AUTOREN

Dr. Johannes Voit
ist Abteilungsdirektor beim Deutschen Sparkassen- und Giroverband in Berlin und Projektleiter Operationelle Risiken.

Markus Quick
ist Senior Manager bei der Unternehmensberatung Dr. Peter & Company AG.

STRATEGIE der Sparkassen-Finanzgruppe

Operationelle Risiken

Lernen aus den Fehlern anderer ist ein gutes Rezept

Ein in die Zukunft gerichtetes Management operationeller Risiken (OpRisk) ist auf die Analyse externer Schadensfälle angewiesen. Derzeit liefern bereits mehr als 150 Sparkassen ihre Schadensfälle an den DSGV-Datenpool. Doch geben auch die Medien nahezu täglich einen Einblick in die schlagend gewordenen Risiken anderer Institute. Pool-Daten wie auch Medienberichte bieten reichlich Anschauungsmaterial, das für die Risikoanalyse im eigenen Haus und von den Entscheidungsträgern sinnvoll genutzt werden kann.

Den Bankangestellten Richard Bierbaum kannten nur die wenigsten. Doch der Kredithändler der Crédit-Agricole-Tochter Calyon gelangte im Herbst 2007 zu zweifelhafter Berühmtheit, nachdem das Management der französischen Bank ihn beschuldigt hatte, mit nicht autorisierten Transaktionen 250 Mio. Euro Verlust angehäuft zu haben. Bierbaum kann die gegen ihn erhobenen Vorwürfe nicht verstehen. Seine Antwort: „Meine Chefs wussten, was ich tat. Sie nannten mich nicht umsonst den ‚Goldjungen des Kredithandels'."[1]

Im Handel mit Erdgas verspekulierte sich die kanadische Bank of Montréal um 663 Mio. Dollar. Die Höhe des Verlusts beruht weniger auf einer falschen Markteinschätzung als vielmehr auf Manipulationen bei der Bewertung der Kontrakte, um aufgetretene Verluste zu verschleiern. Auch in deutschen Kreditinstituten führten im vergangenen Jahr Fehlspekulationen in Verbindung mit Verlustverschleierung zu Schäden in dreistelliger Millionenhöhe.

Diese Fälle zeigen eindrucksvoll das potenzielle Ausmaß operationeller Risiken für Finanzdienstleister und machen deutlich, ▶

1 Financial Times Deutschland, 24. Januar 2008.

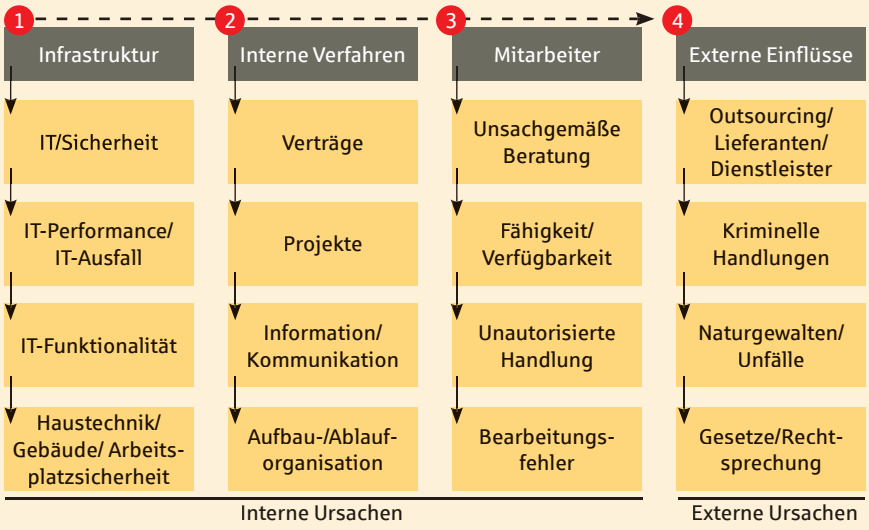
Quelle: dpa

Die Skylines der Banken können noch so imageträchtig sein, auch hinter ihnen verbergen sich operationelle Risiken. Das mussten in jüngster Zeit auch so bekannte Banken wie die französische Crédit Agricole (rechts) und die Société Générale (links) schmerzhaft erleben.

Quelle: dpa

ABBILDUNG 1

Kategorisierung operationeller Risiken



Quelle: Handbuch Operationelle Risiken der Sparkasse, V 1.8. DSGV, Dezember 2007

- dass das strukturierte Management und Controlling dieser Risikoart vor allem unter betriebswirtschaftlichen Aspekten eine lohnenswerte Aufgabe darstellt. Dabei sollten Sparkassen und Banken nach dem Motto „Lernen aus Fehlern – idealerweise aus denen der anderen!" verfahren.

