ComplianceBusiness
Ausgabe 1 // März 2016

Frühzeitig erkennen, konsequent analysieren

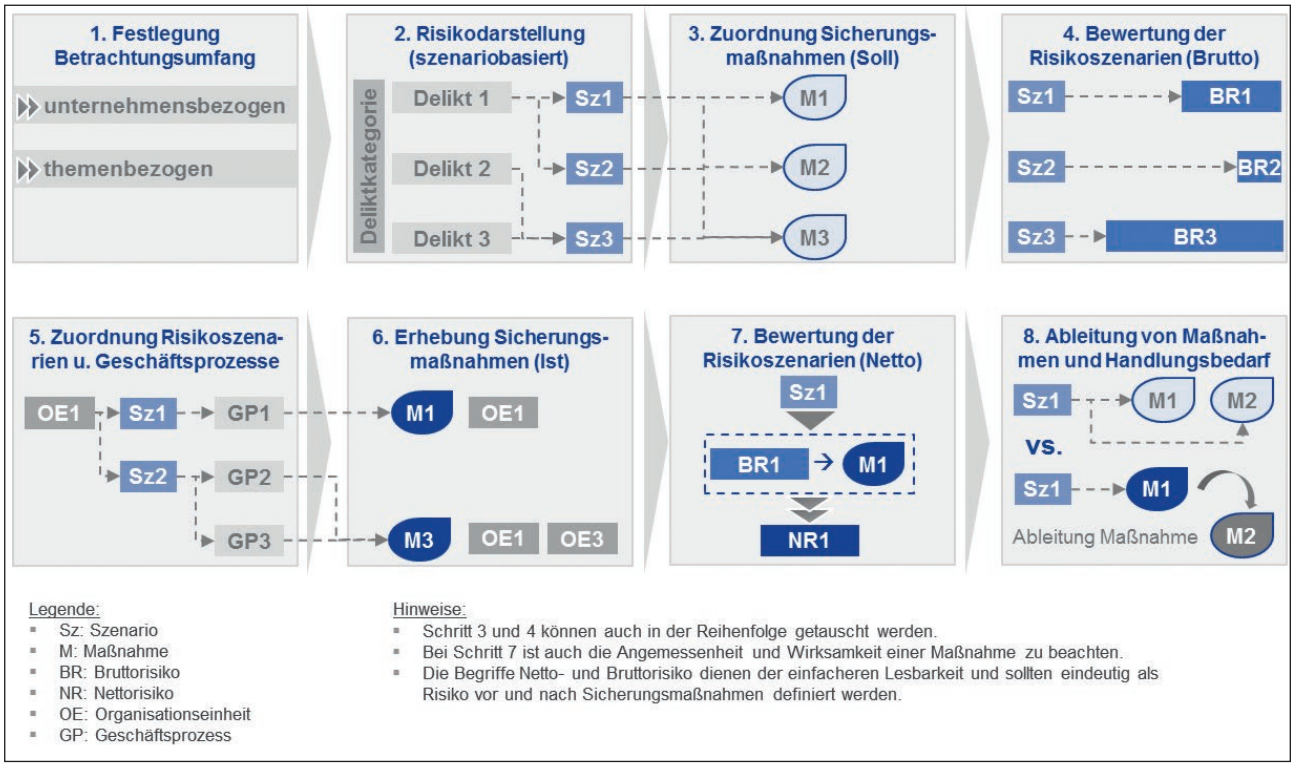
Schwerpunkt Kreditinstitute: Ausgangslage und aktuelle Herausforderungen im Fraud-Risk-Management

Von Bernd Michael Lindner und Susanne Schenk

Trotz verstärkter Maßnahmen deutscher Kreditinstitute zur Risikoreduzierung und -steuerung können Schäden aus sonstigen strafbaren Handlungen (wie Betrug, Korruption, Untreue, Unterschlagung, Ausspähen und Abfangen von Daten) nicht immer verhindert werden. Insbesondere das frühzeitige Erkennen von sonstigen strafbaren Handlungen stellt vor dem Hintergrund der sich sehr schnell an technische Möglichkeiten anpassenden Betrugsstrategien eine große Herausforderung für die Institute dar. Häufig liegt der Fokus zu stark auf der Erfüllung regulatorischer Anforderungen, und das eigentliche Ziel des wirksamen Risikomanagements und der ungetrübte Blick auf potentielle neue Risiken (Cyberkriminalität) für das Institut werden vernachlässigt.

