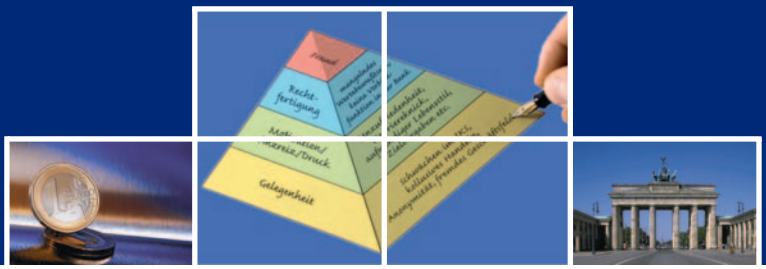


Prävention und Bekämpfung von betrügerischen Handlungen/ Wirtschaftskriminalität

Leitfaden zur praxisorientierten Einführung in die Gefährdungsanalyse und Maßnahmen

Stand: April 2010

VÖB Bundesverband Öffentlicher Banken Deutschlands

Prävention und Bekämpfung von betrügerischen Handlungen/ Wirtschaftskriminalität

Leitfaden zur praxisorientierten Einführung in die Gefährdungsanalyse und Maßnahmen

Vorwort

Für die Kreditwirtschaft hat die Prävention und Bekämpfung von betrügerischen Handlungen und Wirtschaftskriminalität in den letzten Jahren erheblich an Bedeutung gewonnen. Neben den materiellen Schäden aus betrügerischen Handlungen drohen Kreditinstituten insbesondere auch Reputationsverluste sowie negative Auswirkungen auf die Moral der Mitarbeiter. Internationale standardsetzende Organisationen und nationale Aufsichtsbehörden haben die Tragweite der Problematik erkannt und Banken empfohlen, angemessene Geschäftsgrundsätze und Verfahrensweisen zu etablieren, die einen hohen ethischen Standard im Finanzsektor fördern. Es soll verhindert werden, dass die Institute - mit oder ohne Vorsatz - für das Begehen strafbarer Handlungen genutzt werden. Dieser Grundsatz wurde in Deutschland in § 25a Abs. 1, § 25c Abs. 1 und § 25g Kreditwesengesetz verankert. Kreditinstitute werden vom Gesetzgeber angehalten, durch die Schaffung angemessener geschäfts- und kundenbezogener Sicherungssysteme sowie Kontrollen betrügerische Handlungen zu Lasten der Institute bereits im Vorfeld zu verhindern. Zu diesen Maßnahmen gehören nach unserer Auffassung die Festlegung von Verantwortlichkeiten, die Durchführung einer Gefährdungsanalyse, die Etablierung eines Werte-, Reputationsmanagement- und Hinweisgebersystems, die Optimierung der internen Sicherungs- und Kontrollsysteme sowie die Erstellung geeigneter Notfall- bzw. (Krisen-)Reaktionspläne.

Die Kreditinstitute in Deutschland sehen einen hohen Bedarf, ihre Strategien und Maßnahmen zur Betrugsprävention und Bekämpfung der Wirtschaftskriminalität zu überdenken und zu organisieren. Insbesondere interessiert die Institute eine praxisorientierte Aufbereitung und Analyse der Risiken sowie realer Betrugsfälle, -muster und –typologien. Mit dem vorliegenden Leitfaden möchte der Bundesverband Öffentlicher Banken Deutschlands, VÖB, einen Beitrag zur fachlichen Diskussion über Betrugsprävention und Bekämpfung der Wirtschaftskriminalität leisten. Das Werk wurde dankenswerterweise in Zusammenarbeit mit Vertretern unserer Mitgliedsinstitute im Rahmen einer Sonderarbeitsgruppe erstellt und vom Arbeitskreis „Betrugsprävention/ Wirt-

schaftskriminalität" des VÖB fachlich unterstützt. Wir hoffen, dass der Leitfaden den mit der Betrugsprävention und Bekämpfung der Wirtschaftskriminalität befassten Mitarbeitern der Kreditinstitute eine praxisbezogene Einführung sowie eine theoretisch fundierte aktuelle Orientierungs- und Arbeitshilfe bietet.

Karl-Heinz Boos

Indranil Ganguli
Stefanie Hetzler
Rüdiger Quedenfeld
Hans Dieter Rühle
Joachim Schanz

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung

Prävention und Bekämpfung von betrügerischen Handlungen sowie der Wirtschaftskriminalität[1] standen noch vor kurzem nicht im Fokus der Compliance- und Präventionsmaßnahmen deutscher Kreditinstitute. Dies wurde u. a. auch durch den Umstand reflektiert, dass sich die Erstellung der Gefährdungsanalyse auf der Grundlage der Anforderungen des § 25a Abs. 1 Satz 6 Nr. 3 Kreditwesengesetz (KWG)[2] zunächst schwerpunktmäßig mit der Bekämpfung der Geldwäsche befasste. Allerdings bahnte sich bereits in den letzten Jahren eine Änderung der Situation an. Die durch betrügerische Handlungen und Wirtschaftskriminalität entstandenen Schäden erreichten beachtliche volks- und betriebswirtschaftliche Dimensionen[3]; es entstand Handlungsbedarf hinsichtlich präventiver Maßnahmen. Die zunehmende Bedeutung der Betrugsprävention spiegelt sich insbesondere auch in § 25c Abs. 1 KWG wider, der durch das Geldwäschebekämpfungsergänzungsgesetz (GwBekErgG) vom 13. August 2008[4] eingeführt wurde und nunmehr Pflichten der Institute zur Bekämpfung betrügerischer Handlungen zu Lasten des Instituts normiert (siehe Anlage 1 im Anhang). Ferner hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) vor dem Hintergrund der durch das GwBekErgG neu ge-

1 Im Rahmen der nachfolgenden Ausführungen werden aus Gründen der Zweckmäßigkeit und besseren Lesbarkeit an verschiedenen Stellen die Begriffe „Betrugsprävention", „Anti-Betrugsmaßnahmen" oder „Betrugsbekämpfung" verwendet, wohl wissend, dass zwischen „Prävention" und „Bekämpfung" - auf Grund der unterschiedlichen Zielrichtungen der beiden Ansätze - unterschieden werden muss. Gemeint ist i.d.R. jedoch der Themen-/ Begriffskomplex: „Prävention und Bekämpfung von betrügerischen Handlungen sowie der Wirtschaftskriminalität".

2 Ursprünglich waren die Anforderungen in § 25a Abs. 1 Satz 1 Nr. 4 und sodann in § 25a Abs. 1 Satz 3 Nr. 6 KWG enthalten.

3 Zu Angaben über die Schäden für die Volkswirtschaft und für den Finanzsektor siehe Bundeskriminalamt (BKA), Bundeslagebild Wirtschaftskriminalität 2008 (im Folgenden: BKA 2008), Abschnitt 2.1.3 und Bussmann, Kai et al., Wirtschaftskriminalität bei Banken und Versicherungen - Tatort Deutschland 2006 (im Folgenden: Bussmann et al.), im Internet abrufbar unter: http://www.business-keeper.com/cms/Docs/Attachements/474b7ac9-60de-4b58-a484-6a6fc449f0bb/Wikri_Banken_Versicherungen-06.pdf (Stand: 12.02.2010)

4 Kreditwesengesetz i.d.F. der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Art. 3 des Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäschebekämpfungsergänzungsgesetz - GwBekErgG) vom 13. August 2008, BGBl. I S. 1690. Mit Inkrafttreten des GwBekErgG wurde § 25a Abs. 1 Satz 6 Nr. 3 KWG durch die § 25c KWG, § 9 Abs. 1 i.V.m. Abs. 2 Nr. 2 GwG ersetzt.

schaffenen Rechtslage avisiert, ihre aufsichtsrechtlichen Anforderungen weiter zu konkretisieren.[5]

Der vorliegende Leitfaden bietet den insbesondere in größeren und komplexen Kreditinstituten mit der Prävention und Bekämpfung betrügerischer Handlungen sowie der Wirtschaftskriminalität befassten Mitarbeitern[6] eine praxisbezogene Einführung in die Thematik sowie eine theoretisch fundierte aktuelle Orientierungs- und Arbeitshilfe.[7] Das Werk stellt den größten gemeinsamen Nenner im Umgang mit der Thematik dar. Der Leitfaden enthält keinerlei Verpflichtung zur Beachtung oder Umsetzung der diskutierten Sachverhalte, Lösungsvorschläge und Maßnahmen. Alle Empfehlungen sind nach dem Grundsatz der Proportionalität nur eingeschränkt auf kleinere und mittlere Institute anwendbar (oder im Extremfall für diesen Institutskreis sogar ungeeignet).[8] Des Weiteren gilt: Die Entscheidung, welche Präventions- und Bekämpfungsmaßnahmen Institute zu ergreifen haben bzw. tatsächlich ergreifen, hängt, wie im Folgenden zu sehen sein wird, von einer Vielzahl von Faktoren ab und liegt letztendlich in der Verantwortung des einzelnen Instituts. Und auch: Die ergriffenen Maßnahmen können sich je nach Struktur und Komplexitätsgrad der Geschäfte, Gefährdungssituation sowie Bedarf der Institute unterhalb der im

5 In diesem Zusammenhang ist beispielsweise bei öffentlich-rechtlichen Instituten, die sich mehrheitlich oder ganz im Besitz des Bundes und/oder der Länder befinden und auf der Grundlage eines Förderauftrags operieren, auch zu prüfen, ob und in welchem Maße zusätzliche Vorgaben, wie etwa die „Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung" (einschließlich Anlagen) vom 25. August 2004, Anwendung finden können. Die Richtlinie ist im Internet abrufbar unter: http://www.bmi.bund.de/cae/servlet/contentblob/134460/publicationFile/13313/Richtlinie_zur_Korruptionspraevention_in_der_Bundesverwaltung.pdf;jsessionid=4D5F6AB15A58475ED4F10B03FCC0714E (Stand: 15.03.2010). Da jedoch fraglich ist, ob die Anti-Korruptionsvorgaben des Bundes für andere Institute eine Relevanz haben, werden diese im Folgenden nicht behandelt.

6 Aus Gründen der besseren Lesbarkeit wird der Begriff „Mitarbeiter" verwendet. Dieser bezieht sich auch auf „Mitarbeiterinnen".

7 Insoweit knüpft der vorliegende Leitfaden an das erste, vom VÖB zu dieser Thematik im Jahre 2008 herausgegebene Werk an und ergänzt dieses um weitere aktuelle Fragestellungen und Entwicklungen aus der Praxis; siehe VÖB (Hrsg.), Betrugsbekämpfung – Leitfaden zur Erstellung der Gefährdungsanalyse zur Verhinderung betrügerischer Handlungen zu Lasten des Instituts nach § 25c KWG (Verfasser: Olaf Christoph Achtelik), Berlin 2008 (im Folgenden: VÖB-Leitfaden 2008).

8 Dies liegt auch in dem Umstand begründet, dass die in kleineren und mittleren Instituten vorherrschenden spezifischen Risikostrukturen erheblich von denen bei größeren und komplexen Häusern abweichen können.

Leitfaden vorgeschlagenen Möglichkeiten bewegen, aber auch weitreichender ausgestaltet sein.

Der Leitfaden ist wie folgt aufgebaut: Im Anschluss an eine Darstellung der Grundlagen und die Überlegungen zum Aufbau der Gefährdungsanalyse und zur Risikoerhebung in Kapitel 2 werden Betrachtungen zum Erstellungsprozess und Aufbau einer institutsbezogenen Risikomatrix zur Gefährdungsanalyse „Betrugsbekämpfung und Wirtschaftskriminalität" in Kapitel 3 angestellt. Dabei werden Hinweise zur Festlegung von Risikogruppen und zu ihrer Bewertung gegeben. Das Kapitel enthält zudem eine Diskussion zu den Themen Überprüfung und Bewertung der Gefährdungslagen in den einzelnen Bereichen/ Strukturen des Instituts sowie zu einem aus diesem Prozess abgeleiteten Maßnahmenkatalog. Kapitel 4 enthält Schlussfolgerungen für die institutsintern zu ergreifenden Präventions- und Sicherungsmaßnahmen, aber auch eine kritische Erörterung der Grenzen. Im Mittelpunkt stehen jedoch mögliche Handlungsempfehlungen zur Risikominimierung, internen Berichterstattung, Maßnahmenüberprüfung und zur Ausarbeitung von Notfall- und Krisenreaktionsplänen. In Kapitel 5 werden die Folgen einer unzureichenden Präventionsstrategie aus der rechtlichen sowie aus ökonomischer Perspektive gewürdigt. Kapitel 6 enthält eine kurze Zusammenfassung der Ergebnisse und einen Ausblick über künftige Entwicklungen auf dem Gebiet.

2 Grundlagen

2.1 Wirtschaftskriminologische Grundlagen

Bei einer grundlegenden Betrachtung der Thematik empfiehlt es sich im Institut die Vorüberlegung anzustellen, welche Aspekte für kriminelles Handeln überhaupt ausschlaggebend sind, dies unabhängig von der konkreten Gefährdungssituation sowie des individuell ermittelten Risikopotenzials zu betrügerischen und wirtschaftskriminellen Handlungen missbraucht zu werden. Denn die effektivsten Präventionsstrategien und Maßnahmen sind diejenigen, die bereits bei den Ursachen ansetzen, statt sich darauf zu beschränken, lediglich die Auswirkungen zu bekämpfen.

Dabei kann auf ein Modell des US-amerikanischen Kriminologen Cressey aus den 40er Jahren des letzten Jahrhunderts zurückgegriffen werden, der sich mit den Entstehungsgründen von Kriminalität beschäftigt hat.[9] Er kam dabei zu der Erkenntnis, dass Wirtschaftskriminalität auftritt, wenn drei Faktoren gleichzeitig erfüllt sind:

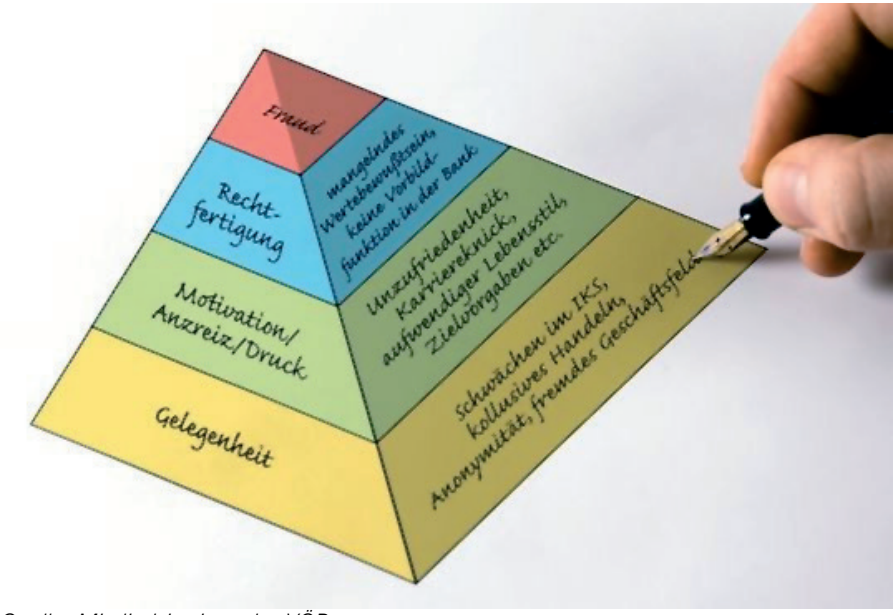
1. Es muss eine Gelegenheit bzw. Möglichkeit zur Tat geben,

2. der Täter muss eine Motivation, einen Anreiz oder gar einen (subjektiven) Zwang für die Tat haben,

3. schließlich muss er die Tat im Nachgang vor sich selbst rechtfertigen können.

Auf diese Weise entstand das berühmte „Fraud Triangle" (Betrugsdreieck), ein heute in Praxis und Literatur weit verbreitetes Analysemodell für wirtschaftskriminelle Handlungen, in dem die drei genannten Schlüsselfaktoren in einem interaktiven Verhältnis zueinander stehen. Das Fraud Triangle ist in der nachfolgenden Abbildung um einige anschauliche Beispiele ergänzt und als „Fraud Pyramide" dargestellt.

9 Zu Donald R. Cressey und dem von ihm entwickelten Ansatz zur Erforschung der Wirtschaftskriminalität wird verwiesen auf:
http://www.kriminologie.uni-hamburg.de/wiki/index.php/Donald_R._Cressey
(Stand: 15.03.2010)

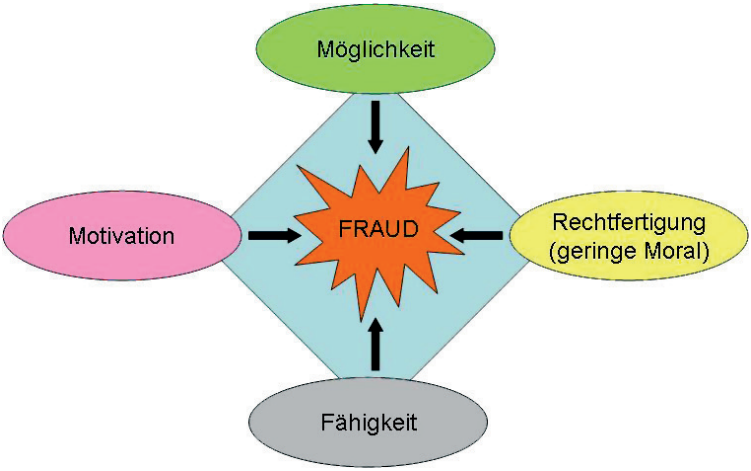


Quelle: Mitgliedsinstitute des VÖB

Abbildung 1: Fraud Pyramide

In einem jüngeren kriminologischen Forschungsansatz von Wolfe und Hermanson[10] tritt neben die drei Schlüsselfaktoren ein weiterer, vierter Faktor: Die Fähigkeit, das heißt, die individuelle Befähigung des Täters zur Ausführung der Tat. Das Fraud Triangle wird auf diese Weise zum „Fraud Diamond" erweitert.

10 Wolfe, David T., und Hermanson, Dana R., The Fraud Diamond – Considering the Four Elements of Fraud, in: The CPA Journal, 1. Dezember 2004 (im Folgenden: Wolfe/ Hermanson).



Quelle: Wolfe/Hermanson
Abbildung 2: Fraud Diamond

2.1.1 Motivation

Die Motivation für die Begehung betrügerischer Handlungen kann insbesondere aus Habgier, wirtschaftlichem Druck oder einem finanziellen Engpass des Täters herrühren. Der wirtschaftliche Druck kann auch in zu hohen Erwartungshaltungen im Privatumfeld (Lebensstil muss gehalten werden) in Kombination mit einem starken Geltungsbedürfnis des Täters begründet sein. Nicht selten ist auch mangelnde Loyalität das Tatmotiv, bedingt z. B. durch eine als unfair empfundene Behandlung oder ein schlechtes Betriebsklima. Weiterhin kommen Langeweile bzw. der Ehrgeiz, seine „technische Überlegenheit" auszuprobieren, als Tatmotive in Betracht. Daneben existiert noch eine Reihe von Fällen, in denen Täter durch Einflussnahmen Dritter zur Tat motiviert werden. Das kann neben einer bestechlichen auch eine erpresserische Einflussnahme sein (im Extremfall im Rahmen der Organisierte Kriminalität).

2.1.2 Rechtfertigung

Um sein schlechtes Gewissen neutralisieren zu können, muss der Täter die Tat vor sich selbst rechtfertigen können. Typische Rechtfertigungen

sind: *„Das machen doch alle“* und *„Es steht mir zu“*. Gängig ist auch die Rechtfertigung im Bereich des Mitarbeiterbetruges: *„Es tue doch keinem weh“* bis hin zu der Begründung: *„Es sei zum Wohl des Unternehmens“*.

2.1.3 Gelegenheit

Gelegenheit bedeutet meist das Fehlen oder die Ineffektivität von Kontrollen, was dem Täter überhaupt erst die Möglichkeit zur Begehung krimineller Handlungen eröffnet. Begünstigt wird die Möglichkeit zur Tatbegehung durch interne Täter häufig auch durch fehlende Organisationsanweisungen oder undurchsichtige Prozesse.

Im Gegensatz zu den drei anderen Faktoren, die eine starke individuelle Komponente haben, ist der Faktor Möglichkeit von Unternehmen vergleichsweise einfach zu beeinflussen. Der Schwerpunkt der Präventionsmaßnahmen sollte daher auf diesem Aspekt liegen. Dies gilt umso mehr, als die Wahrscheinlichkeit krimineller Handlungen auch durch die subjektiv erwartete Entdeckungswahrscheinlichkeit bestimmt wird, die umso höher ist, je konsequenter Kontrollprinzipien umgesetzt sind. Studienergebnisse bestätigen diese Annahme: 61 % der Unternehmen gaben an, dass unentdeckte erste Anzeichen die wirtschaftskriminellen Handlungen begünstigt haben.[11]

Darüber hinaus hat die Umsetzung von Kontrollmaßnahmen auch Einfluss auf den Faktor Rechtfertigung: Wem bekannt ist, dass an bestimmten Stellen Kontrollen zur Verhinderung betrügerischer Handlungen implementiert sind, kann sich zumindest nicht darauf berufen, seine Taten seien zum Wohl der Firma oder sein Handeln sei normal, da „jeder das doch mache“.

2.1.4 Fähigkeit

Fähigkeit bedeutet, dass der Täter über das für die Tatbegehung nötige Wissen und Können verfügen muss. Insbesondere das Bewusstsein, seine Position ausnutzen zu können sowie die entsprechenden, z. B. techni-

11 KPMG, Studie 2006 zur Wirtschaftskriminalität in Deutschland, S. 14.

schen Fertigkeiten und intellektuellen Kompetenzen, also das Vermögen zur Umsetzung der Tat, spielen dabei eine bedeutsame Rolle.

2.2 Aufsichtsrechtliche Grundlagen

Die Pflicht der Kreditinstitute zur Bekämpfung betrügerischer Handlungen wurde erstmalig im Jahre 2002 im KWG gesetzlich festgeschrieben.[12] Die Vorgaben wurden im Rahmen des GwBekErgG in § 25c KWG unter der Bezeichnung *„Interne Sicherungsmaßnahmen"* zusammengefasst. Nach § 25c Abs. 1 KWG müssen Institute, also Kredit- und Finanzdienstleistungsinstitute i.S.d. § 1 Abs. 1 und Abs. 1a KWG, im Rahmen ihrer ordnungsgemäßen Geschäftsorganisation und des angemessenen Risikomanagements i.S.d. § 25a Abs. 1 KWG

- interne Grundsätze,
- angemessene geschäfts- und kundenbezogene Sicherungssysteme und
- Kontrollen

zur Verhinderung von betrügerischen Handlungen zu ihren Lasten schaffen und laufend aktualisieren. Damit wird - so formuliert es die Gesetzesbegründung - der bisherigen Rechtslage nach § 25a Abs. 1 Satz 6 Nr. 3 KWG entsprochen, wonach Institute über geschäfts- und kundenbezogene Sicherungssysteme nicht nur gegen Geldwäsche, sondern auch gegen betrügerische Handlungen zu Lasten des Instituts verfügen mussten.

Nach § 25c Abs. 2 Satz 1 KWG sollen Kreditinstitute darüber hinaus ausdrücklich dem Stand der Technik angemessene Datenverarbeitungssysteme einsetzen und aktualisieren, mittels derer sie in der Lage sind, Ge-

12 Der durch das 4. Finanzmarktförderungsgesetz vom 26. Juni 2002 eingefügte § 25a Abs. 1 Satz 1 Nr. 4 KWG (der seinerseits durch Inkrafttreten des Finanzkonglomeraterichtlinie-Umsetzungsgesetzes am 1. Januar 2005 in den inhaltlich nahezu unveränderten § 25a Abs. 1 Satz 3 Nr. 6 KWG und sodann durch das Finanzmarktrichtlinie-Umsetzungsgesetz [FRUG] vom 16. Juli 2007 in den § 25a Abs. 1 Satz 6 Nr. 3 KWG überführt wurde) sah bereits vor, dass die Institute über angemessene geschäfts- und kundenbezogene Sicherungssysteme gegen Geldwäsche und gegen betrügerische Handlungen zu Lasten des Instituts verfügen müssen.

schäftsbeziehungen und einzelne Transaktionen zu erkennen, die auf Grund des öffentlich und im Kreditinstitut verfügbaren Erfahrungswissens über die Methoden betrügerischer Handlungen zu Lasten von Instituten - und darüber hinaus auch hinsichtlich der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung - als zweifelhaft oder ungewöhnlich anzusehen sind. Liegen solche Sachverhalte vor, ist diesen gemäß § 25c Abs. 2 Satz 2 KWG vor dem Hintergrund der laufenden Geschäftsbeziehung und einzelner Transaktionen nachzugehen, um das Risiko der jeweiligen Geschäftsbeziehungen und Transaktionen zu überwachen, einschätzen und gegebenenfalls das Vorliegen eines Verdachtsfalls prüfen zu können. Nach § 25c Abs. 2 Satz 3 KWG kann die BaFin Kriterien bestimmen, bei deren Vorliegen Kreditinstitute vom Einsatz derartiger Datenverarbeitungssysteme absehen können.[13] Ferner ist zu erwähnen, dass auch die Prüfungsberichtsverordnung (PrüfbV)[14], die grundlegende Anforderungen an die Beurteilung der im Institut ergriffenen Maßnahmen durch die Prüfer festschreibt, im Nachgang zur Verabschiedung des GwBekErgG überarbeitet worden ist (siehe Anlage 2 im Anhang). Nach der PrüfbV hat der Prüfer insbesondere zu beurteilen, ob die Gefährdungsanalyse der Risikosituation des Instituts im Hinblick auf Geldwäsche-, Terrorismusfinanzierungs- und Betrugsbekämpfung entspricht.[15]

Konkrete aufsichtsrechtliche Vorgaben der BaFin zum Umgang mit betrügerischen Handlungen und Risiken liegen bislang kaum vor. Einzig das Rundschreiben 8/2005 der BaFin[16] nimmt ansatzweise dazu Stellung, wenngleich die Anfertigung der institutsinternen Gefährdungsanalyse im Hinblick auf die Bekämpfung von Geldwäsche im Vordergrund steht. Ebenso wie bei der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung bestehe das Ziel der Gefährdungsanalyse hinsichtlich betrügerischer Handlungen zu Lasten des Instituts darin, insoweit bestehende institutsspezifische Risiken zu erfassen, zu identifizieren, zu kategorisie-

13 Derartige Ausnahmen können im Einzelfall bestehen insbesondere für Institute mit einer Bilanzsumme von weniger als EUR 250 Mio. (vgl. Schreiben der BaFin vom 8. November 2005, GZ: GW 1 – B 590) sowie für Spezialinstitute, wie etwa Förderbanken (Schreiben der BaFin vom 25. März 2004, GZ: GW 1 – F 405).

14 Prüfungsberichtsverordnung (PrüfbV) vom 23. November 2009 (BGBl. I S. 3793)

15 § 21 PrüfbV

16 BaFin, Rundschreiben 8/2005 vom 24. März 2005, „Institutsinterne Implementierung angemessener Risikomanagementsysteme zur Verhinderung der Geldwäsche, Terrorismusfinanzierung und Betrug zu Lasten der Institute gemäß §§ 25a Abs. 1 Satz 3 Nr. 6, Abs. 1a KWG, 14 Abs. 2 Nr. 2 GwG" (GZ: GW 1 – E 100) (im Folgenden: BaFin-RS 8/2005).

ren, zu gewichten sowie darauf aufbauend geeignete Präventionsmaßnahmen zu treffen.[17] Die BaFin vertritt zudem die Auffassung, dass die Maßnahmen zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und betrügerischen Handlungen zu Lasten der Institute ungeachtet ihrer unterschiedlichen Struktur ähnliche und in hohem Maße gemeinsame Risiken aufweisen und nahezu deckungsgleiche Präventionsmaßnahmen erfordern. Vor diesem Hintergrund hält die BaFin eine getrennte Gefährdungsanalyse der drei Teilbereiche für nicht erforderlich.[18]

Von besonderer Bedeutung für die gesetzliche Regelung zur Betrugsbekämpfung in § 25c KWG sind auch die einschlägigen Äußerungen des Baseler Ausschusses für Bankenaufsicht (BCBS). Bereits nach der Gesetzesbegründung für den 2002 in das KWG eingefügten (und dem § 25c KWG inhaltlich weitgehend entsprechenden) § 25a Abs. 1 Satz 1 Nr. 4 KWG dient die Vorschrift in erster Linie der Umsetzung des Grundsatzes 15 der im September 1997 veröffentlichten Baseler Grundsätze für eine wirksame Bankenaufsicht.[19] Diese Grundsätze wurden im Oktober 2006 überarbeitet.[20] Dabei wurde Grundsatz 15 durch den inhaltlich nahezu identischen Grundsatz 18 ersetzt. Aufsichtsinstanzen haben demnach darauf zu achten, dass Institute über angemessene Geschäftsgrundsätze und Verfahrensweisen einschließlich strenger Vorschriften zur Feststellung der Kundenidentität verfügen, die einen hohen ethischen und professionellen Standard im Finanzsektor fördern und verhindern, dass das Institut - mit oder ohne Vorsatz - für das Begehen strafbarer Handlungen genutzt wird.

17 Siehe BaFin-RS 8/2005, Ziffer 2.

18 So auch ausdrücklich die BaFin im Eingangsteil des RS 8/2005. Der Vollständigkeit halber sollte erwähnt werden, dass das Bundesministerium der Finanzen und die BaFin auf Grund der im Rahmen des GwBekErgG erfolgten Änderung des § 25c KWG bereits erste Überlegungen und mögliche Eckpunkte zur Formulierung aufsichtsrechtlicher Anforderungen an die Schaffung interner Sicherungsmaßnahmen zur Betrugsprävention mit der Kreditwirtschaft diskutiert haben. Es ist davon auszugehen, dass die BaFin noch in 2010 hierzu ein Rundschreiben veröffentlichen wird, welches folgende Aspekte adressiert: (a) Schaffung von verbindlichen Vorgaben für die Betrugsprävention als Bestandteil eines angemessenen Risikomanagements; (b) Schaffung von Rechtssicherheit und Planungssicherheit für die Institute, auch im Hinblick auf die externe Revision; (c) effizienter Einsatz von materiellen und personellen Ressourcen im Institut bei Implementierung des § 25c Abs. 1 und 2 KWG; (d) Orientierung des Einsatzes institutsinterner Anti-Betrugsinstrumente - so weit wie möglich - an bereits eingeführte Anti-Geldwäscheinstrumente, dies zur Herstellung von Synergieeffekten.

19 BCBS, Grundsätze für eine wirksame Bankenaufsicht, September 1997 (im Folgenden: „BCBS Grundsätze 1997").

20 BCBS, Grundsätze für eine wirksame Bankenaufsicht, Oktober 2006.

Grundsatz 18 wird in der ebenfalls im Oktober 2006 überarbeiteten „Methodik der Grundsätze für eine wirksame Bankenaufsicht" des BCBS näher erläutert.[21] Im Hinblick auf die Betrugsbekämpfung sind insbesondere folgende Punkte bedeutsam:

- Institute sollen verdächtige Machenschaften und Betrugsfälle, die ihre Sicherheit, Solidität oder ihren Ruf bedrohen, der Financial Intelligence Unit (FIU) oder anderen zuständigen Stellen sowie der Bankenaufsicht melden,

- sie müssen über gut dokumentierte Geschäftsgrundsätze und Verfahrensweisen zur Feststellung der Kundenidentität verfügen,

- über ausreichende Kontrolleinrichtungen und Systeme verfügen, die geeignet sind, einen möglichen Missbrauch von Finanzdienstleistungen zu verhindern, zu erkennen und anzuzeigen sowie

- einen Mitarbeiter benennen, an den mögliche Missbräuche von Finanzdienstleistungen zu melden sind. Ferner müssen angemessene Grundsätze und Verfahren für die Auswahl von Mitarbeitern bestehen, die gewährleisten, dass bei deren Einstellung hohe ethische und professionelle Standards beachtet werden. Mitarbeiter im Bereich der Feststellung der Kundenidentität und der Aufdeckung verdächtiger und strafbarer Handlungen sind darüber hinaus laufend aus- und fortzubilden.

Sowohl die Gesetzesbegründung zu § 25a Abs. 1 Satz 1 Nr. 4 KWG als auch diejenige zu § 25c KWG nehmen zudem ausdrücklich auf das „Sorgfaltspflicht"-Papier des BCBS vom Oktober 2001 Bezug.[22] Die dort getroffene Präzisierung des Grundsatzes 15 bzw. des nunmehrigen Grundsatzes 18 erfolgte jedoch im Wesentlichen allein für die Feststellung der Kundenidentität und nicht speziell im Hinblick auf die Bekämpfung wirtschaftskrimineller oder betrügerischer Handlungen.

Die Tatsache, dass die Einfügung der Pflicht zur Betrugsbekämpfung laut Gesetzesbegründung vorrangig der Umsetzung des damaligen Grundsat-

21 BCBS Methodik 2006, Grundsatz 18, Zentrale Kriterien.

22 BCBS, Sorgfaltspflicht der Banken bei der Feststellung der Kundenidentität, Oktober 2001 (im Folgenden: „BCBS Sorgfaltspflicht 2001").

zes 15 BCBS Grundsätze 1997 dienen sollte, macht jedoch zwei Dinge deutlich:

1. Sinn und Zweck dieser gesetzlichen Normierung liegt in erster Linie darin, den Missbrauch der Institute durch kriminelle Elemente zu verhindern.

2. Zu diesem Zweck sind die Institute angehalten, eine strenge „Know Your Customer" (KYC)-Politik zu betreiben.

Wesentliche Grundlage der Betrugsprävention sind hiernach also die Maßnahmen zur Feststellung der Kundenidentität. Mit dem KYC-Prinzip sollen, neben der zwingenden Identifizierung des Kunden, die Institute in die Lage versetzt werden, Betrugsfälle im eigenen Institut besser zu erkennen, diesen Fällen mit geeigneten Sicherungsmaßnahmen zu begegnen und somit sich selbst gegen Schäden zu schützen[23]. Dies erscheint schon vor dem Hintergrund sinnvoll, dass betrügerische Handlungen durch eigene Mitarbeiter des Instituts und/oder durch externe Täter zu Lasten von Instituten in ihrer Anzahl und Vielfalt kontinuierlich zunehmen[24]. Als wirksame Präventionsmaßnahme gegen potenzielle Betrugsfälle und dadurch verursachte Schäden liegt eine strenge KYC-Politik somit im ureigenen Interesse des Instituts bzw. der Institutsgruppe.[25]

2.3 Definition und Abgrenzungsfragen zum Begriff „Betrügerische Handlungen zu Lasten des Instituts"

Unklarheit besteht darüber, was genau unter dem Begriff der „Betrügerischen Handlung zu Lasten des Instituts" zu verstehen ist. Es existiert weder eine Legaldefinition noch eine Stellungnahme der BaFin und so wird der Begriff noch immer recht unterschiedlich ausgelegt. Bereits hier stößt derjenige, der mit der Erstellung der Gefährdungsanalyse i.S.d. KWG betraut ist, auf das erste Problem: wer nicht weiß, was unter dem Begriff zu verstehen ist, weiß auch nicht, was er genau zu bekämpfen hat. Somit herrscht auch Unkenntnis darüber, welche Präventions- und Bekämpfungsmaßnahmen zu ergreifen sind und folglich auch über die Risiken, die

23 Braun, U., Kreditwesengesetz, Kommentar, 2. Auflage, München 2004, § 25a Rdnr.189.
24 BKA 2008, Abschnitt 2.1.3 und Bussmann et al.
25 Siehe hierzu auch Abschnitt 3.4

bei der Gefährdungsanalyse Berücksichtigung finden müssen. Eine erfolgreiche Erstellung der Gefährdungsanalyse steht und fällt daher mit der richtigen Definition des Begriffs „Betrügerische Handlung zu Lasten des Instituts". Sie ist die Basis für alle weiteren Arbeiten und sollte somit weder allzu leichtfertig abgehandelt noch unreflektiert übernommen werden.