Lernen aus Schadensfällen

2007 war reich an Schadensfällen aus operationellen Risiken. In diesem Jahresrückblick werden exemplarisch sechs Fälle herausgegriffen, die die Bandbreite des Themas aufzeigen und eine besondere Relevanz für die Sparkassen haben. Um aus Fehlern lernen zu können, muss methodisch vorgegangen werden. Zunächst wird der jeweilige Schadensfall, über den die Medien berichtet haben, zusammengefasst, um ihn daraufhin der Systematik der Sparkassen folgend nach Funktionen und Ursachen zu kategorisieren.

Dies ist allerdings auf Grundlage der vorliegenden Informationen nicht immer abschließend zweifelsfrei möglich. So kann eine finale Kategorisierung etwa vom Ausgang einer juristischen Auseinandersetzung abhängen. Daher müssen teilweise mehrere in Frage kommende Ursachenkategorien herangezogen werden. Schließlich werden anhand jedes Falls mögliche Fragestellungen erarbeitet, die Ansatzpunkte für einen Dialog zwischen den Experten eines einzelnen Instituts[2], vor allem aber auch zwischen Experten und dem Vorstand bieten können.

Wichtig dabei ist, darüber zu reflektieren, inwieweit ein bestimmter Vorfall unter Berücksichtigung der Spezifika und Rahmenbedingungen des eigenen Instituts auch hier auftreten könnte und welche Maßnahmen dagegen ergriffen werden können.

In der Sparkassen-Finanzgruppe werden OpRisk-Schadensfälle nach Funktionen und Ursachen kategorisiert.[3] Als mögliche Funktionen stehen dabei Aktivprozesse, Geldanlage- und Passivprozesse, Dienstleistungs- und Serviceprozess, das Vermittlungsgeschäft sowie Geschäftsunterstützungsprozesse zur Verfügung. Die ursachenbasierte Kategorisierung erfolgt anhand der Kategorien Infrastruktur, Mitarbeiter, interne Verfahren und externe Einflüsse, die jeweils in vier weitere Kategorien unterteilt sind (s. Abb. 1).

Ein Beispiel veranschaulicht das Prinzip der Systematik. Wegen eines Rohrbruchs gelangt Wasser durch die Decke in einen Raum der Sparkasse, in dem Gemälde als Leihgaben ausgestellt werden. Dabei werden sie schwer beschädigt. Die entstandenen Kosten verteilen sich wie folgt: Reparatur Rohrbruch 1 200 Euro, Schaden an den Gemälden 25 000 Euro, Gutachterhonorar 400 Euro. Dieser Schadensfall wird der Funktion „Geschäftsunterstützungsprozesse –Verwaltung" zugeordnet und fällt in die Ursachenkategorie „Infrastruktur – Haustechnik, Gebäude, Arbeitsplatzsicherheit". Für eine vollständige Erfassung in der Schadensfalldatenbank müssten unter anderem Fragen nach Versicherungsschutz oder weiteren Maßnahmen beantwortet werden.

Herausforderung Kategorisierung

Was in diesem Beispiel intuitiv logisch erscheint, gestaltet sich in der Praxis oftmals um Einiges schwieriger. Zum einen findet man in der Praxis häufig mehrere Ursachenkategorien, die für einen eingetretenen Schadensfall in Frage kommen. Zum anderen sind die tatsächlichen Wirkungszusammenhänge nicht immer offenkundig. Um diesen Problemen zu begegnen, sieht das vom Deutschen Sparkassen- und Giroverband (DSGV) gemeinsam mit Regionalverbänden und Sparkassen erarbeitete Konzept vor, die Kategorienabfrage für einen eingetretenen Schadensfall jeweils in einer genau festgelegten Reihenfolge durchzuführen (s. Abb. 1). Unser Fallbeispiel wird der ersten zutreffenden Kategorie auf dem Prüfpfad zugeordnet.

Zwei Überlegungen standen für dieses Konzept Pate:

- Eine einheitliche Kategorisierung auch komplizierter Fälle mit mehreren beteiligten Faktoren ist unabdingbar für die Befüllung und die Analyse des Datenpools.
- Die Kategorisierung soll auch interne Steuerungsimpulse geben. Die Gestaltung wirksamer Steuerungsmaßnahmen wird umso schwieriger, je weiter man in dem Kategorienbaum voranschreitet.