Darüber hinaus ist zu beobachten, dass die Schnittstelle der gemäß § 25h KWG zu implementierenden „Zentralen Stelle" innerhalb der Compliancefunktion (zweite Verteidigungslinie) zu den operativen Organisationseinheiten (erste Verteidigungslinie) oftmals nicht intensiv genug ausgestaltet ist. Die direkte Zusammenarbeit ist Voraussetzung für ein effektives Fraud-Risk-Management.

In vielen Kreditinstituten herrscht eine Vertrauenskultur – der Mitarbeiter leistet einen Beitrag zum Unternehmenserfolg und stellt in erster Linie keinen Risikofaktor dar. Somit verwundert es nicht, dass deutsche Kreditinstitute oder die jeweiligen Compliancefunktionen Hemmungen haben, interne Betrugsszenarien zu definieren und entsprechende Sicherungsmaßnahmen daraus abzuleiten. Man möchte den Mitarbeiter ja nicht unter ▸



ComplianceBusiness
Ausgabe 1 // März 2016

„Generalverdacht“ stellen. Der Grat zwischen der Compliancefunktion als „Berater“ sowie Risikosteuerungseinheit und als „Polizei“ sowie „Geschäftsverhinderer“ ist schmal und stellt ebenfalls eine wesentliche Herausforderung dar.

Gefährdungsanalyse als Grundlage jeglicher Prävention sonstiger strafbarer Handlungen

Eines der wichtigsten Präventionsinstrumente gegen sonstige strafbare Handlungen ist die jährlich durchzuführende Gefährdungsanalyse. Die gesetzliche Grundlage für ihre Durchführung bildet § 25h KWG, wonach Institute über geschäfts- und kundenbezogene Sicherungssysteme, Kontrollen und interne Grundsätze zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen verfügen müssen. Die Anforderungen werden mit den Auslegungs- und Anwendungshinweisen der deutschen Kreditwirtschaft konkretisiert. Jedes Institut hat die Vorgaben unter Berücksichtigung der individuellen Risikosituation sowie des Proportionalitätsgrundsatzes umzusetzen. Es ist ein adäquates Vorgehensmodell zu definieren, die betrachteten Risiken sind nachvollziehbar zu dokumentieren und das Vorgehensmodell entsprechend umzusetzen.

Die Gefährdungsanalyse zu sonstigen strafbaren Handlungen kann dabei auch Bestandteil einer, weitere (Compliance-)Themen (etwa Geldwäsche und Terrorismusfinanzierung, Finanzsanktionen und Kapitalmarktcompliance) umfassenden, Gefährdungs- oder Risikoanalyse sein. Im Folgenden werden ein Einblick in ein mögliches Vorgehensmodell im Rahmen der Gefährdungsanalyse sowie Hinweise zur wirksamen und kosteneffizienten Durchführung gegeben.

Mögliches Vorgehensmodell

Festlegung des Betrachtungsumfangs

Zu Beginn einer jeden Gefährdungsanalyse ist festzulegen, welche Gesellschaften und Geschäftsbereiche des Instituts betrachtet werden sollen. Hierbei ist die Pflicht zur gruppenweiten Umsetzung zu beachten. Zudem sind die für das Institut potentiell relevanten Deliktkategorien und Delikte zu definieren. Dabei sind die jeweiligen Produkte, Dienstleistungen, Kundengruppen etc. zu berücksichtigen, um der geforderten institutsspezifischen Betrachtungsweise gerecht zu werden. Bei der Definition der Deliktkategorien ist eine Orientierung an Normen ratsam. Die getroffene Auswahl des Betrachtungsumfangs ist zu begründen und zu dokumentieren.

Szenariobasierte Risikodarstellung

Ein wesentlicher Erfolgsfaktor der Gefährdungsanalyse ist eine umfassende und auf das jeweilige Institut ausgerichtete Risikoidentifizierung. Dazu sind intern vorhandene Informationen wie beispielsweise aus Prozessen, dem internen Kontrollsystem oder der Schadenfalldatenbank sowie Erkenntnisse aus externen Quellen wie etwa aus aktuellen Schadenfällen anderer Institute oder Berichten der Financial Intelligence Unit (FIU) heranzuziehen.

