

Juli 2014

OpRisk und RepRisk in der SREP-Leitlinie der EBA

Konsultation der Elemente zu operationellen Risiken und Reputationsrisiken als Teil eines holistischen Ansatzes für den aufsichtlichen Überprüfungs- und Überwachungsprozess

Executive Summary

Am 7. Juli 2014 hat die EBA den Entwurf einer Leitlinie zum aufsichtlichen Überprüfungs- und Überwachungsprozess (SREP – Supervisory Review and Evaluation Process) veröffentlicht und zur Konsultation gestellt. Der Entwurf richtet sich an alle Aufsichtsbehörden der Staaten der Europäischen Union. Die Konsultationsfrist läuft bis 7. Oktober 2014; nach der aktuell geäußerten Erwartungshaltung soll die Leitlinie spätestens ab 2016 angewendet werden.

Die EBA verfolgt im Entwurf der Leitlinie einen ganzheitlichen SREP-Ansatz und gibt eine EU-weit einheitliche Säule II-Behandlung vor. Dies schließt neben der Beurteilung von Risiken für die Kapital- und Liquiditätsausstattung auch die regelmäßige Überwachung von Indikatoren zur Finanz- und Risikolage sowie die Analyse des Geschäftsmodells und die Beurteilung des internen Kontrollsystems (IKS) mit ein.

Der Entwurf umfasst bezüglich der Risiken für die Kapitalausstattung Kredit- und Kontrahentenrisiken, Marktpreisrisiken, Zinsänderungsrisiken im Anlagebuch und operationelle Risiken (OpRisk). Er benennt die in der Capital Requirements Regulation (CRR) für Säule I festgelegten Regelungen für die einzelnen Risikoarten als Mindestanforderungen und geht in Säule II für alle EU-Staaten in Zukunft weit über diese hinaus.

Insbesondere die Behandlung von OpRisk wird im SREP gegenüber den in Deutschland geltenden Mindestanforderungen an das Risikomanagement der Institute (MaRisk) sehr stark konkretisiert und erweitert. So sind zukünftig neben OpRisk auch explizit Reputationsrisiken (RepRisk) zu beachten. Zu den weiteren Neuerungen zählen ferner die explizite Betrachtung der Unterkategorien Verhaltensrisiken („Conduct Risk“), IT- und Modellrisiken.

Nicht zuletzt sollen die Aufsichtsbehörden die Beurteilung des OpRisk-Profiles noch stärker in den Zusammenhang mit der Angemessenheit von IKS und Auslagerungsvereinbarungen sowie bestehender Maßnahmenpläne für Notfälle beurteilen. Bereits vor der anstehenden grundlegenden Überarbeitung der OpRisk-Kapitalansätze in Säule I wird somit erhöhter Druck über die Säule II ausgeübt.

Der neue SREP für OpRisk kann im Ergebnis zu neuen Unternehmenssteuerungsansätzen für diese „nicht-klassischen Finanzrisiken“ sowie im Rahmen der vollständigen Abdeckung der konkretisierten Anforderungen zu erhöhten Kapitalbedarfen unter Säule II führen. Wir empfehlen deshalb, sich auf diesen Änderungsprozess durch eine strukturierte Bestandsaufnahme vorzubereiten.

Inhalt

Executive Summary
Seite 1

Operationelle Risiken und Reputationsrisiken im Rahmen des SREP-Ansatzes
Seite 2

Implikationen und möglicher Handlungsbedarf für deutsche Institute
Seite 3

Nächste Schritte
Seite 6



Operationelle Risiken und Reputationsrisiken im Rahmen des SREP-Ansatzes

Der Turnus, die Intensität und der Detailgrad der Anwendung des SREP-Ansatzes hängen zunächst von der Eingruppierung der Institute in vier Kategorien ab. Diese sollen die Systemrelevanz eines Instituts reflektieren und somit das **Proportionalitätsprinzip** bei der Beaufsichtigung sicherstellen. Die SREP-Anwendung mündet in ein durch die Aufsicht festgelegtes Gesamturteil (Score) für das Institut, der sich wiederum aus Teil-Scores ableitet.