Darüber hinaus liegt das Potenzial der Kategorisierung gerade in der Analyse der Schadensfälle und der ihnen zugrundeliegenden Wirkungszusammenhänge. Nur wenn sie bekannt sind, können effektive Maßnahmen als Reaktion auf Schadensfälle ergriffen werden. Wie die folgenden Beispiele zeigen, ist hier gegebenenfalls eine vertiefte Analyse notwendig, um Ursache-Wirkungs-Ketten

INFOBOX 1

Operationelle Risiken

Operationelle Risiken sind definiert als „die Gefahr von Schäden, die in Folge der Unangemessenheit oder des Versagens von

- internen Verfahren,
- Mitarbeitern,
- der internen Infrastruktur oder
- in Folge externer Einflüsse

eintreten." Diese Definition beinhaltet auch „Rechtsrisiken" sowie „Reputationsrisiken" als Folge operationeller Risiken, jedoch nicht die „strategischen Risiken".

Quelle: Handbuch Operationelle Risiken der Sparkasse, V 1.8. DSGV, Dezember 2007

2 Beispielsweise für den Einsatz der Methode „Risikolandkarte" in einer Sparkasse.

3 M. Daferner, M. Quick und J. Voit, Modernes Management operationeller Risiken, Betriebswirtschaftliche Blätter 4/2006, S. 197.

Quelle: dpa

In einem Müllcontainer eines Hinterhofs lagen die geheimen Baupläne für den Tresor der Berliner Hauptverwaltung der Deutschen Bundesbank.

und die damit verbundenen Steuerungsmöglichkeiten erkennen zu können.

Lernprozess

Die Schadensbeispiele eignen sich dafür, von dem eigentlichen Vorfall zu abstrahieren und entsprechende Fragen zur Sicherheit des eigenen Instituts zu stellen. Daraus werden die Voraussetzungen für die "Internalisierung" des Vorfalls geschaffen.

Konkret steht dabei die Frage im Mittelpunkt, ob ein solcher oder ähnlicher Fall auch im eigenen Institut zu Schäden führen könnte oder ob wirkungsvolle Gegenmaßnahmen bereits vorgesehen sind. Die Ergebnisse dieses Prozesses sollten dann den Entscheidungsträgern der Sparkasse bis hin zum Vorstand vorgestellt werden.

Hagen verklagt Deutsche Bank

Sachverhalt

Die Stadt Hagen vereinbarte im Frühjahr 2005 mit der Deutschen Bank Swap-Geschäfte für langfristige Kredite. Die Verantwortlichen der Stadt hofften dadurch, die Zinszahlungen für Kredite in einem Volumen von insgesamt 170 Mio. Euro deutlich verringern zu können. Die Zinsentwicklung lief jedoch anders als erwartet und erhofft. Dadurch sank der Kurs der im Rahmen dieses Geschäfts erworbenen Wertpapiere. Im Juni des Jahres vereinbarte die Stadt daraufhin mit der Bank nachträglich eine Verlustobergrenze. Dadurch konnte der Gesamtverlust aus den bis 2010 laufenden Geschäften 50 Mio. Euro nicht mehr überschreiten.

Zudem strengte die Stadt eine Klage gegen die Deutsche Bank an. Sie argumentierte, sie sei über mögliche Verluste durch diese Papiere nicht ausreichend beraten bzw. aufgeklärt worden. Nach dem Scheitern eines ersten Schlichtungsversuchs befinden sich die Parteien derzeit noch in der juristischen Auseinandersetzung.

Kategorisierung

Dieser Schaden wird im OpRisk-Funktionsmodell der Sparkassen-Finanzgruppe der Funktion Aktivprozesse zugeordnet. Für die Ursachenkategorisierung kommen je nach Ausgang der juristischen Auseinandersetzung zwei Aspekte in Betracht. Wird die Bank schuldig gesprochen, deutet vieles auf eine Einordnung unter „Mitarbeiter – Unsachgemäße Beratung" hin. Eine genaue interne Analyse des Vorfalls könnte jedoch auch Vertrags- oder Organisationsprobleme offenbaren und zu einer Kategorisierung unter „Interne Verfahren" führen.

Wird die Deutsche Bank freigesprochen, ist der klagefreudige Kunde die Ursache des operationellen Risikos, das sich dann auf den Rechtsstreit beschränkt. In diesem Fall wäre die Kategorie „Externe Einflüsse – Gesetze/Rechtsprechung" sachgerecht. Unabhängig davon ist ein Reputationsrisiko für die Bank eingetreten. Dieses kann vor allem im Falle einer Niederlage der Bank vor Gericht einen erhöhten Schaden durch Opportunitätskosten nach sich ziehen.