Zur Darstellung der potentiellen Risiken empfiehlt sich die Definition von Risikoszenarien. Dazu werden in Abhängigkeit vom Betrachtungsumfang für jede Deliktkategorie Risikoszenarien zur Konkretisierung definiert. Dabei ist der Anspruch der Vollständigkeit zu beachten – mit den Risikoszenarien sollte man alle für das Institut relevanten Delikte abdecken. Daher empfiehlt es sich, keine Kombinationsszenarien zu wählen, da aufgrund der hohen Detaillierungstiefe und Komplexität die Anforderungen an die Szenariodefinition erheblich steigen würden.

Bei der Definition der Szenarien ist zwischen intern und extern verursachten Risiken zu unterscheiden. Darüber hinaus sind die Risikodimensionen Produkt-, Transaktions-, Länder- und Kundenrisiken sowie Risiken, die sich aus dem Vertriebsweg ergeben, und gegebenenfalls sonstige relevante Risiken zu beachten.

Zuordnung Soll-Sicherungsmaßnahmen

Sicherungsmaßnahmen können aus gesetzlichen, aufsichtsrechtlichen oder internen Vorgaben abgeleitet werden. Zudem ist eine Orientierung am Marktstandard (Best Practice) empfehlenswert. Die Festlegung der Soll-Sicherungsmaßnahmen sollte vor dem Hintergrund der vorab definierten Risikoszenarien erfolgen, um eine gezielte Risikoreduzierung und -vermeidung erreichen zu können. Die Pflicht zur Umsetzung kann sowohl in den operativen Organisationseinheiten als auch in der Compliancefunktion liegen. Liegt die Umsetzungsverantwortung in der ersten Verteidigungslinie, ist die Hinwirkungspflicht der Compliancefunktion zu beachten.

ComplianceBusiness
Ausgabe 1 // März 2016

Bei der Festlegung der Sicherungsmaßnahmen ist auf deren Angemessenheit hinsichtlich Ausgestaltung und Umfang zu achten, um das zugrundeliegende Risiko geeignet reduzieren bzw. vermeiden zu können. Zudem ist bei der Zuordnung der Sicherungsmaßnahmen zu den definierten Risikoszenarien die n:n-Beziehung zu beachten, das bedeutet, dass einem Risikoszenario mehrere Soll-Sicherungsmaßnahmen zugeordnet werden können und eine Soll-Sicherungsmaßnahme mehreren Risikoszenarien zugeordnet werden kann.

Bruttobewertung der Risikoszenarien

Zunächst: Die Begriffe Netto- und Bruttorisiko dienen der einfacheren Lesbarkeit und sollten eindeutig als Risiko vor und nach Sicherungsmaßnahmen definiert werden. Die Risikoszenarien sollten hinsichtlich der Eintrittswahrscheinlichkeit und des potentiellen Schadens bewertet werden. Dabei empfiehlt sich eine Unterscheidung in Sanktions-, Reputations- und finanzielle Risiken.

Bei der Bewertung des Risikos vor Sicherungsmaßnahmen bleiben die bestehenden Maßnahmen zur Verminderung des Risikos außer Acht. Es wird folglich der größtmöglich negative Verlauf des Risikoszenarios (Worst Case) bewertet. Eine quantitative Einschätzung ist nicht zu empfehlen, da kein mathematisches Modell hinterlegt ist (bspw. im Gegensatz zur Bewertung von operationellen Risiken) und somit die Einschätzung aufgrund der sogenannten „Scheingenauigkeit“ angreifbar ist.

Im Rahmen der Bewertungsskala ist es ratsam, eine gerade numerische Anzahl zu wählen, da ansonsten die Gefahr eines Übergewichts im mittleren Wert besteht. Bei der Festlegung der Schwellenwerte ist auf die Angemessenheit zu achten. Zudem sollte die „0“ als Skalenwert für „kein Risiko“ vermieden werden, da es unter der Prämisse, dass nur für das Institut relevante Risikoszenarien in die Betrachtung einbezogen werden, immer ein Risiko geben kann, wenn auch nur ein geringes. Darüber hinaus kann die Orientierung an den Bewertungsskalen anderer Complianceanalysen sinnvoll sein, um eine bessere Vergleichbarkeit, insbesondere vor dem Hintergrund eines gemeinsamen Reportings, zu erreichen.

Für die Zuordnung und Bewertung der Risiken je Szenario empfiehlt sich eine Expertenschätzung. Da die Expertenschätzung somit die Grundlage der Risikobewertung darstellt, ist es von essentieller Bedeutung, dass die gewählte Methodik einen hohen Grad an Objektivität gewährleistet und die Experten anhand vorab definierter Kriterien ausgewählt werden.

