen.

29. Die Geschäftsleitung sollte regelmässig Spartenberichte erhalten, z.B. von Geschäftseinheiten, Gruppenfunktionen, den für das Management operationeller Risiken zuständigen Mitarbeitern und der internen Revision. Die Berichterstattung über operationelle Risiken umfasst interne Finanz-, Betriebs- und Compliance-Daten, ausserdem externe Marktinformationen über Ereignisse und Bedingungen, die für die Entscheidungsfindung wichtig sind. Die Berichte sind an die angemessenen Führungsebenen und an potenziell betroffene Bereiche der Bank zu verteilen. Sie sollten erkannte Problembereiche vollständig darstellen und zu zeitigem Handeln motivieren, um offene Probleme zu lösen. Um den Nutzen und die Zuverlässigkeit dieser Risiko- und Revisionsberichte zu gewährleisten, sollte die Geschäftsleitung regelmässig die Aktualität, Richtigkeit und Relevanz der Berichtssysteme und internen Kontrollen generell prüfen. Sie kann auch von Berichten externer Quellen (Buchprüfer, Bankenaufsicht) Gebrauch machen, um den Nutzen und die Zuverlässigkeit interner Berichte zu bewerten. Die Berichte sollten mit dem Ziel analysiert werden, die Leistung des aktuellen Risikomanagements zu verbessern sowie neue Strategien, Verfahren und Praktiken für das Risikomanagement zu entwickeln.

30. Grundsätzlich sollte das oberste Verwaltungsorgan ausreichende abstrahierte Informationen erhalten, damit es das generelle operationelle Risikoprofil der Bank verstehen und sich auf seine materiellen und strategischen Folgen für das Geschäft konzentrieren kann.

Grundsatz 6: Die Banken sollten über Strategien, Verfahren und Praktiken zur Steuerung erheblicher operationeller Risiken verfügen. Sie sollten ihre Strategien zur Risikobegrenzung und -minderung periodisch revidieren und ihr operationelles Risikoprofil mithilfe geeigneter Strategien auf ihre gesamte Risikobereitschaft und ihr gesamtes Risikoprofil abstimmen.

31. Kontrollverfahren dienen dazu, die operationellen Risiken zu handhaben, die eine Bank erkannt hat.[6] Für jedes erhebliche operationelle Risiko, das erkannt wurde, muss die Bank entscheiden, ob sie geeignete Massnahmen zu seiner Begrenzung/Minderung ergreifen oder ob sie es tragen will. Kann ein Risiko nicht begrenzt werden, muss die Bank entscheiden, ob sie es in Kauf nimmt oder ob sie die damit behafteten Tätigkeiten verringert bzw. ganz einstellt. Die Banken sollten Verfahren und Praktiken zur Risikokontrolle einführen und über ein Kontrollsystem verfügen, das die Einhaltung

[6] Näheres s. das *Rahmenkonzept für interne Kontrollsysteme in Bankinstituten*, Basler Ausschuss für Bankenaufsicht, September 1998.

eines dokumentierten Kodexes interner Strategien für das Risikomanagement gewährleistet. Grundelemente dieses Systems könnten z.B. sein:

- Überprüfung des Fortschritts der Bank bei der Realisierung ihrer Ziele auf höchster Ebene
- Überprüfung der Einhaltung der Kontrollverfahren (Compliance)
- Strategien, Verfahren und Praktiken zur Prüfung, Behandlung und Lösung von Compliance-Problemen
- ein System dokumentierter Genehmigungen und Ermächtigungen, das die Rechenschaftspflicht gegenüber einer geeigneten Führungsebene gewährleistet

32. Ein formeller Kodex von Strategien und Verfahren in Schriftform ist unverzichtbar, bedarf jedoch der Bestätigung durch ein starkes Kontrollumfeld, das sachgerechten Praktiken zum Risikomanagement förderlich ist. Sowohl das oberste Verwaltungsorgan als auch die Geschäftsleitung sind verantwortlich dafür, ein starkes Umfeld interner Kontrollen zu schaffen, in dem aktive Risikokontrolle ein fester Bestandteil des Tagesgeschäfts der Bank ist. Wenn die Kontrollen Bestandteil des Tagesgeschäfts sind, kann rasch auf sich ändernde Bedingungen reagiert werden, und unnötige Kosten werden vermieden.