Ein gesonderter Teil-Score wird auch für die Beurteilung des OpRisk durch die zuständige Aufsichtsbehörde entwickelt. Dieser beruht gemäß dem Leitlinien-Entwurf aus zwei Komponenten:

- der Beurteilung des **inhärenten Risikogehalts** für OpRisk und
- der Würdigung der **Steuerungs-, Bewertungs- und Kontrollverfahren**.

RepRisk werden zwar als Teil des OpRisk betrachtet, jedoch bei der Bewertung des Teil-Scores für das Geschäftsmodell und/oder des Liquiditätsprofils berücksichtigt, da sich dort potentielle Auswirkungen durch einen Verlust von Vertrauen durch Investoren, Gläubiger, Kunden oder Teilnehmer am Interbankenmarkt und damit einhergehende Gewinnrückgänge materialisieren.

Inhärenter Risikogehalt

Zur Beurteilung des inhärenten Risikogehalts werden in einem ersten Schritt eine Vielzahl verfügbarer Informationen wie OpRisk-Strategien, Geschäftsumfeld, regulatorischer und ökonomischer Kapitalanteil für OpRisk, materielle Ereignisse im Institut wie Übernahmen und Restrukturierungen, wesentliche Änderungen an Prozessen und IT-Landschaft und Auslagerungsstrategien begutachtet.

So sollen die potentiellen Quellen des OpRisk identifiziert werden. Ausdrücklich erwähnt werden ferner Informationen zu Compliance-Verstößen gegen externe oder interne Regelungen, die Realisierbarkeit von Geschäftsplanungen und die Angemessenheit von Anreiz- und Vergütungssystemen und die Komplexität von Prozessen, Produkten und IT-Landschaft.

Die identifizierten Risiken werden in einem zweiten Schritt auf einer detaillierteren Ebene hinsichtlich des Wesens und der Materialität der OpRisk-Risikopositionen analysiert. Dabei sollen sowohl quantitative (z.B. Bewertungen aufgrund Verlustdatensammlungen) als auch qualitative Verfahren (z.B. Szenario-Analysen der Institute) zum Einsatz kommen.

Grundsätzlich soll eine Unterscheidung zwischen Risiken mit sogenanntem „low frequency/high severity“- und „high frequency/low impact“-Profil möglich sein, da insbesondere erstgenannte den Schwerpunkt des Risikomanagements darstellen sollen. Insgesamt gesehen sollen auch die Unterkategorien Conduct Risk, IT-Risiken sowie Modellrisiken näher beleuchtet werden.

Der Leitlinien-Entwurf spezifiziert Ausprägungen von **Verhaltensrisiken („Conduct Risk“)** im Kundengeschäft wie z.B. Verkaufspraktiken von Produkten, Interessenskonflikte und Anreizverfahren in Vertriebskanälen sowie Marktmanipulationen. Als mögliche Indikatoren werden neben Sanktionen und Strafzahlungen auch Kundenbeschwerden genannt.

Unter Conduct Risk werden grundsätzlich gemäß EBA-Entwurf Gefährdungen der Ertrags- oder Vermögenslage eines Instituts durch unangemessenes oder bewusstes Fehlverhalten bei der Erbringung von Finanzdienstleistungen

verstanden. Diese Verhaltensrisiken sind auch im Zusammenhang mit Rechtsrisiken zu sehen, die bereits heute per Definition Teil von OpRisk sind.

Hinsichtlich der **IT-Risiken** werden Sachverhalte genannt, die genauer beurteilt werden sollen. Dazu gehören die bereits aus den MaRisk bekannten Themen wie Business Continuity Management, Zugriffsberechtigungen und Datenintegrität für das Reporting. Dies sind auch Schwerpunkte von bereits heute zunehmenden Sonderprüfungen der Aufsicht zu IT-Themen. Hier steht der konkrete Eingang in die Bewertung des OpRisk-Profiles im Vordergrund.