Abgeleitete Fragestellungen

Der Fall „Deutsche Bank gegen Stadt Hagen" gibt Anlass, intensiv nachzuprüfen, ob das eigene Haus dagegen gefeit wäre. Dazu drängen sich etwa die folgenden Fragen auf:

- Welche (komplexeren) Produkte werden im Firmenkunden- bzw. Kommunalgeschäft aktuell vertrieben?
- Sind die Mitarbeiter durchgängig in der Lage, das Produkt angemessen zu erläutern, also Chancen und Risiken adäquat darzustellen?
- Existiert ein standardisierter Prozess zur Einführung neuer Produkte im (Firmenkunden-)Vertrieb? Werden im Rahmen dieses Prozesses auch alle mit dem Produkt für die Sparkasse einhergehenden einschließlich der operationellen Risiken betrachtet?
- Werden für neue Produkte regelmäßige Trainings bzw. Schulungen für die Mitarbeiter angeboten? Ist die Teilnahme verpflichtend?
- In welcher Form wird die ausreichende Fach- bzw. Produktkenntnis des Ansprechpartners auf Kundenseite vor allem im Firmenkundengeschäft eingeschätzt, geprüft und dokumentiert?
- Welche Dokumente, Prospekte und sonstige schriftliche Informationen werden den Kunden zur Verfügung gestellt?
- Sind Produktinformationen und -prospekte vor ihrer Ausgabe einer umfassenden, darunter auch rechtlichen Prüfung unterzogen worden?
- Wie wird das Beratungs- bzw. Verkaufsgespräch dokumentiert? Ist die Dokumentation rechtssicher?

Banktresor-Bauplan im Hausmüll

Sachverhalt

Vier Wochen nach dem Umzug der Bundesbank-Hauptverwaltung Berlin in ein neues Gebäude wurden detailgetreue Zeichnungen des hoch gesicherten Tresorraums in einem Müllcontainer eines Berliner Hinterhofs gefunden. Die Pläne enthielten geheime Informationen unter anderem zu Sicherheitsvorkehrungen wie Personalmeldern oder der Dicke der Wände. Die Pläne wurden zwar der Deutschen Bundesbank zurückgegeben, doch lief dies nicht ohne eine entsprechende mediale Berichterstattung ab. Sie prüft nun strafrechtliche Schritte gegen den oder ▶

INFOBOX 2

Die Top 10 operationellen Risiken im Jahr 2008

1. Transparenz über Subprime-Risiken
2. Betrug durch Insider (einschließlich Identitätsdiebstahl, Datenraub, Schläfer)
3. Risiken aus Verbraucherschutzvorschriften
4. Modellrisiko
5. Rechtsrisiko, insbesondere auch die Durchsetzbarkeit von Verträgen
6. Schubladendenken und fehlender Gesamtüberblick im Risikomanagement
7. Reputationsrisiko
8. Abwicklungsrisiko
9. Pandemierisiko und Notfallplanungen
10. Umweltrisiken

Quelle: D. Beyon und E. Davis, OpRisk & Compliance, Dezember 2007, S. 20

- die Verursacher. Allerdings ist noch nicht geklärt, ob interne Mitarbeiter oder externe Dienstleister, die am Bau beteiligt waren, für den Vorfall verantwortlich gemacht werden können. Zudem muss davon ausgegangen werden, dass aus Sicherheitsgründen die bisher getroffenen Vorkehrungen verändert werden müssen. Dadurch sind zahlreiche kostspielige Neuregelungen und Umbauarbeiten notwendig.

Kategorisierung

Dieser Schaden wird im Modell der Sparkassen-Finanzgruppe der Funktion Geschäftsunterstützungsprozess zugeordnet. Für die Einordnung in eine Ursachenkategorie kommen nach dem vorliegenden Kenntnisstand drei Kategorien in Frage, da noch unklar ist, wie die Pläne in den Müllcontainer gelangt sind. Möglich ist zunächst die Kategorie „Mitarbeiter – Bearbeitungsfehler", vorausgesetzt ein Bundesbank-Mitarbeiter hat diesen Schaden durch einen Fehler verursacht. Die zweite mögliche Kategorie wäre „Externe Einflüsse – Outsourcing/Lieferanten/Dienstleister", wenn ein Mitarbeiter der am Bau beteiligten Dienstleister den Schaden verursacht hat. Als dritte Möglichkeit kommt noch die Kategorie „Interne Verfahren – Aufbau- und Ablauforganisation" in Betracht, sofern der Schaden auf einen fehlerhaften internen Prozess zurückzuführen ist. Unabhängig von der Kategorisierung wurde das Reputationsrisiko als Folgerisiko schlagend.