Zuordnung von Risikoszenarien und Geschäftsprozessen

Die Zuordnung von Risikoszenarien und Geschäftsprozessen sollte je Organisationseinheit erfolgen. Die Zuordnung ist insbesondere in der initialen Durchführung sinnvoll, da hiermit Transparenz hinsichtlich vorhandener Geschäftsprozesse geschaffen wird sowie gegebenenfalls nicht (zwingend) erforderliche Geschäftsprozesse identifiziert werden können. Nach der initialen Durchführung dient die Zuordnung der einfacheren Erhebung der Ist-Sicherungsmaßnahmen (siehe dazu den folgenden Abschnitt).

Je nach Qualität der Prozesslandschaft eines Instituts ist zu beachten, dass ggf. nicht alle notwendigen Geschäftsprozesse vorhanden oder Teil der schriftlich fixierten Ordnung sind. Eine risikoorientierte Erhebung der Geschäftsprozesse kann unter Umständen sinnvoll sein. Dies sollte jedoch insbesondere unter Berücksichtigung der Reputationsrisiken in Bezug auf Kunde, Aufsicht oder Wirtschaftsprüfer erfolgen. Zudem ist auf eine für Dritte nachvollziehbare Dokumentation zu achten.

Im Rahmen der Zuordnung kann zwischen zwei Alternativen gewählt werden. Zum einen kann sie im Zuge einer Abfrage vorhandener Geschäftsprozesse auf Basis der Risikoszenarien je Organisationseinheit erfolgen. Zum anderen kann die Zuordnung der Geschäftsprozesse und Risikoszenarien zentral durch die Compliancefunktion erfolgen, und die Organisationseinheiten identifizieren und markieren anschließend, an welchen Prozessen sie beteiligt sind. Die zweite Alternative bietet sich insbesondere an, wenn das Institut über eine aktuelle und umfassende Prozesslandkarte verfügt.

Erhebung Ist-Sicherungsmaßnahmen

Für jedes Risikoszenario sind die vorhandenen Sicherungsmaßnahmen je betroffene Organisationseinheit zu erheben. Im Rahmen der Erhebung empfiehlt sich die Abfrage von Dokumenten-IDs, um eine eindeutige Zuordnung und ein schnelles Auffinden bei Bedarf zu ermöglichen. Die Erhebung sollte sich an den Soll-Sicherungsmaßnahmen (siehe dazu oben) orientieren, um eine leichte Zuordnung und gegebenenfalls die Ableitung notwendiger Maßnahmen zu gewährleisten.

ComplianceBusiness
Ausgabe 1 // März 2016

Für die Erhebung ist die Nutzung von Fragebögen zu empfehlen. Bei initialer Durchführung sollten die Fragebögen vorab mit den hiervon betroffenen Organisationseinheiten in Workshops besprochen werden. Zusätzlich kann auch eine Befragung hinsichtlich der Einschätzung der Angemessenheit und Wirksamkeit erfolgen. Dies ersetzt jedoch nicht die Angemessenheits- und Wirksamkeitsbeurteilung durch die Compliancefunktion.

Nettobewertung der Risikoszenarien

Die im vorherigen Schritt erhobenen Sicherungsmaßnahmen werden durch die Compliancefunktion hinsichtlich ihrer Angemessenheit und Wirksamkeit überprüft. Es ist auch grundsätzlich ein risikoorientierter Ansatz denkbar. Dabei sollten insbesondere Reputationsrisiken in Bezug auf Kunde, Aufsicht oder Wirtschaftsprüfer berücksichtigt werden. Zudem ist auf eine für Dritte nachvollziehbare Dokumentation zu achten. Eine reine Unterscheidung in „angemessen“ bzw. „wirksam“ und „nicht angemessen“ bzw. „nicht wirksam“ ist nicht zu empfehlen, da man hierbei nicht dem tatsächlichen Risikopotential gerecht werden kann.

Eine Bewertung des Risikos nach Sicherungsmaßnahmen sollte in Zusammenarbeit mit den relevanten Organisationseinheiten, die die Maßnahmen und Geschäftsprozesse verantworten, erfolgen. Im Rahmen der Bewertung kann eine Gewichtung der Sicherungsmaßnahmen durchaus sinnvoll sein. Zudem sollten Ergebnisse vorhandener Prüfungen (intern und extern), Auffälligkeiten in Kontrollhandlungen etc. berücksichtigt werden.