33. Damit ein internes Kontrollsystem wirksam ist, muss eine angemessene Aufgabentrennung bestehen, und Mitarbeitern sollten keine Verantwortlichkeiten zugewiesen werden, die zu Interessenkonflikten führen können. Personen oder Teams mit Interessenkonflikten könnten in der Lage sein, Verluste, Fehler oder Fehlverhalten zu vertuschen. Deshalb sind Bereiche mit möglichen Interessenkonflikten zu ermitteln, möglichst klein zu halten und von einer unabhängigen Stelle sorgfältig zu überwachen.

34. Zusätzlich zur Aufgabentrennung sollten die Banken über weitere interne Praktiken verfügen, die geeignet sind, operationelle Risiken zu steuern. Beispiele hierfür sind:

- sorgfältige Überwachung der Einhaltung von Risikolimits oder -schwellenwerten
- Einschränkung des Zugangs zu und der Verwendung von Vermögensgegenständen und Unterlagen der Bank
- Gewährleistung ausreichender Kenntnisse und Ausbildung der Mitarbeiter
- Erkennung von Geschäftssparten oder Produkten, deren Erträge nicht dem entsprechen, was man eigentlich erwarten dürfte (wo z.B. eine Geschäftstätigkeit mit vermeintlich geringem Risiko und geringen Margen hohe Erträge einbringt, könnte sich die Frage stellen, ob diese Erträge infolge eines Verstosses gegen die internen Kontrollgrundsätze erzielt wurden)
- regelmässige Überprüfung und Abstimmung von Transaktionen und Konten

Das Versäumnis, solche Praktiken einzuführen, hat für einige Banken in den letzten Jahren erhebliche operationelle Verluste zur Folge gehabt.

35. Operationelle Risiken können ausgeprägter sein, wenn eine Bank neue Tätigkeiten oder neue Produkte entwickelt (insbesondere wenn diese nicht den Strategien der Bank für ihr Kerngeschäft entsprechen), in ihr nicht vertraute Märkte eintritt und/oder sich in Unternehmen engagiert, die geografisch weit vom Hauptsitz entfernt sind. Darüber hinaus sorgen Banken in solchen Fällen oft nicht dafür, dass die Kontrollinfrastruktur für das Risikomanagement mit dem Wachstum der Geschäftstätigkeit Schritt hält. Mehrere der höchsten und spektakulärsten Verluste der letzten Jahre traten in Banken ein, auf die einer oder mehrere dieser Punkte zutrafen. Daher müssen die Banken unbedingt sicherstellen, dass unter solchen Bedingungen besonders auf die interne Kontrolle geachtet wird.

36. Einige erhebliche operationelle Risiken haben zwar einen geringen Wahrscheinlichkeitsgrad, aber potenziell sehr umfangreiche finanzielle Folgen. Darüber hinaus lassen sich nicht alle Risikoereignisse kontrollieren (z.B. Naturkatastrophen). Instrumente oder Programme zur Risikominderung können dazu dienen, die Anfälligkeit gegenüber solchen Ereignissen, ihre Häufigkeit und/oder Schwere zu verringern. So können Versicherungspolicen, insbesondere solche mit prompter und garantierter Auszahlung, Risiken vom Typ „niedrige Schadenshäufigkeit/hoher Schadensumfang“ (z.B. Haftpflichtansprüche infolge von Fehlern und Versäumnissen, des physischen Verlusts von Wertpapieren, Betrug von Mitarbeitern oder Dritten sowie Naturkatastrophen) externalisieren.

37. Dennoch sollten die Banken Instrumente zur Risikominderung als Ergänzung einer gründlichen internen Risikokontrolle und nicht als Ersatz dafür ansehen. Mechanismen zur raschen Erkennung und Korrektur zu erwartender Fehler bei der Bestimmung des operationellen Risikos können die Risikoanfälligkeit deutlich verringern. Auch ist sorgfältig zu prüfen, ob und inwieweit Instrumente zur Risikominderung wie Versicherungen ein Risiko wirklich verringern oder ob sie es auf einen anderen Geschäftsbereich übertragen oder ob sie gar ein neues Risiko schaffen (z.B. Rechts- oder Kontrahentenrisiko).