Abgeleitete Fragestellungen

Der Umgang mit sensiblen Daten ist für alle Finanzdienstleister relevant. In diesem Zusammenhang stellen sich einer Sparkasse unter anderem die Fragen:

- Welche Dienstleister haben Zugang zu sensiblen Daten der Sparkasse?
- Wie wird bei ausgelagerter Aufgabenerfüllung die Vertraulichkeit von Informationen sichergestellt?
- Ist der Umgang mit dem Datenmaterial Bestandteil des Vertrags bzw. Service-Level-Agreements? Wie werden Haftungsfragen geregelt?
- Wird der vertrauliche Umgang mit sensiblen sparkasseneigenen und kundenspezifischen Daten im Rahmen etwa von Dienstanweisungen verbindlich geregelt? Werden die Mitarbeiter für dieses Thema regelmäßig sensibilisiert?
- Wie werden Datenmüll bzw. sensible Daten entsorgt? Erfolgt eine Mülltrennung (Reißwolf etc.) und werden auch CD-ROM und andere elektronische Datenträger sicher entsorgt bzw. zerstört? Werden die Festplatten von Computern vor Reparaturen gesäubert?
- Wo und wie werden etwa Kreditakten gelagert? Ist der Zugriff für Externe möglich, eventuell auch nur temporär (Handwerker etc.)?
- Werden bei hausexternen und -internen Umzügen sensible Daten durchgängig vor dem unbefugten Zugriff durch Externe geschützt?

Prospekthaftung

Sachverhalt

Eine Sparkasse hat in den 90er Jahren kreditfinanzierte Beteiligungen an geschlossenen Immobilienfonds (Hauck-Immobilienfonds) verkauft. Dabei hatte sie unter anderem damit geworben, dass die Beteiligungsgewinne die Kosten für Darlehenszins und -tilgung übersteigen würden. Aufgrund überteuerter bzw. nicht marktgerecht bewerteter Immobilien war dies jedoch nicht der Fall. Einem Anleger entstand durch diese „Schrottimmobilien" ein Schaden von rund 12 000 Euro. Inzwischen hat das Landgericht der Klage eines Kunden stattgegeben und die Sparkasse nach dem Haustürwiderrufsgesetz zur Rücknahme der Anteile sowie zur Rückzahlung sämtlicher Zins- und Tilgungsleistungen verpflichtet.

Kategorisierung

Dieser Schaden ist der Funktion Vermittlungsgeschäft zuzuordnen. Die entsprechende Ursachenkategorie ist nach dem vorliegenden Kenntnisstand „Mitarbeiter – Unsachgemäße Beratung". Hinzu kommt das Reputationsrisiko als Folgerisiko sowohl für die Sparkasse als auch den Anbieter der Fonds.

Abgeleitete Fragestellungen

Um ähnlich gelagerte Schadensfälle im eigenen Haus zu vermeiden, sollten die zum Fall „Deutsche Bank gegen Stadt Hagen" formulierten Fragen analog für das Privatkundengeschäft beantwortet werden. Zusätzlich empfiehlt es sich, diese Fragen dahingehend zu erweitern, dass in diesem Fall die Produkte eines Drittanbieters vertrieben wurden. Außerdem bietet es sich an, hier bewusst den Umgang mit Kundenbeschwerden zu thematisieren („Musste es zwangsläufig zu einer juristischen Auseinandersetzung mit dem einhergehenden Reputationsrisiko kommen?").

Manipulationen an Geldautomaten

Sachverhalt

In jüngster Zeit sind vermehrt Manipulationsversuche an Geldautomaten zu beobachten. Die Täter greifen dabei zu immer neuen, fortgeschritteneren Verfahren wie dem „Skimming". Bei diesem Verfahren präparieren die Täter Geldautomaten, um an die Daten auf dem Magnetstreifen der EC-Karten zu gelangen und spähen zudem mit Videokameras oder speziellen Tastaturaufsätzen die PIN der Karten aus. Anschließend werden die Daten auf eine Blankokarte kopiert. Gemeinsam mit der ausgespähten PIN wird dann an ausländischen Automaten Geld abgehoben, da hier die falsche Karte wegen der geringeren Sicherheitsstandards nicht als Fälschung erkannt wird. Derzeit erstatten die Sparkassen ihren Kunden den durch Betrug entstandenen Fehlbetrag.