Fazit

Unbestritten ist die Gefährdungsanalyse Baustein jeglicher Prävention von sonstigen strafbaren Handlungen. In der Praxis stellt häufig das frühzeitige Erkennen von sonstigen strafbaren Handlungen die Institute vor Herausforderungen.

Im Rahmen dieses Artikels wurde unter anderem ein mögliches Vorgehensmodell zur Durchführung der Gefährdungsanalyse dargestellt, welches auf den rechtlichen Anforderungen, langjährlicher Projekterfahrung sowie aktuellen Marktstandards basiert. Kreditinstitute haben ihre Methodik und das Vorgehen unter Berücksichtigung der individuellen Risikosituation sowie geltender Proportionalitätsgrundsätze zu entwickeln und umzusetzen.

Die Vielzahl an Risiko- und Gefährdungsanalysen führt vermehrt zu dem Wunsch, die bestehenden Complianceanalysen zu harmonisieren und möglichst zu vereinheitlichen. Darüber hinaus ist auch eine Annäherung mit complianceübergreifenden Analysen wie etwa einem internen Kontrollsystem oder Risikocontrolling zu empfehlen. Durch die Bündelung der institutsinternen Erkenntnisse zur Risikosituation und die Vergleichbarkeit von Ergebnissen werden unter anderem ein konsistentes Reporting an das Management ermöglicht sowie eine langfristige Ressourcenschonung der operativen Organisationseinheiten erreicht.

Ableitung von Maßnahmen und Handlungsbedarf

Um das Risiko nach Sicherungsmaßnahmen weiter zu reduzieren und hierbei gegebenenfalls erkannte Defizite zu beheben, sind neue Sicherungsmaßnahmen abzuleiten oder bereits vorhandene Sicherungsmaßnahmen anzupassen oder auszuweiten. Die Ableitung des Handlungsbedarfs ist durch die Compliancefunktion unter Einbindung der betroffenen Organisationseinheiten in Abhängigkeit vom zugrundeliegenden Risiko nach Sicherungsmaßnahmen und der institutsindividuellen Risikostrategie vorzunehmen. Liegt die Umsetzungsverantwortung in der ersten Verteidigungslinie, ist die Hinwirkungspflicht der Compliancefunktion zu beachten.

Trend zur Harmonisierung von (Compliance-) Risiko- und Gefährdungsanalysen

Vor dem Hintergrund der Vielzahl an Risiko- und Gefährdungsanalysen sehen sich Kreditinstitute vor einige Herausforderungen gestellt. Zum einen fordert das Management vermehrt einen konsistenten und nachvollziehbaren Überblick über die Risikosituation des Instituts. Zum anderen sollten die Belastung der operativen Organisationseinheiten durch die Mitwirkung an den Risiko- und Gefährdungsanalysen aus Effizienz- und Motivationsgesichtspunkten reduziert und die Ansprache optimiert werden. Um diesen Herausforderungen adäquat begegnen zu können, ist eine Annäherung

der jeweils verwendeten Methoden unerlässlich. Nur auf diesem Wege kann ein konsistentes Reporting mit vergleichbaren Ergebnissen der Risikoidentifizierung und -bewertung erreicht werden. Dabei sind die je Themengebiet bestehenden rechtlichen Anforderungen zu beachten und im Rahmen der Annäherung zu berücksichtigen. Die Harmonisierung von Methoden geht im besten Fall mit einer konsolidierten, um Dopplungen und Überschneidungen bereinigten Datenbasis für die Risikoidentifizierung und einheitlichen Dokumentationsmöglichkeiten einher. Darüber hinaus sollte auch durch ein möglichst zeitgleiches Vorgehen der Zeitpunkt der Ansprache der mitwirkenden Organisationseinheiten optimiert werden. Zudem empfiehlt sich in diesem Zuge auch eine Optimierung der Ansprechpartnerstrukturen. Durch die beschriebene Schaffung von Synergien und die Nutzung bestehender Schnittstellen ist eine erhebliche Ressourcenschonung der operativen Organisationseinheiten möglich, was die Akzeptanz der Durchführung von Risiko- oder Gefährdungsanalysen erhöht.

Bernd Michael Lindner,
Partner Financial Services, KPMG AG, Wirtschaftsprüfungsgesellschaft München
KPMG AG, München

blindner@kpmg.com
www.kpmg.com

Susanne Schenk,
Managerin Financial Services, KPMG AG, Wirtschaftsprüfungsgesellschaft Hamburg

sschenk@kpmg.com
www.kpmg.com