Die zuständigen Aufsichtsbehörden sollen auch Risiken aus der fehlerhaften Anwendung von **Modellen** beurteilen, die z.B. für Zwecke der Produktkalkulation, Bewertung von Finanzinstrumenten oder Risikoquantifizierung eingesetzt werden. Dabei sind Kontrollen wie z.B. Validierungen, Back-Testings und Kalibrierungen von Marktparametern sowie Vorsichtsmaßnahmen zu bewerten.

Erstmalig ist im Kontext von OpRisk auch eine Bewertung der **Reputationsrisiken** vorgesehen. Diese soll sowohl auf RepRisk als eigenständige Risikoart (anhand aufgeführter qualitativer Indikatoren wie Medienkampagnen und Kundenbeschwerden) als auch im Zusammenhang mit anderen Risikoarten wie z.B. OpRisk – sowohl als Ursache als auch als Folge – abzielen.

Sowohl bei organisatorischen Strukturen für Management und Controlling als auch bezüglich einsetzbarer Instrumente sieht der Entwurf Verbindungen zu OpRisk. Ferner ist die prominente Erwähnung der Bedeutung und erforderlichen Überprüfung der Risikokultur bei Instituten bemerkenswert. Dazu hatte der Financial Stability Board erst im April 2014 Leitlinien für Aufsichtsbehörden veröffentlicht.

Steuerungs-, Bewertungs- und Kontrollverfahren

Als zweite Komponente des SREP-Ansatzes für OpRisk ist eine Überprüfung der OpRisk-Strategie und -neigung, des Organisationsrahmens, der Richtlinien und Prozesse, der Risikoidentifikation, -bewertung, -überwachung und -berichterstattung, der Business Continuity-Prozesse sowie des internen Kontrollsystems geplant. Dies wird durch die Beurteilung des Rahmenwerks für Reputationsrisiken ergänzt.

Für alle oben genannten Analysegebiete der Aufsicht werden detaillierte Vorgaben gemacht, die in Umfang und Detailgrad deutlich über die bekannten Regelungen der MaRisk hinausgehen. Als Ergebnis der Untersuchungen ist ein **Score des OpRisk-Profiles** des untersuchten Instituts in eine von vier Ausprägungen (kein erkennbares, geringes, mittleres bzw. hohes Risiko) vorgesehen.

Implikationen und möglicher Handlungsbedarf für deutsche Institute

Der Entwurf der EBA-Leitlinie lässt erwarten, dass sich der aufsichtliche Überprüfungs- und Überwachungsprozess auch für OpRisk fundamental ändern wird, inklusive der von den Instituten anzuwendenden Verfahren für die Ermittlung der Risikotragfähigkeit. Ferner wird erstmalig RepRisk als Untersuchungsgegenstand eingeführt. Auch wenn die vorgeschlagenen Änderungen noch Gegenstand eines Konsultationsprozesses sind, empfehlen wir insbesondere allen zukünftig direkt von der EZB beaufsichtigten Instituten, sich auf diesen Änderungsprozess vorzubereiten.

Wichtig ist jetzt, folgende Punkte schrittweise zu adressieren:

Auswirkungsanalyse auf den Kapitalbedarf

Bereits jetzt zeichnen sich wesentliche methodische Änderungen im Risikotragfähigkeitskonzept ab. So wird die Risikodeckungsmasse in der Säule II in Zukunft primär auf regulatorische Eigenmittel abstellen. Darüber hinaus wird der Säule I-Kapitalbedarf je Risikoart als Untergrenze wirken und Diversifikationseffekte zwischen Risikoarten nicht mehr angerechnet werden. Wir empfehlen, erste Analysen auch auf den Kapitalbedarf für OpRisk durchzuführen und im Weiteren laufend zu konkretisieren, um frühzeitig eventuelle Kapitallücken zu identifizieren.

Überprüfung des Weiterentwicklungsbedarfs der Unternehmenssteuerung

Der Umfang der unter OpRisk im Leitfaden-Entwurf der EBA angesprochenen Themen verdeutlicht den starken Bedarf eines integrierten Ansatzes für das Controlling und Management von OpRisk. Bei Beurteilungen des OpRisk-Profiles eines Instituts durch die zuständigen Aufsichtsbehörden werden diese auf zahlreiche Zentralstäbe und Marktbereiche zugreifen.