38. Investitionen in geeignete Sicherheitstechnik für die Verarbeitungs- und IT-Systeme sind ebenfalls wichtig für die Risikominderung. Die Banken sollten jedoch wissen, dass infolge der zunehmenden Automatisierung Risiken vom Typ „hohe Schadenshäufigkeit/geringer Schadensumfang" durch Risiken vom Typ „geringe Schadenshäufigkeit/hoher Schadensumfang" abgelöst werden könnten. Diese Schadensfälle könnten mit dem Verlust oder dem längeren Ausfall von Systemen verbunden sein und von internen Faktoren oder von Faktoren verursacht werden, über die die Bank keine unmittelbare Kontrolle hat (z.B. externe Ereignisse). Solche Probleme können eine Bank in ernstliche Schwierigkeiten bringen und sie sogar daran hindern, wichtige Geschäftstätigkeiten weiterzuführen. Wie weiter unten zu Grundsatz 7 dargelegt, sollten die Banken Notfallpläne und Vorkehrungen zur Fortführung der Geschäfte einführen, die diesem Risiko Rechnung tragen.

39. Auch für die mit Auslagerungen („Outsourcing") verbundenen Risiken sollten die Banken Risikomanagement-Strategien einführen. Eine Auslagerung kann das Risikoprofil einer Bank verringern, da Tätigkeiten auf Externe übertragen werden, die die Risiken spezialisierter Leistungen mit mehr Fachwissen und Grössenvorteilen steuern können. Allerdings entlässt die Auftragsvergabe an Externe das oberste Verwaltungsorgan und die Geschäftsleitung einer Bank nicht aus der Pflicht, sicherzustellen, dass die Leistungen Dritter in einer sicheren und seriösen Weise und in Einklang mit den einschlägigen Rechtsvorschriften erbracht werden. Auslagerungsvereinbarungen sollten auf soliden Verträgen und/oder Leistungsvereinbarungen beruhen, die eine klare Zuordnung der Verantwortlichkeiten zwischen externen Auftragnehmern und der auslagernden Bank gewährleisten. Des Weiteren müssen die Banken Restrisiken der Auslagerung, einschliesslich eines Systemausfalls, berücksichtigen.

40. Je nach Umfang und Art der Tätigkeit sollten die Banken wissen, welche Folgen es für ihr Geschäft und ihre Kunden haben kann, wenn Dienstleistungen von externen Anbietern, sonstigen Dritten oder anderen Konzerngesellschaften mangelhaft sind – sowohl Betriebsausfälle als auch potenzielles Scheitern von Geschäften oder Ausfall ihrer Geschäftspartner. Das oberste Verwaltungsorgan und die Geschäftsleitung haben dafür zu sorgen, dass die Erwartungen und Pflichten aller Beteiligten eindeutig definiert, verstanden und durchsetzbar sind. In welchem Masse externe Auftragnehmer haftbar und finanziell in der Lage sind, die Bank für Fehler, Versäumnisse und sonstige operationelle Mängel zu entschädigen, ist als Bestandteil der Risikobewertung ausdrücklich zu klären. Die Banken sollten externe Auftragnehmer zu Beginn der Zusammenarbeit sorgfältig überprüfen und dann ihre Tätigkeit überwachen – insbesondere wenn sie nicht über Erfahrungen mit dem regulierten Umfeld des Bankgeschäfts verfügen –, und dieser Prozess sollte regelmässig evaluiert werden, einschliesslich erneuter Überprüfungen. Für zentrale Tätigkeiten muss die Bank möglicherweise Notfallpläne und Vorkehrungen zur Fortführung der Geschäfte in Betracht ziehen, einschliesslich der Verfügbarkeit alternativer externer Auftragnehmer und der Kosten eines – möglicherweise sehr rasch zu vollziehenden – Wechsels zu einem anderen externen Auftragnehmer.

41. In manchen Fällen entscheiden sich Banken, ein gewisses Mass an operationellem Risiko selbst zu tragen oder selbst zu versichern. Wenn dies ein erhebliches Risiko betrifft, sollte die Entscheidung für den Selbstbehalt oder die Eigenversicherung innerhalb der Organisation transparent sein und der generellen Geschäftsstrategie der Bank sowie ihrer Risikobereitschaft entsprechen.

Grundsatz 7: Die Banken sollten über Notfallpläne und Vorkehrungen zur Fortführung der Geschäfte verfügen, um die Kontinuität ihrer Tätigkeit und die Schadensbegrenzung im Falle einer schwerwiegenden Geschäftsunterbrechung zu gewährleisten.