Eine einheitliche Definition wäre insofern wünschenswert, als sie einiges vereinfachen würde. Eine Legaldefinition birgt jedoch immer auch das Risiko, zu eng gefasst zu sein und Einzelfälle, die nach dem Willen des Gesetzgebers oder dem Sinn und Zweck der Vorschrift eigentlich erfasst sein sollten, von vornherein (versehentlich) nicht abzudecken, oder aber sich in der Zukunft neu entwickelnde Tatbestände nicht zu erfassen. Die fehlende Legaldefinition hat im Übrigen auch einen Vorteil für den für Betrugsprävention/ -bekämpfung Verantwortlichen[26]: Die Definition der „betrügerischen Handlung" bleibt bis zu einem gewissen Grad seiner eigenen Auslegung überlassen und der daraus resultierende Umfang der Betrugsbekämpfung wird auf diese Weise von ihm mitbestimmt. Entscheidend ist aber, dass der Verwender der Definition deren Herleitung nachvollziehbar begründen kann. Daher kann und soll im vorliegenden Leitfaden auch keine fertige Definition präsentiert, sondern vielmehr eine Hilfestellung gegeben werden, wie eine derartige Definition vernünftigerweise aussehen könnte.

2.3.1 Strafrechtlicher Begriff, Wirtschaftskriminalität

Beim Begriff „betrügerische Handlung" liegt es nahe, an Straftatbestände - insbesondere an Vermögensdelikte - des Strafgesetzbuches (StGB) zu denken. Betrug im strafrechtlichen Sinne ist als Grundtatbestand in § 263 StGB geregelt; darüber hinaus existiert eine ganze Reihe an Spezialtatbeständen, die sich überwiegend, aber nicht ausschließlich im StGB finden. Die strafrechtliche Definition des Begriffs „Betrug" kann sicherlich als Hilfestellung bei der Konkretisierung des Begriffs „betrügerische Handlung" i.S.d. § 25c KWG dienen, eine völlige Übereinstimmung wird hingegen be-

26 Da in Deutschland bislang eine gesetzlich oder aufsichtsrechtlich vorgegebene und somit „offizielle" Funktionsbezeichnung „Betrugsbeauftragter" (analog zur gesetzlich verankerten Position des „Geldwäschebeauftragten") nicht existiert, wird im Leitfaden diese Funktion wie folgt umschrieben: Der für Prävention/ Bekämpfung betrügerischer Handlungen und Wirtschaftskriminalität Verantwortliche" bzw. in abgekürzter Form als „der für Betrugsprävention/ -bekämpfung Verantwortliche".

reits mangels Bezugnahme auf den strafrechtlichen Begriff zu verneinen sein. Dies gilt umso mehr, als der Gesetzgeber im KWG anders als im StGB gerade nicht von „Betrug", sondern von „betrügerischer Handlung" spricht.

Dennoch kann davon ausgegangen werden, dass die verschiedenen strafrechtlichen Betrugsformen in jedem Fall unter den Begriff „betrügerische Handlung" des KWG zu subsumieren sind; die „betrügerische Handlung" ist jedoch weiter gefasst und geht über die strafrechtlich normierten Tatbestände hinaus. Insbesondere sollten zu dem Begriff „betrügerische Handlung" i.S.d. KWG nicht ausschließlich solche Straftatbestände gezählt werden, die auch begrifflich einen „Betrug" darstellen. So können etwa Straftaten durch Mitarbeiter des Instituts, wodurch sich diese auf Kosten des Instituts bereichern, auch in Form von Unterschlagung, Untreue, Bestechlichkeit bzw. Vorteilsannahme o. ä. begangen werden. Derartige Straftatbestände stellen auch eine Form der betrügerischen Handlung zu Lasten des Instituts dar, vor der sich dieses schützen muss.

In weiten Teilen können betrügerische Handlungen zu Lasten des Instituts auch dem Bereich der Wirtschaftskriminalität zugeordnet werden. Unter das Wirtschaftsstrafrecht werden in der Praxis u. a. Straftaten nach den Gesetzen über das Bank-, Depot-, Börsen- und Kreditwesen und dem Wertpapierhandelsgesetz, der Kapitalanlage- und Kreditbetrug sowie unter bestimmten Voraussetzungen Betrug, Computerbetrug, Untreue sowie Korruptionstatbestände subsumiert. Auch hier gilt jedoch, dass die betrügerische Handlung i.S.d. KWG mit dem Begriff „Wirtschaftskriminalität" nicht gleichgesetzt werden kann, sondern über das Gebiet des Wirtschaftsstrafrechts hinausgeht.

2.3.2 Finanzbetrug, Bankbetrug

Im Zusammenhang mit betrügerischen Handlungen zu Lasten des Instituts wird auch häufig von „Finanzbetrug" gesprochen. Dieser Begriff bezeichnet jedoch keinen Straftatbestand und stellt auch keine Legaldefinition des deutschen Rechts dar. Es handelt sich vielmehr um einen Oberbegriff, unter den verschiedene Betrugsvarianten im Zusammenhang mit Finanzdienstleistungen (bzw. Finanzdienstleistungsinstituten) subsumiert werden. Betrug gegen Institute, Betrug im Zusammenhang mit Finanzdienstleistungen (z. B. Kapitalanlage, Kredit) und Betrug mit Finanz-

papieren (z. B. Scheck, Wechsel, Wertpapier) werden hier zu einem Begriff zusammengefasst. Institute können beim Finanzbetrug - je nach Fallkonstellation - unmittelbar oder mittelbar geschädigt werden.

Der Finanzbetrug kann weiter in (Kredit-)Vermittlungs-, Kapitalanlage- und Bankbetrug untergliedert werden, wobei jedoch regelmäßig nur beim Bankbetrug eine unmittelbare betrügerische Handlung zu Lasten des Instituts vorliegt. Als Unterbegriff des Finanzbetrugs ist der Bankbetrug wiederum Oberbegriff für eine Vielzahl von Betrugsformen, die einen Bezug zu den unterschiedlichsten Produkten und Dienstleistungen eines Instituts haben und somit auch die verschiedensten Bereiche des Instituts betreffen können. Zum klassischen Bankbetrug zählen u. a. der Betrug im Lastschriftverkehr, Scheck-, Wechsel- und Überweisungs- sowie Kreditbetrug.

2.3.3 Fraud

Seit einigen Jahren findet im Zusammenhang mit der Betrugsbekämpfung ein weiterer aus dem Englischen stammender Begriff Verwendung: „Fraud". „Fraud" steht u. a. für Betrug oder betrügerische Handlung, geht aber weit darüber hinaus und wird auch mit List, Schwindel, Täuschung, (Ver)Fälschung und sogar mit Unterschlagung übersetzt.

Der Begriff „Fraud" findet sich auch in der Originalfassung der Baseler Aufsichtsgrundsätze, die in Englisch, der Arbeitssprache des Bankenausschusses, abgefasst ist. Legt man nun die Tatsache zugrunde, dass der damalige § 25a Abs. 1 Satz 1 Nr. 4 KWG laut Gesetzesbegründung ausdrücklich der Umsetzung des ursprünglichen Grundsatzes 15 (bzw. des neuen Grundsatzes 18) der BCBS Grundsätze 1997[27] dienen sollte, stellt sich die Frage, ob der Begriff „Fraud" mit dem im KWG verwendeten Begriff „betrügerische Handlung" gleichzusetzen ist.

Für „Fraud" besteht jedoch keine allgemeingültige Definition. Der Begriff wird auch im britischen und US-amerikanischen Recht je nach Kontext unterschiedlich verwendet und ausgelegt. Auch hierbei werden verschiedene Tatbestände wirtschaftskrimineller Handlungen darunter subsumiert. Insofern kann auch der Begriff „Fraud" mangels Bestimmtheit lediglich als

27 Siehe hierzu Abschnitt 2.2

Orientierungshilfe beim Konkretisieren der betrügerischen Handlung dienen.

2.3.4 Die Bedeutung des Begriffs „betrügerisch"

Unterschiedlich beurteilt wird die Frage, was unter den Begriff „betrügerisch" zu subsumieren ist. Einigkeit besteht darüber, dass Betrugstatbestände und andere betrügerische Delikte, die ein Täuschungselement beinhalten, in jedem Fall unter § 25c KWG fallen.[28] Ob aber auch Delikte wie Diebstahl oder Raub, die gerade kein Täuschungselement aufweisen, als betrügerische Handlung anzusehen sind, wird unterschiedlich beantwortet. Aus juristischer Sicht besteht ein nicht unerheblicher Unterschied zwischen den sogenannten Selbstschädigungsdelikten wie Betrug, die das genannte Täuschungselement enthalten, und den sogenannten Fremdschädigungsdelikten wie Diebstahl, deren Begehung nicht auf einer Täuschung des Opfers und einer damit einhergehenden Einflussnahme auf dessen Willen beruht. Die Abgrenzung eines Betruges von einem Diebstahl kann im Einzelfall jedoch eine hochkomplexe juristische Fragestellung sein, die - wenn überhaupt - erst nach detaillierter Sachverhaltsaufklärung beantwortet werden kann.

Wenn es aber für das Vorliegen einer betrügerischen Handlung schon auf die konkrete Strafbarkeit nicht ankommt, erscheint es wenig einleuchtend, Delikte, die aus strafrechtlicher Sicht keine Täuschung beinhalten, vom Anwendungsbereich des § 25c KWG auszuklammern. Aus nichtjuristischer Sicht beinhalten auch auf Diebstahl und ähnliche Delikte gerichtete Begehungsweisen häufig eine Täuschung - und sei es nur zur Erleichterung der Tatbegehung oder zur Vertuschung der unmittelbar bevorstehenden oder bereits begangenen Tat. In der Praxis wird es auch vielfach Überschneidungen der beiden Deliktstypen geben, so dass es letztlich nicht sachgerecht ist, die Fremdschädigungsdelikte von der Betrugsbekämpfung auszuklammern.

Zu berücksichtigen ist auch, was mit der Gefährdungsanalyse zur Betrugsbekämpfung erreicht werden soll: Sofern das Ziel lautet, nur das Minimum der gesetzlichen Regelung mit möglichst wenig Aufwand abzude-

28 An dieser Stelle sei darauf hingewiesen, dass auch Korruptionstatbestände Täuschungselemente enthalten können.

cken, so mag es sachgerecht sein, Fremdschädigungsdelikte von der Definition der betrügerischen Handlung auszuklammern. Wird aber der Anspruch verfolgt, das Institut möglichst wirksam und umfassend vor Schäden zu schützen, so ist es nur folgerichtig, anhand einer allumfassenden Definition auch Fremdschädigungsdelikte und ähnliche Taten in die Betrugsbekämpfung nach § 25c KWG einzubeziehen.

2.3.5 Die Bedeutung des Begriffs „zu Lasten des Instituts"

§ 25c KWG spricht von betrügerischen Handlungen *zu Lasten der Institute*. Die Formulierung legt die Frage nahe, ob betrügerische Handlungen, bei denen nicht oder nicht unmittelbar die Institute geschädigt werden, von der Bekämpfung nach § 25c KWG ausgeklammert werden können.

Streng genommen gehören zu einem Institut aber auch die Kunden, vielleicht sogar sonstige Dritte wie Lieferanten, Vermittler u. ä. Dafür spricht auch, dass § 25c KWG die Institute verpflichtet, „geschäfts- und *kunden*bezogene Sicherungssysteme" zu schaffen. Dass der Schutz der von den Kunden eingebrachten Vermögenswerte zu den originären Pflichten eines Instituts gehört, liegt im Übrigen unabhängig von dieser Verpflichtung auf der Hand. Bei einer derartigen Betrachtungsweise wäre eine betrügerische Handlung zu Lasten eines Kunden immer auch eine betrügerische Handlung zu Lasten des Instituts.

Unabhängig von der Beantwortung dieser Frage ist es jedoch in jedem Fall zu kurz gedacht, Betrugsbekämpfung und die dazu erforderliche Erstellung der Gefährdungsanalyse auf die Fälle zu beschränken, bei denen die Institute einen unmittelbar sicht- oder messbaren Schaden davontragen, wie die folgenden Absätze zeigen.

2.3.5.1 Reputations- und sonstige Schäden

Bei einer ganzen Reihe von betrügerischen Handlungen, die im Zusammenhang mit Finanzdienstleistungen und Kreditinstituten begangen werden, werden auf den ersten Blick nicht die Institute unmittelbar geschädigt, sondern die Bankkunden oder auch sonstige Dritte. Dennoch liegt in sehr vielen Fällen eine Schädigung der Institute (z. B. durch Haftung, Folge- oder Reputationsschäden) vor. Dabei sei zunächst der sogenannte

„Betrug zu Lasten Dritter" genannt, wie etwa der klassische Anlagebetrug. Unabhängig davon, dass hier in manchen Fällen eine Schadensersatzpflicht der Institute wegen Verletzung von Hinweis-, Beratungs- oder Aufklärungspflichten bestehen kann, können sie sich einem Kreditausfallrisiko aussetzen, sofern der Kunde eigens für die Anlage einen Kredit bei seiner Bank aufnimmt.

Bei der Diskussion über die Reichweite der in § 25c KWG statuierten Verpflichtung zur Betrugsbekämpfung ist nicht zuletzt auf die Problematik von Reputationsschäden hinzuweisen. Es darf nicht verkannt werden, dass die Reputation des Instituts erheblich leiden kann, wenn sich Kunden bei ihrer Hausbank nicht „sicher aufgehoben" fühlen. Dementsprechend übernehmen viele Institute die ihren Kunden entstandenen Schäden selbst dann ohne Diskussion, wenn alle institutsseitig erforderlichen Präventionsmaßnahmen ergriffen wurden. Schließlich wiegt der unmittelbar entstandene Vermögensschaden in der Regel wesentlich geringer als der befürchtete mittelbare Reputationsschaden.[29]

2.3.5.2 Haftung wegen unzureichender Prävention

Betrugsprävention ist immer auch ein Kostenfaktor. Dementsprechend wird auch aus wirtschaftlichen Gründen von manchen Kontrollen und anderen Präventionsmaßnahmen abgesehen. Hier sollte in jedem Fall eine Abwägung im Rahmen des Risikomanagements erfolgen, in der Häufigkeit, Eintrittswahrscheinlichkeit und Höhe der potenziellen Schäden dem finanziellen und sonstigen Aufwand der Präventionsmaßnahmen gegenübergestellt werden.

Dabei muss sich ein Institut über folgende Konsequenz bewusst sein: Sofern erforderliche und zumutbare Präventionsmaßnahmen nicht ergriffen wurden, kann das Institut für den entstandenen Schaden haftbar gemacht werden, wenn dieser bei Umsetzung der entsprechenden Maßnahmen hätte verhindert werden können. Mit anderen Worten: Geht die Abwägung aus Kostengründen zu Gunsten des Risikos aus, wird also gegen die Ergreifung der in Rede stehenden Maßnahme entschieden, so sind auch die Schäden, die wegen der fehlenden Maßnahme unmittelbar dem Kunden entstehen, vom Institut zu tragen. Denn in einem solchen Fall ist das

29 Vgl. Abschnitt 5.1

Institut seiner Pflicht, die vom Kunden eingebrachten Vermögenswerte zu schützen, nicht hinreichend nachgekommen. An dieser Stelle sei noch einmal auf den Begriff „geschäfts- und *kunden*bezogene Sicherungssysteme" aus § 25c Abs. 1 KWG hingewiesen. Aus Sicht des Instituts mag es nachvollziehbar sein, bestimmte Maßnahmen wegen Unverhältnismäßigkeit nicht zu ergreifen. Aus Sicht des Kunden aber hat das Institut mögliche Maßnahmen zum Schutze seines Vermögens nicht getroffen, die den Vermögensverlust hätten verhindern können.

Die dem Institut durch die Schadensübernahme entstehenden Kosten sollten also in die oben genannte Abwägung mit einbezogen werden. Nach Berücksichtigung dieses Aspekts kann es als Ergebnis einer derartigen Abwägung sinnvoller sein, die eine oder andere Präventionsmaßnahme zu implementieren, statt sich dem Risiko auszusetzen, durch vermeidbare Betrugsfälle entstandene Schäden wirtschaftlich ausgleichen zu müssen.

2.3.6 Täter einer betrügerischen Handlung (interner/externer Betrug)

Täter einer betrügerischen Handlung können sowohl Außenstehende, das heißt Kunden oder sonstige Dritte, als auch die eigenen Mitarbeiter des Instituts sein. Dementsprechend sollte sich die Gefährdungsanalyse sowohl auf externe als auch auf interne betrügerische Handlungen erstrecken. Trotz einiger Überschneidungen hat es sich in der Praxis bewährt, diese beiden Betrugssparten getrennt voneinander zu betrachten, nicht zuletzt, da sie weitgehend unterschiedliche Präventionsmaßnahmen erfordern.

Neben den typischen internen Betrugsvarianten wie Unterschlagung von Kundengeldern, Veruntreuung von Vermögen kommt eine Beteiligung der Mitarbeiter an allen Arten von betrügerischen Handlungen durch Außenstehende in Betracht.[30] Die Kollusion von internen und externen Tätern ist als besonders gefährlich einzustufen, da zum einen das spezielle, Außenstehenden sonst in dieser Form nicht zugängliche Insiderwissen des Mitarbeiters missbraucht werden kann und der Mitarbeiter daneben viel weitergehende Zugriffsmöglichkeiten hat. Zum anderen eröffnet die

30 Diese schließen auch Korruptionstatbestände mit ein.

Involvierung Externer dem Mitarbeiter ganz andere Verschleierungsmöglichkeiten.

Keinesfalls sollte der Fehler gemacht werden, den Fokus ausschließlich auf den externen Betrug zu richten und dabei die Bedeutung des internen Betruges zu verkennen. Diese Gefahr darf angesichts der weiten Verbreitung der letztgenannten Betrugsvariante und des damit einhergehenden Reputationsrisikos nicht unterschätzt werden.[31]

2.3.7 Fazit

Eine feststehende, allgemeingültige Definition des Begriffs „Betrügerische Handlung zu Lasten des Instituts" existiert derzeit nicht. Unstreitig ist aber zum einen, dass der in Frage stehende Begriff über den in § 263 StGB normierten Betrugsbegriff hinausgeht, also neben dem strafrechtlichen Betrugsbegriff auch andere strafrechtliche Tatbestände umfasst. Darüber hinaus sollten unter dem Begriff auch solche Taten subsumiert werden, die weder einen vorhandenen Straftatbestand erfüllen noch gegen sonstiges geltendes Recht verstoßen, bei denen das Institut aber dennoch durch einen oder mehrere Täter vorsätzlich (das heißt absichtlich bzw. wissentlich; nicht nur versehentlich) geschädigt wird. Einigkeit herrscht zum anderen darüber, dass betrügerische Handlungen durch Mitarbeiter wie auch durch Externe als betrügerische Handlung i.S.d. § 25c KWG zu werten sind. Dabei steht bei all diesen Handlungen die (meist persönliche) Bereicherung(sabsicht) des Täters zu Lasten des Instituts bzw. der diesem anvertrauten Vermögenswerte im Vordergrund. Die in der Anlage 3 im Anhang gesammelten anonymisierten Fallbeispiele aus der Praxis verdeutlichen die erwähnten Aspekte und können auch als Beispiele zur Definition von Typologien betrügerischer Handlungen verwendet werden.

Die Frage, ob nur solche Taten darunter zu subsumieren sind, deren Begehung auch tatsächlich auf einer Täuschungshandlung beruht, oder auch solche, die - wie etwa Diebstahl oder Raub - gerade kein Täuschungselement beinhalten, wird unterschiedlich beantwortet und ist letztlich auch eine sehr juristische Diskussion. Vertretbar sind beide Ansätze, so dass jedes Institut die genaue Reichweite der Definition selbst festlegen muss

31 Vgl. Abschnitt 5.1

und kann. Dies gilt zumindest, so lange keine gesetzliche, aufsichtsrechtliche oder richterliche Konkretisierung der „betrügerischen Handlung" erfolgt ist. Bei Instituten, die eine wirksame und umfassende Prävention anstreben, empfiehlt es sich, die Betrugsbekämpfung nicht auf Selbstschädigungsdelikte zu beschränken.

Aus diesem Grund sei hier nochmals darauf hingewiesen, dass die vom Institut zu verwendende endgültige Definition mit Bedacht festzulegen ist, da der Umfang der in der Gefährdungsanalyse zu berücksichtigenden Risiken von der zugrunde gelegten Definition bestimmt wird. Auf Grund dieser Überlegungen könnte eine operationalisierte Definition des Begriffs „betrügerische Handlungen" für Zwecke des Instituts folgende Merkmale beinhalten:

*Eine **Handlung**, die*

- ***durch** einen oder mehrere **Externe und/oder Interne***
- ***vorsätzlich** (wissentlich oder absichtlich) und/oder*
- *mit der **Absicht** begangen wird,*
- *sich **rechtswidrige** oder sonstige **ungerechtfertigte Vorteile** zu ver*schaffen und
- *zu vermeidbaren Vermögens-, Reputations- oder sonstigen **Schäden**[32] **für das Institut** führen kann.*

2.4 Überlegungen zum Aufbau und zur Struktur der Gefährdungsanalyse

Bei der Erstellung der Gefährdungsanalyse zu betrügerischen Handlungen zu Lasten eines Instituts und Wirtschaftskriminalität stellt sich zunächst die Frage, ob diese mit der Gefährdungsanalyse zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung verbunden werden soll.[33] Die

32 Darunter sind auch Sabotageakte zu subsumieren.

33 Denkbar und sinnvoll kann unter Umständen auch eine Kombination/ Verbindung der beiden Instrumente im Rahmen einer (erweiterten) Analyse zum Thema operationelle Risiken sein.

BaFin hat dazu im RS 8/2005 ausgeführt, dass aus ihrer Sicht getrennte Gefährdungsanalysen nicht notwendig sind.[34] Der „Düsseldorfer Kreis" der Datenschutzbeauftragten hat sich dahingehend geäußert, dass einer gemeinsamen Gefährdungsanalyse keine datenschutzrechtlichen Bedenken entgegenstehen.[35] In der Praxis wird - auch vor dem Hintergrund unterschiedlicher Präferenzen der Wirtschaftsprüfer - bislang uneinheitlich verfahren. Neben gemeinsamen Gefährdungsanalysen für Zwecke der Bekämpfung der Geldwäsche, der Terrorismusfinanzierung und betrügerischer Handlungen werden zum Teil getrennte Analysen erstellt oder diese dergestalt verbunden, dass der Gefährdungsanalyse ein allgemeiner, für alle Teilbereiche geltender Abschnitt vorangestellt wird (z. B. über die allgemeine Kriminalitätslage im Geschäftsgebiet, die Geschäftstätigkeit des Instituts) und sodann Geldwäsche-, Terrorismus- und Betrugsrisiken separat dargestellt werden. Welche Methodik die Institute bevorzugen, bleibt ihnen - auch im Hinblick auf die Aussage der BaFin im RS 8/2005 - freigestellt[36] und ist u. a. abhängig von Art und Umfang der Risiken sowie der Größe des Instituts.

Vor diesem Hintergrund erscheint es angezeigt, vor bzw. während der Erstellung der Gefährdungsanalyse folgende Fragen/ Aspekte zu adressieren:

- Wann und weshalb sie erstellt wird?
- Auf welcher Grundlage geschieht dies?
- Wer ist der Adressat?

Neben der Darstellung des Instituts sollte in der Analyse auch auf das gesellschaftliche, politische und ökonomische Umfeld sowie alle objektiven und subjektiven Kriterien, die auf das Institut einwirken und zu Risiken und Gefährdungen führen können, eingegangen werden. Wirtschaftsprüfer und Aufsichtsbehörden, aber auch die Eigentümer oder Aufsichtsgremien des Instituts sollen in die Lage versetzt werden, über die Risiken und Gefährdungen des Instituts in Bezug auf Wirtschaftskriminalität informiert zu werden oder sich informieren zu können. Aus diesem Grund sollte die Gefährdungsanalyse möglichst einfach strukturiert und nachvollziehbar ge-

34 Siehe hierzu auch Abschnitt 2.2

35 Arbeitspapier „Datenschutzrechtliche Anforderungen für Research-Systeme zur Aufdeckung von Geldwäsche" vom 17. September 2007.

36 So auch Rott/Schmitt, Geldwäsche, Stuttgart 2005, S. 11.

gliedert werden. Sie sollte ein übersichtliches Bild über das Institut, dessen Struktur, die Geschäftstätigkeit, die Kundengruppen, das Umfeld in dem es tätig ist sowie dessen Risiken und Gefahren und die daraus gezogenen Schlussfolgerungen geben.

2.4.1 Anlass und Ziel der Erstellung

Die Erstellung einer Gefährdungsanalyse ist nicht explizit gesetzlich vorgeschrieben. Unabhängig davon ist jedes Institut schon aus wirtschaftlichen Gründen des Selbstschutzes daran interessiert, Risiken zu minimieren oder auszuschalten und Gefährdungen wirkungsvoll zu begegnen. Im bereits erwähnten RS 8/2005 der BaFin wird empfohlen, die Gefährdungsanalyse regelmäßig, zumindest einmal im Jahr einer Überprüfung zu unterziehen und, soweit erforderlich, zu aktualisieren.[37] Ob sich der Zeitrahmen „einmal im Jahr" auf das Kalenderjahr bezieht oder auf zwölf Monate, kann hierbei unberücksichtigt bleiben. Zum Ende des gewählten Zeitraums sollte in jedem Fall eine überprüfte bzw. aktualisierte Gefährdungsanalyse vorliegen. Wird festgestellt, dass sich seit der letzten Überprüfung Bedingungen wie z. B.

- Organisationsstruktur,
- Produktstruktur,
- Kundenstruktur,
- die Geschäftstätigkeit oder
- andere Rahmenbedingungen (wie z. B. Typologien)

stark verändert haben, ist die Gefährdungsanalyse zeitnah zu überarbeiten. Insoweit gilt, dass eine Gefährdungsanalyse einmal im Jahr oder anlassbezogen überprüft und wenn erforderlich aktualisiert werden sollte. Bei kleineren überschaubaren Instituten mit festem Kundenstamm, gleichbleibender Geschäftstätigkeit und sich nicht verändernden territorialen Bedingungen, ist eine Überarbeitung möglicherweise nicht so häufig notwendig wie im Falle größerer Institute.

37 Siehe BaFin-RS 8/2005, Ziffer 6.

Das Ziel einer Gefährdungsanalyse besteht darin, institutsspezifische Risiken zum Missbrauch vor betrügerischen Handlungen zu Lasten des Instituts oder der Institutsgruppe zu erkennen, zu identifizieren, zu erfassen und zu kategorisieren. In Betracht kommen hierbei:

- Kundenrisiken,
- Produktrisiken,
- Transaktionsrisiken,
- Vertriebswegerisiken,
- Länderrisiken und
- sonstige Risiken.

Die relevanten Risiken sind zu gewichten und im Detail einzuschätzen. Des Weiteren sind daraus Schlussfolgerungen zum Schutz des Instituts zu ziehen und entsprechende Maßnahmen einzuleiten. Zu den Maßnahmen gehören die Implementierung angemessener geschäfts- und kundenbezogene Sicherungssysteme sowie die Durchführung von Kontrollen zur Verhinderung von betrügerischen Handlungen und Wirtschaftskriminalität.

Die Angemessenheit wird durch jedes Institut selbst eingeschätzt. Daher gilt: Ziel der Gefährdungsanalyse sollte sein, möglichst alle Risiken und Gefahren zu erkennen und geeignete Maßnahmen zum Schutz des Instituts einzuleiten. Das sind notwendige Präventionsmaßnahmen zur Gefahrenabwehr in Form interner organisatorischer (bzw. sogenannter „weicher") Maßnahmen, wie zum Beispiel:

- interne Anweisungen,
- schriftlich fixierte Ordnungen,
- Festlegungen von Maßnahmen zur Mitarbeitervorprüfung,
- Identifizierung, Legitimations- und KYC-Prüfung,
- Festlegung einer Kundenakzeptanzpolitik,

- Festlegung eines Produkteinführungsprozesses,
- Festlegung von Zuständigkeiten und Verantwortlichkeit für die Bekämpfung von betrügerischen Handlungen und Wirtschaftskriminalität im Institut bzw. in der Gruppe,
- Aufgaben, Kompetenzen und Verantwortung der verantwortlichen Stelle,
- Eskalations- und Notfallpläne,
- Unterrichtung/ Sensibilisierung der Mitarbeiter (einschließlich der Führungskräfte).

Hinzu kommen könnten folgende „harte" Maßnahmen:

- Implementierung und ständige Weiterentwicklung von IT-basierten Researchsystemen,
- Festlegung der Indizien und der Kategorisierung,
- Wertung der Indizien zur Aussteuerung der Researchsysteme.

2.4.2 Zuständigkeit für die Erstellung

Dem für Betrugsprävention/-bekämpfung Verantwortlichen sollte es obliegen, die erkannten institutsspezifischen Risiken zum Missbrauch für betrügerische Handlungen und Wirtschaftskriminalität federführend zu erfassen, zu kategorisieren, zu gewichten sowie notwendige Maßnahmen aus der Bewertung der Risiken abzuleiten. Im Konzern hat der Konzernverantwortliche für die Prävention/ Bekämpfung betrügerischer Handlungen gemäß § 25g KWG dafür Sorge zu tragen, dass für die einzelnen Tochtergesellschaften separate Gefährdungsanalysen erstellt werden. Seiner Verantwortlichkeit obliegt es auch, die einzelnen Gefährdungsanalysen der Tochtergesellschaften in eine Konzern-Gefährdungsanalyse zusammenzuführen.

2.4.3 Adressaten

Adressaten der Gefährdungsanalyse können Folgende sein:

- Geldwäsche- und/ oder Sanktions-/ Embargobeauftragter,
- Vorstand/ Geschäftsleitung sowie andere Organe,
- andere Geschäftsbereiche/ Organisationseinheiten des Instituts (z. B. Operationelle Risiken [OpRisk], Interne Revision etc.) sowie weitere Gremien und Institutionen.

Diese Aufzählung ist nicht abschließend und kann, je nach Erfordernis um andere/ weitere Adressaten (siehe unten) erweitert werden.

2.4.3.1 Geldwäschebeauftragter und/oder Sanktions-/ Embargobeauftragter

Im Falle, dass für die Geldwäsche- und Betrugsbekämpfung separate Gefährdungsanalysen erstellt werden, ist es empfehlenswert, dass sich die jeweils Verantwortlichen ihre Analysen gegenseitig zur Verfügung zu stellen.

2.4.3.2 Vorstand/ Geschäftsleitung

Als gesetzliche Vertreter des Instituts sind der Vorstand bzw. die Mitglieder der Geschäftsleitung Adressaten der Gefährdungsanalyse. Hervorzuheben ist, dass Vorstand bzw. Geschäftsleitung

- als geschäftsführendes Organ zunächst für den Schutz des Instituts verantwortlich sind,
- demzufolge über die Risiken und Gefahren informiert sein müssen,
- über die vorgeschlagenen Maßnahmen entscheiden müssen und
- die konkrete Umsetzung der Maßnahmen zu veranlassen haben.

2.4.3.3 Andere Geschäftsbereiche/ Organisationseinheiten, Gremien des Instituts und weitere Institutionen/ Adressaten

Andere an der Erstellung der Gefährdungsanalyse beteiligte Geschäftsbereiche/ Organisationseinheiten und Gremien des Instituts erhalten die Gefährdungsanalyse auszugsweise im Hinblick auf ihre Aufgabenerfüllung oder bei berechtigtem Interesse vollständig.

Weitere Adressaten der Gefährdungsanalyse sind

- die Eigentümer eines Instituts,
- das Aufsichtsgremium,
- die BaFin und
- die internen und externen Prüfer

Die vorstehend Genannten sollen hierdurch über die Risiken und Gefährdungen des Instituts in Bezug auf betrügerische Handlungen und Wirtschaftskriminalität informiert werden.

2.4.4 Darstellung des Instituts, Aufbau, Struktur und Geschäftstätigkeit

Einleitend sollte eine Gefährdungsanalyse das Institut darstellen: die Gesellschaftsform, die wesentlichen Eigentümer im Sinne des wirtschaftlich Berechtigten gemäß GwG, den Aufbau des Instituts (inklusive Konzernaufbau) mit den jeweiligen konsolidierten Mehrheitsbeteiligungen und die Organisationsstruktur. Wenn notwendig, kann der Aufbau des Instituts mit seinen konsolidierten Beteiligungen („Töchter“) und deren Beteiligungen („Enkeltöchter“) zum besseren Verständnis grafisch dargestellt werden.

Die Darstellung der Organisationsstruktur ist die Wiedergabe des Organigramms des Instituts. Alle Organisationseinheiten, die im Organigramm dargestellt sind, sollten in der Gefährdungsanalyse ebenfalls genannt werden. Der für die Betrugsprävention/ -bekämpfung im Institut oder im Konzern Verantwortliche bzw. die dafür zuständige Organisationseinheit ist in der Gefährdungsanalyse ausdrücklich zu benennen, unabhängig von

der Abbildung im Organigramm. Ferner sind bei der Darstellung der Organisationseinheiten eines Instituts auch ausländische Niederlassungen, Filialen und Repräsentanzen aufzuführen, da z. B. geschäftliche Aktivitäten in bestimmten Ländern höhere Risiken bergen. Aber auch die Standorte der inländischen Filialen sind für die Darstellung eines Instituts von Interesse. Handelt es sich hierbei um besonders für betrügerische Handlungen oder für mögliche „Betrüger" interessante Standorte, wie z. B. Ballungszentren mit riskanten Branchen oder problematischen Bevölkerungsgruppen, Ortschaften in Grenznähe, Bahnhöfe und Flughäfen, so sollten diese Schwerpunkte ebenfalls genannt werden.