Kategorisierung

Diese Schäden werden in einer betroffenen Sparkasse der Kategorie Dienstleistungs-/Serviceprozesse zugeordnet. Als Ursachenkategorien kommt zunächst die Kategorie „Infrastruktur – IT-Funktionalität" in Frage.

Quelle: Sparkasse KölnBonn

Mit diesem Foto und anderen erklärenden Abbildungen warnt die Sparkasse KölnBonn im Internet ihre Kunden vor Manipulationen am Geldautomaten. In diesem Fall verdeckt eine Schiene eine dahinter angebrachte Mini-Kamera.

Diese Zuordnung ist richtig, solange nicht feststeht, ob die Sicherheitsstandards an den Geldautomaten als „Best Practice" einzustufen sind. „Externe Einflüsse – Kriminelle Handlungen" ist dagegen zu wählen, wenn die Gerätesicherheit so gut ist, dass sie als mögliche Mitursache ausscheidet. Dann liegt die alleinige Ursache in der kriminellen Handlung von Externen.

Im ersten Fall kann das operationelle Risiko durch eine Verbesserung des Sicherheitsstandards verringert werden. Eine solche Steuerungsmöglichkeit hat das Institut bei der zweiten Kategorie „Externe Einflüsse" nicht. Das Risiko kann in diesem Fall nur noch akzeptiert bzw. transferiert werden. Auf jeden Fall besteht für das betroffene Institut ein Reputations- als Folgerisiko.

Abgeleitete Fragestellungen

Diese Schadensfälle zwingen daher alle Institute unter anderem zu folgenden Fragen:

- Wer ist für die IT-Sicherheitsstandards bei Servicegeräten zuständig? Wie werden Haftungsfragen allgemein und innerhalb der Organisation geregelt?
- Welche Vorgaben und Standards gibt es für die Kommunikation mit Polizei und Presse?
- Wie wird mit Kundenbeschwerden umgegangen? Gibt es einheitliche Prozesse etwa über mögliche Erstattungen?
- Wie funktioniert die sparkassen- bzw. institutsübergreifende Erstellung von IT-Sicherheitsstandards?
- Welche zusätzlichen IT-Sicherheitsmaßnahmen sind gegen Skimming und ähnliche Kartendelikte denkbar? Welche Kosten verursachen sie? Welche Kosten würden eingespart, wenn solche Systeme eingesetzt würden?
- Gibt es ein Frühwarnsystem, das neue Betrugsverfahren und -methoden an andere Häuser innerhalb der Organisation meldet?
- Wie werden solche Fälle bei Kosten/Nutzen-Überlegungen zur Sicherheitstechnik berücksichtigt? Werden dabei nur die Kosten für die einzelne Sparkasse oder auch für die gesamte Sparkassen-Finanzgruppe berücksichtigt?

Verstoß gegen externe Vorgaben

Sachverhalt

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ermittelt gegen die DekaBank, da mehrere Sparkassen Anteile am Immobilienfonds Real Estate Plus 1 verkauft haben, obwohl dieser noch nicht von der BaFin genehmigt und zum Vertrieb freigegeben war, wie es nach dem Investmentgesetz vorgeschrieben ist. Nach Darstellung der Verantwortlichen wurde der Fonds vor der Genehmigung noch nicht vertrieben, vielmehr kam es lediglich zu einem „Private Placement" bei den Sparkassen. Dabei wird das Produkt nicht beworben, sondern lediglich einem ausgewählten Kundenkreis angeboten. Dieses Vorgehen sei bekannt und marktüblich. Die Prüfung, inwieweit gegen Gesetze oder Verordnungen verstoßen wurde, ist noch nicht abgeschlossen. Gegebenenfalls könnten auch noch den betroffenen Sparkassen Sanktionen drohen.

Kategorisierung

In den vorangangenen vier Fällen war operationelles Risiko unzweifelhaft schlagend geworden. Bei diesem Sachverhalt hängt die Einstufung als operationelles Risiko noch vom Ausgang der BaFin-Prüfung ab. Ergeben sich keine Beanstandungen, liegt nach den vorliegenden Informationen kein operationelles Risiko vor. Unter der Hypothese, dass die Prüfung zu Beanstandungen führt, würde der Fall der Funktion „Vermittlungsgeschäft" zugeordnet. Die Ursache wäre dann in „Interne Verfahren – Aufbau- und Ablauforganisation" zu suchen. Hier wurden nach allen bisher bekannten Informationen sparkassenintern Abläufe im Drittvertrieb nicht klar strukturiert. Ein Reputationsrisiko besteht unabhängig vom Ausgang des Verfahrens jedoch bereits jetzt.