Dazu gehören u.a. Risikocontrolling, Compliance, Organisation/IT, Recht und Kommunikation, aber auch dezentrale Ansprechpartner in Kredit- und Handelsbereichen. Es ist zu erwarten, dass das Ausmaß der Verzahnung insbesondere von Strukturen, Prozessen, Methoden, Instrumenten und Berichten zu OpRisk-relevanten Sachverhalten in diesen Bereichen, einschließlich möglicher Auslagerungen, zum Maßstab der Beurteilung gemacht wird.

Bestandsaufnahme für den neuen SREP

Als Vorbereitung auf den zukünftigen SREP-Ansatz der Aufsicht sollten Institute die Angemessenheit insbesondere der vorhandenen Governance-Strukturen, qualitativen und quantitativen Methoden und Prozesse sowie IT-Systeme für den Risikomanagementprozess zu OpRisk und RepRisk prüfen. In Abhängigkeit vom Reifegrad der jeweiligen Rahmenwerke können sich Handlungsbedarfe für die jeweiligen Institute ergeben.

Diese können u.a. in folgenden Themenfeldern erwartet werden:

OpRisk-Governance

- Konsistentes OpRisk-Rahmenwerk für alle Gesellschaften einer Institutsgruppe
- Anwendung der OpRisk-Prozesse auf alle Gruppenteile, einschließlich Tochtergesellschaften, Filialen sowie ausgelagerten Tätigkeiten
- Einbeziehung aller am OpRisk-Profil einer Gruppe beteiligten Bereiche und Harmonisierung von Methoden und Instrumenten
- Abstimmung des Informationsflusses zwischen zentralem OpRisk-Controlling sowie dezentralen OpRisk-Managern und Überprüfung der Angemessenheit der vorhandenen Personalkapazitäten

OpRisk-Steuerung

- Kompatibilität der Risikosteuerungsmaßnahmen mit der definierten Risikostrategie/-neigung
- Adäquate Abdeckung und Funktionsfähigkeit des internen Kontrollsystems
- Umfassende und getestete Business Continuity-Pläne
- Systematische Prüfung der Wirksamkeit von Risikosteuerungsmaßnahmen

Datengranularität und -qualität

- Systematische Erfassung von Ursachen von OpRisk-Ereignissen sowie deren Auswirkungen (auch bzgl. entgangenen Gewinnen, Beinaheverlusten etc.)
- Abbildung von Ereignistypen, Geschäftsbereichen, Produkten, Prozessen, Ländern sowie rechtlicher Einheiten
- Erweiterung des AMA-Modells bzw. ökonomischen Kapitalmodells zur Abbildung erhöhter Anforderungen an die Ergebnisgranularität

Berücksichtigung von Modellrisiken im OpRisk-Rahmenwerk

- Sicherstellung angemessener Kontrollen für alle wesentlichen Modelle in Bankprozessen (einschließlich unabhängiger Validierung)
- Kommunikation der Ergebnisse der Modellvalidierung an das zentrale OpRisk-Controlling, Einschätzung der bestehenden Modellrisiken
- Einbindung der Modellrisiken in das OpRisk-Rahmenwerk (z.B. Berücksichtigung in der Ursachenanalyse von OpRisk Ereignissen, im Risk-Self-Assessment, in der Szenarioanalyse sowie in den ökonomischen und ggf. regulatorischen Kapitalmodellen)
- Kommunikation von Modellrisiken aus den OpRisk-Modellen an Geschäftsleitung und Senior Management

Berücksichtigung von Conduct Risk im OpRisk-Rahmenwerk

- Überschneidungsfreie Integration von Conduct Risk in die Risikoinventur und -landkarte des Instituts
- Untersuchung von möglichen Ursachen für Conduct Risk-Ereignisse auf Basis einer Analyse u.a. des Geschäftsmodells, der Anreizsysteme, bestehender Strafzahlungen
- Sicherstellung der Abbildung aller Aspekte von Conduct Risk (u.a. Misselling, Interessenkonflikte, Manipulationen) im OpRisk-Rahmenwerk, einschließlich angewandeter Methoden und definierter Verantwortlichkeiten