Zum besseren Verständnis für die Größe des Instituts und seiner Geschäftstätigkeit können die wesentlichen Bilanzzahlen sowie bedeutende Kunden- und Umsatzzahlen aus dem Geschäftsbericht herangezogen werden. Die prognostizierte Geschäftsentwicklung und Schwerpunkte der künftigen Geschäftstätigkeit, wie z. B. angestrebte Geschäftsbeziehungen zu besonderen Kundengruppen oder mit für betrügerische Handlungen besonders anfälligen Produkten, sollten bei der Darstellung des Instituts ebenfalls ihren Niederschlag finden.

2.4.5 Gesellschaftliche und wirtschaftliche Situation

Ist ein Institut ausschließlich in Deutschland tätig, so kann die Darstellung der gesellschaftlichen und wirtschaftlichen Situation relativ kurz ausfallen. In diesem Fall kann davon ausgegangen werden, dass (insbesondere auch im Inland ansässige) institutsfremde Personen über die aktuelle gesellschaftliche und wirtschaftliche Situation und Entwicklung im Lande informiert sind. Relevante wirtschaftliche Krisen in bestimmten Regionen im In- und Ausland sollten ebenfalls erwähnt werden. Politische und gesellschaftliche Auseinandersetzungen, Machtkämpfe oder Krisen bergen immer die Gefahr, dass die „Organisierte Kriminalität" versucht, solche Ausnahmesituationen für sich zu nutzen. Insbesondere geht von politischen Krisen die Gefahr von Anarchie sowie der Abkehr von der Achtung und Anerkennung bestehender politischer und gesellschaftlicher Werte aus. Hieraus resultieren außergewöhnliche Möglichkeiten und Potenziale für betrügerische Handlungen und Wirtschaftskriminalität. Auch der bevorstehende Abbau von Arbeitsplätzen in Unternehmen/ Betrieben in der Region oder gar im Institut kann ein darzustellendes Kriterium bei der Einschätzung der Situation und des Umfeldes, in dem sich das Institut

befindet, sein. Oftmals sind solche Situationen der Anlass für betrügerische Handlungen von Unternehmens- bzw. Institutsmitarbeitern, um sich selbst zu bereichern oder eventuell auch nur, um ihren bisherigen Lebensstandard zu halten.[38]

Zur gesellschaftlichen Situation gehört die Einschätzung der Kriminalitätslage im Land und in besonderen (bzw. besonders gefährdeten) Regionen. Hierzu sollten die öffentlich zugänglichen Medien genutzt werden, insbesondere die Lagebilder des Bundeskriminalamtes und der Landeskriminalämter. Aber auch Lagebilder oder Statistiken von größeren Polizeibezirken und Städten können herangezogen werden. Da die Kreditwirtschaft ein integrierter Bestandteil der Wirtschaft und Gesellschaft ist, richten sich viele Straftaten statistisch gesehen auch in proportionalem Maße gegen Institute wie auch gegen andere Unternehmen. Die Täter sind ebenfalls proportional gleichmäßig auf die Bevölkerung aufgeteilt, also auch innerhalb der Belegschaft eines Instituts. Diese Kriterien und Statistiken können bei der Erstellung der Gefährdungsanalyse behilflich sein.

Zur Darstellung eines Instituts gehört auch die Einbeziehung der gesammelten internen Erfahrungen auf dem Gebiet der Wirtschaftskriminalität. Die im letzten Berichtszeitraum festgestellten kriminellen Aktivitäten zu Lasten des Instituts, seiner Kunden oder seiner Mitarbeiter sollten genannt und statistisch aufbereitet werden. Das entspricht indirekt auch der Forderung des § 25c KWG, der den Einsatz und die Nutzung des öffentlichen, im Institut vorhandenen Erfahrungswissens über betrügerische Handlungen fordert.

Nach diesem allgemeinen Teil der Gefährdungsanalyse können die Risiken dargestellt, analysiert und bewertet werden. Daraus schlussfolgernd können die institutsspezifischen, risikobasierten Präventions-, Bekämpfungs- und Sicherungsmaßnahmen abgeleitet und Handlungsempfehlungen sowie Maßnahmen zum möglichen Ausschluss bzw. zur Minimierung der Risiken empfohlen oder festgelegt werden.

38 Siehe hierzu auch Abschnitt 2.1

2.5 Erhebung der Risiken

Zur umfassenden Ermittlung der Gefährdungssituation des Instituts ist eine Erhebung der Risiken unverzichtbar. Die jeweilige Methodik zur Erlangung der Informationsquellen kann hierbei, je nach Untersuchungsbreite der Gefährdungsanalyse und Institutsart bzw. –größe, unterschiedlich ausfallen. Neben einer moderierten Selbstauskunft („Self Assessment"), bei der ausgewählte Bereiche des Instituts mittels strukturierter Fragen in persönlichen Interviews nach deren Selbsteinschätzung befragt werden, besteht auch die Möglichkeit einer direkten Expertenbefragung. Hierbei bieten sich als Ansprechpartner zur Befragung die unter Abschnitt 4.1.1.2 ff. genannten Mitglieder eines sogenannten „Betrugsprävention sgremiums" an, welches aus den in der Betrugsprävention/ -bekämpfung involvierten Experten des Instituts besteht. Insoweit stellt die moderierte Selbstauskunft in Verbindung mit dem Expertenwissen eine Möglichkeit der Risikoerhebung dar.

Bei der erstmaligen Erstellung einer Gefährdungsanalyse kann i.d.R. eine Fragebogenaktion für das gesamte Institut empfohlen werden. Die nachfolgenden Ausführungen beruhen deshalb auf dieser bewährten, praxisorientierten Vorgehensweise und geben Hinweise hinsichtlich der zu erhebenden Risikoarten sowie zur Durchführung der Risikoerhebung mit Fragebögen.

2.5.1 Risikoarten

2.5.1.1 Kundenrisiken

Jedes Institut sollte im Rahmen seiner Geschäftsstrategie eine Kundenakzeptanz-Policy erstellen. Darin wird festgelegt,

- wer die bevorzugten Zielkunden sind,
- in welchen Ländern und Territorien das Institut tätig sein möchte und
- welche Arten von Geschäftsbeziehungen angestrebt werden bzw. abzulehnen sind.

Wichtig bei der Einschätzung und Beschreibung der Gefährdungssituation ist, ob das Institut seine Kunden kennt, ob es viele Neukunden akquiriert oder ob zahlreiche Gelegenheitskunden zu verzeichnen sind. Welche politisch exponierten Personen (PEP)[39] zu Kunden des Instituts zählen, wie groß die Möglichkeit ist, dass PEPs Kunden des Instituts werden, wie der Umgang mit dieser Kundengruppe zu gestalten ist, sind weitere Fragen, die bei der Einschätzung der Gefährdungslage hilfreich sein könnten.

Kunden mit Sitz in Risikoländern sind zu erfassen. Unternehmen mit relativ undurchsichtiger Eigentümer- oder Gesellschafterstruktur sollten separat erfasst werden, da die Überwachung solcher Kunden intensiver ausfallen kann. Wenn bei der Erfassung von Auffälligkeiten schnelle, nicht nachvollziehbare Transaktionen festgestellt werden, so sind die Transaktionen, Auftraggeber und Begünstigten ebenfalls gesondert zu überwachen. Entsprechende Transaktionen sollten auch in der Gefährdungsanalyse erfasst werden. Ebenfalls einer besonderen Überwachung sollten Kunden unterstellt werden, die eine unerklärliche Distanz zwischen ihrem Wohn- oder Arbeitsort und dem Institut haben. Konten von speziellen Kunden, wie z. B. Waffenhändlern, -produzenten und Mittlern, sind ebenso einer besonderen Überwachung zu unterziehen wie beispielsweise die von Juwelen- und Antiquitätenhändlern. Diese Kunden sind auch für die Zwecke der Gefährdungsanalyse zu erfassen.

Betrügerische Handlungen und wirtschaftskriminelle Straftaten bedingen stets aktives Handeln oder Unterlassen von Handlungen von Menschen. In den Instituten sind Menschen auf der einen Seite entweder als Gremienmitglieder, gesetzliche Vertreter, Mitarbeiter im Angestelltenverhält-

39 Richtlinie 2005/60/EG des EU-Parlaments und des EU-Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, in: EU-Amtsblatt L 309 vom 25. November 2005, S. 15 ff. (im Folgenden: „Dritte EU-Anti-Geldwäscherichtlinie" bzw. „3. AGwR"). In Art. 3 Nr. 8 der 3. AGwR werden politisch exponierte Personen definiert als *„diejenigen natürlichen Personen, die wichtige öffentliche Ämter ausüben oder ausgeübt haben, und deren unmittelbare Familienmitglieder oder ihnen bekanntermaßen nahe stehende Personen*". Dieser so definierte Personenkreis wird näher bestimmt durch Art. 2 der Richtlinie 2006/70/EG der EU-Kommission vom 1. August 2006 mit Durchführungsbestimmungen für die Richtlinie 2005/60/EG des EU-Parlaments und des EU-Rates hinsichtlich der Begriffsbestimmung von „politisch exponierte Personen" und der Festlegung der technischen Kriterien für vereinfachte Sorgfaltspflichten sowie für die Befreiung in Fällen, in denen nur gelegentlich oder in sehr eingeschränktem Umfang Finanzgeschäfte getätigt werden, in: EU-Amtsblatt L 214 vom 4. August 2006, S. 29 ff. Dort findet sich eine genaue Auflistung der betroffenen Personengruppen.

nis oder auf vertraglich vereinbarter Basis als Vertreter für das Institut tätig. Sie treten auf der anderen Seite als Kunden oder Geschäftspartner des Instituts in Erscheinung.

Zur Erstellung der Gefährdungsanalyse sollten daher zunächst die Kunden oder Geschäftspartner eines Instituts und die Risiken betrachtet werden, die von ihnen und von ihrem Handeln ausgehen können. Hierzu werden alle Kunden in Kundengruppen eingeteilt. Als mögliche Kundengruppen, die auch im institutsinternen IT-System zu hinterlegen wären, können folgende in Betracht kommen:

- Deutsche Bundesbank
- Landesbanken/ Girozentralen
- Sonstige Kreditinstitute Inland
- Direktbanken
- Eigene Tochterinstitute Inland
- Kreditinstitute Ausland
- Eigene Tochterinstitute Ausland
- Sparkassen
- Volks- und Raiffeisenbanken
- Privatrechtliche Unternehmen Inland
- Inländische Organisationen, Vereinigungen, Religionsgemeinschaften
- Privatpersonen Inland
- Privatrechtliche Unternehmen Ausland
- Ausländische Organisationen, Vereinigungen, Religionsgemeinschaften
- Privatpersonen Ausland
- Interne Konten

- Gemeinden
- Öffentliche Haushalte Inland
- Juristische Personen des öffentlichen Rechts Inland
- Öffentliche Haushalte Ausland
- Juristische Personen des öffentlichen Rechts Ausland

Um eine weitere Einschätzung der Kunden vornehmen zu können, sind alle Kunden entsprechend ihrer wirtschaftlichen Tätigkeit in Branchen einzugruppieren. Denkbar sind folgende Branchenkategorisierungen, ohne einen Anspruch auf Vollständigkeit zu erheben[40]:

- Baugewerbe
- Chemie und Pharmazie
- Energie und Wassererzeugung/-versorgung
- Fahrzeugbau/-handel
- Finanzdienstleistungen und Versicherungen
- Gesundheitswesen
- Hotel und Gaststätten
- Land- und Forstwirtschaft
- Leasinggesellschaften
- Maschinenbau und Elektrotechnik
- Religiöse Organisationen und Einrichtungen
- Telekommunikation
- Sonstige bzw. spezielle Branchen
- Natürliche Person

Geht man davon aus, dass stets Menschen die Akteure sind, die betrügerische/ wirtschaftskriminelle Handlungen begehen, so könnte gegebenenfalls die Kundengruppe „Privatkunden" weiter differenziert werden. Hier wäre folgende Unterteilung denkbar:

40 Weitere differenziertere Unterteilungen sind jederzeit möglich.

- Eigene Mitarbeiter und Pensionäre (ehemalige Mitarbeiter) sowie deren Angehörige
- Minderjährige
- Schüler und Studenten
- Angestellte des öffentlichen Dienstes und deren Familienangehörige
- Angestellte in Unternehmen der Privatwirtschaft (Kapitalgesellschaften)
- Freiberuflich Tätige und deren Familienangehörige
- Abgeordnete, Politiker (PEPs) und deren Familienangehörige
- Wirtschaftlich Berechtigte für abweichende Konten
- Kunden mit Wohnsitz im Ausland
- Sonstige

Jeder Kunde sollte abschließend im Rahmen der KYC-Prüfung - je nach Sitz/ Wohnsitz - eingruppiert werden. Hierbei sollte darauf geachtet werden, ob der Kunde seinen Sitz oder Wohnsitz im Einzugsgebiet des Instituts und der Filiale hat, in der das Konto eröffnet wurde. Ist dies nicht der Fall, wäre die Frage zu stellen, warum der Kunde ausgerechnet diese Filiale auswählt. Ist die Erklärung des Kunden zu dieser Frage nicht plausibel, so kann bei Aufnahme einer Geschäftsbeziehung eine höhere Gefahr von diesem Kunden ausgehen.

Besondere Vorsicht könnte auch geboten sein, wenn es sich um Kunden handelt, die ihren Sitz im Ausland haben und keine wirtschaftliche Tätigkeit oder einen anderen plausiblen Bezug zum Einzugsgebiet des Instituts haben. Geschäftsbeziehungen zu Kunden mit Sitz in offiziell - z. B. von der BaFin oder Financial Action Task Force on Money Laundering (FATF) klassifizierten - Risikoländern sind zudem einer besonderen Risikoeinschätzung zu unterziehen. Geschäftsbeziehungen mit Kunden aus Branchen, die in besonderer Weise anfällig sind, für betrügerische Zwecke missbraucht zu werden, bedürfen einer besonderen Überwachung.

Ein weiteres Kriterium für die Einschätzung des Kunden könnte sein, ob er im Rahmen der Kontoeröffnung persönlich anwesend war, durch Vermittler zum Institut kam oder die Identifizierung und Legitimationsprüfung von Dritten vorgenommen wurde.

2.5.1.2 Produktrisiken

Eine zusätzliche Risikoart zur Bestimmung des objektiven Risikopotenzials des Instituts stellen die sogenannten „Produktrisiken" dar. Hierbei ist zu unterscheiden, wie gefährdet das einzelne, angebotene Produkt ist, zu betrügerischen Handlungen missbraucht zu werden und in welcher Kombination (Produkt/ Branche/ Region/ Land) bzw. in welchem Umfang es vom Institut auch tatsächlich angeboten wird.

Ein Großteil aller Bankprodukte könnte zunächst grundsätzlich der erhöhten Risikogruppe zugeordnet werden. Hierbei handelt es sich jedoch im Wesentlichen um sogenannte banktypische „Massenprodukte", wie z. B. Girokonten und jede Art von Bankkarten. Auch wenn der einzelne Schadensfall dieser Produkte von der Höhe her begrenzt ist, kann die Kumulation dieser „kleinen" Risikofaktoren zu einem erheblichen Gefährdungspotenzial führen.

In den nachfolgenden Abbildungen ist beispielhaft der Analyseprozess aufgezeigt, mit dem berechnet wird, welche Produkte von welchen Betrugsmustern gefährdet werden bzw. für welches Produkt die Gefahr, zu betrügerischen Handlungen missbraucht zu werden, am höchsten ist. Dabei wird die Bewertung der Betrugsgefahr nach einem einfachen Schema definiert: Besteht eine hohe Betrugsgefahr („ja") erfolgt eine Bewertung mit „9" Risikopunkten, bei einer mittleren Betrugsgefahr („teilweise") mit „6" und bei einer geringen Betrugsgefahr („nein") mit „3" Risikopunkten.

Betrugsgefahr	Bewertung in Risikopunkten
ja	9
teilweise	6
nein	3

Quelle: Mitgliedsinstitute des VÖB

Abbildung 3: Beispiel für die Risikopunktebewertung der Betrugsgefahr

Von dieser Einschätzung wird anschließend ein mathematischer Durchschnitt errechnet, der in der nachfolgenden Tabelle als „Risikograd" bezeichnet ist. Dieser Risikograd spiegelt die entsprechende Risikogruppe, in der sich das jeweilige Produkt befindet, wider.

Risikograd	Risikogruppe
3,00 – 4,99	1
5,00 – 6,99	2
7,00 – 9,00	3

Quelle: Mitgliedsinstitute des VÖB

Abbildung 4: Bewertung Risikograd zu Risikogruppe

Um eine Vergleichbarkeit der Produktrisiken herzustellen, wird – wie in der nachfolgenden Tabelle verdeutlicht – die geschätzte Betrugswahrscheinlichkeit („ja/teilweise/nein") mit den entsprechenden Risikopunkten bewertet (9/6/3).

Produktgruppe	Produktkategorie	Anzahl der Produkte in der Bank gesamt	Betrügerische Handlungen (am Beispiel von vier Betrugarten)				Risikopotenzial	
			Kontoeröffnungsbetrug	Zahlungsverkehr Betrug	Kreditbetrug	sonstiger Betrug	Risikograd	Risikogruppe
Geschäfts- und Privatgirokonten	Geschäftskonten	82.000	9	9	3	6	6,75	2
	Girokonto privat	668.500	9	9	3	6	6,75	2
	…	…	…	…	…	…	…	…
Spareinlagen und Vertragssparen	Sparkonto kurzfristig	5.900	9	9	3	6	6,75	2
	…	…	…	…	…	…	…	…
Kreditgeschäft/ Darlehen	Baufinanzierung Annuitätendarlehen	52.460	6	3	9	6	3,75	1
	…	…	…	…	…	…	…	…

Quelle: Mitgliedsinstitute des VÖB

Abbildung 5: Beispiel für eine Bewertung der Produktrisiken

Zur Verdeutlichung des Sachverhalts ein Beispiel: Die Produktgruppe „Geschäfts- und Privatgirokonten" wird aufgeschlüsselt: Werden hierbei

nur die privaten Girokonten betrachtet, bekommt das Produkt für die mögliche betrügerische Handlung „Kontoeröffnungsbetrug" die höchste Punktzahl von neun Risikopunkten. Da das private Girokonto ebenfalls für den Zahlungsverkehrsbetrug (z. B. Überweisungsbetrug) mit einer relativ hohen Wahrscheinlichkeit missbraucht werden kann, sind weitere neun Risikopunkte zu addieren. Für den „reinen" Kreditbetrug eignet sich dieses Produkt im allgemeinen nur eingeschränkt, ein Umstand, welcher sich in der niedrigen Risikopunktzahl von 3 widerspiegelt. Nach Überprüfung aller möglichen betrügerischen Handlungen und der entsprechenden Zuordnung und Addition der Risikopunkte wird ein arithmetisches Mittel gebildet: Gesamtpunktezahl dividiert durch die Anzahl der möglichen betrügerischen Handlungen. Das jeweilige Ergebnis findet sich wieder im Risikograd. Im Beispiel der Privatgirokonten ergibt das arithmetische Mittel einen Risikograd von 6,75 Punkten, was der Risikogruppe 2 (mittleres Risiko) entspricht. Das Risikopotenzial des Instituts besteht insofern aus dem Risikograd bzw. der Einteilung in der Risikogruppe.

Wie bereits erwähnt, ist bei der anschließenden Bewertung auch das stückzahlmäßige Vorkommen der jeweiligen Produktkategorie im Institut von großer Bedeutung. In unserem Beispiel haben die Produktkategorien „privates Girokonto" und „kurzfristiges Sparkonto" auf den ersten Blick einen identischen Risikograd. Dies ändert sich jedoch deutlich zu Gunsten des Sparkontos, wenn dessen geringe Anzahl im Institut mit dem hohen Volumen an privaten Girokonten verglichen wird. Auf Grund des hohen Volumens würde das Girokonto eher in die Risikogruppe 3 steigen und das kurzfristige Sparkonto in der Risikogruppe 2 verbleiben (im Gegensatz zu mittel- und langfristigen Sparbüchern, die sich in der Risikogruppe 1 wiederfinden).

2.5.1.3 Transaktions- und Vertriebswegerisiken

2.5.1.3.1 Transaktionsrisiken

Transaktionsrisiken sind Risiken, die auf dem gesamten Prozessweg einer Transaktion entstehen können. Bei grenzüberschreitenden Transaktionen umfasst dies insbesondere auch die Länderrisiken. Der Einfachheit halber sei dies beispielhaft an Transaktionen im Rahmen des Zahlungsverkehrs erläutert. Hierbei ist zunächst die Qualität des für die Transaktionen genutzten Zahlungsverkehrssystems zu bewerten. Zu prüfen und zu bewer-

ten ist ferner die Herkunft einer Transaktion. Transaktionen im Inland sind auf Grund eines engmaschigen Rechts- und Kooperationsrahmens zwischen den Akteuren des Finanzsektors grundsätzlich problemlos. Bei Transaktionen aus dem Ausland ist bei einer Bewertung konkret auf das Herkunftsland abzustellen. Existieren in dem Herkunftsland analoge Bestimmungen zur Legitimationsprüfung und Identifizierungspflicht wie in Deutschland, können auch hier die Kontrollen auf verhältnismäßig niedrigem Niveau gehalten werden. In Betracht kommen zunächst die EU-Mitgliedstaaten und die von der BaFin in ihrem Rundschreiben 7/2008[41] veröffentlichten Länder und Gebiete mit gleichwertigen Anforderungen bei der Verhinderung von Geldwäsche und Terrorismusfinanzierung, die vergleichbare gesetzliche Regelungen und Finanzaufsichten haben und von denen die Legitimationsprüfung durch den gleichen Berechtigtenkreis gemäß GwG anerkannt werden kann.

Ob ein Institut prinzipiell alle von der BaFin als unbedenklich eingestuften Länder ebenfalls als unbedenklich kategorisiert, bleibt ihm letztlich selbst überlassen. Kommen Transaktionen aus Ländern, die nur schwache oder unwirksame Regelungen im Rahmen des Kundenannahmeprozesses haben, ist erhöhte Vorsicht geboten. Ferner ist zu erwägen, die Transaktion sowie den Empfänger der Transaktion zu überwachen und gegebenenfalls in eine höhere Gefährdungsklasse bzw. Risikogruppe einzugruppieren. Die Gefahr, dass Gelder aus Straftaten transferiert werden oder für Straftaten genutzt werden sollen, ist in solchen Fällen eher zu vermuten. Kommt eine Transaktion über mehrere Institute und nicht auf dem kürzesten Weg, und sind darüber hinaus notwendige oder übliche Angaben gemäß der Geldtransfer-Verordnung[42] nicht vorhanden, müssen solche Transaktionen ebenfalls mit erhöhtem Risiko eingestuft werden.

Entsprechende Transaktionsrisiken bergen auch solche Geschäftsvorgänge, die durch Bareinzahlungen ausgelöst wurden. Bareinzahlungen sind

41 BaFin, Rundschreiben 7/2008 (GW) vom 1. August 2008 - I. Länder und Gebiete mit gleichwertigen Anforderungen bei der Verhinderung von Geldwäsche und Terrorismusfinanzierung II. Deutsche Übersetzung des Leitfadens der Financial Action Task Force on Money Laundering (FATF) zum risikoorientierten Ansatz der Bekämpfung von Geldwäsche und Terrorismusfinanzierung vom Juni 2007 (GZ: GW 1-QIN 4101-2008/0001) (im Folgenden: BaFin-RS 7/2008).

42 Verordnung (EG) Nr. 1781/2006 des EU-Parlaments und des EU-Rates vom 15. November 2006 über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers (Text von Bedeutung für den EWR), in: EU-Amtsblatt L 345 vom 8. Dezember 2006, S. 1 ff. (im Folgenden: „Geldtransfer-Verordnung").

außerhalb der jeweiligen gesetzlich vorgeschriebenen Grenzen/ Schwellenbeträge stets zu hinterfragen. Wenn jedoch Bareinzahlungen aus Ländern mit höherem Risiko eingehen, können die Hintergründe der Transaktion vom eigenen Institut trotz Bemühens häufig nicht wirksam geklärt werden. Die Transaktionsrisiken sind für die Bewertung zur Erstellung der Gefährdungsanalyse nach hiesiger Auffassung stets dann zu beachten, wenn das eigene Institut entweder Empfänger- oder Auftraggeberinstitut ist.

2.5.1.3.2 Vertriebswegerisiken – Vermittler, Direktbanken, Förderbanken und Konsortialgeschäft

Jeder Prozess der Geschäftsanbahnung, der Vermittlung von Geschäften bzw. Kunden und der Kundenbetreuung birgt Risiken. Diese Risiken sind festzustellen und zu minimieren; dies insbesondere, wenn das Institut keinen direkten Kontakt zu dem Kunden hat. Das ist immer dann der Fall, wenn die Kunden von Dritten vermittelt werden und das kontoführende Institut sich auf die Informationen und die Echtheit der beizubringenden Dokumente und Unterlagen auf Dritte verlassen muss. Der Vertrieb findet nicht direkt zwischen kontoführendem Institut und Kunden, sondern zwischen kontoführendem Institut, einem Dritten und dem Kunden statt.

Vermittler

Vermittler sind Dritte, die auf der Grundlage von Vermittlerverträgen Kunden akquirieren und/ oder Produkte der Institute verkaufen bzw. vermitteln.[43] Oftmals nehmen sie auch die Legitimationsprüfung (gemäß § 154 Abgabenordnung) vor oder bereiten die Geschäftsbeziehung des Kunden mit dem Institut umfassend vor. Sie organisieren die notwendigen Unterlagen und Dokumente, sichten sie auf Vollständigkeit und bescheinigen gegenüber dem Institut oftmals, dass die Originale vorgelegen haben.

Das Risiko bei vermittelten Geschäften besteht darin, dass Vermittler vertragsgemäß teilweise oder ganz erfolgsorientiert vergütet werden. Jedes vermittelte Geschäft wird dem Vermittler entsprechend seiner Höhe vergütet. Bedauerlicherweise neigen Vermittler in manchen Fällen dazu, die

43 Zu den Anforderungen an Dritte siehe auch § 7 GwG.

Bonität ihrer vermittelten Kunden „schön zu rechnen" oder Geschäfte zu vermitteln, die der Kunde oder das Institut bei seriöser Beratung und intensiver Prüfung in der Art oder Höhe nicht unbedingt abgeschlossen hätten. Insbesondere im sonst unkritischen Bauspargeschäft kommt es durch Vermittler leider immer wieder zum Abschluss von Bausparverträgen mit älteren Menschen oder gering verdienenden Kunden. Das Argument der Vermittler ist dann, dass Sonderzahlungen erwartet würden, wodurch das Ansparziel lebenswirklichkeitsnah realisiert werden könne.

Auch die Vermittlung von ausländischen Kunden birgt große Risiken, wenn der Kunde nicht persönlich zum Institut kommt und das Geschäft vollständig über Vermittler angebahnt und abgewickelt wird. Treten dann Probleme in der Geschäftsbeziehung auf, ist der Kunde oft nur schwer oder gar nicht erreichbar.

Das Vermittlergeschäft sollte demzufolge stets als Geschäft mit höherem Risiko eingestuft werden.

Direktbanken

Das Geschäftsmodell der Direktbanken ist darauf abgestellt, dass kein direkter Kundenkontakt hergestellt wird. Die Legitimationsprüfung und die Identifizierung (gemäß § 4 GwG) wird durch Dritte (i.S.d. § 7 Abs. 1 GwG) oder auf Grund vertraglicher Vereinbarungen (gemäß § 7 Abs. 2 GwG) vorgenommen. Die Direktbanken müssen sich demnach darauf verlassen, dass Dritte die Legitimationsprüfung und Identifizierung sorgfältig vornehmen. Des Weiteren ist der Dritte angehalten, die vom Kunden vorgelegten Dokumente und Unterlagen (Personaldokumente, Gehaltsbescheinigungen, Grundbuchauszüge, Vermögensaufstellungen, Liquiditätsnachweise, Bürgschaftserklärungen etc.) auf ihre Echtheit hin zu überprüfen, um sie anschließend in Kopie dem kontoführenden Institut unmittelbar zu übersenden. Wird dabei von dem Dritten bewusst oder unbewusst ein Fehler begangen, so besteht die Gefahr, dass das kontoführende Institut wirtschaftlichen Schaden erleidet. Geschäfte mit „nicht existierenden Personen" oder auf der Grundlage falscher Dokumente führen regelmäßig zum wirtschaftlichen Verlust. So werden eingeräumte Dispositionslinien, Kreditrahmen oder ausgereichte Kredite zwar in Anspruch genommen, jedoch nicht zurückgezahlt und können vom Institut auch nicht geltend gemacht werden. Sie sind uneinbringlich und müssen als Verlust wertberichtigt

und ausgebucht werden. Insoweit bergen die Geschäfte der Direktbanken von sich aus ein erhöhtes Risiko und sind in der Gefährdungsanalyse besonders darzustellen. Ferner sind während des Kundenannahmeprozesses und der Geschäftsbeziehung entsprechende Sicherungsmechanismen zu installieren.

Förderbanken

Bei der Ausgabe von staatlichen Fördermitteln oder Fördermitteln der Europäischen Union besteht meist ein direkter Kontakt zwischen Förderbank und dem Kunden. Die Legitimationspapiere, Kontoeröffnungsunterlagen und weitere Unterlagen, die nachweisen, dass der Kunde förderungswürdig und förderungsberechtigt ist, können von der Förderbank direkt eingesehen und auf Echtheit überprüft werden. In Fällen, in denen das Förderinstitut jedoch keinen direkten Kundenkontakt hat, da die Legitimationsprüfung von der Hausbank des Kunden oder einer staatlichen oder kommunalen Institution vorgenommen wird und die notwendigen Unterlagen von dort zur kreditausreichenden Förderbank gesandt werden, muss sich die Förderbank auf diese Institution verlassen. Die hier bestehenden Risiken sind auf Grund der Zuverlässigkeit der die CDD-Maßnahmen durchführenden Institutionen jedoch als gering einzuschätzen.

2.5.1.4 Konsortialgeschäft

Im Konsortialgeschäft bahnt der Konsortialführer die Geschäftsbeziehung an und führt die Legitimationsprüfung sowie die KYC-Prüfung im Rahmen des Customer Due Diligence (CDD)-Prozesses durch.[44] Bei Bedarf stellt er den Konsorten die Unterlagen und Dokumente in Kopie zur Verfügung und übernimmt die Verantwortung dafür, dass alles im Original vorgelegen hat und eingesehen wurde. Die am Konsortium beteiligten Institute verlassen sich auf den Konsortialführer (als zuverlässigen Dritten i.S.d. GwG[45]), der wiederum im Namen aller beteiligten Konsorten handelt. Der Konsortialführer handelt mit der Sorgfalt eines ordentlichen Kaufmannes im Namen

44 Zu einer Würdigung des Konsortialgeschäfts aus geldwäscherechtlicher Sicht siehe Ganguli, Indranil/ Achtelik, Olaf et al., Risikoorientierte Geldwäschebekämpfung - Praktikerhandbuch auf Basis des neuen Geldwäschegesetzes (GwG), Heidelberg 2008 (im Folgenden: Ganguli/Achtelik et al.), S. 74 ff.

45 Vgl. Ganguli/Achtelik et al., S. 75.

und auf Rechnung der beteiligten Konsorten genauso wie er für sich selbst handelt. Der Kunde muss nicht unbedingt alle Konsortialbanken kennen (Innenkonsortium). Das hat den Vorteil, dass Konsortialbeteiligungen veräußert werden können, ohne dass der Kunde davon Kenntnis erlangt. Die Aufteilung der Risken wird genauso vertraglich vereinbart wie die Gewinnverteilung. Konsortialgeschäfte werden i.d.R. nur von Instituten gemeinsam getätigt, die sich bekannt sind, über das entsprechende Bankenrating verfügen und die meist gegenseitig in Korrespondenzbankbeziehung stehen. Damit sind die Risiken für betrügerische Handlungen im Konsortialgeschäft eher als gering bis normal einzustufen.

2.5.1.5 Länderrisiken

Bei der Bewertung von Kunden mit Sitz oder Wohnsitz im Ausland, sind Länderrisiken ebenfalls als Kriterium für die Gefährdungsanalyse mit zu berücksichtigen. Länderrisiken sind Risiken, die wegen der im jeweiligen Land herrschenden politischen und wirtschaftlichen Bedingungen kriminalitätsbegünstigend sein können, weil in diesen Ländern keine in der EU übliche Legitimationsprüfung und Identifizierung stattfindet oder die KYC-Prüfung nicht den Standards der FATF und der EU entspricht.

Zudem ist die politische Situation jedes Landes einzuschätzen. Regierungsformen wie parlamentarische Demokratie, Monarchie, Diktatur einzelner Personen, Parteien oder Familienclans und die Integration dieser Länder in internationale Organisationen, wie z. B. den Vereinten Nationen (VN), der Europäischen Union oder dem Baseler Ausschuss, sind als Kriterien heranzuziehen.

Ein weiteres Kriterium für die Bewertung des Länderrisikos ist die ökonomische und gesellschaftliche Situation eines Landes. Ökonomisch unterentwickelte Länder oder Länder mit instabilen wirtschaftlichen Entwicklungen bzw. Krisen, in denen z. B.

- die Gefahr von Enteignungen drohen,
- Korruption immanenter Bestandteil des Wirtschaftssystems ist oder
- in denen Akteure aus Wirtschaft und Politik personell eng miteinander verflochten sind,

sind mit höherem Risiko einzustufen.

Länder, in denen sich Unternehmen oder sogar Finanz- und Kreditinstitute in den Händen krimineller Eigentümer oder der Organisierten Kriminalität befinden und politischen Einfluss ausüben, sind mit hohem Risikograd zu versehen. Nicht funktionierende oder gegebenenfalls korrupte Strafverfolgungsbehörden sind ein weiterer Anhaltspunkt für ein höheres Risiko des Landes[46]. Für die Bewertung der Länderrisiken auf Grund der politischen und ökonomischen Situation und der Währungsstabilität sollten, soweit vorhanden, auch die volkswirtschaftlichen Analysen des Internationalen Währungsfonds, der Europäischen Zentralbank und der Institute oder Institutsverbände mit herangezogen werden.

Die Qualität, Zusammensetzung und Eigentümerstruktur der Finanz- und Kreditwirtschaft ist ein weiteres Kriterium für die Einschätzung des Länderrisikos. Wenn es ohne Probleme möglich ist, dass die Organisierte Kriminalität oder andere kriminelle Akteure in einem Land Eigentümer von Finanz-/ Kreditinstituten sein können bzw. eine Prüfung oder Kontrolle durch eine in der EU vergleichbare Finanzaufsicht nicht stattfindet, müssen solche Länder zwangsläufig mit erhöhtem oder hohem Risiko kategorisiert werden.

Für die Einschätzung eines Länderrisikos können ferner national anerkannte Typologiepapiere, z. B. der Financial Intelligence Unit (FIU) des Bundeskriminalamtes oder anderer FIUs und internationale Einschätzungen/ Bewertungen der FATF, von Transparency International u. a. genutzt werden. Länderrisiken werden auch von internationalen Organisationen und nationalen Stellen, wie VN, EU, OECD[47], OFAC[48], vom Auswärtigen Amt oder den (Geheim-)Diensten, erkannt bzw. ermittelt und beschrieben und sollten in der Gefährdungsanalyse Berücksichtigung finden.