Abgeleitete Fragestellungen

Sparkassen sollten sich anhand dieses Beispielfalls unter anderem die folgenden Fragen stellen:

- Wie werden neue Produkte entwickelt bzw. welche Prozesse werden durchlaufen, bevor (Dritt-)Produkte in den Vertrieb aufgenommen werden?
- Wie wird die Rechtsabteilung in Produktentwicklung und Marketing-Maßnahmen eingebunden?
- Existieren für interne und externe Anbieter, deren Produkte von der Sparkasse vertrieben werden, verbindliche Standards?
- Wie werden Entscheidungen in der Produktentwicklung bzw. der entsprechende Prozess dokumentiert?
- Wie wird sichergestellt, dass relevante Rechtsvorschriften eingehalten werden?
- Gibt es standardisierte Prozesse mit den Anbietern von (Dritt-)Produkten in der Finanzgruppe? Informieren diese Anbieter regelmäßig auch über mögliche Risiken, die mit diesen Produkten verbunden sind?
- Wie werden Haftungsfragen innerhalb der Finanzgruppe mit dem Anbieter geregelt?

Unregelmäßigkeiten im Handel

Sachverhalt

Durch die eingangs geschilderte Fehlspekulation eines Händlers musste die französische Großbank Crédit Agricole in der New Yorker Niederlassung ihrer Investment-Banking-Tochter Calyon Verluste von 250 Mio. Euro verbuchen. Dabei wurden nach vorliegendem Kenntnisstand interne Limite überschritten. Nach Darstellung der Bank sind die Verantwortlichen inzwischen zur Rechenschaft gezogen und die entsprechenden Sicherheitsvorkehrungen verstärkt worden.

Kategorisierung

Dieser Schadensfall würde der Funktion „Geldanlage – Passivprozesse" zugeordnet. ▸

Als Ursachenkategorie kommen sowohl die Kategorie „Mitarbeiter – Unautorisierte Handlung" als auch „Interne Verfahren – Aufbau- und Ablauforganisation" in Frage. Zwar deutet die Limit-Überschreitung zunächst auf die erste Kategorie hin, doch könnten auch mangelhafte Kontrollsysteme, die eine Limit-Überschreitung erst zulassen, Ursache für den entstandenen Schaden sein. Darauf deutet auch die in einer Zeitung zitierte Aussage des Händlers Richard Bierbaum hin. Eine abschließende Kategorisierung kann demnach nur nach Prüfung der Vorkommnisse durch die Bank selbst erfolgen. Auch dieser Schaden ist mit einem Reputationsrisiko für die Bank verbunden.

Abgeleitete Fragestellungen

Um den Lernprozess zu unterstützen, empfiehlt es sich in diesem Fall beispielhaft, Antworten auf die folgenden Fragen zu suchen:

- Wie erfolgt die Risikobegrenzung/Limitierung im (Eigen-)Handel? Welche Kontroll- bzw. Sicherheitsmaßnahmen existieren hier? Gibt es Hinweise auf Schwachstellen? Werden Kosten/Nutzen-Überlegungen bei zusätzlichen Maßnahmen angestellt?
- Wie wird die Einhaltung von Limiten angemessen kontrolliert? Wie sieht der Berichtsweg aus?
- An wie viele Personen gehen automatische Warnsignale bei Limitüberschreitung? Reicht ein einzelner Komplize aus, um unautorisierte Positionen verschleiern zu können?
- Wo ist die Compliance-Funktion organisatorisch verankert? Wie ist diese Funktion in den Informationsfluss eingebunden? Wie ist das Thema Compliance im Anreizsystem berücksichtigt?
- Wie werden Risiken im Anreizsystem berücksichtigt? Wie werden Haftungsfragen dabei geregelt?
- Wie ist die Zusammenarbeit zwischen Compliance, Rechts-, Personalabteilung und Verwaltungsrat geregelt?