Berücksichtigung von IT-Risiken im OpRisk-Rahmenwerk

- Sicherstellung der Behandlung sämtlicher Aspekte von IT-Risiken (u. a. Business Continuity Management, IT-Sicherheit, IT-Projektrisiken)
- Anpassung relevanter Methoden, Instrumente und ggf. Verantwortlichkeiten
- Sicherstellung der Kommunikation der Ergebnisse von IT-Risikoerhebungen an das zentrale OpRisk-Controlling

Rahmenwerk für RepRisk

- Identifikation für die Reputation des Instituts wesentlicher Stakeholder und möglicher Risiken
- Schaffung von Strategien und Richtlinien für das Controlling und Management von RepRisk
- Etablierung von Prozessen zur Identifikation, Steuerung und Überwachung sowie eines Berichtswesens
- Einbindung in Stress Testing/Szenarioanalyse und das Krisenmanagement einschließlich Kommunikationsstrategien

Nächste Schritte

Nach Ende der Konsultationsfrist wird die EBA den Entwurf in eine finale Leitlinie überführen. Inwieweit zu erwartende Kommentare seitens der betroffenen Institute hierin Berücksichtigung finden, bleibt abzuwarten. Die Umsetzung dieser Leitlinie wird auch entscheidend von der Positionierung der EZB abhängen. Sicherlich wird der deutsche Ansatz der Säule II-Betrachtung nicht kurzfristig abgelöst werden. Ein allmählicher Übergang beginnend im Laufe des Jahres 2015 ist jedoch zu erwarten.

Die hier beschriebenen beabsichtigten Änderungen an Methoden und Prozessen zu operationellen Risiken sollten auch in Verbindung mit den von der EBA im Juni 2014 veröffentlichten *Draft Regulatory Technical Standards on assessment methodologies for the Advanced Measurement Approaches (AMA) for operational risk* gesehen werden. Dies betrifft insbesondere den Themenkomplex zur Abgrenzung von operationellen Risiken von Kreditrisiken in Zusammenhang mit Betrugsfällen, Datenqualität sowie Umfang der Verlustdatensammlung.

Ferner werden im Rahmen weiterer Konsultationen seitens des Basler Ausschusses für Bankenaufsicht sowie der EBA zu einem späteren Zeitpunkt in 2014 weitere Änderungen erwartet. Nach heutigem Kenntnisstand ist mit einer Neukalibrierung und Überarbeitung des Basisindikator- und Standardansatzes für OpRisk unter Säule I zu rechnen, die zu einem deutlichen Anstieg der Kapitalanforderungen für operationelle Risiken führen kann. Auf der Seite der Fortgeschrittenen Messansätze (AMA) erwartet die Branche eine Verschärfung und Harmonisierung der qualitativen und quantitativen Anforderungen.

Sprechen Sie uns an! Unser Team aus erfahrenen Experten für alle qualitativen und quantitativen Aspekte der operationellen Risiken und Reputationsrisiken unterstützt Sie gerne dabei, sich optimal für diesen Änderungsprozess aufzustellen und diesen mitzugestalten.

Impressum / Kontakt

KPMG AG Wirtschaftsprüfungsgesellschaft
THE SQUAIRE
Am Flughafen
60549 Frankfurt am Main

Thilo Kasprowicz (V.i.S.d.P.)

Partner, Consulting – Financial Services
T +49 69 9587-3198
tkasprowicz@kpmg.com

Prof. Dr. Thomas Kaiser

Director, Consulting – Financial Services
T +49 69 9587-6283
thomaskaiser@kpmg.com

Carsten Zecher

Manager, Consulting – Financial Services
T + 49 69 9587-2316
czecher@kpmg.com

www.kpmg.de/lexlinks
www.kpmg.de/regulierung

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2014 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Konzerngesellschaft der KPMG Europe LLP und Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International Cooperative.