46 Anhaltspunkt für eine entsprechende Beurteilung könnten u. a. die von der zivilgesellschaftlich tätigen und weltweit anerkannten Anti-Korruptionsorganisaton Transparency International entwickelten Korruptionsindices sein; im Internet abrufbar unter: http://www.transparency.de/korruptionsindices.382.0.html (Stand: 15.03.2010).

47 Die Abkürzung OECD steht für Organisation for Economic Co-operation and Development.

48 Die Abkürzung OFAC steht für Office of Foreign Assets Control, eine nachgeordnete Behörde des US-Finanzministeriums, die für die Durchführung der Sanktionsmaßnahmen in den USA zuständig ist.

2.5.1.6 Sonstige Risiken

Die Bewertung der Risiken sollte stets aktuell erfolgen. Risiken können sich ändern. Risiken können auch zusammen auftreten in Form sogenannter Kombinationsrisiken. Anhand einer Transaktion mit einer öffentlichen Stelle eines anderen Staates, z. B. des Finanzministeriums, soll dies verdeutlicht werden: Das Finanzministerium eines anderen Staates ist von sich aus mit einem geringen Risiko eingestuft. Wird jedoch der andere Staat gleichzeitig mit hohem Länderrisiko bewertet, weil dort Korruption weit verbreitet ist und kaum bekämpft wird, so erhöht sich das Risiko der Transaktion. Sofern eine mit dieser Transaktion verbundene Zahlung auf das Konto einer im Inland ansässigen natürlichen Person eingeht und diese Person sonst keine weiteren nennenswerten Geldeingänge hat, sollte diese Transaktion als riskant bewertet und überprüft werden. Wenn anschließend eine sehr zeitnahe Barverfügung des eingegangenen Geldbetrags erfolgt, ist der Verdacht, dass das Institut für betrügerische Handlungen und Geldwäsche missbraucht wird, hoch. Es kann sich dabei um einen Finanzagenten handeln, der nur sein Konto zum Verschleiern von Zahlungen zur Verfügung stellt und die eingegangene Transaktion einen kriminellen Ursprung hat. Zusammengefasst stellen sich die Risiken wie folgt dar:

Öffentlichen Haushalt Ausland	- geringes Risiko
Herkunftsland mit hohem Kriminalitätsindex	- hohes Risiko
Natürliche inländische Person	- geringes Risiko
Hoher außergewöhnlicher Geldeingang	- hohes Risiko
Schnelle Barverfügung nach Geldeingang	- hohes Risiko

Insgesamt ist die Transaktion mit einem hohen Risiko behaftet.

Ein anderes Beispiel für ein Kombinationsrisiko ist die Verwendung von Krediten oder zugesagten Kreditlinien. Dazu ein Beispiel: Eine im Inland ansässige Firma nimmt nach eingehender Prüfung einen Kredit auf. Die Geschäftsanbahnung erfolgt über einen Vermittler. Die eingeräumte Kreditlinie entspricht der vom Vermittler dargestellten Geschäftstätigkeit. Es handelt sich um ein junges Unternehmen, welches im Rahmen der Unter-

nehmensgründung über eine geringe Bonität, aber ein überzeugendes Geschäftsmodell verfügt. Als Sicherheit dient das Grundstück des Geschäftführers. Der Grundbuchauszug wurde vom Vermittler beschafft. Die Bewertung des Grundstückes durch einen Gutachter wird ebenfalls vom Vermittler beigebracht. Kurz nach Geschäftsabschluss wird die eingeräumte Kreditlinie vollständig in Anspruch genommen und das Geld ins Ausland überwiesen. Das Grundstücksgutachten stellt sich später als Fälschung heraus.

Auch hier stellen sich die Risiken zusammengefasst wie folgt dar:

Inländisches Unternehmen	- mittleres Risiko
Junges Unternehmen	- mittleres Risiko
Vermittlergeschäft	- hohes Risiko
Mit einer Grundschuld abgesichertes Geschäft	- geringes Risiko
Schnelle Abverfügung des Kredites und Überweisung ins Ausland	- hohes Risiko

In diesem Fall ist trotz Vorhandensein eines mittleren Risikos der Kreditbetrug dennoch vollendet worden.

2.5.2 Herangehensweise und Methodik – Risikoerhebung mit Hilfe von Fragebögen

Im Rahmen der Informationsbeschaffung für die Erstellung der Gefährdungsanalyse sollte über eine Fragebogenaktion das Basiswissen und die Selbsteinschätzung der Bereiche zum Thema betrügerische Handlungen im Institut eingefordert werden.

2.5.2.1 Instrument des Fragebogens (Inhalt und Aufbau)

Der Fragebogen beinhaltet zum einen Fragen über die jeweiligen Einschätzungen des Risikos in den Verantwortungsbereichen, von betrügerischen Handlungen in der Gegenwart bzw. in der Zukunft missbraucht zu

werden, wie auch Fragen über bereits aufgetretene Betrugsfälle und gegenwärtige Präventionsmaßnahmen. Da Bereiche in einem größeren Institut regelmäßig gebeten werden, mitunter an verschiedenen Fragebogenaktionen teilzunehmen, sollte vorab hausintern geklärt werden, ob zum geplanten Zeitpunkt der Durchführung weitere Umfragen anstehen.

Wenn themengleiche Umfragen geplant sind, bietet es sich z. B. im Rahmen der Gefährdungsanalyse Geldwäscheprävention oder des operationalen Risikomanagements an, hier eine terminlich und gegebenenfalls inhaltlich abgestimmte Vorgehensweise zu praktizieren. Denn auch die beste Fragebogenaktion wird schwer vermittelbar und sorgt in den vom operativen Tagesgeschäft stark in Anspruch genommenen Abteilungen für Unmut, wenn innerhalb kurzer Zyklen identische Fragen von unterschiedlichen Stabs- oder anderen Einheiten gestellt werden.

Das Beispiel für einen ausführlichen Fragebogen befindet sich im Anhang als Anlage 4.

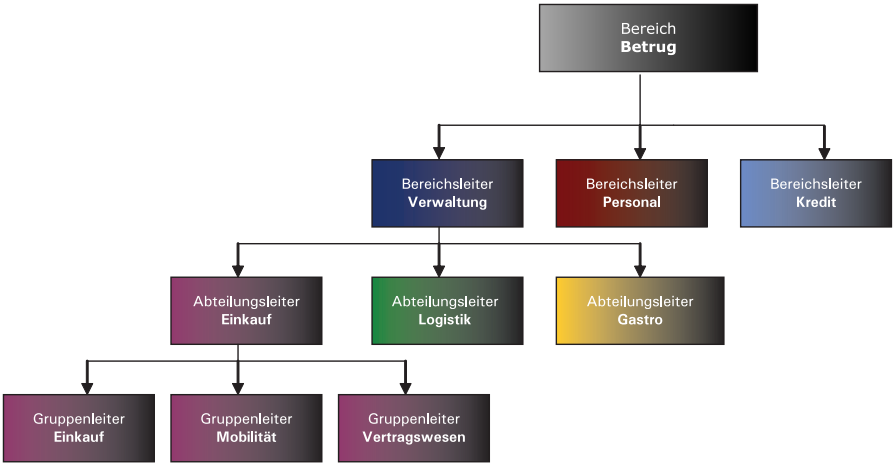
2.5.2.2 Durchführung der Fragebogenaktion

Hinsichtlich der „richtigen" Verteilung der Fragebogenaktion (Versandart und Adressaten) hat sich die E-Mail mit kurzem Anschreiben an alle Bereichsleiter des gesamten Instituts mit angehängtem Fragebogen bewährt. Die Vorgehensweise beinhaltet mehrere Vorteile: Von der Bedeutung der Thematik kommen als Adressaten nur die Bereichsleiter eines Instituts in Frage. Die verantwortliche Beantwortung der Fragen wird so an zweithöchster Stelle im Institut aufgehängt. Die E-Mail (immer mit „Eingangsbestätigung") erlaubt es der Führungskraft, Fragen unverzüglich an die Experten auf der nächstniedrigeren Hierarchieebene weiter zu delegieren. Der so organisierte E-Mail-Versand hat zudem den Vorzug, dass in Fällen, in denen ein befragter Bereich unterschiedlich gefährdete Abteilungen umfasst, die Fragebögen an die verantwortlichen Abteilungsleitern zur individuellen Beantwortung weitergegeben werden können.

Wenn eine Beantwortung durch den Abteilungsleiter auf Grund der Abteilungsgröße ebenfalls nicht möglich ist, erlaubt diese Form eine ebenso unkomplizierte Weitergabe an z. B. die Gruppenleiter der Organisationseinheiten. Diese könnten die Fragen auf Grund ihrer Detailkenntnisse aus dem Tagesgeschäft möglicherweise fokussierter beantworten. Das Her-

unterbrechen auf die Gruppenleiterebene dürfte in der Praxis aber eher die Ausnahme sein und nur für sehr große Häuser gelten. Die Anschreiben per E-Mail erleichtern zudem auch das spätere „Mahnverfahren", da erfahrungsgemäß nicht immer alle Fragebögen zum festgesetzten Termin zurückgesendet werden.

Die nachfolgende Abbildung stellt ein Beispiel für eine hierarchische Delegation der Fragebögen dar:



Quelle: Mitgliedsinstitute des VÖB

Abbildung 6: Hierarchische Delegation der Fragebögen

Sollte die sehr intensive und tiefgehende Befragung über betrügerische Handlungen erstmalig im Institut durchgeführt werden, sollten Auswahl und Struktur der Fragen gut vorbereitet werden. Zum einen besteht dadurch die Chance, durch die anschließende Auswertung eine Bestandsanalyse des Instituts mit einem hohen Differenzierungsgrad zu erhalten. Zum anderen kann durch eine geschickte Fragestellung auch eine Sensibilisierung in den Bereichen hinsichtlich des Themas „Betrugsprävention" erreicht werden. Die Beantwortung des Fragenkatalogs führt in jedem Fall zu einer intensiveren Auseinandersetzung mit dem Thema.

Die Fragestellung zur Selbsteinschätzung und Bestandsaufnahme sollte zu Beginn allgemeine Sachverhalte berühren und anschließend immer tiefer ins Detail gehen. Fragen zum „allgemeinen" Betrugspotenzial, wie z. B.

„Wie stark schätzen Sie die Gefahr ein, in Ihrem Bereich von betrügerischen Handlungen missbraucht zu werden?"

können hierbei einen ersten Eindruck verschaffen, ob sich die Beteiligten über die generelle Gefährdungssituation ihres Bereichs überhaupt bewusst sind.

2.5.2.3 Auswertung der Fragebögen (Erkenntnisse/ Maßnahmen)

Um eine für alle Bereiche des gesamten Instituts vergleichbare Auswertung der Antworten zu bekommen, wird jeder Frage eine entsprechende Risikopunkteanzahl zugeordnet (z. B. werden den Risikokategorien geringes/ mittleres/ hohes Risiko die entsprechenden Risikopunkte 1/2/3 vergeben). Eine maximale Anzahl von drei Risikopunkten gibt es bei der Auswertung einer Frage, wenn z. B. keine schriftlichen Regelungen zum Thema „Betrugsprävention" im Bereich existieren, keine Mitarbeiterunterrichtungen (z. B. Schulungen) durchgeführt oder die vorhandenen Präventionsmaßnahmen gegen betrügerische Handlungen als nicht ausreichend eingestuft wurden.

Die Gesamtaddition aller Risikopunkte der einzelnen Fragen ermöglicht die Eingruppierung der Bereiche in die unterschiedlichen Risikogruppen 1–3 (geringe, mittlere und hohe Gefahr). Zum besseren Verständnis sei auf die nachfolgende Abbildung verwiesen, die eine tabellarische Aufschlüsselung der Risikopunkte und -gruppen enthält.

Risiko-punkte	Risiko-gruppe	Beschreibung	Risiko-ampel
ab 20 Risikopunkte	3	**hohe Gefahr** von betrügerischen Handlungen missbraucht zu werden	rot
10 - 19 Risikopunkte	2	**mittlere Gefahr** von betrügerischen Handlungen missbraucht zu werden	gelb
0 - 9 Risikopunkte	1	**geringe Gefahr** von betrügerischen Handlungen missbraucht zu werden	grün

Quelle: Mitgliedsinstitute des VÖB

Abbildung 7: Risikopunkte im Verhältnis zu Risikogruppen (aus Fragebogenauswertung)

Zur besseren optischen Unterstützung der Darstellung kann eine farbliche „Risikoampel" verwendet werden, mit z. B. der Farbe „rot" für eine hohe und „grün" für eine geringe Gefährdung.

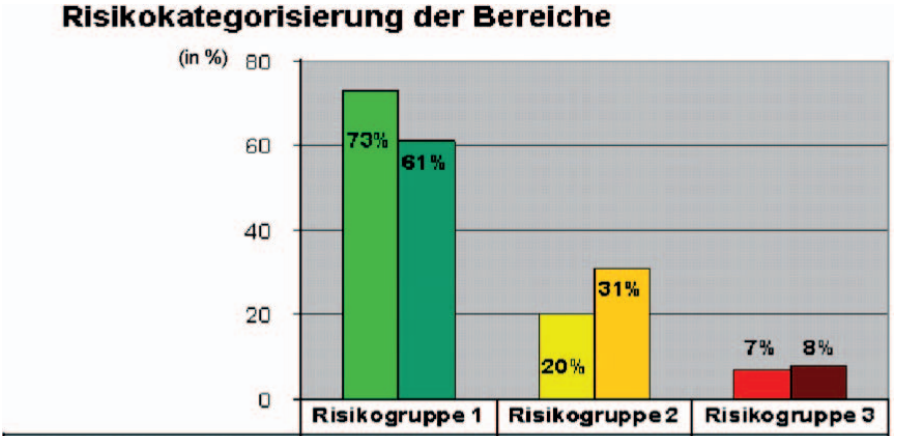
Eines der Ziele am Ende des Auswertungsprozesses ist die Objektivierung der Ergebnisse aus der Selbsteinschätzung. Dies erfolgt z. B. anhand einer Gegenüberstellung der Selbsteinschätzung mit der objektiven Betrachtung der folgenden - bereits aus Abschnitt 2.5.1 - bekannten Risikoarten:

- Kundenrisiken,
- Produktrisiken,
- Transaktionsrisiken,
- Vertriebswegerisiken und
- sonstigen Risiken (z. B. Länderrisiken etc.)

sowie den Ergebnissen aus

- der Experteneinschätzung und
- der Zuordnung zu bestehenden Informationen über bereits eingetretene Betrugsfälle (inklusive Schadensfalldatenbank).

Aus der Praxis einer in einem größeren Institut durchgeführten Fragebogenaktion wird Folgendes deutlich: Die Ergebnisse der jeweiligen Selbsteinschätzungen der befragten Bereiche bezüglich des Risikopotenzials, von betrügerischen Handlungen missbraucht zu werden, weichen in der höchsten Risikogruppe 3 nur geringfügig von der sachlichen (also objektiven) Gegenüberstellung ab. Dies zeigt, dass die Bereiche mit hohen Risiken sich ihrer entsprechenden Gefährdung im Allgemeinen sehr wohl bewusst sind. Auffallend sind dagegen die Abweichungen bezüglich der Risikogruppe 2 (mittlere Gefährdung): Hierbei wurde die Risikosituation von einer deutlich größeren Anzahl der Bereiche unterschätzt. Weniger überraschend war die Tatsache, dass sich keiner der Bereiche bezüglich einer Gefährdung „überschätzt" hat.



	Risikogruppe 1	Risikogruppe 2	Risikogruppe 3
nach Selbsteinschätzung	73%	20%	7%
nach Risikopunkten	61%	31%	8%

Quelle: Mitgliedsinstitute des VÖB

Abbildung 8: Selbsteinschätzung versus objektive Bewertung – Beispiel für eine Gegenüberstellung

3 Die Risikomatrix als ein Instrument der Gefährdungsanalyse und Überlegungen zum Maßnahmenkatalog

Zur Erhebung und Darstellung der Gefährdungslage des Instituts empfiehlt sich die Abbildung in einer Risikomatrix.[49] Hierbei werden die Risiken, das heißt die verschiedenen Betrugsmuster, den einzelnen Bereichen des Instituts gegenüber gestellt und bewertet. Im Abschnitt 2.5.2 wurde aufgezeigt, mit welchen Instrumenten und Herangehensweisen die Grundlagen zur Analyse der Risiken geschaffen werden. In den nachfolgenden Ausführungen wird beschrieben, wie diese gesammelten Informationen unter Würdigung der im Institut vorhandenen Maßnahmen verdichtet, bewertet und in der Risikomatrix als zentraler Bestandteil der Gefährdungsanalyse abgebildet werden.

3.1 Aufbau der Risikomatrix

In den Zeilen der Risikomatrix werden die Bereiche (Abteilungen/ Organisationseinheiten) des Instituts abgebildet. Dabei sollten neben den eigentlichen Abteilungen bzw. Organisationseinheiten auch alle Organe und Aufsichtsgremien aufgeführt werden. In den Spalten werden die Betrugstypologien, geordnet nach Risikokategorien, aufgeführt. Auf Grund der unterschiedlichen Typologien kann es sinnvoll sein, eine interne Risikomatrix, die die betrügerischen Handlungen durch Mitarbeiter und sonstige Interne abdeckt, und eine externe Risikomatrix für Handlungen durch Kunden und andere Externe zu erstellen.

3.1.1 Untergliederung nach Risikokategorien/ Betrugstypologien und Bereichen

Eine Herausforderung stellt erfahrungsgemäß die Festlegung der Systematik dar, nach der die Betrugstypologien erfasst, geordnet und dargestellt werden sollen. Eine Untergliederung nach Straftatbeständen ist hier

49 Die Darstellung der Risiken in Form einer Matrix ist für Institute jedoch nicht zwingend erforderlich.

nicht zweckmäßig und empfiehlt sich daher nicht. Zum einen ist die Strafbarkeit kein taugliches Unterscheidungskriterium, da die betrügerische Handlung i.S.d. KWG, wie bereits oben festgestellt[50], weit über strafrechtliche Tatbestände hinausgeht. Zum anderen sind die Straftatbestände für die hier verfolgten Zwecke zu allgemein gehalten, so dass von einem einzigen Straftatbestand die unterschiedlichsten Betrugsmuster abgedeckt werden. So wird etwa in vielen Fällen, in denen eine betrügerische Handlung gegeben ist, ein strafrechtlicher Betrug i.S.d. § 263 StGB vorliegen; die Begehungsformen können allerdings erheblich variieren. Das ist schon deshalb problematisch, als die zu ergreifenden Präventionsmaßnahmen und deren Wirksamkeit von der spezifischen Begehungsform der betrügerischen Handlung abhängen.

Vielfach kommen bei ein und derselben Betrugstypologie auch unterschiedliche Strafbarkeiten in Betracht, wobei die Abgrenzung mitunter schwierig und von vielen juristisch-dogmatischen Feinheiten abhängig sein kann. In derartigen Fällen ist die Zuordnung zu einem Straftatbestand nicht zweifelsfrei möglich; eine solche Kategorisierung wäre somit wenig hilfreich.

Empfehlenswert ist deshalb eine Unterteilung nach der spezifischen Tat unabhängig von der Strafbarkeit der Handlung, dies auch mit Blick auf jeweils speziell ableitbare, wirksame Präventionsmaßnahmen. Diesbezüglich wären im externen Bereich Lastschriftbetrug und Überweisungsbetrug trotz möglicherweise ähnlicher Strafbarkeit ebenso voneinander zu trennen wie Hacking, Phishing und Skimming. Im internen Bereich kommen beispielsweise die unterschiedlichsten Zugriffe durch Mitarbeiter in Betracht, die jedoch je nach betroffenem Bereich oder Vermögenswert streng differenziert werden sollten, da sie völlig unterschiedliche Präventionsmaßnahmen erfordern.

Eine umfassende Darstellung aller denkbaren Methoden betrügerischer Handlungen ist kaum möglich. Das Erfahrungswissen über Betrugsfälle aus der Vergangenheit ist aber in jedem Fall einer der wichtigsten Ansätze überhaupt. So sollten alle bekannten Betrugstypologien gesammelt und gemeinsam mit allen weiteren theoretisch denkbaren Betrugsszenarien in der Risikomatrix dargestellt werden. Wie sehr bei der endgültigen Untergliederung ins Detail gegangen wird, bleibt letztlich dem einzelnen Institut

50 Vgl. Abschnitt 2.3

selbst überlassen und hängt u. a. vom institutsspezifischen Gefährdungspotenzial jedes einzelnen Bereichs ab, aber auch von der gewünschten Detaillierung bzw. Übersichtlichkeit. Ein Ausschnitt einer „internen" und „externen" Risikomatrix ist in den Anlagen 5 a) und b) im Anhang abgebildet.

3.1.2 Erste Bewertung der Gefährdungslage

Zur Feststellung der Gefährdungslage des Instituts erfolgt zunächst ein Abgleich der Bereiche mit den einzelnen Betrugstypologien danach, ob der jeweilige Bereich grundsätzlich von der genannten Betrugstypologie betroffen sein kann. Für den internen Betrug bedeutet dies, dass ein Bereich nur dann gefährdet sein kann, wenn für die Mitarbeiter dieses Bereichs die theoretische Möglichkeit besteht, einen derartigen Betrug zu begehen. Im Anwendungsbereich des externen Betruges kann immer nur die Abteilung gefährdet sein, die mit der Betreuung des jeweiligen Tatobjekts oder Vermögenswerts bzw. dem betroffenen Vorgang betraut ist.

Nach der so vorgenommenen ersten Bewertung wird sichtbar, an welcher Stelle im Institut grundsätzlich welche Gefährdungen für betrügerische Handlungen vorliegen und welche generell ausgeschlossen werden können.

3.2 Maßnahmenkatalog

Die tatsächliche Gefährdungssituation des Instituts hängt u. a. stark von den implementierten Präventions- und Bekämpfungsmaßnahmen ab. Eine abschließende Bewertung der Gefährdungslage ist somit erst nach Bestandsaufnahme der im Institut bereits ergriffenen Maßnahmen möglich. Hilfreich ist hierbei, sich zunächst einen Überblick über alle potenziell möglichen Präventions- und Bekämpfungsmaßnahmen zu verschaffen, die man in einem Maßnahmenkatalog darstellt. Dabei ist zu empfehlen, alle bekannten Maßnahmen, gleich welcher Natur, unter Einbeziehung der Fachbereiche zu sammeln und geordnet darzustellen. Die Zuordnung zu bestimmten Oberbegriffen in Abhängigkeit von der jeweiligen Art der Maßnahme erleichtert die Übersicht. Die Sammlung ist dabei nicht als abschließend zu verstehen; auch nach intensiver Recherche wird es kaum möglich sein, alle potenziell möglichen Maßnahmen darzustellen. Darüber

hinaus hat die Entstehung neuer Betrugsmuster gezwungenermaßen auch die Entwicklung neuer Bekämpfungsmaßnahmen zur Folge, so dass die Auflistung im Bedarfsfall entsprechend ergänzt werden sollte.

Die Sammlung potenzieller Maßnahmen sollte in dem zu erstellenden Maßnahmenkatalog erfasst und danach mit den zuvor in der Risikomatrix festgelegten Betrugstypologien abgeglichen werden. Mit dieser Vorgehensweise kann ermittelt werden, welche Maßnahme gegen welche Typologie wirksam sein kann. Erst dann erfolgt auf Basis des so erstellten Maßnahmenkataloges die „Gap-Analyse“[51] hinsichtlich der im Institut implementierten Maßnahmen als weitere Grundlage für die Bestimmung der konkreten Gefährdungssituation des Instituts. Beispiele für einen „internen“ und „externen“ Maßnahmenkatalog sind als Anlagen 6 a) und b) im Anhang abgebildet.

3.3 Abschließende Bewertung der Gefährdungslage

Die institutsspezifische Gefährdungslage ergibt sich nach abschließender Bewertung der Restrisiken. Die abschließende Bewertung erfolgt unter Einbeziehung aller für die Risiken bedeutsamen Faktoren, zu denen auch die im Institut implementierten Maßnahmen gehören. Das bedeutet aber auch, dass mit Einführung jeder neuen Maßnahme das spezifische Risiko sinkt und die diesbezügliche Bewertung neu vorzunehmen ist.

Wie bereits im Abschnitt 2.2 ausgeführt, sollen gemäß Bankenaufsicht die Risiken nach erfolgter Erfassung, Identifizierung und Kategorisierung auch gewichtet werden. Dabei bietet es sich an, die im Abschnitt 2.5.1.2 vorgenommene Einteilung in mindestens drei Stufen (hoch/ mittel/ niedrig) zu verwenden. Eine feinere Abstufung ist möglich, aber nicht zwingend.

51 Mit der „Gap-Analyse“ oder auch Lückenanalyse sollen vorhandene Lücken, das heißt Abweichungen des Ist-Zustandes vom Soll-Zustand gefunden werden. Dies erfolgt durch Gegenüberstellung der potenziell möglichen wirksamen Maßnahmen und der bereits implementierten Maßnahmen.

3.4 Gruppenweite Überprüfung und Bewertung der Gefährdungslage

Im Zusammenhang mit der gruppenweiten Überprüfung und Bewertung der Gefährdungsanalyse ist insbesondere auf die im Rahmen des Gesetzes zur Fortentwicklung des Pfandbriefrechts vom 20. März 2009 erfolgte Neufassung der Vorschrift des § 25g KWG hinzuweisen[52]. Gemäß § 25g Abs. 1 KWG haben die in § 25c Abs. 1 KWG genannten Institute und Unternehmen

> *„…als übergeordnete Unternehmen in Bezug auf ihre nachgeordneten Unternehmen, Zweigstellen und Zweigniederlassungen gruppenweite interne Sicherungsmaßnahmen nach § 9 des Geldwäschegesetzes und § 25c Abs. 1 zu schaffen, die Einhaltung der Sorgfaltspflichten nach den §§ 3, 5 und 6 des Geldwäschegesetzes und den §§ 25d und 25f sowie der Aufzeichnungs- und Aufbewahrungspflicht nach § 8 des Geldwäschegesetzes sicherzustellen."*

Die Neuregelung hat zu einer erheblichen Verschärfung bei den Anforderungen zur gruppenweiten Einhaltung der im Zusammenhang mit der Geldwäsche-Bekämpfung stehenden Organisations- und Kundensorgfaltspflichten geführt, die zahlreiche und grundsätzliche Umsetzungsprobleme mit sich bringt. So hat nach Abs. 1 ein Institut als übergeordnetes Unternehmen - im Unterschied zur bisherigen Rechtslage - nunmehr zwingend sicherzustellen, dass seine

- internen Sicherungsmaßnahmen,
- Kundensorgfaltspflichten sowie
- Aufzeichnungs- und Aufbewahrungspflichten

nach den einschlägigen Vorschriften des GwG und KWG gruppenweit, das heißt in allen im In- und Ausland befindlichen nachgeordneten Unternehmen, Zweigstellen und Zweigniederlassungen, eingehalten werden.

Speziell zu den für die Kreditwirtschaft relevanten internen Maßnahmen nach § 25c Abs. 1 KWG gehören auch die Maßnahmen zur Verhinderung von betrügerischen Handlungen zu Lasten der Institute, die nach § 25g

52 § 25g KWG i.d.F. des Gesetzes vom 20. März 2009, BGBl. I, S. 607

KWG ebenfalls gruppenweit - mit der oben beschriebenen geografischen und organisatorischen Reichweite - umzusetzen sind. Hinsichtlich der Implementierung bedarf es zunächst der Analyse des Ist-Zustandes in den nachgeordneten Unternehmen, der Feststellung der bestehenden Risiken und der Festlegung von Maßnahmen zum Ausschluss bzw. zur Minimierung dieser Risiken. Das bedeutet, dass nachgeordnete Unternehmen, die Tochtergesellschaften und auch die „Enkeltöchter", eigene Gefährdungsanalysen zu erstellen haben bzw. eigenständig zu analysieren sind.

In einem weiteren Schritt werden die Gefährdungsanalysen der ausländischen Tochtergesellschaften dahingehend überprüft, ob sie den gesetzlichen und aufsichtsrechtlichen Bestimmungen ihrer Länder entsprechen. Das ist in der Praxis äußerst schwierig, da oftmals keine ausreichenden Kenntnisse des nationalen Rechts des anderen Landes in vorhanden sind. Die Kriterien für die Einschätzung von Gefahren in anderen Ländern können auf Grund vielfältiger rechtlicher oder kultureller Faktoren stark von den deutschen Einschätzungen abweichen. Es ist somit zu beachten, dass die von der ausländischen Tochtergesellschaft durchgeführte Gefährdungsanalyse auf Basis eines abweichenden Bewertungshintergrundes erfolgt. Hier sollte deshalb die eigene Bewertung der Risiken, insbesondere die eigene Länderrisikoeinschätzung des Instituts, als wichtiges Kriterium und objektivere Beurteilungsgrundlage verwendet werden.

4 Schlussfolgerungen für institutsinterne Präventions-, Bekämpfungs- und Sicherungsmaßnahmen

Betrug ist offensichtlich ein weit verbreitetes Phänomen mit einem hohen Dunkelfeld. Trotz eines (immer) verbleibenden Restrisikos existiert jedoch eine ganze Reihe von wirksamen Bekämpfungsmaßnahmen. Welche Maßnahmen im Einzelnen sinnvoll und notwendig sind, ist hinsichtlich Art und Umfang vom jeweiligen Risikopotenzial des Instituts abhängig. Ausgangspunkt einer zielgerichteten Prävention ist immer die strukturierte Erfassung des eigenen Risikos. Bei der Risikoidentifizierung, -erfassung und -bewertung ist daher im Hinblick auf die Wirksamkeit der auf dieser Basis zu formulierenden Maßnahmen besonders sorgfältig vorzugehen. Wie bereits erläutert, ist eine gründlich durchgeführte Gefährdungsanalyse die Grundvoraussetzung für den Erfolg der zu konzipierenden Präventionsmaßnahmen. In dieser Betrachtung sollten aber auch die in Abschnitt 2.1 angesprochenen fundamentalen Ursachen der Kriminalität berücksichtigt werden, um diese im Rahmen der institutsinternen Präventionsmaßnahmen angemessen zu adressieren.

4.1 Mögliche Handlungsempfehlungen/ Maßnahmen zum Ausschluss bzw. zur Minimierung festgestellter Risiken

In Instituten werden bereits verschiedenste Maßnahmen zur Minimierung bzw. zum Ausschluss von festgestellten Betrugsrisiken implementiert: Diese reichen i.d.R. von Mitarbeiterschulungen bis zu fest organisierten Arbeitskreisen, die entsprechende Handlungsempfehlungen für das gesamte Institut zur Verhinderung von betrügerischen Handlungen und Wirtschaftskriminalität formulieren können.

Als kontraproduktiv könnte sich dabei die Verteilung der Betrugspräventionsaufgaben auf unterschiedliche Organisationseinheiten innerhalb des Instituts auswirken. Bei einer entsprechenden Kommunikation untereinander lässt sich dieser Nachteil jedoch kompensieren. Wichtig ist in jedem Fall, dass der Gesamtvorstand bereit ist, die vorgeschlagenen institutionellen Maßnahmen zur Behebung der entsprechenden Schwachstellen/ Lücken im Institut zu unterstützen.

4.1.1 Aufbauorganisatorische Maßnahmen

4.1.1.1 Aufteilung der verschiedenen Verantwortungsbereiche

So vielfältig wie die Thematik der betrügerischen Handlungen und Wirtschaftskriminalität ist (siehe nachfolgende Abbildung), so unterschiedlich wird deren Bekämpfung sowohl fachlich als auch von der Zuordnung der verantwortlichen Personen in den Instituten gehandhabt.

Quelle: Mitgliedsinstitute des VÖB

Abbildung 9: Betrugsfelder der Wirtschaftskriminalität

In den wenigsten Instituten dürften die Verantwortungsbereiche für die Aufgabenfelder

- externer und interner Betrug,
- Geldwäscheprävention/ Finanzsanktionen/ Embargo,
- Wertpapier-Compliance,

- IT- bzw. Corporate Security
- usw.

in der Verantwortung einer einzigen Abteilung stehen.

Die Aufzählung weiterer Bereiche oder Abteilungen, welche zusätzlich direkt oder indirekt in die Thematik „betrügerische Handlungen" (möglicherweise mit Randgebieten) involviert sind, ließe sich wie folgt fortsetzen:

- Controlling (u. a. OpRisk mit Schadensfalldatenbank),
- Rechtsabteilung (u. a. Erstattung von Betrugsanzeigen, Insolvenzverschleppung),
- Schadens-/ Reklamationsabteilung (u. a. Benachrichtigung von Drittbanken),
- Personalabteilung (u. a. Aufstellung von Grundsätzen zur Geschenkannahme für Mitarbeiter und weitere disziplinarische und/oder arbeitsrechtliche Maßnahmen bei Verstößen etc.).

Über die Vorteile einer Ansiedlung der vorbezeichneten Betrugs- und Compliance-Themen in einem Bereich und die damit verbundenen Synergieeffekte für das Institut können derzeit keine abschließend verbindlichen Aussagen gemacht werden, da es hierfür keine Praxisbeispiele in Deutschland gibt. Die Entwicklung, die Aufgabengebiete Prävention bzw. Bekämpfung der Geldwäsche und betrügerischer Handlungen auf Grund der ähnlich gelagerten Thematik[53] zusammen in einer Einheit anzusiedeln, zeigt in der Tendenz, dass dies eine sinnvolle Ergänzung sein dürfte. In kleineren Instituten bietet es sich an, den Geldwäschebeauftragten und den für Betrugsprävention/ -bekämpfung Verantwortlichen in Personalunion abzubilden; dennoch sollten diese beiden Aufgaben stets aus zwei getrennten Blickwinkeln betrachtet werden. Ansonsten besteht die Gefahr, interne betrügerische Handlungen zu vernachlässigen. Zwar liegt einem Geldwäscheverdacht meist eine betrügerische Handlung aus dem Vorta-

53 Bei vielen Verdachtsfällen ist es am Anfang des Bearbeitungsprozesses oft unklar, ob zunächst in Richtung Geldwäscheverdacht oder Betrug ermittelt werden muss.

tenkatalog nach § 261 StGB zugrunde. Jedoch sind sämtliche Delikte, die aus dem Inneren eines Unternehmen entstehen, größtenteils nicht mit der Geldwäsche verknüpft.

In einigen Instituten ist bis heute die Bekämpfung des internen (Mitarbeiter-)Betruges traditionsgemäß bei der Internen Revision angesiedelt. Hingegen wird die Gefährdungsanalyse i.d.R. vom für Betrugsprävention/ -bekämpfung Verantwortlichen und/ oder Geldwäschebeauftragten federführend für das Institut erstellt. Für die praktische Umsetzung bedeutet dies jedoch nicht, dass der interne Betrug von der Gefährdungsanalyse deshalb ausgeklammert sein sollte; dies wäre nicht zielführend. Vielmehr ist darauf zu achten, dass auf diesem Gebiet eine enge Zusammenarbeit der beiden Einheiten stattfindet. Die spezifische Risikoanalyse zu betrügerischen Handlungen und Wirtschaftskriminalität sollte zentral vom Verantwortlichen für Betrugsprävention/-bekämpfung erstellt werden.