Die britische Fachzeitschrift „OpRisk & Compliance" hat Experten zu den für das laufende Jahr am höchsten eingeschätzten operationellen Risiken befragt. Die Ergebnisse sind in der Infobox 2 zusammengefasst. Bereits Anfang 2008 sprechen spektakuläre Fälle wie der Betrug eines Händlers der französischen Großbank Société Générale oder der Datenraub in Liechtenstein, aber auch die fortwährenden Abschreibungen zahlreicher Banken auf strukturierte Kreditderivate dafür, dass diese Einschätzungen ernstzunehmen sind.

Vorstand ist verantwortlich

Die Mindestanforderungen an das Risikomanagement (MaRisk) bekräftigen, dass die Verantwortung für das Risikomanagement unabhängig von der internen Zuständigkeitsregelung auf allen Geschäftsleitern eines Instituts liegt. Dies gilt auch für die operationellen Risiken, die in den MaRisk als wesentliche Risiken eingestuft werden. Diese Verantwortung kann nicht delegiert werden. Auch die Schaffung einer offenen Risikokultur im Institut ist erfahrungsgemäß in hohem Maß vom Management des Instituts abhängig.

Die anhand der Beispielfälle entwickelten Fragen sollen dabei helfen, aus den Schäden anderer Häuser zu lernen und für das eigene Institut die richtigen Rückschlüsse zu ziehen. In diese Analyse sollten sowohl Spezialisten als auch die Entscheidungsträger des Instituts, bis hin zum Vorstand, einbezogen werden. Bei einer Betrachtung dieser Fälle im Rahmen der Methode „Risikolandkarte" wird dem Vorstand über die Erkenntnisse berichtet.

In zahlreichen Sparkassen werden so erarbeitete Maßnahmenvorschläge direkt in der Ergebnispräsentation vorgelegt. In einigen Fällen empfehlen sich auch Ad-hoc-Analysen. So wird berichtet, dass der Deutsche-Bank-Chef Josef Ackermann unmittelbar nach Bekanntwerden des 6-Mrd.-Euro-Betrugsfalls bei der Société Générale Anfang 2008 eine interne Untersuchung beauftragte, die klären sollte, inwieweit ein ähnlicher Betrugsfall auch in seinem Haus auftreten könne.

Fazit

Wichtige Fragen, die sich Entscheidungsträger in der Sparkassen-Finanzgruppe zum Thema operationelle Risiken stellen sollten, sind in der Infobox 3 zusammengestellt. Wenn diese Fragen positiv beantwortet werden können, ist das Institut gut aufgestellt, die verbleibenden Risiken sind zu akzeptieren. Dennoch wird auch im weiteren Verlauf des Jahres 2008 der ein oder andere OpRisk-Schadensfall schlagend werden. Von spektakulären Fällen bleibt die Finanzgruppe aber hoffentlich verschont. Institute der Sparkassen-Finanzgruppe können eine weiterführende Analyse der dargestellten Schadensfälle im Web unter www.umsetzungsbaukasten.de abrufen.

INFOBOX 3

Fragen der Entscheidungsträger zu operationellen Risiken:

- Werden die Instrumente Schadensfalldatenbank, Risikolandkarte, Risikoinventur zur Ermittlung, Bewertung und Steuerung der operationellen Risiken in der Sparkasse bereits angemessen eingesetzt?
- Werden diese Instrumente durch den DSGV-Datenpool optimal unterstützt?
- Wird der Vorstand bzw. das Top-Management regelmäßig und mit den relevanten Informationen zum Status quo der einzelnen Risikobereiche versorgt (OpRisk-Berichtswesen)? Sind die Informationen geeignet, wenn notwendig, entsprechende Managementmaßnahmen einzuleiten?
- Wird der Risikoart im Kreise der Führungskräfte und Mitarbeiter ein ausreichender Stellenwert eingeräumt bzw. ist das Bewusstsein für OpRisk in ausreichendem Maße vorhanden? Wird die Akzeptanz durch den Vorstand und das Top-Management „vorgelebt" bzw. gefördert?
- Gibt es einen strukturierten Prozess zur Einführung neuer Produkte oder Prozesse? Wird dieser Prozess federführend vom oder unter maßgeblicher Mitwirkung des OpRisk-Managements durchgeführt?
- Ist das OpRisk-Management in die Entscheidungen zum Outsourcing von Aufgaben oder in die Erstellung der Notfallplanung eingebunden?
- Werden zentrale Ertragsquellen der Sparkasse regelmäßig auch auf operationelle Risiken hin geprüft?
- Gibt es einen eingeübten Prozess für die Kommunikation mit Kunden und der Öffentlichkeit, um das Reputationsrisiko in der Folge eines Schadensfalls zu begrenzen?