42. Tritt ein schwerwiegender Schadensfall ein, über dessen Ursache die betroffene Bank vielleicht keine Kontrolle hat, kann die Fähigkeit der Bank, ihren geschäftlichen Verpflichtungen nachzukommen, teilweise oder ganz zum Erliegen kommen, insbesondere wenn ihre Gebäude, ihre Telekommunikations- und/oder ihre IT-Infrastruktur beschädigt oder unzugänglich geworden sind. Dies kann wiederum erhebliche finanzielle Verluste für die Bank, aber auch – durch Zahlungsverkehrssysteme und andere Übertragungskanäle – weiter reichende Störungen des gesamten Finanzsystems zur Folge haben. Angesichts dieses Schadenspotenzials muss die Bank über Notfallpläne und

Vorkehrungen zur Fortführung der Geschäfte verfügen, die auf verschiedene plausible Szenarien, in denen die Bank verwundbar wäre, sowie auf den Umfang und die Komplexität ihrer Tätigkeit abgestimmt sind.

43. Die Banken sollten die für ihr Geschäft entscheidenden Prozesse identifizieren (auch solche, bei denen sie von externen Zulieferern oder sonstigen Dritten abhängig sind), deren rasche Wiederaufnahme am dringendsten notwendig wäre. Für diese Prozesse sollten die Banken über Ausweichmöglichkeiten verfügen, um ihre Tätigkeit nach einem Ausfall weiterzuführen. Insbesondere sollten sie darauf achten, dass elektronische oder physische Dokumentationen, die für die Wiederaufnahme ihrer Geschäftstätigkeit erforderlich sind, wiederhergestellt werden können. Werden Kopien solcher Daten ausserhalb der Bank gelagert bzw. gespeichert oder muss die Bank ihren Standort verlegen, so ist darauf zu achten, dass diese Standorte weit genug von dem betroffenen Bereich entfernt sind, um das Risiko zu minimieren, dass die Backups gleichzeitig mit den primären Daten und Systemen ausfallen.

44. Die Banken sollten ihre Notfall- und Wiederanlaufpläne kontinuierlich überprüfen, damit sie auf ihre aktuellen Tätigkeiten und Geschäftsstrategien abgestimmt bleiben. Darüber hinaus sind diese Pläne regelmässig zu testen, um sicherzustellen, dass sie im unwahrscheinlichen Fall eines schwerwiegenden Störfalls auch funktionieren.

Die Rolle der Bankenaufsicht

Grundsatz 8: Die Bankenaufsicht sollte von den Banken unabhängig von deren Grösse verlangen, dass sie als Bestandteil ihres generellen Risikomanagements ein wirksames System zur Erkennung, Bewertung, Überwachung und Begrenzung/Minderung erheblicher operationeller Risiken einrichten.

45. Die Aufsichtsinstanzen sollten von den Banken verlangen, dass sie Risikomanagement-Konzepte für operationelle Risiken entwickeln, die den Leitlinien in diesem Papier entsprechen und jeweils auf ihre Grösse, ihre Komplexität und ihr Risikoprofil abgestimmt sind. Sofern operationelle Risiken die Sicherheit und finanzielle Solidität einer Bank gefährden, ist es die Pflicht der Aufsichtsinstanzen, die Bank zur Entwicklung und Anwendung besserer Methoden für das Management dieser Risiken anzuhalten.

Grundsatz 9: Die Bankenaufsicht sollte direkt oder indirekt regelmässige, unabhängige Prüfungen der Strategien, Verfahren und Praktiken einer Bank im Hinblick auf ihre operationellen Risiken durchführen. Die Aufsichtsinstanzen sollten sicherstellen, dass geeignete Mechanismen vorhanden sind, damit sie über die Entwicklungen in den Banken auf dem Laufenden sind.