Es ist allerdings fraglich, ob die interne Betrugsbekämpfung durch die Interne Revision nach MaRisk Ziffer AT 4.4 Nr. 3[54] sowie angesichts neuerer Entwicklungen im Risikomanagement noch tragbar ist und daher institutsübergreifend zu überdenken wäre. Unter Compliance-Experten überwiegt die Einschätzung, dass die Vorgaben der BaFin die Zuständigkeit der Internen Revision für die Betrugsprävention/-bekämpfung explizit ausschließen. Die Interne Revision hat vielmehr zu kontrollieren, ob die Betrugsprävention/-bekämpfung im Institut ordnungsgemäß durchgeführt wird und interne Regelungen von allen Beteiligten eingehalten werden. Bestimmte Recherche- oder Ermittlungsaufgaben kann und sollte die Interne Revision in Abstimmung mit dem für Betrugsprävention/-bekämpfung Verantwortlichen und nach Anweisung des Vorstandes durchführen. Verantwortlich darf sie aber nicht sein; dies liegt vielmehr in der Zuständigkeit des für Betrugsprävention/-bekämpfung Verantwortlichen.

Vor diesem Hintergrund dürften in der deutschen Bankenlandschaft sehr heterogene organisatorische Konstellationen hinsichtlich der Betreuung des Themas betrügerische Handlungen und Wirtschaftskriminalität anzutreffen sein. Diese aufgeteilten Verantwortlichkeiten können in den Bereichen zu teils überlappenden Kompetenzen oder auch zu fehlenden Zuständigkeiten führen. Im Interesse der Effizienz und Herstellung von

54 BaFin, Rundschreiben 15/2009 (BA) vom 14. August 2009 - Mindestanforderungen an das Risikomanagement – MaRisk (GZ: BA 54-FR 2210-2008/0001) (im Folgenden: MaRisk).

Synergieeffekten erscheint eine Bündelung der Zuständigkeiten in einer Organisationseinheit optimal.

4.1.1.2 Gründung eines Betrugspräventionsgremiums[55]

Die Praxis zeigt, dass die Kommunikationsstrukturen/-prozesse besonders innerhalb der größeren Institute nicht immer optimal ausgestaltet sind. Dies trifft auch für die Betreuung der Betrugsthemen zu. Vor dem Hintergrund der im vorangegangenen Abschnitt erwähnten Problematik überlappender bzw. fehlender Zuständigkeiten erschweren komplizierte Kommunikationswege zudem eine bereichsübergreifend koordinierte und zeitnahe Bearbeitung konkreter Fälle, die erforderlich wäre, um eine effiziente und effektive Gefahrenabwehr sicherzustellen.

Spätestens bei der Erstellung einer Gefährdungsanalyse zu betrügerischen Handlungen sollte jedem Beteiligten bewusst werden, auf welche aufsichtsrechtlichen Grundlagen sich dieses Instrument bezieht: Im bereits erwähnten RS 8/2005 der BaFin werden angemessene Sicherungssysteme und Kontrollen zum Schutz des Instituts gefordert. Diese klare Aussage der BaFin weist darauf hin, dass es der Bankenaufsicht nicht in erster Linie darauf ankommt, wer im Institut für welche Aufgabengebiete verantwortlich ist. Vielmehr lässt sich die Vorgabe wie folgt interpretieren: Es sind alle Risiken, bei denen betrügerische Handlungen vorkommen, zu berücksichtigen und dies setzt unstreitig einen „Zwang zur Zusammenarbeit" zwischen den einzelnen Geschäftsbereichen bzw. Organisationseinheiten eines Instituts voraus.

55 Wie bereits im Abschnitt 2.3.3 ausgeführt, bietet die englische Bezeichnung „Fraud" nur eine Orientierungshilfe zum Thema „betrügerische Handlungen". Allerdings hat sich in der angelsächsischen Praxis und in einigen Instituten in Deutschland der Begriff „Fraud Prevention Board" als Bezeichnung für ein bereichsübergreifendes Gremium zur institutsinternen Prävention betrügerischer Handlungen und der Wirtschaftskriminalität durchgesetzt. Da die Verwendung der englischen Bezeichnung im deutschen Kontext nach Ansicht einiger Experten (besonders wegen des Namensbestandteils „Board") eher zur Verwirrung hinsichtlich der hierarchischen Einordnung im Institut führen könnte, soll stattdessen im Folgenden der neutralere Begriff „Betrugspräventionsgremium" verwendet werden. Der Vollständigkeit halber sei erwähnt, dass das Betrugspräventionsgremium alternativ auch als „Komitee", „Fraud Board", „Anti-Fraud Management Einheit" etc. bezeichnet werden könnte. Die Wahl der Bezeichnung bleibt dem Institut überlassen.

In der Praxis zeigt sich häufig, dass die Verpflichtung, zur Erstellung der Gefährdungsanalyse einen Beitrag leisten zu müssen, einen Lerneffekt bei den Vertretern der beteiligten Bereiche im Institut auslöst und letztere den „Mehrwert" des Informationsaustausches im Verlauf des Prozesses erkennen. Daher könnte der erste folgerichtige Schritt darin bestehen, ein befristetes Projekt (nur) zur Erstellung der Gefährdungsanalyse mit entsprechender (offizieller) Freistellung der Mitarbeiter durch den Vorstand zu initiieren. Sollte nach Projektabschluss der Fortbestand des Gremiums von allen Teilnehmern als wünschenswert und notwendig angesehen werden, könnte der Vorstand mit einer entsprechenden Vorlage um die Genehmigung zur dauerhaften Einrichtung eines sogenannten „Betrugspräventionsgremiums" ersucht werden.

4.1.1.3 Teilnehmer eines Betrugspräventionsgremiums

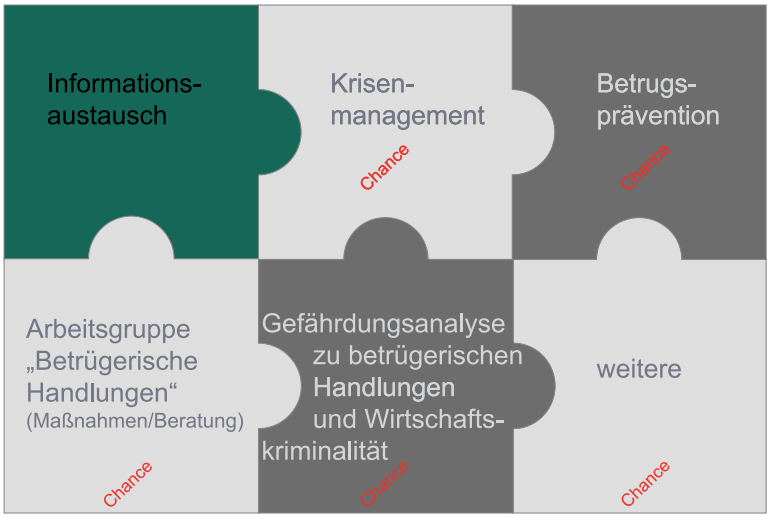
Zunächst wäre die Frage zu stellen, ob das Gremium nach angloamerikanischem Vorbild aus hochkarätigen Persönlichkeiten, das heißt aus Vorstandsmitgliedern und Bereichsleitern (ähnlich einem Risk Committee) besetzt werden sollte oder mit Fachleuten und Praktikern aus den nachgeordneten Hierarchieebenen. Letztere könnten die benötigte Zeit und das spezifische Fachwissen aus dem Tagesgeschäft einbringen. Die Frage, welche Konstellation effektiver sein dürfte, ist jedoch institutsindividuell zu beantworten.

Wichtig ist, dass einem Betrugspräventionsgremium gewisse Kompetenzen zugesprochen und gemeinschaftliche Beschlüsse nicht durch verschiedene Hierarchieebenen konterkariert werden (Stichwort: Handlungskompetenz). Insofern sollte dieses Kompetenzzentrum mit der Entscheidungsbefugnis ausgestattet sein, direkt an den Vorstand zu berichten, dies mit Kenntnis des jeweiligen Bereichsleiters. Ebenso wichtig ist, eine Unterscheidung zwischen regelmäßigen und unregelmäßigen Teilnehmern zu treffen. So sollten z. B. bei personalrechtlichen Maßnahmen i.w.S. neben Vertretern der Personalabteilung auch der Personalrat mit einbezogen werden.

4.1.1.4 Aufgaben des Betrugspräventionsgremiums

Zur wichtigsten Aufgabe des Betrugspräventionsgremiums zählt die gemeinsame Erstellung der gegenwärtigen und zukünftigen Gefährdungsanalysen nach § 25c KWG sowie die Überwachung der Umsetzung und Einhaltung empfohlener Präventionsmaßnahmen. Insoweit könnten die Aufgaben des Betrugspräventionsgremiums wie folgt beschrieben werden: Unterstützung von/ bei

1. Sammlung, Analyse sowie Bündelung bzw. Optimierung vorhandener Präventionsmaßnahmen,
2. Bewertung potenzieller Gefahren durch betrügerische Handlungen zu Lasten des Instituts,
3. Entwicklung von umfassenden und ganzheitlichen/ nachhaltigen Präventionskonzepten mit geeigneten Maßnahmen, Leitlinien und Prozeduren,
4. Festlegung der generellen Tragweite des Gesamtmaßnahmenpakets,
5. Umsetzung, Kommunikation, Koordination und Kontrolle einzelner Präventionsmaßnahmen innerhalb des Instituts und der Konzerneinheiten.



Quelle: Mitgliedsinstitute des VÖB

Abbildung 10: Betrugspräventionsgremium

4.1.1.5 Exkurs: Task Force als weitere Aufgabe des Betrugspräventionsgremiums

Da es in einigen Instituten bereits sogenannte „Task Force"-Einsatzgruppen[56] zur anlassbezogenen Untersuchung von Betrugsfällen gibt, läge die Vorstellung nahe, solche Aktivitäten unter Umständen als ein weiteres Aufgabengebiet an die Mitglieder des Betrugspräventionsgremiums zu delegieren.

Ob dies begleitend zur Bearbeitung eines Betrugsfalles oder beispielsweise im Rahmen der Einführung eines Hinweisgebersystems[57] geschieht, ist wiederum eine Frage, die nur institutsindividuell beantwortet werden kann. Die Varianten der Einsatzmöglichkeiten der hauseigenen Experten des Betrugspräventionsgremiums ließen sich entsprechend ausbauen. Auch hier gelten die entsprechend eingeräumten Kompetenzen als Schlüssel zum Erfolg.

4.1.2 Sonstige Maßnahmen

4.1.2.1 Unterrichtung/ Sensibilisierung der Mitarbeiter

Wie in der Geldwäschebekämpfung ist auch im Bereich der Betrugsbekämpfung eine regelmäßige Unterrichtung und Sensibilisierung der Mitarbeiter über aktuelle Betrugsformen (Typologien u. ä.) von herausragender Bedeutung. Hierbei kann sich - abhängig von der Größe und der Risikosituation des Instituts - eine Integration mit den Geldwäscheschulungen anbieten. Zu erwägen ist, bereits institutionalisierte Einrichtungen bzw. bewährte Kommunikationsinstrumente, die bislang „nur" für die Geldwäscheprävention verwendet wurden, im Rahmen der Mitarbeitersensibilisierung mit Betrugspräventionsthemen anzureichern.[58]

Eine ebenso wichtige Unterrichtungs- bzw. Sensibilisierungsmaßnahme ist die rasche Weitergabe aktueller Informationen, wie z. B. von Warnmel-

56 Zum Begriff „Task Force" siehe auch Abschnitt 4.3.2

57 Siehe hierzu auch Abschnitt 4.1.2.3

58 In Frage kämen beispielsweise sogenannte „GwG-Berater" als Multiplikatoren des Geldwäschebeauftragten in größeren Abteilungen bzw. Filialen eines Instituts sowie der Einsatz von Informationsmittel, wie regelmäßige „GwG-Berater-Rundmail" oder andere Informationen an einen solchen Teilnehmerkreis.

dungen der Verbände bzw. Ermittlungsbehörden. Schließlich sind sensibilisierte Mitarbeiter, die regelmäßig über die aktuelle Gefahrenlage informiert werden, ein unersetzlicher Schutz eines jeden Unternehmens vor betrügerischen Handlungen.

4.1.2.2 Weitere Maßnahmen

Neben dem bereits diskutierten Themenkomplex „Unterrichtung und Sensibilisierung der Mitarbeiter" können als weitere allgemeine Sicherungsmaßnahmen gegen betrügerische Handlungen in Instituten u. a. angeführt werden:[59]

- Informationssammlung,
- Kundenakzeptanzrichtlinie und Kundenannahmeprozess (KYC-Prinzip),
- Schufa-Anfragen,
- Legitimationsprüfung/ Identifizierung der Kunden im Rahmen des CDD-Prozesses gemäß GwBekErgG,
- Schriftlich fixierte Ordnungen und Geschäftsanweisungen (u. a. auch „Fraud"-Policies/ Ethik- und Verhaltenskodices),
- Prüfung künftiger Organe/ Mitarbeiter/ Beschäftigten vor Einstellung in das Unternehmen,
- Screening- und Researchmaßnahmen.

Da zum Täterkreis wirtschaftskrimineller Handlungen in Instituten erfahrungsgemäß sowohl externe Personen als auch Mitarbeiter der Institute selbst gehören (teilweise auch beide gemeinsam im kollusiven Handeln), sollten gerade bei der Mitarbeiterüberprüfung strenge Maßstäbe angelegt und entsprechende Maßnahmen durchgeführt werden.[60] Insbesondere sollte hinsichtlich neuer Mitarbeiter beachtet werden, dass diese bei einer

59 Eine ausführliche Besprechung der in Kreditinstituten zu ergreifenden allgemeinen Sicherungsmaßnahmen befindet sich im VÖB-Leitfaden 2008, S. 17 ff.

60 Siehe hierzu auch Abschnitt 2.3.6

Identitätsüberprüfung gültige Ausweisdokumente (u. a. Personalausweis[61]) sowie Zeugnisse im Original vorlegen. Ergänzend könnten als Maßnahmen erwogen werden:

- Vorlage von Beurteilungen/Referenzen im Original (mit möglichen Rückfragen bei ehemaligen Arbeitgebern),
- Vorlage eines polizeilichen Führungszeugnisses,
- gegebenenfalls Durchführung einer kleinen/ großen Sicherheitsüberprüfung,
- Abgleich mit eigener Warndatei,
- Überprüfung mit Zugriff auf öffentlich zugängliche Quellen (z. B. World check, Internet, Creditreform) hinsichtlich folgender Merkmale:
  - einschlägig bekanntes Mitglied der kriminellen Szene,
  - einschlägig bekanntes Mitglied der rechts- oder linksextremistischen Szene,
  - Unterstützer des Terrorismus,
  - hinlänglich bekannte Persönlichkeit (durch Presse oder andere Medien),
  - Familienangehöriger einer bekannten Persönlichkeit oder eines PEP[62].

Im Rahmen bestehender Beschäftigungsverhältnisse bietet sich darüber hinaus eine turnusmäßige Zuverlässigkeitsprüfung der Mitarbeiter als Teil des internen Beurteilungssystems wie folgt an:

- turnusmäßig im Rahmen der Leistungsgespräche,

61 Als Orientierungsmaßstab können hierbei die sehr detaillierten Ausführungen des Gesetzgebers zu Ausweisdokumenten, die in der Begründung zum Entwurf des § 4 Abs. 4 Satz 1 Nr. 1 GwG im Rahmen des GwBekErgG enthalten sind, dienen (siehe BR-Drs. 168/08, S. 78 ff.).

62 Siehe hierzu Abschnitt 2.5.1.1

- jährlich im Rahmen der Leistungseinschätzungen/ Bonuszahlungen,

- bei Versetzungen.

Ziel dieser internen Überprüfungsmaßnahmen ist, dass die Unternehmen ihre Mitarbeiter und die Arbeitsabläufe der Beschäftigten besser kennenlernen („Know Your Employee") und das in die Mitarbeiter gesetzte Vertrauen im Hinblick auf ihre Zuverlässigkeit besser beurteilen können.[63] Hierbei können - ergänzend - folgende Indikatoren mögliche Anhaltspunkte für die Unzuverlässigkeit eines Mitarbeiters liefern:

- krankhafte Spiel- oder Verschwendungssucht (z. B. häufiger Besuch von Spielcasinos oder Spielhallen),

- Alkohol-, Medikamenten- oder Drogenabhängigkeit (auffälliges Verhalten, Ausfallerscheinungen, versteckte volle oder leere Alkoholflaschen/ Medikamentenverpackungen am Arbeitsplatz etc.),

- aufwändiger Lebenswandel (Kraftfahrzeuge, Urlaub, Haus, Wohnung, Kleidung, Schmuck, etc.), welcher nicht mit den bekannten Vermögensverhältnissen (z. B. Gehalt oder bekanntes persönliches Vermögen) übereinstimmt,

- gravierende Verschlechterung der Arbeitsleistung ohne ersichtlichen Grund,

- auffällig viele (private) Gespräche über Mobiltelefon/ Institutstelefonapparat und private Internetnutzung am Arbeitsplatz,

- keine Inanspruchnahme des zustehenden Erholungsurlaubs durch den Mitarbeiter, um keine Abwesenheitszeiten entstehen zu lassen,

- häufige Aufenthalte des Mitarbeiters allein im Büro nach Arbeitsende/ Geschäftsschluss oder an Wochenenden.

Die vorstehend aufgeführten Maßnahmen sind nicht als eine abschließende Aufzählung zu verstehen und beliebig erweiterbar. Die Indikatoren geben jedoch eine Vorstellung davon, welch potenzieller Risikofaktor ein

63 Vgl. VÖB-Leitfaden 2008, S. 19 f.

durch vielschichtige negative Beweggründe (u. a. private finanzielle Engpässe, Gier, Illoyalität, berufliche Unzufriedenheit oder Vertriebsdruck) motivierter Mitarbeiter für das Unternehmen darstellen kann[64]. Die bisherige Erfahrung aus zahlreichen Fällen zeigt, dass wirtschaftskriminelle Handlungen der eigenen Mitarbeiter wirksam verhindert werden können, wenn die bestehenden unternehmensinternen Vorkehrungen um eine holistische Betrachtung des Schlüsselfaktors „Mensch" ergänzt und in die Arbeitsprozesse in Form der beispielhaft aufgezeigten weiteren Sicherungsmaßnahmen und Kontrollen integriert werden.[65] Dabei sind in jedem Fall die Persönlichkeitsrechte sowie die datenschutzrechtlichen Anforderungen zu beachten.[66]

4.1.2.3 Hinweisgebersystem

Während betrügerische Handlungen durch Kunden bereits im Fokus der Prävention stehen, ist die Abwehr interner betrügerischer Handlungen noch weitgehend ungeregelt. Erschwerend kommt hinzu, dass der Rechtsbegriff „betrügerische Handlungen" weit gefasst ist[67] und somit den Betrug als auch Verstöße gegen Compliance-Regelungen (z. B. Korruption und „kick back"-Vereinbarungen) oder Tatbestände wie z. B. Diebstahl und Erpressung umfasst. Eine wirkungsvolle Prävention dieser Verstöße würde jedoch einen laufenden Kontrollumfang bedeuten, der unverhältnismäßig hohe Kosten bewirkt. Begrenzt schützen kann sich ein Unternehmen aber auch durch klare Vorschriften und regelmäßige Prüfungen. Die zuletzt in der Presse bekannt gewordenen Fälle (u. a. Siemens, BaFin, Telekom, Bahn) haben die Virulenz der Problematik in größeren Unternehmen und Organisationen deutlich gemacht.

Der denkbar beste Schutz ist jedoch ein aufmerksamer Mitarbeiter, der sachdienliche Hinweise bezüglich unregelmäßig erscheinender oder betrügerischer Vorgänge gibt. Daher empfehlen standardsetzende internationale Gremien wie der Baseler Ausschuss für Bankenaufsicht und nationale Aufsichtsbehörden die Einführung eines so genannten Hinweisgebersys-

64 Vgl. Abschnitt 2.1
65 Vgl. auch Zawilla, Peter, Der Mensch als Risikofaktor, in: Ostwestfälische Wirtschaft 9/2007, S. 44 (im Folgenden: Zawilla 2007).
66 Vgl. Abschnitt 4.5
67 Siehe Abschnitt 2.3

tems (englisch: „Whistleblowing“[68]).[69] „Whistleblowing“, das im anglo-amerikanischen Recht durch das Sarbanes-Oxley Act (SOA oder SOX)[70] bereits eingeführt worden ist, soll die Aufdeckungswahrscheinlichkeit von Wirtschaftsdelikten in den Instituten erhöhen, indem Mitarbeitern bei absoluter Wahrung ihrer Anonymität die Möglichkeit gegeben wird, über die Weitergabe entsprechender Hinweise die Institute als Unternehmen vor Schaden zu bewahren. Die Beauftragung zur Annahme von Informationen kann in verschiedener Weise erfolgen. Dabei stehen grundsätzlich folgende Optionen zur Wahl:

- eine interne vertrauenswürdige Person,
- das Betrugspräventionsgremium[71],
- ein externer Anwalt (als Ombudsmann) oder
- eine externe Stelle, die sich auf die Sammlung[72] und vertrauliche Weitergabe dieser Informationen spezialisiert hat.

Angesichts der Vielzahl der zwischenzeitlich am Markt angebotenen Hinweisgebersysteme sollte ein Institut Vor- und Nachteile jeder Option kritisch abwägen und dasjenige auswählen, das für seine Bedürfnisse geeignet erscheint (siehe dazu auch die im Anhang als Anlage 7 abgebildete Matrix). Bei der Beurteilung und Auswahlentscheidung spielen Faktoren wie Größe des Instituts, Art und Weise der im Institut bestehenden Wertekultur, Kostengesichtspunkte u.v.m. eine Rolle.

68 Das Lexikon von Juraforum.de erläutert den Begriff wie folgt: *„Whistleblowing bezeichnet dem anglo-amerikanischen Begriff entsprechend die Weitergabe eines im Unternehmen begangenen Verstoßes an Stellen in- oder außerhalb des Unternehmens.“*; Internet: http://www.juraforum.de/lexikon/Whistleblowing (Stand: 12.02.2010)

69 Vgl. hierzu BCBS Methodik 2006, Grundsatz 18, Ziffer 9, Zentrale Kriterien und Financial Services Authority (FSA) des Vereinigten Königreichs, Full Handbook, SYSC 18, Guidance on Public Interest Disclosure Act: Whistleblowing; Internet: http://fsahandbook.info/FSA/html/handbook/SYSC/18/2 (Stand: 12.02.2010).

70 Sarbanes-Oxley Act of 2002, Public Law 107–204—July 30, 2002; Internet: http://www.sec.gov/about/laws/soa2002.pdf (Stand: 12.02.2010)

71 Siehe Abschnitt 4.1.1.2 ff.

72 Dies wird zumeist durch Einsatz unterschiedlicher Zugangskanäle (u. a. E-Mail, Telefon, Post etc.) sichergestellt.

Zusammenfassend ist zu sagen, dass für eine zielgerichtete Prävention bzw. Bekämpfung betrügerischer Handlungen und Wirtschaftskriminalität die strukturierte Erfassung des eigenen Risikos von großer Bedeutung ist. Besonders für größere bzw. komplex strukturierte Institute könnte die Einrichtung eines Hinweisgebersystems einen Weg zur Aufdeckung möglicher Risiken darstellen. Insofern ist den Instituten zu empfehlen, sich mit der Frage nach der Einrichtung eines effektiven, auf ihre individuelle Struktur und Bedürfnisse zugeschnittenen Hinweisgebersystems gründlich und vorurteilsfrei zu befassen und gegebenenfalls eine vorausschauende Lösung zu finden, dies insbesondere auch unter dem Blickwinkel möglicher bankaufsichtsrechtlicher Anforderungen zu internen Sicherungsmaßnahmen nach § 25c KWG in der Zukunft.

4.2 Berichterstattung/ Reporting (Organe und andere)

In der Praxis ist es üblich, dem Vorstand mindestens einmal im Jahr den vorgeschriebenen Geldwäschebericht vorzulegen.[73] Idealerweise bietet es sich in diesem Zusammenhang an, in dieser Vorlage auch einen separaten Bericht zu betrügerischen und wirtschaftskriminellen Handlungen sowie die vom Institut ergriffenen Abwehrmaßnahmen zu integrieren. Neben einem Überblick über das Betrugsgeschehen im Institut, kann dabei auch die Gefährdungsanalyse (gekürzt auf ein sogenanntes „Management Summary") als Vorstandsinformation eingereicht werden. Beim Auftreten erheblicher Schäden bzw. außergewöhnlicher Betrugsaktivitäten sollten die zuständigen Institutseinheiten/ -mitarbeiter mit einer Meldung an den Vorstand nicht bis zum Jahresultimo warten, sondern eine sofortige Unterrichtung, vornehmen, dies gegebenenfalls unter Einbeziehung der Internen Revision.

Zwar ist nachvollziehbar, dass verschiedene Bereiche ihre Vorstandsberichte, wie z. B. den OpRisk-, den Security- oder den geforderten Geldwäschebericht, separat an den Vorstand einreichen. Dennoch sollte das Betrugspräventionsgremium über die Inhalte dieser Einzelberichte rechtzeitig, das heißt vorher, informiert sein, so dass es zu keinen widersprüchlichen Aussagen in den jeweiligen Berichten kommen kann. Hierzu ein Negativbeispiel aus der Praxis:

73 Parallel dazu wäre auch eine Präsentation mit dem OpRisk-Bericht, der u. a. eine Analyse aufgetretener Schadensfälle beinhaltet, denkbar.

Die zuständige Schadensabteilung schreibt dem Vorstand in ihrem jährlichen Schadensbericht, dass der Überweisungsbetrug keine ernsthafte Gefahr mehr für das Institut darstellt, da die Schadensfälle auf den niedrigsten Stand seit der Erfassung zurückgegangen sind. Im Bericht des Betrugsbeauftragten wird der Überweisungsbetrug hingegen völlig anders interpretiert. Dank der Plausibilitätsprüfung zur Verhinderung von Überweisungsbetrug sind die Schadensfälle stark rückläufig; die Anzahl der Überweisungsbetrugsversuche ist jedoch stark angestiegen. Insofern ist das Gefahrenpotenzial weiterhin groß, dies erkennbar an der hohen Anzahl abgewehrter Fälle mit einem bestimmten Volumen am eingesparten Schadensbetrag für das Institut.

So können zu ein und demselben Betrugssachverhalt zwei völlig unterschiedliche Einschätzungen zum künftigen Risikopotenzial abgegeben werden. Die Gefahr besteht nun darin, dass bei einer schnelleren Vorlage des Berichts der Schadensabteilung an den Vorstand, dieser unter Umständen die (falsche) Entscheidung treffen könnte, bei der entsprechenden Prävention beträchtliche Einsparungen vorzunehmen, dies auf Grund des deutlich zurückgegangenen Schadensniveaus.

4.3 Notfall- und Krisenreaktionsplan in Schadensfällen

Im Rahmen der in den §§ 25a und 25c KWG geforderten Sicherungssysteme für ein angemessenes Risikomanagement ist die Einführung und das Vorhalten eines wirksamen Notfall- und Krisenreaktionsplanes ein wichtiger Baustein zur Vermeidung von unkontrollierten Handlungen im Falle einer betrügerischen Handlung. Die Planungen sollten auch (De-)Eskalationsstrategien im Sinne klarer Zuweisung von Verantwortlichkeiten umfassen. Es kann nicht immer davon ausgegangen werden, dass Frühwarnindikatoren („red flags“) eingeführt wurden. Wenn betrügerische Handlungen ein Institut treffen, dann sind sie vom Täter vorbereitet worden und treffen das Institut meistens unerwartet. Insoweit erfordern solche Vorfälle ein systematisches Handeln und eine checklistenartig konsequente Abarbeitung. Gelingt dies nicht, ist die Gefahr groß, dass mögliche Beweise verloren gehen und der oder die Täter ihren zeitlichen Vorsprung hinsichtlich Verschleierung und Flucht weiter ausbauen können. Darüber hinaus könnte durch ein falsches oder fehlendes Kommunikationsverhalten innerhalb des Instituts ein möglicher Vermögens- oder Reputationsschaden entstehen. Der Reputationsschaden ist dabei häufig die größte

Sorge eines Instituts. Hieraus können Markteinbußen (oder gar Ausschluss) mit der Folge reduzierten Wachstums, Vertrauensschwund, gerichtliche Auseinandersetzungen mit Kunden, Mitbewerbern etc. resultieren. In den meisten Fällen entsteht der größere Schaden durch eine zu späte und/oder falsche Reaktion und Bewältigung des Notfalls oder der Krise.

4.3.1 Notfall-/ Krisenreaktionsmanagement für betrügerische Handlungen

Als bestes Krisenmanagement ist dasjenige anzusehen, welches durch angemessenen Umgang mit einem sich anbahnenden Notfall[74] den Ausbruch einer wirklichen Krise verhindert. Oberstes Ziel eines Notfallplanes ist dabei die Aufrechterhaltung der Geschäftsprozesse sowie die Minimierung des Schadens und der Auswirkungen bzw. die Ergreifung von Maßnahmen zur wirksamen und vollständigen Eindämmung des Schadens. Das sich dahinter verbergende Notfallmanagement ist ein wachsender Prozess, der stets an die aktuellen Gegebenheiten und Umstände angepasst und erweitert werden muss.

Der Notfall- und Krisenreaktionsplan sollte klare organisatorische Strukturen aufweisen, um Erreichbarkeit und zügige Reaktionen sicherzustellen. Dazu gehören eindeutige personelle Zuständigkeitsregelungen, die damit verbundenen Kompetenzen und Verantwortlichkeiten, der Aufbau der internen und externen Kommunikationswege einschließlich der Sprachregelungen sowie die Festlegung von Sofort- und Mittelfristmaßnahmen. Der so entwickelte Notfall- und Krisenreaktionsplan für Betrugsfälle ist im Rahmen der schriftlich fixierten Ordnung beispielsweise als verbindliche Arbeitsanweisung zu dokumentieren.

74 aicooma IT CO Management, Whitepaper, BSI 100-4-Notfallmanagement: *„Von einem Notfall ist die Rede, wenn ein Prozess oder eine Ressource nicht planmäßig funktioniert, aber innerhalb des vorgesehenen Zeitrahmens wieder hergestellt werden kann. Der Geschäftsbetrieb ist in der Wiederherstellungszeit stark beeinträchtigt, die Service Level Agreements können nicht eingehalten werden. Es entsteht ein umfangreicher Schaden, der außerhalb des akzeptablen Bereiches liegt. Ein gesondertes Notfallbewältigungsteam kümmert sich um die Behebung und Wiederherstellung des Normalbetriebs."*

4.3.2 Organisatorische Elemente

Durch Überschneidungen und teilweise Verknüpfung der gemäß Geldwäschegesetz und Kreditwesengesetz einzurichtenden internen Sicherungsmaßnahmen und den damit wahrzunehmenden Sorgfaltspflichten auch bei betrügerischen Handlungen bietet es sich an, die Funktionen des für die Bekämpfung der Geldwäsche und Terrorismusfinanzierung Beauftragten und des für Betrugsprävention und -bekämpfung Verantwortlichen zusammen in einer Einheit anzusiedeln.[75]

Zur weiteren Unterstützung könnte ein internes Gremium in Gestalt eines „ad hoc-Ausschusses", „Krisenstabs" oder einer „Task Force" installiert werden, das sich mit dem Betrugsfall beschäftigt und die weitere Vorgehensweise beschließt. [76] Das Gremium könnte z. B. aus dem für Betrugsprävention/-bekämpfung Verantwortlichen (möglicherweise auch gleichzeitig Leiter dieses Gremiums) bzw. dem Geldwäschebeauftragten, den Leitern der Bereiche Interne Revision, Recht, Personal, Kommunikation/Marketing und/oder dem Pressesprecher bestehen. Je nach Schwere des Betrugsfalles können weitere Bereiche des Instituts hinzugezogen werden (gegebenenfalls Vorstand, Personalrat, Leiter der betroffenen Bereiche, Fachkraft für Arbeitssicherheit/Schutzbeauftragter, Datenschutzbeauftragter usw.). Bei Abwesenheit der Gremienmitglieder sind die jeweiligen Stellvertreter zu konsultieren. Entscheidend ist, dass eine Erreichbarkeit der ordentlichen Gremienmitglieder bzw. ihrer Stellvertreter immer gegeben ist, um eine schnelle und angemessene Reaktion des Instituts auf eingetretene Betrugsfälle (und möglicherweise dadurch verursachter Notfälle sowie Krisen) sicherzustellen. In der nachfolgenden Tabelle ist beispielhaft ein zeitliches Ablaufschema eines Aktionsplans mit den entsprechenden Aktivitäten im Krisenreaktionsfall dargestellt. Bewährt hat sich dabei das 1-1-1-1-Schema, welches die Maßnahmen in Schritte unterteilt, die nach Tag 1, der Woche 1, dem Monat 1 bzw. im Quartal 1 abgeschlossen sein sollten. Der genaue Zeitraum hängt natürlich von der konkreten Situation ab. Überschneidungen der Aktivitäten bezüglich der einzelnen Phasen sind in manchen Fällen zwangsläufig.

75 Siehe hierzu auch Abschnitt 4.1.1.1. In manchen Instituten sieht die Organisations- und Kommunikationsstruktur vor, dass der Geldwäschebeauftragte auch als erste Anlaufstelle für die Meldung von Fällen betrügerischer Handlungen fungiert.

76 Auch das im Abschnitt 4.1.1.2 ff. besprochene Betrugspräventionsgremium könnte mit der Betreuung dieser Aufgaben beauftragt werden.

Zeitliches Ablauf schema	Beispielhafte Darstellung von möglichen Sofort- und Kommunikationsmaßnahmen im Rahmen eines Aktionsplans
Tag 1	• Information des (Betrugspräventions-)Gremiums • Sicherung gefährdeter Vermögenswerte • Sicherung von Beweisen, Widerruf aller erteilten Vollmachten, Freistellung der verdächtigen Person • Sicherstellung der Aufgabenfortführung • Information des Vorstandes, ggf. des Aufsichtsrates durch den für Betrugsprävention/-bekämpfung Verantwortlichen
Woche 1	• Einleitung/ Beauftragung der Untersuchung • Identifikation möglicher Zeugen • Abwägung der geschäftlichen Konsequenzen • Festlegung arbeitsrechtlicher Strategien • Einleitung von Maßnahmen zur Schadensreduzierung • Information des Versicherers • Kommunikation nach innen, das heißt, Information der Mitarbeiter über das Vorgefallene und über getroffene Maßnahmen (beispielsweise über Intranet, Mitarbeiter-Zeitung, Mitarbeiter-Versammlung, Schreiben des Vorstandes) • Zügige, bedarfsorientierte Information nach außen (z. B. Journalisten) • Zuständigkeit liegt in den dafür verantwortlichen Bereichen
Monat 1	• Einleitung von Maßnahmen zur Vermögensrückgewinnung • Festlegung rechtlicher Konsequenzen • Bewertung steuerlicher bzw. bilanzieller Auswirkungen • Zuständigkeit liegt in den dafür zuständigen Bereichen
Quartal 1	• Ermittlung begünstigender Umstände (das heißt, Erhebung und Beseitigung von Schwachstellen im Kontrollumfeld bzw. in Geschäftsprozessen) • Identifikation der möglicherweise vorher vorhandenen Frühwarnindikatoren • Einleitung von Präventionsmaßnahmen • Überprüfung der Risikoeinschätzungen und der Maßnahmen in der vorhandenen Gefährdungsanalyse und ggf. Prozesse mit entsprechenden Anpassungen im Bedarfsfall • Zuständigkeit liegt in den dafür zuständigen Bereichen

4.3.3 Beispielhafte Notfall-/ Krisenreaktionsszenarien

Aus der institutsspezifischen Gefährdungsanalyse ergeben sich die Risikokategorien und -potenziale, die gegebenenfalls zu einem Notfall- oder gar zu einer Krise im Institut führen können. Auszugsweise sind in der nachfolgenden Tabelle einige Szenarien dargestellt, die möglicherweise über ein Krisenpotenzial verfügen. Dokumentiert ist auch, welche Sofortmaßnahmen zu ergreifen sind, um einen größeren Schaden abzuwehren. Bei den Sofortmaßnahmen ist zusätzlich hinterlegt, wer bzw. welcher Bereich die entsprechende Verantwortung und Zuständigkeit hat, diese Sofortmaßnahmen einzuleiten.

Risiko	Notfallreaktion	Vorbeugende Maßnahmen	Sofortmaßnahmen
Korruption	Sofortiges Handeln erforderlich, da ein sehr hohes Reputationsrisiko besteht und Korruptionsfälle außerdem häufig große Ausmaße annehmen und meist weitere Beteiligte haben.	➢ Führungsgrundsätze, Compliance-Richtlinien ➢ Begrenzung von Kompetenzen und Berechtigungen, Vier-Augen-Prinzip, Funktionstrennung, Rotationssysteme ➢ Nachvollziehbares Ausschreibungs- und Vergabeverfahren ➢ Sorgfältige Auswahl von Lieferanten ➢ Sorgfältige Überprüfung von Lieferantenrechnungen ➢ Hinweisgebersystem ➢ Beschwerdemanagement	➢ Widerruf von Vollmachten ➢ Entzug von Berechtigungen ➢ Beweissicherung ➢ Ggf. Zusammenarbeit mit Strafverfolgungsbehörden/ externen Ermittlern ➢ Ggf. Strafanzeige ➢ Arbeitsrechtliche Maßnahmen gegenüber Mitarbeiter/Vorstand (Abmahnung, Freistellung, Kündigung, Aufhebungsvertrag) ➢ Geltendmachung zivilrechtlicher Ansprüche gegen Mitarbeiter/ Vorstand (Regress) zwecks Vermögensrückführung (Asset Tracing)

Risiko	Notfallreaktion	Vorbeugende Maßnahmen	Sofortmaßnahmen
Erpressung	Sehr kritisch ist zum einen die Erpressung eines Mitarbeiters zur Herausgabe von bankinternen Daten und Informationen, Geschäfts- und Betriebsgeheimnissen. Kritisch ist zum anderen die Erpressung der Bank mit der Preisgabe derartiger Daten und Informationen.	➢ Gebäudesicherheitskonzept ➢ Begrenzung von Kompetenzen und Berechtigungen, Need-to-know-Prinzip ➢ Gesperrte Laufwerke ➢ Verschließen der Büroräume, Schränke, Schreibtische ➢ Clean Desk Policy ➢ Sorgfältige Auswahl von Lieferanten ➢ Hinweisgebersystem	➢ Widerruf von Vollmachten, Entzug von Berechtigungen ➢ Zusammenarbeit mit Strafverfolgungsbehörden ➢ Ggf. Strafanzeige
Insidergeschäft	Sehr hohes Reputationsrisiko.	➢ Compliance-Richtlinien, Ethikgrundsätze, Führungsgrundsätze, Mitarbeiter-Leitsätze ➢ Chinese Walls ➢ Sprachaufzeichnung ➢ Analyse von Mitarbeiter-Konten ➢ Begrenzung von Kompetenzen und Berechtigungen, Funktionstrennung, Rotationssysteme, Need-to-know-Prinzip ➢ Hinweisgebersystem	➢ Widerruf von Vollmachten, Entzug von Berechtigungen ➢ Beweissicherung ➢ Arbeitsrechtliche Maßnahmen gegenüber Mitarbeiter (Abmahnung, Freistellung, Kündigung, Aufhebungsvertrag) ➢ Ggf. Strafanzeige

Risiko	Notfallreaktion	Vorbeugende Maßnahmen	Sofortmaßnahmen
Datendiebstahl; Weitergabe von Daten bzw. Informationen	Je nach Qualität der Daten sehr kritisch. Neben einem Verstoß gegen Bankgeheimnis und andere Geheimhaltungsvorschriften ist es problematisch, sofern Wettbewerber in Besitz von bankinternen Daten und Informationen, Geschäfts- und Betriebsgeheimnissen kommen.	➢ Begrenzung von Kompetenzen und Berechtigungen, Need-to-know-Prinzip ➢ Gesperrte Laufwerke ➢ Verschließen der Büroräume, Schränke, Schreibtische ➢ Clean Desk Policy ➢ Hinweisgebersystem	➢ Widerruf von Vollmachten, Entzug von Berechtigungen ➢ Beweissicherung ➢ Sicherung gefährdeter Vermögenswerte ➢ Arbeitsrechtliche Maßnahmen gegenüber Mitarbeiter (Abmahnung, Freistellung, Kündigung, Aufhebungsvertrag) ➢ Ggf. Strafanzeige

4.3.4 Weitere vorbeugende Maßnahmen

Zu einem vorbereitenden Notfall-/ Krisenmanagement mit klar festgelegter Abfolge der Aktionen gehört auch ein permanentes Monitoring unternehmensrelevanter Krisenthemen in Medien, Öffentlichkeit, Wirtschaft und Politik sowie die Auswertung von Statistiken und Studien. Mit dem dadurch gewonnenen Wissen kann sich ein Institut auf bedrohliche Situationen vorbereiten und so die Entstehung von Notfällen/ Krisen bereits im Vorfeld abwenden. Für den zuständigen Betrugs-/ Geldwäschebereich geschieht dies durch ausführliche Informationssammlung bezüglich aller in der Vergangenheit vorgekommenen Betrugsfälle, dies sowohl im eigenen als auch in anderen Instituten, Ländern und Branchen. Um die zentrale Informationssammlung zu ermöglichen, sind von den einzelnen Bereichen die entsprechenden Informationen an den Betrugs-/ Geldwäschebereich zu liefern.

4.4 Überprüfung der empfohlenen/ ergriffenen Maßnahmen

Die nach Auswertung der Gefährdungsanalyse ergriffenen und empfohlenen Maßnahmen sind regelmäßig bzw. anlassbezogen auf ihren Sinn und ihre Wirksamkeit hin zu überprüfen. Im eigenen Interesse und zur Erfüllung seiner Aufgaben ist an erster Stelle der für Betrugsprävention/ -bekämpfung Verantwortliche für die regelmäßige Überprüfung der Einhaltung und Umsetzung der Maßnahmen zur institutsinternen Prävention und Bekämpfung betrügerischer Handlungen und der Wirtschaftskriminalität verantwortlich. Dabei helfen die Rückmeldungen aus den betreffenden Bereichen, ob die Maßnahmen praxiswirksam sind oder ob sie weiter ausgestaltet werden sollten. Zu empfehlen ist, dass die Interne Revision die Einhaltung der festgelegten Maßnahmen kontrolliert und den für Betrugsprävention/ -bekämpfung Verantwortlichen über eventuell festgestellte Mängel informiert.

Der für Betrugsprävention/ -bekämpfung Verantwortliche sollte zur Wahrnehmung seiner Aufgaben auf entsprechende EDV-Unterstützung zurückgreifen können. Das beinhaltet den vollständigen Zugriff auf alle Bankkonten, Kundenkonten, Mitarbeiterkonten und interne Konten. Zu beachten sind hierbei erforderliche Abstimmungen mit der Personalvertretung und dem Datenschutzbeauftragten.

Für die jeweiligen Führungskräfte in den Bereichen, Abteilungen und Teams sollte es ebenfalls selbstverständlich sein, die Einhaltung der Maßnahmen zur Betrugsprävention und -bekämpfung in ihren Verantwortungsbereichen ständig mit zu überprüfen. Insbesondere bei Zeichen von Unzuverlässigkeit von Mitarbeitern ist die Kontaktaufnahme zu dem für Betrugsprävention/ -bekämpfung Verantwortlichen zu empfehlen, um schnell, zielgerichtet und möglichst präventiv tätig werden zu können.[77]

Die Überprüfung der empfohlenen und ergriffenen Maßnahmen sollte anlassbezogen durchgeführt werden. Die bestehenden Sicherungsmaßnahmen stets sind besonders gründlich auf ihre Wirksamkeit hin zu überprüfen, wenn betrügerische Handlungen zu Lasten des Instituts oder weitergehende Angriffe (u. a. Sabotageakte) versucht, vollendet und/ oder festgestellt wurden. Bei der Erstellung und Aktualisierung der Gefährdungsanalyse sind ebenfalls alle Maßnahmen zu überprüfen.

4.5 Grenzen der Maßnahmen gegen betrügerische Handlungen

4.5.1 Allgemeines Persönlichkeitsrecht

Maßnahmen zur Betrugsbekämpfung müssen das allgemeine Persönlichkeitsrecht beachten. Dieses aus Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 Grundgesetz (GG) abzuleitende Grundrecht schützt die Ausstrahlungen der Persönlichkeit eines Menschen in allen Beziehungen und stellt bestimmte Teilbereiche der Persönlichkeitsentfaltung unter einen besonderen Schutz. Hierzu gehört auch das Recht auf informationelle Selbstbestimmung, das heißt das Recht des Einzelnen, selbst über Preisgabe und Verwendung seiner persönlichen Daten und Lebenssachverhalte zu bestimmen. Das Grundrecht soll den Einzelnen u. a. auch vor einer nicht gebotenen Überwachung und Ausforschung seiner Person bewahren.

Eine Verletzung des allgemeinen Persönlichkeitsrechts liegt aber nicht schon in jeder Kontrollmaßnahme, denn diese kann durch schutzwürdige Interessen des Arbeitgebers gerechtfertigt sein. Anhand der Umstände des Einzelfalls ist eine Güter- und Interessenabwägung zwischen den Belangen des Arbeitgebers und denjenigen des Arbeitnehmers vorzunehmen, wobei Richtschnur hinsichtlich „ob“ und „wie“ der Grundsatz der

77 Siehe hierzu auch Abschnitt 4.1.2.2

Verhältnismäßigkeit ist. Für die Praxis bedeutet dies, dass jeder Einzelfall unter Berücksichtigung aller Interessen zu betrachten und sodann nach entsprechender Abwägung zu bewerten ist. Eine allgemeingültige Aussage, welche Maßnahmen generell zulässig oder unzulässig sind, kann nur in Ausnahmefällen vorab getroffen werden. In Zweifelsfällen empfiehlt sich deshalb eine Abstimmung mit dem Datenschutzbeauftragten.

4.5.2 Mitbestimmung des Betriebs-/ Personalrats

Bei der Einführung von Kontrollmaßnahmen sind an einigen Stellen Mitbestimmungsrechte des Betriebs- bzw. Personalrats zu beachten. So hat dieser gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) bzw. § 75 Abs. 3 Nr. 17 Bundespersonalvertretungsgesetz (BPersVG)[78] ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer bzw. Beschäftigten zu überwachen (Beispiel: Videokamera-Überwachung).

Arbeitsrechtliche Maßnahmen nach Aufdeckung eines Mitarbeiterbetruges bedürfen ebenfalls der Mitbestimmung durch den Betriebs-/ Personalrat. Dies gilt gemäß § 99 BetrVG schon bei personellen Einzelmaßnahmen, wie z. B. Versetzung, außerdem nach § 102 Abs. 1 BetrVG bei jeder - auch fristlosen - Kündigung.

Datenschutzrelevante Sachverhalte, die das informationelle Selbstbestimmungsrecht von Mitarbeitern[79] berühren, können in Betriebs- bzw. Dienstvereinbarungen geregelt werden. Gleiches gilt für die genannten technischen Einrichtungen zur Verhaltensüberwachung.

4.5.3 Offenlegung von Kontrollen

Unabhängig von etwaigen Mitbestimmungsrechten des Betriebs- oder Personalrats empfiehlt es sich, Mitarbeiter über den Einsatz von Kontrollmaßnahmen aufzuklären. Denn den Arbeitgeber trifft eine Informationspflicht gegenüber seinen Arbeitnehmern, wenn er bestimmte Maßnah-

78 Oder nach den entsprechenden länderspezifischen Personalvertretungsgesetzen.
79 Vgl. Abschnitt 4.5.1

men ergreifen will. Dies gilt etwa für eine - ohnehin nur in engen Grenzen zulässige - Videoüberwachung hochsensibler Bereiche im Institut (z. B. Kassenraum). Dabei genügt es aber, die Mitarbeiter generell in Kenntnis zu setzen, dass bestimmte Kontrollen durchgeführt werden. Die auf diese Weise erhöhte (subjektive) Entdeckungswahrscheinlichkeit hat abschreckende Wirkung und bewirkt eine Senkung der Kriminalität im Institut.

4.5.4 Zulässigkeit von Research-Systemen

Wie bereits in Abschnitt 4.5.2 ausgeführt, besteht bei der Einführung und Anwendung von technischen Einrichtungen, die zur Überwachung von Verhalten (oder Leistung) der Arbeitnehmer bzw. Beschäftigten bestimmt sind, ein Mitbestimmungsrecht des Betriebs-/Personalrats. Sinn und Zweck des Mitbestimmungsrechts liegt darin, unverhältnismäßige oder sonst unbegründete Kontrollen der Arbeitnehmer zu verhindern und zu vermeiden, dass diese unter Missachtung ihrer Grundrechte von ihrem Arbeitgeber in unzulässiger Weise überwacht werden. Angemessene Kontrollmaßnahmen, die im Verhältnis zum angestrebten Zweck stehen, sind aber grundsätzlich zulässig.[80] Für den Betriebs-/Personalrat besteht daher kein genereller Grund, die Zustimmung zu derartigen Maßnahmen zu verweigern. Dies gilt umso mehr, als die datenschutzrechtliche Zulässigkeit von Datenverarbeitungssystemen zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und betrügerischen Handlungen nunmehr ausdrücklich in § 25c Abs. 2 Satz 3 KWG geregelt ist. Hiernach dürfen Institute personenbezogene Daten erheben, verarbeiten und nutzen, soweit dies zur Erfüllung der Pflichten aus § 25c Abs. 2 KWG erforderlich ist.

Üblich ist zudem, dass Daten vom Research-System zunächst anonymisiert und nur nach Erhärtung eines konkreten Verdachtsfalls kenntlich gemacht werden, welche Person hinter den Daten steht. Datenschutz ist Persönlichkeitsschutz, bezweckt also nicht den Schutz der Daten an sich, sondern der Person, die hinter den Daten steht und auf die sich diese beziehen. Letztlich liegt es in der Natur der Sache, dass Mitarbeiter, die mit der Verwaltung von Vermögenswerten von Kunden betraut sind, einer angemessenen Kontrolle unterliegen.

80 Vgl. Abschnitt 4.5.1

4.5.5 Kontrollen nicht um jeden Preis

Beim Einsatz von Kontrollmaßnahmen zur Überwachung von Mitarbeitern sollten Institute bedenken, dass derartige Maßnahmen sorgfältig begründet kommuniziert werden müssen. Anderenfalls könnte ein Klima des Misstrauens und der Distanz entstehen und auf diese Weise die Entwicklung krimineller Energien bei Institutsmitarbeitern gefördert werden. Ein angenehmes Betriebsklima und angemessene Entlohnung tragen dagegen zur Verhinderung von betrügerischen Handlungen und Wirtschaftskriminalität bei. Die Bindung der Mitarbeiter an das Unternehmen, etwa durch Übertragung von Verantwortung, aber auch durch gelebte Praxis ethischer Mindeststandards, fördert die Loyalität und ist die Basis jeder wirksamen Präventionsstrategie gegen internen Betrug. Denn wer sich mit dem Unternehmen identifizieren kann, der schädigt es nicht. Die Hemmschwelle ist hier regelmäßig höher.[81] Die Herausforderung besteht somit darin, im Unternehmen die richtige Balance zwischen Kontrolle und Vertrauen zu finden.

81 Zu einer Diskussion dieser Sachverhalte im Rahmen des ökonomischen Schadensmessungsansatzes siehe Abschnitt 5.7

5 Folgen einer unzureichenden Präventionsstrategie

5.1 Häufigkeit betrügerischer Handlungen und daraus resultierende Schäden[82]

Die Schäden, die in Deutschland jährlich durch Betrug oder artverwandte Delikte entstehen, sind beträchtlich. Konkrete Zahlenangaben sind jedoch sowohl hinsichtlich Deliktshäufigkeit als auch hinsichtlich Schadenshöhe sehr schwierig, denn Entdeckungswahrscheinlichkeit und Anzeigebereitschaft sind in diesem Kriminalitätsbereich aus mehreren Gründen vergleichsweise gering. Zum einen handelt es sich bei den einschlägigen Delikten oftmals um sogenannte opferlose Straftaten, das heißt es gibt keine individuell Geschädigten; die Opfereigenschaft verteilt sich vielmehr auf Staat, Steuerzahler, Verwaltung und Unternehmen. So bleiben die Delikte oft unerkannt und werden, wenn überhaupt, am ehesten durch Zufall aufgedeckt. Zum anderen hängt die Entdeckungswahrscheinlichkeit auch stark mit der Wirksamkeit bzw. dem Vorhandensein von Kontrollen zusammen. Ohne (wirksames) Kontrollsystem bleiben die meisten Delikte im Dunkeln.

Eine weitere Ursache für die Lückenhaftigkeit der vorhandenen Statistiken liegt darin, dass auch die Anzeigebereitschaft derjenigen, die einen Betrug bzw. betrügerische Handlungen überhaupt bemerkt haben, eher gering ist. Melde- oder Anzeigepflichten, wie die der Institute bei Verdachtsfällen der Geldwäsche oder der Terrorismusfinanzierung nach § 11 GwG, stellen die Ausnahme dar. Die Gründe für unterlassene Anzeigen hingegen sind vielfältig, jedoch fast immer reputationsbedingt. Der wirtschaftliche Schaden wird mit dem Nutzen einer Anzeige verglichen, was oft zu Gunsten der Reputationsschonung ausgeht. Tatsächlich besteht aus empirischer Sicht jedoch kein Grund, wegen befürchteter Reputationsschäden auf eine Strafanzeige zu verzichten. Studienergebnisse zeigen, dass Unternehmen nicht häufiger über Reputationsschäden berichteten, wenn sie eine Strafanzeige gestellt hatten. Vielmehr scheinen die Medien mehr denn je

82 Bzgl. der im folgenden Abschnitt aufgeführten Zahlen, Daten und Fakten vgl. im Einzelnen die folgenden Studien: *Euler Hermes*: Wirtschaftskriminalität – Das diskrete Risiko, Wirtschaft Konkret Nr. 300, 2003; *KPMG:* Studie 2006 zur Wirtschaftskriminalität in Deutschland; *PwC:* Wirtschaftskriminalität 2005 – Internationale und deutsche Ergebnisse; *PwC:* Wirtschaftskriminalität bei Banken und Versicherungen – Tatort Deutschland 2006; *PwC:* Wirtschaftskriminalität 2007 – Sicherheitslage der deutschen Wirtschaft.

eine Strafanzeige als Zeichen konsequenter Haltung geradezu zu erwarten.

Schätzungen zufolge stellen die bekannt gewordenen Fälle nur die Spitze des Eisbergs dar. Die Dunkelziffer - so wird vermutet - ist bei allen Arten von Wirtschaftskriminalität sehr hoch. Das ist schon deshalb problematisch, weil ein hohes Dunkelfeld ein geringeres Aufdeckungsrisiko garantiert und somit kriminalitätsfördernd wirkt.

Nationalen und internationalen Studien zufolge ist keine Branche vor betrügerischen Handlungen und Wirtschaftskriminalität gefeit, wobei die Finanzdienstleistungsbranche regelmäßig mit an der Spitze der betroffenen Wirtschaftszweige steht. Zu bewerten sind diese Ergebnisse allerdings auch vor dem Hintergrund der existierenden rechtlichen Regularien für die Finanzbranche und der deswegen bereits implementierten Präventions- und Entdeckungsmaßnahmen, so dass von einer höheren Entdeckungsquote auszugehen ist.

Neben den durch betrügerische Handlungen unmittelbar verursachten materiellen Schäden spielen immaterielle Schäden, die einen mittelbaren Vermögensschaden nach sich ziehen, eine gravierende Rolle. Reputationsverlust ist dabei nur eine von einer Vielzahl möglicher Schädigungen, die ein Unternehmen in der Folge erleiden kann. In der Regel führt ein Imageverlust auch zu einem Verlust von Kunden, die das Institut als nicht mehr vertrauenswürdig und somit als nicht mehr zuverlässig einstufen. Unter Umständen kann dies für das Geschäftsergebnis des Instituts spürbare Folgen haben. Das gilt umso mehr, wenn eigene Mitarbeiter des Instituts in die kriminellen Vorgänge verwickelt sind. Unternehmen machen weltweit die Erfahrung, dass fast die Hälfte der Wirtschaftsstraftäter aus dem eigenen Unternehmen stammt.[83] Zwar sieht diese Verteilung in der Finanzdienstleistungsbranche etwas anders aus, doch auch hier werden immerhin noch etwa ein Drittel der Taten durch eigene Mitarbeiter begangen. Erstaunlich ist, dass die Delikte sehr häufig von langjährigen, erfahrenen Mitarbeitern mit hohem Ansehen verübt werden, also gerade von denjenigen, die bereits ein gewachsenes Maß an Vertrauen genießen. Täter von Wirtschaftsdelikten in Deutschland sind wissenschaftlichen Erkenntnissen zufolge im Durchschnitt seit etwa zehn Jahren im Unterneh-

83 Zur nachfolgenden Analyse vgl. auch PwC / Martin-Luther-Universität Halle-Wittenberg, Global Economic Crime Survey 2007

men beschäftigt und seit etwa acht Jahren in der gleichen Position tätig. Legt man diese Erkenntnisse zugrunde, kann sich die Gewährung eines besonderen „Vertrauensbonus" für langjährige Mitarbeiter als folgenschwerer Irrtum erweisen.

5.2 Verletzung von gesellschaftsrechtlichen Pflichten

Nach den gesetzlichen Vorgaben haben Vorstände und ihre Geschäftsleiter bei der Führung ihrer Geschäfte die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden.[84] Zu diesen grundsätzlichen Pflichten zählt als originäre Leitungsaufgabe auch die Verhinderung von Wirtschaftskriminalität, das heißt die Implementierung entsprechender Präventionsmaßnahmen. Auch bei Delegation dieser Pflicht bleibt die grundsätzliche Verantwortlichkeit der Geschäftsleiter bestehen. Eine Exkulpation ist nur in Ausnahmefällen möglich.

Daneben ist der Vorstand einer Aktiengesellschaft nach § 91 Abs. 2 AktG dazu verpflichtet, ein Überwachungssystem einzurichten, um den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkennen zu können. Obwohl die Vorschrift sich vom Wortlaut her nur an Aktiengesellschaften richtet, ist sie auch für andere Rechtsformen von Bedeutung und besitzt entsprechende Ausstrahlungswirkung auf diese. Im Falle von Pflichtverletzungen sind die Geschäftsleiter der Gesellschaft gegenüber für den daraus entstandenen Schaden ersatzpflichtig.

5.3 Verletzung von Pflichten nach dem KWG

Die BaFin kann gemäß § 6 Abs. 3 KWG gegenüber den Instituten oder ihren Geschäftsleitern Anordnungen treffen, die geeignet und erforderlich sind, um Missstände in einem Institut zu beseitigen, die die Sicherheit der dem Institut anvertrauten Vermögenswerte gefährden können oder die ordnungsgemäße Durchführung der Bankgeschäfte beeinträchtigen. Dabei muss noch keine konkrete Gefährdung der Vermögenswerte eingetreten sein. Ausreichend ist bereits, dass eine Gefährdung der Vermögenswerte nicht ausgeschlossen werden kann.

84 § 93 Abs. 1 Aktiengesetz (AktG), § 43 Abs. 1 GmbH-Gesetz (GmbHG), § 34 Abs. 1 Genossenschaftsgesetz (GenG)

Sofern Pflichten nach dem KWG nicht eingehalten werden, kann dies gemäß § 35 Abs. 2 KWG unter Umständen zur Aufhebung der nach § 32 KWG erforderlichen Erlaubnis für die Zulassung zum Geschäftsbetrieb führen. Dies namentlich bei Unzuverlässigkeit oder fehlender fachlicher Eignung des Geschäftsleiters, aber auch wenn die erforderlichen organisatorischen Vorkehrungen zum ordnungsmäßigen Betreiben der Geschäfte fehlen oder bei sonstigen nachhaltigen Verstößen gegen Bestimmungen des KWG oder die zur Durchführung erlassenen Verordnungen oder Anordnungen. Anstelle der Aufhebung der Erlaubnis kommt gemäß § 36 KWG auch die Abberufung von Geschäftsleitern oder die Übertragung von deren Befugnissen auf Sonderbeauftragte in Betracht.

Für die in § 25a KWG verlangte ordnungsgemäße Geschäftsorganisation und die Einhaltung der hierzu erforderlichen Pflichten, wozu auch § 25c KWG gehört, sind gemäß § 25a Abs. 1 Satz 2 und § 1 Abs. 2 Satz 1 KWG die Geschäftsleiter verantwortlich. Verstöße gegen § 25c KWG können folglich mit erheblichen Konsequenzen für das Institut und auch für den Einzelnen verbunden sein, so dass die vollumfängliche Beachtung dieser Vorschrift durch sämtliche Mitglieder der Geschäftsleitung von ganz wesentlicher Bedeutung ist.

Bei Nichteinhaltung ihrer Pflichten aus § 25c KWG setzen sich die Institute der Gefahr aus, durch Sonderprüfungen gemäß § 44 KWG genauer unter die Lupe genommen zu werden. Derartige Prüfungen sind jederzeit - auch ohne besonderen Anlass - zulässig und werden von der BaFin insbesondere dann angeordnet, wenn die Jahresabschlussprüfung aus ihrer Sicht Unregelmäßigkeiten oder Mängel ergeben hat. Die durch die Sonderprüfung entstehenden Kosten trägt das Institut.

Die Bekämpfung betrügerischer Handlungen hat im Rahmen von Prüfungen lange Zeit keine große Bedeutung eingenommen. Sowohl Jahresabschluss- als auch Sonderprüfungen beschränkten sich bei der Überprüfung der Einhaltung der Pflichten aus dem ehemaligen § 25a Abs. 1 Satz 3 Nr. 6 KWG weitgehend auf die Geldwäscheproblematik. Hier ist inzwischen ein Umdenken zu beobachten. In der jüngeren Vergangenheit haben die Jahresabschlussprüfer das Augenmerk bereits verstärkt auf die Betrugsbekämpfung der Institute gerichtet. Sie entsprechen damit nicht nur den Vorgaben nationaler und internationaler Prüfungsstandards,[85]

85 Auf § 21 PrüfbV und auf die Ausführungen in Abschnitt 2.2 wird verwiesen.

sondern auch denen des KWG. § 29 Abs. 2 KWG sieht eine ausdrückliche Prüfpflicht des Jahresabschlussprüfers hinsichtlich der Frage vor, ob das Institut seinen Verpflichtungen aus § 25c KWG nachgekommen ist. Dies zeigt, dass die Betrugsprävention sich verstärkt zu einem eigenen Thema entwickelt und sich sukzessive von der Geldwäscheproblematik abkoppelt.

5.4 Ordnungswidrigkeiten, Geldbußen

Die Unterlassung erforderlicher Aufsichtsmaßnahmen durch Betriebs- oder Unternehmensinhaber kann als Ordnungswidrigkeit gemäß § 130 des Gesetzes über Ordnungswidrigkeiten (OWiG) mit einer Geldbuße bis zu einer Million Euro geahndet werden. Eine derartige Ordnungswidrigkeit liegt dann vor, wenn die Aufsichtspflichtverletzung eine mit Strafe oder Geldbuße bedrohte Verletzung von den Inhaber als solchen treffenden Pflichten zur Folge hat. Eintreten kann dies bei diversen internen betrügerischen Handlungen, wie beispielsweise einer Verletzung der Buchführungspflicht nach § 283b StGB oder der Steuerhinterziehung gemäß § 370 Abgabenordnung (AO) zu Gunsten des Instituts durch einen Mitarbeiter. Begehen Unternehmensverantwortliche (gesetzliche Vertreter, Generalbevollmächtigte etc.) eine Straftat oder Ordnungswidrigkeit, so kann gemäß § 30 OWiG unter bestimmten Umständen auch gegen das Unternehmen eine selbständige Geldbuße bis zu einer Million Euro festgesetzt werden.[86]

5.5 Vertrauensschadenversicherung

Für Institute besteht die Möglichkeit, Vermögensschäden, die ihnen durch betrügerische Handlungen der eigenen Mitarbeiter drohen, durch Vertrauensschadenversicherungen abzusichern. Wie bei anderen Versicherungen auch, können Schadensfälle - insbesondere, wenn sie gehäuft auftreten -

86 Verwiesen wird im Übrigen auf die Entscheidung des Bundesgerichtshofes (BGH) vom 17. Juli 2009 (Az.: 5 StR 394/08) zur Garantenstellung des Corporate Compliance Officers. In seiner Entscheidung hat der BGH einen Leiter der Rechtsabteilung und Innenrevision einer Anstalt des öffentlichen Rechts wegen Beihilfe zum Betrug durch Unterlassen zu einer Geldstrafe von 120 Tagessätzen verurteilt. Dieses Urteil hat auch wesentliche Bedeutung für das persönliche Haftungsrisiko von Compliance Officers; siehe hierzu auch NJW 2009, S. 3173.

immer zu einer Erhöhung der Versicherungsbeiträge führen. Soweit ein Institut seine Verpflichtungen aus § 25c KWG nicht (ausreichend) erfüllt, besteht außerdem die Möglichkeit, dass die Versicherung die Ersatzleistung im Schadensfall wegen grober Fahrlässigkeit auf Grund Nichteinhaltung gesetzlicher Vorgaben verweigert oder zumindest reduziert.

5.6 Eigenkapitalunterlegung

Die operationellen Risiken eines Instituts umfassen auch Wirtschaftskriminalitätsrisiken. Das operationelle Risiko ist mit Eigenkapital zu unterlegen. Höhere Schadensvolumina können zumindest im forgeschrittenen Bemessungsansatz unmittelbar zu höheren Eigenkapitalanforderungen führen.[87] Eine Vernachlässigung der im Rahmen der Gefährdungsanalyse und der laufenden Überwachung der Geschäftstätigkeit eines Instituts festgestellten Risiken aus Wirtschaftskriminalität kann zudem im Rahmen des bankaufsichtlichen Evaluierungsprozesses der Risikotragfähigkeit des Instituts zu einem Aufschlag bei der Eigenkapitalanfordeung führen.

Präventionsmaßnahmen zur Bekämpfung von Wirtschaftskriminalität sind also nicht nur erforderlich, um unmittelbar aus der Tat entstehende Vermögensschäden zu verhindern; sie tragen auch dazu bei, Eigenkapitalunterlegungen auf ein erforderliches Minimum zu reduzieren. Insbesondere größeren bzw. komplex strukturierten Instituten ist zu empfehlen, sich kritisch mit der Thematik zu befassen und die aus einer unzureichenden Präventions- bzw. Bekämpfungsstrategie gegenüber betrügerischen und/oder wirtschaftskriminellen Handlungen resultierenden Schäden auch verstärkt unter dem Blickwinkel (möglicherweise ansteigender) operationeller Risiken zu betrachten. Hierzu ist eine enge Kupplung der für die Betrugsprävention beauftragten Einheiten mit dem Risikomanagement/-controlling für das operationelle Risiko zu suchen.

87 Ramke, T.: Wirtschaftskriminalität als operationelles Risiko: Herausforderung für die Praxis, BankPraktiker 2007, 136, 139.

5.7 Ökonomischer Schadensmessungsansatz

In den vergangenen Jahren sind insbesondere in der anglo-amerikanischen Praxis unter der Bezeichnung „Anti-Fraud Economics Approach“[88] prozessorientierte Ansätze zur Messung potenzieller Schäden durch betrügerische Handlungen und Wirtschaftskriminalität, mit denen ein Unternehmen bei einer unzureichenden Präventions- bzw. Bekämpfungsstrategie zu rechnen hätte, entwickelt worden.[89] Ausgehend von dem Postulat *„was nicht messbar sei, könne auch nicht überwacht werden“* zielt der Ansatz darauf ab,

- eine Grundlage zur Messung der Wirksamkeit von sogenannten „soft controls“[90] sowie des gegenwärtig herrschenden Niveaus der betrügerischen Handlungen und Wirtschaftskriminalität in einem Unternehmen zu erstellen,

- diesbezügliche Daten- und Prozessanalysen zwecks Identifizierung und Implementierung von Prozessverbesserungen durchzuführen,

- Messungen hinsichtlich aufgedeckter bzw. verhinderter Fälle betrügerischer und/ oder wirtschaftskrimineller Handlungen durchzuführen und an die zuständigen Unternehmenseinheiten zu berichten und

- ein „Benchmarking“ zu betreiben mit der Maßgabe, das System stetig zu verbessern.

In diesem Zusammenhang ist für Institute das im Untersuchungsansatz vorgesehene Instrument des „Fraud Loss Measurement“ zur Messung aufgedeckter bzw. verhinderter Fälle betrügerischer und/ oder wirt-

88 Zum Begriff „Fraud“ siehe Abschnitt 2.3.3

89 Der Untersuchungsansatz wird aus Gründen der Vereinfachung im Folgenden als „Ansatz“ bezeichnet.

90 Dazu gehören wertebezogene Faktoren wie z. B. Unternehmensführung („Governance“), Ehrlichkeit, Integrität, Fairness, Kompetenz- und Qualitätsfokussierung, ethisches Geschäftsgebaren, Transparenz (besonders hinsichtlich der unternehmensinternen Abläufe und Reporting), Arbeitsauftrag und -moral, Kooperations- und Hilfsbereitschaft, etc. Siehe hierzu auch Mitchell, Mark B., Understanding and Evaluating Soft Controls, Präsentation anlässlich der Internal Control Conference 2006 der New York State Internal Control Association; Internet: www.nysica.com/conference/soft-controls-(mitchell).ppt (Stand: 12.02.2010).

schaftskrimineller Handlungen von besonderem Interesse.[91] Es erlaubt den Unternehmen, den realen finanziellen Nutzen aus den Anti-Betrugsmaßnahmen eines Unternehmens zu quantifizieren. Durch die quantifizierte Darstellung der Schäden sollen entsprechende Anreize zur Mobilisierung der redlichen Mehrheit der in einem Unternehmen beschäftigten Mitarbeiter geschaffen werden, dies im Hinblick auf

- eine nachhaltige Unterstützung der unternehmens-individuellen Präventions- und Bekämpfungsstrategie und

- die Erzielung weitergehender wirtschaftlicher Nutzeneffekte für das Unternehmen.