46. Die unabhängige Prüfung der operationellen Risiken durch die Bankenaufsicht sollte z.B. folgende Aspekte umfassen:

- die Wirksamkeit des Risikomanagements einer Bank und ihr generelles Kontrollumfeld in Bezug auf operationelle Risiken
- die Überwachungsmethoden und die Berichterstattung der Bank im Hinblick auf ihr operationelles Risikoprofil, einschliesslich Daten über operationelle Verluste und sonstige Indikatoren potenzieller operationeller Risiken
- die Vorgehensweise der Bank, um operationelle Risikoereignisse und -anfälligkeiten zeitnah und wirksam zu bewältigen
- die Verfahren der Bank zur internen Kontrolle, Überprüfung und Revision, um die Qualität des gesamten Managements operationeller Risiken zu sichern
- die Wirksamkeit der Bemühungen der Bank um die Minderung operationeller Risiken, z.B. durch Versicherungen
- die Qualität und Lückenlosigkeit der Notfall- und Wiederanlaufpläne der Bank
- das Verfahren der Bank zur Bewertung der Angemessenheit ihrer Eigenkapitalausstattung für operationelle Risiken im Verhältnis zu ihrem Risikoprofil und gegebenenfalls ihren internen Eigenkapitalvorgaben.

47. Bei Banken, die Teil eines Finanzkonzerns sind, sollten die Aufsichtsinstanzen darüber hinaus nach Möglichkeit sicherstellen, dass Verfahren vorhanden sind, die ein angemessenes,

integriertes Management operationeller Risiken für den gesamten Konzern gewährleisten. Bei der Durchführung dieser Prüfung können Zusammenarbeit und Informationsaustausch mit anderen Aufsichtsinstanzen gemäss den üblichen Verfahren erforderlich sein. Auch externe Revisoren können für diese Prüfungen hinzugezogen werden.

48. Mängel, die bei der Prüfung durch die Bankenaufsicht aufgedeckt werden, können mithilfe einer Vielzahl von Massnahmen behoben werden. Die Aufsichtsinstanzen sollten die Instrumente einsetzen, die für die jeweilige Situation und das geschäftliche Umfeld der Bank am besten geeignet sind. Um aktuelle Informationen über operationelle Risiken zu erhalten, können Aufsichtsinstanzen Meldeverfahren direkt mit den Banken und externen Revisoren vereinbaren (interne Berichte an die Geschäftsleitung könnten z.B. routinemässig auch der Bankenaufsicht zur Verfügung gestellt werden).

49. Da Verfahren zu einem umfassenden Management operationeller Risiken bei vielen Banken bekanntlich noch in der Entwicklung sind, sollten die Aufsichtsinstanzen laufende interne Entwicklungsbestrebungen aktiv unterstützen, indem sie die jüngsten Verbesserungen sowie die weiteren Entwicklungspläne der Bank überwachen und evaluieren. Diese Arbeiten können dann mit denen anderer Banken verglichen werden, sodass die Bank nützliche Rückschlüsse auf den Stand ihrer eigenen Arbeit ziehen kann. Sofern Gründe dafür erkannt werden, dass bestimmte Entwicklungsbemühungen erfolglos blieben, könnten diese Informationen auch in allgemeiner Form zugänglich gemacht werden, um den Planungsprozess zu unterstützen. Des Weiteren sollten die Aufsichtsinstanzen darauf achten, in welchem Masse eine Bank das Management operationeller Risiken für ihre gesamte Organisation integriert hat, um zu gewährleisten, dass die einzelnen Geschäftsbereiche ihre operationellen Risiken wirksam handhaben, dass klare Kommunikationswege und Verantwortlichkeiten bestehen, dass eine aktive Selbstbewertung bestehender Praktiken gefördert und mögliche Verbesserungen der Risikominderung in Betracht gezogen werden.

Die Rolle der Offenlegung

Grundsatz 10: Die Banken sollten genügend Informationen offen legen, damit Marktteilnehmer sich ein Urteil über ihren Ansatz beim Management der operationellen Risiken bilden können.

50. Der Ausschuss ist überzeugt, dass die zeitnahe und häufige Offenlegung relevanter Informationen durch die Banken zu besserer Marktdisziplin und folglich wirksamerem Risikomanagement führen kann. Der Umfang der Offenlegung sollte der Grösse, dem Risikoprofil und der Komplexität der Tätigkeiten einer Bank entsprechen.

51. Im Hinblick auf operationelle Risiken bestehen noch keine etablierten Offenlegungsgrundsätze, vor allem weil die Banken noch an der Entwicklung von Methoden zur Bewertung operationeller Risiken arbeiten. Dennoch ist der Ausschuss überzeugt, dass eine Bank ihr Konzept für das Management operationeller Risiken in einer Form offen legen sollte, die es Anlegern und Geschäftspartnern ermöglicht, festzustellen, ob sie operationelle Risiken wirksam erkennt, bewertet, überwacht und steuert.