Hervorzuheben ist, dass zwischen 1998 und 2006 im Vereinigten Königreich elf Untersuchungen vom National Health Service (NHS), dem nationalen Gesundheitsdienst, über das NHS-Gesamtbudget mit Hilfe dieses Instruments fortlaufend durchgeführt wurden. Hinsichtlich der aus Fällen betrügerischer Handlungen resultierenden Schäden wurde festgestellt, dass im Berichtszeitraum das Schadensniveau um 60 % der Ausgaben reduziert werden konnte und dies der NHS Einsparungen in Höhe von 811 Millionen Britische Pfund einbrachte.[92] Weitere 57 Untersuchungen in neun Staaten[93] ergaben, dass 50 % der Schäden sich in Höhe von 3-8 % der Ausgaben bewegten, wobei dieser Wert nach Einführung entsprechender Sicherungsmaßnahmen in einigen der untersuchten Staaten sukzessive auf 1-3 % verringert werden konnte. Insofern spricht einiges dafür, dass sich Institute im Rahmen ihrer Strategien zur Prävention und Bekämpfung von betrügerischen und wirtschaftschaftskriminellen Handlungen neben den Überlegungen zu operationellen Risiken auch kritisch mit den ökonomischen Schadensmessungsansätzen befassen sollten. Ziel sollte sein, die aus betrügerischen und wirtschaftskriminellen Handlungen resultierenden ökonomischen Schäden für das Unternehmen zunächst transparent darzustellen und sodann durch die Einführung erwähnter

91 Angewandt wurde der Ansatz erstmals im Vereinigten Königreich im Rahmen einer breit angelegten Untersuchung der Betrugsschäden im Gesundheitssektor. Siehe hierzu auch: World Health Organization, Mobilizing the honest majority to fight health-sector fraud, in: Bull World Health Organ 2009;87:254–255; Internet: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2672570/ (Stand: 12.02.2010) (im Folgenden: WHO 2009).

92 Vgl. WHO 2009, S. 254.

93 Darunter in Frankreich, Neuseeland, Niederlande und USA.

(weicher) Kontrollfaktoren wirksam und dauerhaft zu begrenzen. Hierdurch kann ein nachhaltiger Beitrag zur Stärkung der Unternehmensintegrität und -reputation geleistet werden.

6 Ausblick

Auf Grund der durch das GwBekErgG neu geschaffenen Rechtsgrundlage ist davon auszugehen, dass die BaFin ihren aufsichtlichen Fokus auf die Prävention und Bekämpfung von betrügerischen Handlungen und Wirtschaftskriminalität verstärken und ihre Anforderungen, wie bereits avisiert, im Rahmen eines neuen Rundschreibens weiter konkretisieren wird. Diese Anforderungen werden im Zusammenspiel mit den Vorgaben der novellierten Prüfungsberichtsverordnung Konsequenzen auf die Prüfungstätigkeit der Abschlussprüfer haben. Die Prüfer werden spätestens im Rahmen der Prüfung des Jahresabschlusses eine Beurteilung der Angemessenheit der Sicherungssysteme zur Umsetzung der Vorgaben des § 25c Abs. 1 KWG vornehmen und dabei die Qualität der diesbezüglich erstellten institutsspezifischen Gefährdungsanalyse, der daraus abgeleiteten Sicherungsmaßnahmen und die Abbildung der spezifischen Betrugsrisiken im Risikomanagement prüfen. Somit gehören Betrugsprävention und -bekämpfung zum Katalog der Risikomanagementaufgaben der Compliance-Funktion.

Der vorliegende Leitfaden setzt genau an dieser Stelle an und bietet den mit der Prävention und Bekämpfung betrügerischer Handlungen und der Wirtschaftskriminalität befassten Mitarbeitern in den Instituten eine praxisbezogene Einführung sowie eine theoretisch fundierte aktuelle Orientierungs- und Arbeitshilfe in die Thematik. Der Leitfaden erhebt weder einen Anspruch auf Vollständigkeit noch enthält er verpflichtende „Benchmarks" zur Umsetzung der diskutierten Lösungsvorschläge und Maßnahmen.

Angesichts der wachsenden Gefahr für Institute, zu betrügerischen und wirtschaftskriminellen Zwecken missbraucht zu werden, sowie der zu erwartenden regulatorischen Anforderungen ist es auch ein besonderes Anliegen des Leitfadens, einen Beitrag zur Sensibilisierung in den Instituten für einen angemessenen Umgang mit dieser komplexen Thematik zu leisten. Schließlich gilt es, Folgendes zu beachten: Die Prävention und Bekämpfung betrügerischer und wirtschaftskrimineller Handlungen in den Instituten kann nur dann effektiv sein, wenn die unternehmensinternen ethischen Werte konsequent (vor-)gelebt und die Kontroll-, Präventions- und Bekämpfungsmaßnahmen risikobasiert, systematisch und ganzheitlich konzipiert, umgesetzt und in angemessenen zeitlichen Abständen überprüft/ aktualisiert werden.

Anhang

Anlage 1: § 25c KWG; Auszug aus GwBekErgG vom 13. August 2008, BGBl. I S. 1690

§ 25c

Interne Sicherungsmaßnahmen

(1) Institute haben unbeschadet der in § 25a Abs. 1 dieses Gesetzes und der in § 9 Abs. 1 und 2 des Geldwäschegesetzes aufgeführten Pflichten im Rahmen ihrer ordnungsgemäßen Geschäftsorganisation und des angemessenen Risikomanagements zur Verhinderung von betrügerischen Handlungen zu ihren Lasten interne Grundsätze und angemessene geschäfts- und kundenbezogene Sicherungssysteme zu schaffen und zu aktualisieren und Kontrollen durchzuführen.

(2) Kreditinstitute haben angemessene Datenverarbeitungssysteme zu betreiben und zu aktualisieren, mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr zu erkennen, die auf Grund des öffentlich und im Kreditinstitut verfügbaren Erfahrungswissens über die Methoden der Geldwäsche, der Terrorismusfinanzierung und betrügerischer Handlungen zum Nachteil von Instituten als zweifelhaft oder ungewöhnlich anzusehen sind. Liegen solche Sachverhalte vor, ist diesen vor dem Hintergrund der laufenden Geschäftsbeziehung und einzelner Transaktionen nachzugehen, um das Risiko der jeweiligen Geschäftsbeziehungen und Transaktionen überwachen, einschätzen und gegebenenfalls das Vorliegen eines Verdachtsfalls prüfen zu können. Die Kreditinstitute dürfen personenbezogene Daten erheben, verarbeiten und nutzen, soweit dies zur Erfüllung dieser Pflicht erforderlich ist. Die Bundesanstalt kann Kriterien bestimmen, bei deren Vorliegen Kreditinstitute vom Einsatz von Systemen nach Satz 1 absehen können.

Anlage 2: §§ 20, 21 PrüfbV; Auszüge aus PrüfbV vom 23. November 2009, BGBl. I S. 3793

Unterabschnitt 6
Vorkehrungen zur Verhinderung
von Geldwäsche und Terrorismusfinanzierung
sowie von betrügerischen Handlungen zu Lasten des Instituts

§ 20

Zeitpunkt der
Prüfung und Berichtszeitraum

(1) Die Prüfung findet einmal jährlich statt. Der Prüfer legt den Beginn der Prüfung und den Berichtszeitraum vorbehaltlich der nachfolgenden Bestimmungen nach pflichtgemäßem Ermessen fest.

(2) Der Berichtszeitraum der Prüfung ist jeweils der Zeitraum zwischen dem Stichtag der letzten Prüfung und dem Stichtag der folgenden Prüfung.

(3) Die Prüfung muss spätestens 15 Monate nach dem Anfang des für sie maßgeblichen Berichtszeitraums begonnen worden sein.

(4) Die Einhaltung der Vorschriften des Geldwäschegesetzes sowie der §§ 25c bis 25h des Kreditwesengesetzes ist bei Kreditinstituten, deren Bilanzsumme 400 Millionen Euro zum Bilanzstichtag nicht überschreitet, nur in zweijährigem Turnus, beginnend mit dem ersten vollen Geschäftsjahr der Erbringung von Bankgeschäften oder Finanzdienstleistungen, zu prüfen, es sei denn, die Risikolage des Instituts erfordert ein kürzeres Prüfintervall. Gleiches gilt für Wertpapierhandelsunternehmen, die nicht befugt sind, sich Besitz oder Eigentum an Geldern oder Wertpapieren von Kunden zu verschaffen, und die nicht auf eigene Rechnung mit Finanzinstrumenten handeln.

§ 21

Darstellung und Beurteilung
der getroffenen Vorkehrungen
zur Verhinderung von Geldwäsche
und Terrorismusfinanzierung sowie von
betrügerischen Handlungen zu Lasten des Instituts

(1) Der Prüfer hat zu beurteilen, ob die von dem Institut erstellte Gefährdungsanalyse der tatsächlichen Risikosituation des Instituts entspricht. Darüber hinaus hat er die vom Institut getroffenen internen Sicherungsmaßnahmen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung sowie von betrügerischen Handlungen zu Lasten des Instituts darzustellen und deren Angemessenheit zu beurteilen. Dabei ist einzugehen

1. auf die vom Institut entwickelten und aktualisierten internen Grundsätze, die Angemessenheit geschäfts- und kundenbezogener Sicherungssysteme und Kontrollen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung sowie von betrügerischen Handlungen zu Lasten des Instituts,

2. auf die Stellung und Tätigkeit des Geldwäschebeauftragten und seines Stellvertreters einschließlich ihrer Kompetenzen sowie die für eine ordnungsgemäße Durchführung der Aufgaben notwendigen Mittel und Verfahren; für Institute, die selbst nicht Tochterunternehmen im Sinne des Kreditwesengesetzes eines Instituts oder eines nach dem Geldwäschegesetz verpflichteten Versicherungsunternehmens sind, gilt dies auch in Bezug auf ihre Tochterunternehmen sowie ihre ausländischen Zweigstellen und Zweigniederlassungen sowie darauf,

3. ob die mit der Durchführung von Transaktionen und mit der Anbahnung und Begründung von Geschäftsbeziehungen befassten Beschäftigten angemessen über die Methoden der Geldwäsche und Terrorismusfinanzierung sowie von betrügerischen Handlungen zu Lasten des Instituts und die insofern bestehenden Pflichten unterrichtet werden.

Die Prüfung nach den Sätzen 2 und 3 hat unter Berücksichtigung der von dem Institut erstellten Gefährdungsanalyse sowie der von der Innenrevision im Berichtszeitraum durchgeführten Prüfung und deren Ergebnis zu erfolgen.

(2) Des Weiteren hat der Prüfer darzustellen und zu beurteilen, inwieweit das Institut den kundenbezogenen Sorgfaltspflichten, insbesondere auch den verstärkten Sorgfaltspflichten in Fällen eines erhöhten Risikos, nachgekommen ist.

(3) Zu berichten ist ferner über die Erfüllung der Aufzeichnungs- und Aufbewahrungspflichten sowie die Pflicht zur institutsinternen Erfassung und Anzeige von Verdachtsfällen.

(4) Sofern die Durchführung von internen Sicherungsmaßnahmen oder die Wahrnehmung von kundenbezogenen Sorgfaltspflichten durch das Institut vertraglich auf eine dritte Person oder ein anderes Unternehmen ausgelagert worden ist, ist hierüber zu berichten.

(5) In Bezug auf ein Institut, das übergeordnetes Unternehmen im Sinne des § 25g des Kreditwesengesetzes ist, hat der Prüfer darzustellen und zu beurteilen, inwieweit dieses angemessene Maßnahmen getroffen hat, um in seinen nachgeordneten Unternehmen, Zweigstellen und Zweigniederlassungen die gruppeneinheitliche Schaffung der in § 25g des Kreditwesengesetzes genannten internen Sicherungsmaßnahmen sowie die Einhaltung der dort zusätzlich genannten Pflichten und gegebenenfalls die Erfüllung von am ausländischen Sitz geltenden strengeren Pflichten sicherzustellen. Absatz 1 Satz 4 sowie Absatz 4 gelten entsprechend. Soweit die nach Satz 1 zu treffenden Maßnahmen in einem Drittstaat nicht zulässig oder tatsächlich nicht durchführbar sind, hat der Prüfer ferner darzustellen und zu beurteilen, inwieweit das Institut angemessene Maßnahmen getroffen hat, um sicherzustellen, dass nachgeordnete Unternehmen, Zweigstellen und Zweigniederlassungen dort keine Geschäftsbeziehungen begründen oder fortsetzen, Transaktionen durchführen und bestehende Geschäftsbeziehungen beenden.

(6) Bei Kreditinstituten ist zu prüfen, inwieweit diese im bargeldlosen Zahlungsverkehr ihren Pflichten zur Feststellung, Überprüfung und Übermittlung von vollständigen Auftraggeberdaten nachgekommen sind. Gleiches gilt in Bezug auf die von den vorgenannten Instituten getroffenen Maßnahmen zur Erkennung und Behandlung von eingehenden Zahlungsaufträgen mit unvollständigen Auftraggeberdaten.

(7) Bei Kreditinstituten ist darzustellen, inwieweit diese ihre Verpflichtungen nach § 24c Absatz 1 des Kreditwesengesetzes erfüllt haben. Insbe-

sondere ist zu prüfen, ob die hierzu eingesetzten Verfahren eine zutreffende Erfassung der aufgenommenen Identifizierungsdaten mit richtiger Zuordnung zum Konto oder Depot im Abrufsystem gewährleisten. Gegebenenfalls ist über die ordnungsgemäße Erfüllung der Anordnungen der Bundesanstalt gemäß § 6a des Kreditwesengesetzes zu berichten.

Anlage 3: Fallbeispiele aus der Praxis

Fall 1

Kreditbetrug
Angebliche Investoren aus einem ausländischen Staat gaben vor, ein Projekt (Umbau eines Bahnhofes zu einem Erlebnisbereich mit Geschäften, Diskotheken, Restaurants u. a.) finanzieren zu wollen. Dafür benötigten sie ca. 50 Mio. Euro und sicherten das benötigte Darlehen mit einem Pfandbrief ab.

Der Pfandbrief stellte sich als Fälschung heraus.

Mögliche Maßnahmen:
- Keine Kopien von etwaigen Kreditsicherheiten akzeptieren (in Geschäftsanweisung festgelegt).
- Ablehnung der Geschäftsbeziehung.
- Keine schriftliche Antwort an den „möglichen Investor", da mit einem Originalbriefkopf und Originalunterschriften weitere Betrugshandlungen begangen werden können.
- Erfassung der Personen und genannten Firmen aus dem ausländischen Staat in der eigenen Warndatei.

Quelle: Mitgliedsinstitute des VÖB

Fall 2

Betrug
Zwei Vermittler wollten ein Konto eröffnen. Beide Personen vermittelten angabegemäß Ölhandelsgeschäfte zwischen russischen und amerikanischen Ölkonzernen. Das Geschäft sollte folgendermaßen abgewickelt werden: Amerikanische Ölkonzerne kaufen bei den russischen Ölgesellschaften Erdöl. Sobald das Öl in die Tanker verschifft wurde, sollten die amerikanischen Abnehmer den vereinbarten Betrag auf das bei einem inländischen Kreditinstitut eingerichteten Konto überweisen. Sobald das Öl von dem amerikanischen Abnehmer in Empfang genommen wurde, sollte der gesamte Betrag an den russischen Lieferanten ausgekehrt werden. Die Vermittlungsprovision sollte vom inländischen, kontoführenden Institut an die Vermittler gezahlt werden, sobald die Information über die vollzogene Beladung des Tankers beim amerikanischen Abnehmer und zeitgleich bei dem inländischen Institut eingegangen ist. Die Provision sollte zwei Prozent der vereinbarten Gesamtsumme betragen. Als Nachweis ihrer (angeblichen) Seriosität legten die Vermittler einen „aktuellen Handelsregisterauszug" vor.

Der Handelsregisterauszug stellte sich als Fälschung heraus. Die Vermittler waren bereits einschlägig bekannt.

Mögliche Maßnahmen:
- Keine Kopien von Registerauszügen akzeptieren, die von neuen Kunden beigebracht werden (immer Originale abfordern).

- Umfangreiche Identifizierung und Know Your Customer (KYC)-Prüfung durchführen.

- Im Zusammenhang mit obiger KYC-Prüfung auch Kundenvorprüfung über die Systeme der Fachabteilung Geldwäscheprävention/ Wirtschaftskriminalität durchführen.

- Ablehnung der Geschäftsbeziehung.

- Erfassung der Personen und genannten Firmen in der eigenen Warndatei.

Quelle: Mitgliedsinstitute des VÖB

Fall 3

Anlagebetrug
Ein deutscher Anlageberater offerierte Geldanlagen in den USA, die den Gewinn aus banküblichen Geldanlagen weit übertreffen sollten. Dafür bediente er sich mehrerer Finanzvermittler. Bei diesem Modell handelte es sich um ein sogenanntes Schneeballsystem, in dem angebliche Gewinne aus Anlagen neuer Kunden gezahlt wurden. Die Geschäftsadresse in den USA war ein Servicebüro für mehrere hundert Firmen. Der Anlageberater setzte sich in die USA ab, entnahm alle Geldanlagen und zahlte keine Zwischengewinne mehr aus.

Nachdem Anzeige gegen den Anlageberater erstattet wurde stellte sich heraus, dass bei mehreren deutschen Landeskriminalämtern bereits Anzeigen gegen ihn vorlagen.

Mögliche Maßnahmen:
- Aufnahme des Namens und der Kontoverbindung des Betrügers in den USA in die interne Blacklist der deutschen Korrespondenzbank.

- Zahlungen von Kunden können mittels erstgenannter Maßnahme angehalten und Rücküberweisungen veranlasst werden.

- Die Kunden sind von ihrem kontoführenden Institut zu informieren, dass es sich bei dem beabsichtigten Zahlungsempfänger um einen einschlägig bekannten Betrüger handelt.

Quelle: Mitgliedsinstitute des VÖB

Fall 4

Scheck-Betrug mit Traveller's Checks
Der Kunde legte an zwei verschiedenen Tagen insgesamt 65 gefälschte American Express Travelers Cheques zu einem Wert von je 200,00 Euro (insgesamt 13.000,00 Euro) vor. Die Schecks sahen täuschend echt aus und wurden daher von der Kassiererin entgegengenommen.

Mögliche Maßnahmen:

- Nutzung und konsequente Anwendung von installierter Software, mit der neben der Überprüfung der Echtheit von Ausweispapieren und Geldscheinen auch die Echtheit von Travelers Cheques geprüft werden kann.

- Außerdem: Sensibilisierung der Mitarbeiter im Kassenbereich und Hinweis auf bestehende interne Regularien.

- Erstattung einer Strafanzeige gegen den Kunden wegen des Einlösens gefälschter Travelers Cheques.

Quelle: Mitgliedsinstitute des VÖB

Fall 5

Kreditbetrug
Im Rahmen der Vermittlertätigkeit hat ein Vermittler der Bank diverse Immobilien-Finanzierungen angetragen. Die vom Vermittler eingereichten Bonitätsunterlagen (z. B. Gehaltsbescheinigungen etc.) waren gefälscht, dies zum Teil ohne Wissen des Darlehnsnehmers.

Mögliche Maßnahmen:
- Überprüfung der hausinternen Prozesse.

- Sensibilisierung der Mitarbeiter auf inhaltliche Prüfung der Bonitätsunterlagen (angeblich angestellter Gebäudereiniger mit einem Monatsgehalt von mehr als 3.500 Euro).

- Bedachte Auswahl von Vermittlern und konsequente Anwendung des Geldwäschegesetzes hinsichtlich der Anforderungen an zuverlässige Dritte, die kraft Vertrag bestimmt werden.

- Beendigung der Geschäftsbeziehung zum Kunden in seiner Funktion als Vermittler und in seiner Funktion als Kunde der Bank.

- Rückforderung somit erschlichener Vermittlungsprovisionen.

Quelle: Mitgliedsinstitute des VÖB

Fall 6

Phishing/Trojaner
Über eine neue Masche versuchten Kriminelle, eine betrügerische Überweisung durchzuführen. Hierzu wurde direkt nach der Anmeldung zum Online-Banking unter dem Vorwand einer „Sicherheitskontrolle" des Instituts eine iTAN erfragt.

Mögliche Maßnahmen des Instituts:
- Optimierung des Sicherungsverfahrens im Online-Banking zur Minimierung der eigenen Risiken aus betrügerischen Handlungen. Beispielsweise durch die Einführung des sms-TAN-Verfahrens.

Mögliche Maßnahmen auf Kundenseite:
- Sofern Kunden auf ihrem Rechner das zuvor beschriebene Verhalten beobachten, wird empfohlen, den Rechner durch einen Fachmann auf Viren (Trojanische Pferde) untersuchen zu lassen.

- Zudem ist zu empfehlen, dass sich die betreffenden Kunden bezüglich der Sperrung ihres Internet-Banking-Zugangs umgehend mit ihrem Institut in Verbindung setzen.

- Zur Vermeidung solcher „Infektionen" empfiehlt beispielsweise das Computer-Notfallteam eines Finanzverbundes neben dem Einsatz eines stets aktuellen Viren-Scanners das zeitnahe Einspielen von Sicherheits-Patches für das Windows-Betriebssystem und alle genutzte Anwendungen.

- Grundsätzlich sollten Kunden Verdacht schöpfen, wenn sie direkt nach der Anmeldung zum Online-Banking nach einer iTAN gefragt werden, ohne dass sie eine Überweisung eingegeben haben.

Quelle: Mitgliedsinstitute des VÖB

Fall 7

Phishing/Trojaner
Eine weitere Variante: Der Kunde tätigte eine Online-Überweisung. Diese wurde durch einen Trojaner abgefangen, der Betrag in eine auf 12.130,00 Euro lautende Zahlung umgewandelt und in das Ausland transferiert.

(Mögliche) Maßnahmen des Instituts:
- Schnellstmögliche Rückrufaktion des Geldbetrages und Überprüfung der hausinternen Prozesse.

- In dem konkreten Fall konnte der Betrag nicht erfolgreich zurückgerufen werden.

- Aufgrund der Mitgliedschaft des Instituts am bestehenden Haftungsfonds Zahlungsverkehr eines Finanzverbundes konnte der maximal mögliche Schadensbetrag von 10.000,00 Euro darüber reguliert werden. Die restliche Summe musste das Institut als Schaden ausgleichen.

- Daher empfehlenswert: Teilnahme an Haftungsfonds von Institutsgruppen oder Verbünden.

Mögliche Maßnahmen auf Kundenseite:
- Die gefälschte Überweisung wird vom Kunden bemerkt und dem Institut sofort gemeldet.

- Kunde stellt sodann Strafanzeige.

Quelle: Mitgliedsinstitute des VÖB

Fall 8

Überweisungsbetrug (Auftragsfax)
Über Faxschreiben erhielt ein Institut Kundenaufträge, höhere Geldbeträge ins Ausland zu überweisen. In mehreren Fällen wurden die Faxschreiben mit Absenderangaben von deutschen Kunden, die im Ausland ansässig sind, versehen. In einem der Fälle sollte der Überweisungsbetrag wegen einem wichtigen Geschäft dringend in ein Drittland per SWIFT weitergeleitet werden. Die Unterschriften des angeblichen Kunden waren unterschiedlich.

Mögliche Maßnahmen des Instituts:
- Zur Vermeidung von finanziellen Schäden für das Institut empfiehlt sich beim Überweisungsverkehr auf Grund des hohen Risikos grundsätzlich die Einführung einer Plausibilitätsprüfung zur Verhinderung des Einsatzes gefälschter Überweisungsträger.
- Neben Auffälligkeiten am Überweisungsvordruck (kein Institutslogo, Rechtschreibfehler etc.) sollten auf jeden Fall auch Kundenaufträge, die telefonisch bzw. per Fax eingehen, bei Auffälligkeiten bzw. höheren Beträgen plausibilisiert werden.
- Hierzu gehört die Rückfrage des Kundenberaters über die in den Kontendaten angegebenen Telefonnummern bzw. E-Mail-Adressen des Auftraggebers. Wichtigste Frage an den Kunden ist hierbei, ob und an welchen Empfänger die bewusste Überweisung ausgestellt wurde.

Mögliche Maßnahmen auf Kundenseite:
- Nachdem bekannt geworden ist, dass in vielen Ländern Briefe der Banken bereits in den jeweiligen Postverteilerstellen abgefangen und für betrügerische Handlungen verwendet werden, sollten die Kunden ihre Kundenberater aufsuchen und Schritte zur Umstellung auf das Onlinebanking mit entsprechenden Sicherheitseinrichtungen einleiten.
- Auch wäre der Versand von Bankdokumenten (z. B. Depot- und Kontoauszügen) in E-Mail-Form sicherer und möglicherweise auch günstiger. Ebenso bietet sich die Verwendung eines Passwortes für telefonische Kundentransaktionen an.
- Den Kunden ist zu empfehlen, die nicht ausgeschöpften Überziehungslimite, entsprechend auf ein angepasstes Niveau zu senken.

Quelle: Mitgliedsinstitute des VÖB

Fall 9

Betrug an älteren Kunden (z. B. „Enkeltrick")
Eine Seniorin (i.d.R. handelt es sich um weibliche Opfer) erhält einen Anruf, bei dem sich ein Unbekannter durch geschickte Fragestellung („Rate mal, wer am Telefon ist?") als Verwandter („Enkel") des Opfers ausgibt. Nachdem das Vertrauen erschlichen ist, wird über eine erfundene Notlage berichtet, bei der dringend Geld vom Anrufer benötigt wird. Die Kundin geht zum Institut, hebt ihre Ersparnisse ab und übergibt sie einem Boten.

Weitere Betrugsvarianten mit ähnlich gelagerter Thematik:
Nigeriabriefe; Lotteriegewinne, Erbschaften (Vorauszahlungsbetrug)

Mögliche Maßnahmen des Instituts:
- Sensibilisierung der Mitarbeiter, speziell des Kassenpersonals, sollte in solchen Fällen sichergestellt werden. Neben Schulungen bzw. Warnmeldungen bezüglich aktueller Betrugsgefahren, gehört stets eine erhöhte Sensibilität zu den Aufgaben der Kundenberater, insbesondere wenn ältere Kunden am Schalter unangekündigt hohe Bargeldbeträge abheben möchten.

- Durch gezieltes Nachfragen (mit Hinweis auf die Gefahren des Bargeldtransportes) nach dem Verwendungszweck, lässt sich bereits Schaden verhindern.

- Bei der Beobachtung von Drittpersonen, die den Kunden in die Filiale begleitet haben und die anschließend unauffällig im Hintergrund warten, ist ggf. bei Verdacht sofort die Polizei zu verständigen.

- Über die Präventionsabteilungen der Polizei werden auch kostenfreie Flyer bzw. Poster zu diesen und anderen Betrugsvorgängen ausgegeben, die an die Mitarbeiter zur Sensibilisierung weitergegeben werden können.

Mögliche Maßnahmen auf Kundenseite:
- Da diese Betrugstypologie meist nur bei älteren Personen funktioniert, sollte mit dem Kunden bei einem sachlichen Gespräch ein verfügbares Kontolimit vereinbart werden, dass den Lebensverhältnissen dieser Kunden entspricht (meist sind die verfügbaren Kreditlinien noch aus

Berufszeiten eingegeben, so dass im Rentenalter diesbezüglich nur noch deutlich niedrigere Limite benötigt werden).

- Auch empfiehlt sich bei älteren Kunden die Telefonnummer des nächsten Angehörigen in die Kontodaten mit aufzunehmen, um ggf. einen Kontrollanruf an den echten Enkel durchführen zu können.

Quelle: Mitgliedsinstitute des VÖB

Fall 10

Interner Betrug mit ruhenden Konten
Ein als Kundenberater tätiger Institutsmitarbeiter vergreift sich an Konten von zumeist älteren bzw. im Ausland lebenden Kunden, die zwar hohe Guthaben, aber seit langem keine Geldbewegungen aufweisen. In einem Fall wurden die veruntreuten Gelder für Börsenspekulationen verwendet. In der Hoffnung, dass bei erfolgreichen Spekulationsgeschäften der Schaden wieder zurückbezahlt werden könnte, wird das schlechte Gewissen des Mitarbeiters ruhiggestellt.

Da in den meisten Fällen die Börsenspekulationen nicht aufgehen, wird sukzessive auf weitere ruhende Konten zugegriffen, in der Hoffnung, doch noch größere Gewinne zu realisieren, aus denen alle rechtswidrig in Anspruch genommenen „Kredite" zurückbezahlt werden können.

Zur Vermeidung der schnellen Aufdeckung werden sämtliche betroffene Konten für den Versand der Kontoauszüge auf Selbstabholer geschlüsselt. Der Kundenberater entfernt die entsprechenden Kontoauszüge.

Mögliche Maßnahmen des Instituts:
- Nutzung und konsequente Anwendung von installierter Software zur Prüfung von auffälligen Kontobewegungen.

- Sofortige revisionsseitige Verfolgung von Kundenbeschwerden, falls diese eintreffen.

- Empfehlenswert: Auffälliges Mitarbeiterverhalten entsprechend prüfen.

- Bei Aufdeckung: Entlassung des Mitarbeiters und Erstattung einer Strafanzeige.

Quelle: Mitgliedsinstitute des VÖB

Anlage 4: Fragebogen zur Gefährdungsanalyse

Betrugsprävention
Fragebogen zur Gefährdungsanalyse 20xx der XY-Bank

Antwort bitte bis zum TT.MM.JJJJ an Organisationseinheit xyxy!

Absender:

Name / Funktion / OE-Nr. / Tel.Nr. **Datum / Unterschrift**

1. Bereichsangaben

1.1 OE-Nr./Bezeichnung:

1.2 Leitung:

1.3 Mitarbeiterzahl:

1.4 GwG-Berater /Operational-Risk-M.

1. Teil – Betrugspotenzial / externe Betrugsvorfälle

1.1 Wie stark ist die **Gefahr**, in Ihrem Bereich von betrügerischen Handlungen missbraucht zu werden?

Geringe Gefahr ☐
Mittlere Gefahr ☐
Hohe Gefahr ☐

1.2 Gab es in Ihrem Bereich bereits **in der Vergangenheit betrügerische Handlungen**?

Ja: ☐ weiter bei **1.3**

Nein: ☐ weiter bei **Teil 3**

1.3 Wie **häufig** kamen betrügerische Handlungen in Ihrem Bereich **innerhalb eines Jahres** vor?

Selten (1–2 mal) ☐
Gelegentlich (3–12 mal) ☐
Häufig (mehr als 12 mal) ☐

1.4 In welcher **Art** trat Betrug bei Ihnen auf?

Kontoeröffnungsbetrug	Ja: ☐	Nein: ☐
Zahlungsverkehrsbetrug in Form von:		
Überweisungsbetrug	Ja: ☐	Nein: ☐
Lastschriftbetrug	Ja: ☐	Nein: ☐
Scheckbetrug	Ja: ☐	Nein: ☐
Wechselbetrug	Ja: ☐	Nein: ☐
Kreditbetrug	Ja: ☐	Nein: ☐
Kreditkartenbetrug	Ja: ☐	Nein: ☐
Bankgarantiebetrug	Ja: ☐	Nein: ☐
Kapitalanlagebetrug	Ja: ☐	Nein: ☐

sonstiger Betrug: _____

Betrugsprävention
Fragebogen zur Gefährdungsanalyse 20xx der XY-Bank

2. Teil – Fallbezogene Darstellung

2.1 **Beschreibung** der eingetretenen Betrugsvorfälle:

2.2 Wie wurden diese Vorfälle entdeckt? Welche **Warnhinweise / Indizien** gab es im Vorfeld?

2.3 Wie sahen die anschließenden **internen / externen Maßnahmen** der Bank aus?
Welche **Konsequenzen** gab es?

2.4 Kamen diese Vorfälle im **Jahr 20xx** vor?

Ja: ☐ Nein: ☐

Wenn "Nein", in welchem Jahr dann? _____

2.5 Welcher **Schaden** entstand für die Bank aus diesen Vorfällen?

Vermögensschaden Ja: ☐ Nein: ☐

evtl. Schätzung (pro Jahr) der Schadenshöhe: _____

Reputationsschaden Ja: ☐ Nein: ☐

Schaden nicht bekannt ☐
Schaden nicht eingetreten ☐

Sonstige Schäden / Verluste (evtl. für Kunden)? Haben wir sogar den Kunden verloren?

2.6 An welche Stelle in der Bank wurden die Vorfälle **gemeldet**?

Rechtsabteilung ☐
Schadensabwicklung ☐
Geldwäscheprävention ☐
Finanzermittlungen ☐
Risikocontrolling ☐
Interne Revision ☐
Kontoführung/ Kartenservice ☐
Zentrale Kreditbetreuung ☐

Sonstige: _____

Es erfolgte keine Meldung ☐

Betrugsprävention
Fragebogen zur Gefährdungsanalyse 20xx der XY-Bank

3. Teil – Anweisungen und Schulungen

3.1 Gibt es außer den "Rahmenanweisungen Finanzermittlungen" in Ihrem Bereich **weitere** Regelungen / Anweisungen / Sicherheitshandbücher / Rundschreiben zum Thema "Betrug"?

(Falls "Ja", bitte in Kopie mitsenden)

3.2 Sind diese Regelungen für alle Mitarbeiter im Bereich **einsehbar** bzw. **bekannt**?

einsehbar Ja: ☐ Nein: ☐

wenn "Ja", wo: _____

bekannt Ja: ☐ Nein: ☐

3.3 Wann erfolgte die letzte **Aktualisierung**?

Jahr: ☐

3.4 Finden **Mitarbeiterschulungen** bzw. **interne Besprechungen** zum Thema "Betrug" statt?

Ja: ☐ Nein: ☐

3.5 Wissen die **Mitarbeiter** in Ihrem Bereich, wie sie sich bei Verdacht auf betrügerische Handlungen zu verhalten haben, bzw. wie sie weiter vorgehen müssen?

Ja: ☐ Nein: ☐

3.6 Sind Ihrer Meinung nach die vorhandenen **Präventionsmaßnahmen** gegen Betrug in Ihrem Bereich **ausreichend**?

Ja: ☐ Nein: ☐

Es gibt keine Betrugsprävention: ☐

3.7 Wo liegen Ihrer Meinung nach die **Schwachpunkte** in Ihrem Bereich, von betrügerischen Handlungen missbraucht zu werden?

3.8 Haben Sie **Verbesserungsvorschläge** zur Steigerung der Betrugsprävention bzw. der Mitarbeiter-Sensibilisierung?

Betrugsprävention
Fragebogen zur Gefährdungsanalyse 20xx der XY-Bank

4. Teil – Zukünftige Betrugsgefahren

4.1 Falls Betrugshandlungen in Ihrem Bereich bereits **vorgekommen** sind:

Sehen Sie zukünftig eine **Steigerung** der Betrugsvorfälle in Ihrem Bereich? Ja: ☐ Nein: ☐

Wenn "Ja", wie **hoch** wird diese **Steigerung im Vergleich** zum Vorjahr ausfallen?

Geringe Steigerung (weniger als 10%) ☐
Mittlere Steigerung (zwischen 10% – 25%) ☐
Hohe Steigerung (mehr als 25%) ☐

Oder:

4.2 Falls Betrugshandlungen in Ihrem Bereich **noch nicht vorgekommen** sind:
Sehen Sie zukünftig eine **Gefahr** für Betrugshandlungen in Ihrem Bereich? Ja: ☐ Nein: ☐

Wenn "Ja", wie **stark** schätzen sie zukünftig diese **Gefahr**

Geringe Gefahr ☐
Mittlere Gefahr ☐
Hohe Gefahr ☐

5. Teil – Sonderfälle "Betrug"

5.1 Traten **folgende Betrugsarten** bereits in Ihrem Bereich auf?

Phishingbetrug	Ja: ☐	Nein: ☐
Finanzagenten	Ja: ☐	Nein: ☐
Insiderdelikte	Ja: ☐	Nein: ☐
Korruption	Ja: ☐	Nein: ☐
Betrug durch Mitarbeiter / Angehörige / Praktikanten	Ja: ☐	Nein: ☐
Insolvenzbetrug	Ja: ☐	Nein: ☐
Falschgeldbetrug	Ja: ☐	Nein: ☐

Wenn "Ja": **Beschreibung** der Vorfälle:

5.2 Wie stark schätzen Sie zukünftig die **Gefahr** solcher Betrugsarten in Ihrem Bereich ein?

Geringe Gefahr ☐
Mittlere Gefahr ☐
Hohe Gefahr ☐

Antwort bitte bis zum TT.MM.JJJJ an Organisationseinheit xyxy!

Vielen Dank für die Bearbeitung und Ihre Unterstützung!

Quelle: Mitgliedsinstitute des VÖB

Anlage 5a: Risikomatrix intern

und

Anlage 5b: Risikomatrix extern

sowie

Anlage 6a: Maßnahmenkatalog intern

und

Anlage 6b: Maßnahmenkatalog extern

befinden sich in der Stecktasche auf der hinteren Umschlagseite.

Anlage 7: Matrix zur Beurteilung aktueller Hinweisgebersysteme

Kriterium	Interne Telefon-hotline	Externes Call-Center	Einseitiges E-Mail-System	Ombuds-mann	BKMS System
Zeitliche Erreich-barkeit	Feste Sprech-zeiten	Feste Sprech-zeiten	24/7	Feste Sprechzei-ten	24/7
Örtliche Erreich-barkeit	Ortsunab-hängig	Ortsunab-hängig	Ortsunab-hängig	Fester Ort	Ortsunab-hängig
Anonymität	Unsicher	Unsicher	Unsicher	Vertraulich-keit	Absolut sicher (zertifi-ziert)
Hemmschwelle	Niedrig	Niedrig	Niedrig	Hoch	Niedrig
Dialog mit Hin-weisgeber	Schwierig	Schwierig	Keiner	Kontinuier-lich	Kontinuierlich
Sprachenvielfalt	Schwierig	Schwierig	Möglich	Schwierig	Möglich
Internationaler Einsatz	Möglich	Möglich	Möglich	Schwierig	Möglich
Erfassung der Meldung	Verbal	Verbal	Schriftlich	Verbal	Schriftlich und struktu-riert
Eingrenzung der Meldungsthemen	Nicht möglich	Nicht möglich	Nicht möglich	Möglich	Automatisiert
Bearbeitungs-aufwand	Hoch	Hoch	Mittel	Niedrig	Niedrig
Abspracheauf-wand mit Auf-traggeber	Niedrig	Hoch	Niedrig	Hoch	Niedrig
Statistiken	Manuell	Manuell	Manuell	Manuell	Automatisiert und manuell
Sicherheit der Daten	Unsicher	Unsicher	Unsicher	Sicher	Absolut sicher (zertifiziert)
Folgekosten	Mittel	Hoch	Mittel	Hoch	Niedrig

Quelle: BUSINESS KEEPER AG 2007 „Vergleich Hinweisgebersysteme“

Herausgeber:
Bundesverband Öffentlicher
Banken Deutschlands, VÖB
Lennéstraße 11, 10785 Berlin
Postfach 11 02 72, 10832 Berlin
Telefon 0 30/81 92-0
Telefax 0 30/81 92-2 22
E-Mail: postmaster@voeb.de
Internet: www.voeb.de

Stand: April 2010

Verfasser:
Indranil Ganguli
Stefanie Hetzler
Rüdiger Quedenfeld
Hans Dieter Rühle
Joachim Schanz

Herstellung:
DCM Druck Center Meckenheim GmbH

www.voeb.de

Maßnahmenkatalog zur Risikomatrix „Betrügerische Handlungen intern" zur Gefährdungsanalyse

Risikokategorien		Zugriffe durch MA						IT				Geheimhaltung		Begünstigung				Provisionsbetrug			Korruption				Steuerdelikte		Arbeitgeberdelikte								Insiderverstöße und Marktmanipulation											sonst. MA-Pflichtverletzungen						
Maßnahmen*1	Betrugstypologien	Zugriff auf Bargeld	Zugriff auf Kundenkonten etc.	Zugriff auf Kundenvermögen bei Annahme	Zugriff auf Kundenkredit	Zugriff auf EC-/Kreditkarten (& PIN)	Scheckbetrug	Missbrauch alter DV-Nutzer	Missbrauch neuer DV-Nutzer	Anlage fingierter Kunden/ Konten	DV-Manipulation	Daten-/Informationsweitergabe	Missbrauch von Insiderinformationen zur Erpressung	Schuldnerbegünstigung	Gewährung von Sonderkonditionen	Fehlbewertung von Immobilien	Missachtung von Gw-/Embargovorschriften	Vermittlungsbetrug	Fälschung von Aufträgen/ Verträgen	Fälschung von Anweisungen zur Prov.auszahlung	Absprachen bei Ausschreibungen?	Vorteilsannahme/Bestechlichkeit	Vorteilsgewährung/Bestechung	Annahme von Geschenken	Steuerhinterziehung	Beihilfe zur Steuerhinterziehung	Verletzung von Buchführungspflichten	Bilanzfälschung	Unrichtige Angaben ggü. Abschlussprüfer	Insolvenzverschleppung	Bankrott	Gläubigerbegünstigung	Veruntreuen von Arbeitsentgelt	Verleitung eines Untergebenen zu einer Straftat	Marktmanipulation	Wash sales	Improper matched orders	Pump and dump	Marking the close	Concerning	Insiderhandel	Late Trading	Market Timing	Churning	Scalping	Gefälschte Bewerbungsunterlagen	Arbeitszeitbetrug	Spesen-/RK-Betrug	Unterschlagung/Entwenden von Sachen	Einräumung nicht genehmigter Kreditlinien auf MA-Konto	Zinsmanipulation	Finanzagent
A	**Facility Management**																																																			
1	Gebäudesicherheitskonzept	✔[*2]																																																		
1a	allg. Zutrittskontrollen	✔[*2]																																																		
1b	spezielle Zutrittskontrollen (Chinese Walls)																																																			
1c	Empfang (Kundenhalle)																																																			
1d	Garagenwart																																																			
1e	Kameras (Aufzeichnung)	✔[*2]																																																		
2	Sprachaufzeichnung (Financial Markets)																																																			
3	Clean Desk Policy																																																			
4	Verschließen der Büroräume	✔[*2]																																																		
5	Verschließen der Schränke/Schubladen/ Schreibtische	✔[*2]																																																		
6	Laufwerke (Disketten, CDs, DVDs) gesperrt/ nicht vorhanden																																																			
7	Äußerliche Überprüfung von GA vor Ort (Skimming)																																																			
B	**Risikomanagement**																																																			
1	Controlling/RM-System																																																			
2	IKS																																																			
3	Institutsspezifische Gefährdungsanalyse (SironRAS)																																																			
C	**Schriftlich fixierte Regeln**																																																			
1	Arbeitsanweisungen																																																			
2	Ethikgrundsätze																																																			
3	Compliance-Richtlinien (Wertpapierbereich)																																																			
4	Reisekosten-Regelung																																																			
5	Führungsgrundsätze																																																			
6	MA-Leitsätze (Anzeige von Konten, Vollmachten etc. bei fremden Instituten)																																																			
7	Eindeutige Kompentenzregelungen																																																			
D	**Know your customer**																																																			
1	Identifizierung des Kunden bei Kontoeröffnung																																																			
2	Identifizierung des wirtschaftlich Berechtigten																																																			
3	Identifizierung des Verfügungsberechtigten																																																			
4	Ausweisverifikation (idenTT)																																																			
5	Überprüfung von Visa u. Aufenthaltstiteln (idenTT)																																																			
6	Kenntnisse über Kundenhintergrund (Beruf etc.)																																																			
7	Kenntnis über Herkunft von Geldern																																																			
E	**Know your employee**																																																			
1	Sorgfältige Mitarbeiterauswahl (Pre-Employment Screening)																																																			
1a	Zeugnisse etc. im Original																																																			
1b	Führungszeugnis																																																			
2	Kenntnisse über persönliche Hintergründe der MA																																																			
3	Auszahlung an MA zu Lasten von Kundenkonten nur mit vorheriger Zustimmung d. Vorgesetzten																																																			
4	Verfügungsber. von MA über Kundenkonten nur mit vorheriger Zustimmung d. Vorgesetzten																																																			
5	Analyse von MA-Konten																																																			
6	Sorgfältige Prüfung u. Auswahl von Vermittlern																																																			
F	**Interne Arbeitsprozesse**																																																			
1	Vier-Augen-Prinzip																																																			
2	Funktionstrennung																																																			
3	getrennte Verwahrung u. Versand von EC-/ KK und PIN																																																			
4	Begrenzung von Kompetenzen u. Berechtigungen																																																			
5	Zentralisierung von Kunden-/ Konteneinrichtung (MSC)																																																			
6	Zentralisierung v. Finanzkonteneinrichtung (Gesamtbanksteuerung)																																																			
7	keine Zugriffsmöglichkeit des MA nach Abgabe d. Kassenbestandes in Tresor																																																			
8	regelm. Wechsel der Kombination																																																			
9	Need-to-know-Prinzip																																																			
10	Rotationssysteme																																																			
11	keine Provisionsvorauszahlungen an externe Vermittler																																																			
12	Sorgfältige Auswahl von Lieferanten																																																			
G	**Prozesse im Geschäftsverkehr**																																																			
1	Sparbuchverfügungen nur mit Buchvorlage/ PIN																																																			
2	strenge (Bonitäts-)Prüfungskriterien bei Kreditvergabe																																																			
3	strenge Prüfungskriterien bzgl. kreditrelevanter Unterlagen																																																			
4	Scheckbuchung über Zwischenkonten, Gutschrift valutengerecht																																																			
5	E.V. bei Scheckeinreichungen zugunsten von Konten																																																			
6	Gutschrift ausländischer Schecks erst nach Bezahlt-Meldung																																																			
7	keine Auslage von Blanko-Überweisungsformularen																																																			
8	strenge Unterschriftsprüfung auf Überweisungsträgern																																																			
9	Rückbestätigung (Tel.) beim Kunden ab bestimmter Betragsgrenze bei Überweisung																																																			
10	strenge (Bonitäts-)Prüfungskriterien b. Kartenvergabe (ec/KK)																																																			
11	Lastschriftverfahren nur mit Einreichervertrag																																																			
12	LS-Verfahren nur für Kunden mit guter Bonität																																																			
13	LS-Verfahren nur bei geschäftl. Notwendigkeit des Kunden																																																			
14	Einhaltung der vereinbarten Verschlüsselungen von Telexen im Interbankenverkehr																																																			
15	i-TAN-/ HBCI-Chipkarten-/SMS-TAN-/ Chip-TAN-Verfahren beim Onlinebanking																																																			
16	Betragsobergrenze für Online-Verfügungen pro Tag																																																			
17	Betragsobergrenze für Barauszahlungen am GA pro Tag																																																			
18	Betragsobergrenze für Bareinzahlungen am GA pro Tag																																																			
19	Identifizierungspflicht bei Bareinzahlung/ Finanztransfergeschäft ab bestimmten Betrag																																																			
H	**Kontrolle, Prüfung, Überwachung**																																																			
1	Jahresabschlussprüfungen durch WP																																																			
2	Interne Revision																																																			
2a	IKS																																																			
3	Geldwäsche-Prävention																																																			
4	Compliance																																																			
5	Meldepflicht von Unregelmäßigkeiten/ Verdachtsfällen an Beauftragte																																																			
6	tägliche Bestandsaufnahmen (Kasse, Tresor, GA)																																																			
6a	Dokumentation von Kassenübergaben																																																			
7	Stichprobenkontrollen																																																			
7a	unvermutete Kontrollen ruhender Bestände																																																			
7b	Sonderuntersuchungen in Risikobereichen																																																			
8	Sorgfältige Überprüfung von Reisekosten-Abrechnungen																																																			
9	Sorgfältige Überprüfung von Lieferanten-Rechnungen																																																			
10	BaFin-Sonderprüfungen (§ 44 KWG)																																																			
11	Anordnungen der BaFin (z. B. § 6a KWG)																																																			
I	**Technische/technologische Mittel**																																																			
1	Geldwäsche-Research-System (SironAML)																																																			
2	Betrugsbekämpfungs-System (SironFD)																																																			
3	System zur Aufdeckung von Insiderverstößen/ Marktmanipulation (SironMM)																																																			
4	Abgleich mit VIP-Liste („Schurken")																																																			
5	Abgleich mit PEP-Liste																																																			
6	Ausweisverifikation (idenTT)																																																			
7	Banknotenprüfung (idenTT)																																																			
8	Reisescheckprüfung (idenTT)																																																			
9	maschinelle Prüfung der Echtheit von einzuzahlendem Geld																																																			
10	Anti-Skimming-Geräte																																																			
11	Abschalten der Türöffner (Skimming)																																																			
12	Bankbriefkästen mit Hintergreifschutz u. Rückholsperre																																																			
13	IT-Sicherheit (akt. Virenscanner, Firewall etc.)																																																			
J	**Monitoring von Auffälligkeiten**																																																			
1	Kundenbeschwerden (Beschwerdemanagement)																																																			
2	prozentualer Anteil von Rücklastschriften																																																			
3	eingereichte LS-Aufträge nach Empfänger, Betrag u. Einreichungsart																																																			
4	Abweichung kunden-individueller Betragsgrößen/Auftragsarten/Empfänger																																																			
K	**Informationssammlung**																																																			
1	Datenbank mit Betrugstypologien (inkl. Verdachtsfälle der Vergangenheit)																																																			
2	Erfahrungsaustausch mit anderen Instituten																																																			
3	Seminare, Informationsveranstaltungen																																																			
4	Pressemitteilungen, Zeitungsberichterstattung																																																			
5	Ermittlungsbehörden (BKA, LKA, Kripo, FIU, FATF)																																																			
6	Aufsichtsbehörden (BaFin-Rundschreiben u.-Verlautbarungen)																																																			
7	Verbände (VÖB, Sparkassen- u. Giroverband)																																																			
8	EG-Verordnungen																																																			
9	Statistiken (z. B. PKS), Studien (z. B. zur Wirtschaftskriminalität)																																																			
L	**Sensibilisierung der Mitarbeiter/Kunden**																																																			
1	Mitarbeiterschulungen																																																			
2	Ethik-Training																																																			
3	Sensibilisierung von Führungskräften bzgl. Verhaltensänderungen ihrer MA																																																			
4	Verpflichtungserklärungen (Datenschutz, Bankgeheimnis etc.)																																																			
5	Zeitnahe Weitergabe von Informationen																																																			
6	Aufklärung der Kunden über Risiken und Präventionsmöglichkeiten (z. B. Phishing, POS)																																																			
M	**Verringerung der Motivation für MA-Kriminalität**																																																			
1	Angemessene Entlohnung																																																			
2	Realistische Vertriebsvorgaben																																																			
3	Aufnahme von Integritätskriterien in Vereinbarungen																																																			
4	Bindung an das Unternehmen (Loyalität)																																																			
4a	Übertragung von Verantwortung																																																			
4b	Einbindung der MA in best. Prozesse																																																			
5	Erhöhung der Hemmschwelle																																																			
5a	Kontrollen																																																			
5b	konsequente Sanktionierung betrügerischer Handlungen (Zero Tolerance-Prinzip)																																																			
N	**Versicherungen u. ä.**																																																			
1	Vertrauensschadenversicherung																																																			
2	Vermögensschaden-Haftpflicht-Versicherung (D&O)																																																			
3	Einlagensicherungsfonds																																																			
O	**Hinweisgebersystem**																																																			
1	extern																																																			
2	intern																																																			
P	**Krisenmanagement**																																																			
1	Notfallplan																																																			
2	Ad hoc-Maßnahmen																																																			
2a	Information verantwortlicher Stellen																																																			
2b	Widerruf von Vollmachten/ Entzug von Berechtigungen																																																			
2c	Sicherung gefährdeter Vermögenswerte																																																			
2d	Beweissicherung																																																			
3	Krisenstab																																																			
Q	**Ermittlungen**																																																			
1	Forensische Einheit																																																			
2	externe Ermittler (privatwirtschaftl.)																																																			
3	Zusammenarbeit mit Strafverfolgungsbehörden																																																			
R	**Repressive Maßnahmen ggü. Kunden/ Externe**																																																			
1	Kündigung der Kundenbeziehung																																																			
2	Kontensperre																																																			
3	Kartensperre																																																			
4	Kreditkündigung																																																			
5	Eintrag in Negativliste																																																			
6	Gw-Verdachtsanzeige (§ 11 GwG)																																																			
7	Strafanzeige																																																			
8	Zivilrechtliche Ansprüche (Regress)																																																			
9	Asset Tracing (Rückholung von Vermögenswerten)																																																			
S	**Repressive Maßnahmen ggü. MA**																																																			
1	Kritikgespräch																																																			
2	Widerruf von Vollmachten/ Entzug von Berechtigungen																																																			
3	Abmahnung																																																			
4	Versetzung/Abordnung																																																			
5	Freistellung																																																			
6	Kündigung																																																			
7	Aufhebungsvertrag																																																			
8	Gw-Verdachtsanzeige (§ 11 GwG)																																																			
9	Strafanzeige																																																			
10	Zivilrechtliche Ansprüche (Regress)																																																			
11	Asset Tracing (Rückholung v. Vermögenswerten a. d. Ausland)																																																			

[*1]) Die Maßnahmen sind unterschiedlicher Natur und eignen sich je nach Fallkonstallation zur Generalprävention, Spezialprävention, zur Aufdeckung und/oder Bekämpfung betrügerischer Handlungen; [*2]) Ein Haken an den entsprechenden Stellen bedeutet, dass diese Maßnahme die entsprechende Risikoposition (Beispiel: „Zugriff auf Bargeld") beeinflussen bzw. sich auf diese auswirken kann.
Quelle: Mitgliedsinstitut des VÖB

Maßnahmenkatalog zur Risikomatrix „Betrügerische Handlungen extern“ zur Gefährdungsanalyse

Risikokategorien		Kd.annahme	Zahlungsverkehr (ZV)								Belegloser ZV		Kartenbetrug			Internet/Telekommunikation						Kreditbetrug					Korruption			Erpressung		Gw/TF		sonst. Pflichtverl. durch Externe				
Bereiche	Betrugstypologien	Kontoeröffnungsbetrug	Wechselfalle	Falschgeld	Reisescheckbetrug	Scheckbetrug	Scheckreiterei	Wechselbetrug	Akkreditivbetrug	unautorisierte Vfg. am Schalter	Lastschriftbetrug (Lastschriftreiterei)	Überweisungsbetrug	EC- und Kreditkartenbetrug	Missbrauch durch Karteninhaber	Skimming	Hacking	Phishing/Pharming	Vishing	Finanzagent	Vorschussbetrug/ Nigeria-Connection	Podslurping	Beantragung mithilfe gefälschter Unterlagen	Zessionsbetrug	sonst. vermeintliche Sicherheiten	Traditionsnamensbetrug	gefälschte Gutachten, Bescheinigungen	Absprachen bei Ausschreibungen	Vorteilsannahme/ Bestechlichkeit	Vorteilsgewährung/ Bestechung	Erpressung zur Informationsherausgabe	Erpressung zur Auftragsvergabe	Geldwäsche	Terrorismusfinanzierung	Verl. der Geheimhaltungspflicht durch Abschlussprüfer	Verl. der Geheimhaltungspflicht durch Lieferanten etc.	Überhöhte Lieferantenrechnungen	Kapitalanlagebetrug (Prospektbetrug)	Aktienspam
A	**Facility Management**																																					
1	Gebäudesicherheitskonzept	✔[*1]																																				
1a	allg. Zutrittskontrollen	✔[*1]																																				
1b	spezielle Zutrittskontrollen																																					
1c	Empfang (Kundenhalle)	✔[*1]																																				
1d	Garagenwart																																					
1e	Kameras (Aufzeichnung)	✔[*1]																																				
2	Sprachaufzeichnung (Financial Markets)																																					
3	Clean Desk Policy																																					
4	Verschließen der Büroräume																																					
5	Verschließen der Schränke/Schubladen/ Schreibtische																																					
6	Laufwerke (Disketten, CDs, DVDs) gesperrt/nicht vorhanden																																					
7	Äußerliche Überprüfung von GA vor Ort (Skimming)																																					
B	**Risikomanagement**																																					
1	Controlling/RM-System																																					
2	IKS																																					
3	Institutsspezifische Gefährdungsanalyse (SironRAS)																																					
C	**Schriftlich fixierte Regeln**																																					
1	Arbeitsanweisungen																																					
2	Ethikgrundsätze																																					
3	Compliance-Richtlinien (Wertpapierbereich)																																					
4	Reisekosten-Regelung																																					
5	Führungsgrundsätze																																					
6	MA-Leitsätze (Anzeige von Konten, Vollmachten etc. bei fremden Instituten)																																					
7	Eindeutige Kompentenzregelungen																																					
D	**Know your customer**																																					
1	Identifizierung des Kunden bei Kontoeröffnung																																					
2	Identifizierung des wirtschaftlich Berechtigten																																					
3	Identifizierung des Verfügungsberechtigten																																					
4	Ausweisverifikation (idenTT)																																					
5	Überprüfung von Visa u. Aufenthaltstiteln (idenTT)																																					
6	Kenntnisse über Kundenhintergrund (Beruf etc.)																																					
7	Kenntnis über Herkunft von Geldern																																					
E	**Know your employee**																																					
1	Sorgfältige Mitarbeiterauswahl (Pre-Employment Screening)																																					
1a	Zeugnisse etc. im Original																																					
1b	Führungszeugnis																																					
2	Kenntnisse über persönliche Hintergründe der MA																																					
3	Auszahlung an MA zu L. v. Kd. konten nur mit vorheriger Zustimmung d. Vorgesetzten																																					
4	Verfügungsber. von MA über Kd.konten nur mit vorheriger Zustimmung d. Vorgesetzten																																					
5	Analyse von MA-Konten																																					
6	Sorgfältige Prüfung u. Auswahl von Vermittlern																																					
F	**Interne Arbeitsprozesse**																																					
1	Vier-Augen-Prinzip																																					
2	Funktionstrennung																																					
3	getrennte Verwahrung u. Versand von EC-/ KK und PIN																																					
4	Begrenzung von Kompetenzen u. Berechtigungen																																					
5	Zentralisierung von Kunden-/Konteneinrichtung (MSC)																																					
6	Zentralisierung von Finanzkonteneinrichtung (Gesamtbanksteuerung)																																					
7	keine Zugriffsmöglichkeit des MA nach Abgabe d. Kassenbestandes in Tresor																																					
8	regelmäßiger Wechsel der Kombination																																					
9	Need-to-know-Prinzip																																					
10	Rotationssysteme																																					
11	keine Provisionsvorauszahlungen an externe Vermittler																																					
12	Sorgfältige Auswahl von Lieferanten																																					
G	**Prozesse im Geschäftsverkehr**																																					
1	Sparbuchverfügungen nur mit Buchvorlage/ PIN																																					
2	strenge (Bonitäts-) Prüfungskriterien bei Kreditvergabe																																					
3	strenge Prüfungskriterien bzgl. kreditrelevanter Unterlagen																																					
4	Scheckbuchung über Zwischenkonten, Gutschrift valutengerecht																																					
5	E.V. bei Scheckeinreichungen zugunsten von Konten																																					
6	Gutschrift ausländischer Schecks erst nach Bezahlt-Meldung																																					
7	keine Auslage von Blanko-Überweisungsformularen																																					
8	strenge Unterschriftsprüfung auf Überweisungsträgern																																					
9	Rückbestätigung (Tel.) beim Kunden ab best. Betragsgrenze bei Überweisung																																					
10	strenge (Bonitäts-) Prüfungskriterien bei Kartenvergabe (ec/KK)																																					
11	Lastschriftverfahren nur mit Einreichervertrag																																					
12	LS-Verfahren nur für Kunden mit guter Bonität																																					
13	LS-Verfahren nur bei geschäftl. Notwendigkeit des Kunden																																					
14	Einhaltung der vereinbarten Verschlüsselungen von Telexen im Interbankenverkehr																																					
15	i-TAN-/HBCI-Chipkarten-/SMS-TAN-/Chip-TAN-Verfahren beim Onlinebanking																																					
16	Betragsobergrenze für Online-Verfügungen pro Tag																																					
17	Betragsobergrenze für Barauszahlungen am GA pro Tag																																					
18	Betragsobergrenze für Bareinzahlungen am GA pro Tag																																					
19	Identifizierungspflicht bei Bareinzahlung/ Finanztransfergeschäft ab best. Betrag																																					
H	**Kontrolle, Prüfung, Überwachung**																																					
1	Jahresabschlussprüfungen durch WP																																					
2	Interne Revision																																					
2a	IKS																																					
3	Geldwäsche-Prävention																																					
4	Compliance																																					
5	Meldepflicht von Unregelmäßigkeiten/ Verdachtsfällen an Beauftragte																																					
6	tägliche Bestandsaufnahmen (Kasse, Tresor, GA)																																					
6a	Dokumentation von Kassenübergaben																																					
7	Stichprobenkontrollen																																					
7a	unvermutete Kontrollen der ruhenden Bestände																																					
7b	Sonderuntersuchungen in Risikobereichen																																					
8	Sorgfältige Überprüfung von Reisekosten-Abrechnungen																																					
9	Sorgfältige Überprüfung von Lieferanten-Rechnungen																																					
10	BaFin-Sonderprüfungen (§ 44 KWG)																																					
11	Anordnungen der BaFin (z.B. § 6 a KWG)																																					
I	**Technische/technologische Mittel**																																					
1	Geldwäsche-Research-System (SironAML)																																					
2	Betrugsbekämpfungs-System (SironFD)																																					
3	System zur Aufdeckung von Insiderverstößen/ Marktmanipulation (SironMM)																																					
4	Abgleich mit VIP-Liste („Schurken“)																																					
5	Abgleich mit PEP-Liste																																					
6	Ausweisverifikation (idenTT)																																					
7	Banknotenprüfung (idenTT)																																					
8	Reisescheckprüfung (idenTT)																																					
9	maschinelle Prüfung der Echtheit von einzuzahlendem Geld																																					
10	Anti-Skimming-Geräte																																					
11	Abschalten der Türöffner (Skimming)																																					
12	Bankbriefkästen mit Hintergreifschutz u. Rückholsperre																																					
13	IT-Sicherheit (akt. Virenscanner, Firewall etc.)																																					
J	**Monitoring von Auffälligkeiten**																																					
1	Kundenbeschwerden (Beschwerdemanagement)																																					
2	prozentualer Anteil von Rücklastschriften																																					
3	eingereichte LS-Aufträge nach Empfänger, Betrag u. Einreichungsart																																					
4	Abweichung kunden-individueller Betragsgrößen/Auftragsarten/Empfänger																																					
K	**Informationssammlung**																																					
1	Datenbank mit Betrugstypologien (inkl. Verdachtsfälle der Vergangenheit)																																					
2	Erfahrungsaustausch mit anderen Instituten																																					
3	Seminare, Informationsveranstaltungen																																					
4	Pressemitteilungen, Zeitungsberichterstattung																																					
5	Ermittlungsbehörden (BKA, LKA, Kripo, FIU, FATF)																																					
6	Aufsichtsbehörden (BaFin-Rundschreiben u.-Verlautbarungen)																																					
7	Verbände (VÖB, Sparkassen- u. Giroverband)																																					
8	EG-Verordnungen																																					
9	Statistiken (z.B. PKS), Studien (z. B. zur Wirtschaftskriminalität)																																					
L	**Sensibilisierung der Mitarbeiter/Kunden**																																					
1	Mitarbeiterschulungen																																					
2	Ethik-Training																																					
3	Sensibilisierung von Führungskräften bzgl. Verhaltensänderungen ihrer MA																																					
4	Verpflichtungserklärungen (Datenschutz, Bankgeheimnis etc.)																																					
5	Zeitnahe Weitergabe von Informationen																																					
6	Aufklärung der Kunden über Risiken u. Präventionsmöglichkeiten (z. B. Phishing, POS)																																					
M	**Verringerung der Motivation für MA-Kriminalität**																																					
1	Angemessene Entlohnung																																					
2	Realistische Vertriebsvorgaben																																					
3	Aufnahme von Integritätskriterien in Zielvereinbarungen																																					
4	Bindung an das Unternehmen (Loyalität)																																					
4a	Übertragung von Verantwortung																																					
4b	Einbindung der MA in best. Prozesse																																					
5	Erhöhung der Hemmschwelle																																					
5a	Kontrollen																																					
5b	konsequente Sanktionierung betrügerischer Handlungen (Zero Tolerance-Prinzip)																																					
N	**Versicherungen u. ä.**																																					
1	Vertrauensschadenversicherung																																					
2	Vermögensschaden-Haftpflicht-Versicherung (D&O)																																					
3	Einlagensicherungsfonds																																					
O	**Whistle-Blower-System**																																					
1	extern																																					
2	intern																																					
P	**Krisenmanagement**																																					
1	Notfallplan																																					
2	Ad-hoc-Maßnahmen																																					
2a	Information verantwortlicher Stellen																																					
2b	Widerruf von Vollmachten/ Entzug von Berechtigungen																																					
2c	Sicherung gefährdeter Vermögenswerte																																					
2d	Beweissicherung																																					
3	Krisenstab																																					
Q	**Ermittlungen**																																					
1	Forensische Einheit																																					
2	externe Ermittler (privatwirtschaftl.)																																					
3	Zusammenarbeit mit Strafverfolgungsbehörden																																					
R	**Repressive Maßnahmen ggü. Kunden/Ext.**																																					
1	Kündigung der Kunden-/Geschäftsbeziehung																																					
2	Kontensperre																																					
3	Kartensperre																																					
4	Kreditkündigung																																					
5	Sperre bzgl. Ausweitung der Geschäftsbeziehung																																					
6	Eintrag in Negativliste (VIP-Datei)																																					
7	Gw-Verdachtsanzeige (§ 11 GwG)																																					
8	Strafanzeige																																					
9	Zivilrechtliche Ansprüche (Regress)																																					
10	Asset Tracing (Rückholung von Vermögenswerten)																																					
S	**Repressive Maßnahmen ggü. MA**																																					
1	Kritikgespräch																																					
2	Widerruf von Vollmachten/ Entzug von Berechtigungen																																					
3	Abmahnung																																					
4	Versetzung/Abordnung																																					
5	Freistellung																																					
6	Kündigung																																					
7	Aufhebungsvertrag																																					
8	Gw-Verdachtsanzeige (§ 11 GwG)																																					
9	Strafanzeige																																					
10	Zivilrechtliche Ansprüche (Regress)																																					
11	Asset Tracing (Rückholung von Vermögenswerten)																																					

[*1]) Ein Haken an den entsprechenden Stellen bedeutet, dass diese Maßnahme die entsprechende Risikoposition (Beispiel: „Kontoeröffnungsbetrug“) beeinflussen bzw. sich auf diese auswirken kann.
Quelle: Mitgliedsinstitut des VÖB

Risikomatrix „Betrügerische Handlungen intern“ zur Gefährdungsanalyse

Risikokategorien		Zugriffe durch MA						IT				Geheimhaltung		Begünstigung				Provisionsbetrug			Korruption				Steuerdelikte		Arbeitgeberdelikte									Insiderverstöße und Marktmanipulation				sonst. MA-Pflichtverletzungen						
Betrugstypologien / Bereiche		Zugriff auf Bargeld	Zugriff auf Kundenkonten etc.	Zugriff auf Kundenvermögen bei Annahme	Zugriff auf Kundenkredit	Zugriff auf EC-/ Kreditkarten (& PIN)	Scheckbetrug	Missbrauch alter DV-Nutzer	Missbrauch neuer DV-Nutzer	Anlage fingierter Kunden / Konten	DV-Manipulation	Daten- / Informations-weitergabe	Missbrauch von Insider-informationen zur Erpressung	Schuldner-begünstigung	Gewährung von Sonderkondi-tionen	Fehlbewertung von Immobilien	Missachtung von Gw- / Embargo-vorschriften	Vermittlungsbetrug	Fälschung von Aufträgen / Verträgen	Fälschung von Anweisungen zur Prov.auszahlung	Absprachen bei Ausschreibungen	Vorteilsannahme / Bestechlichkeit	Vorteilsgewährung / Bestechung	Annahme von Geschenken	Steuerhinterziehung (burglary)	Beihilfe zur Steuerhinterziehung	Verletzung von Buchführungs-pflichten	Bilanzfälschung	Unrichtige Angaben gegenüber Abschlussprüfer	Insolvenz-verschleppung	Bankrott	Gläubiger-begünstigung	Veruntreuen von Arbeitsentgelt	Verleitung eines Untergebenen zu einer Straftat	Marktmanipulation	Insiderhandel	Churning	Scalping	Gefälschte Bewerbungs-unterlagen	Arbeitszeitbetrug	Spesen-/ RK-Betrug	Unterschlagung / Entwenden von Sachen	Einräumung nicht genehmigter Kredit-linien auf MA-Konto	Zinsmanipulation	Finanzagent
AR	Aufsichtsrat																																												
10	Vorstand																																												
10	Geldwäschebereich	x*																																											
10	Compliance																																												
10	Immobilien GmbH																																												
20	Stabsbereich Vorstand																																												
20a	Unternehmensentwicklung/Beteiligungen																																												
20b	Rechtsabteilung																																												
25	Kommunikation und Marketing																																												
21	Personalmanagement																																												
23	Interne Revision																																												
24	Organisation und Informatik																																												
26	Gesamtbanksteuerung																																												
27	Unternehmensservice																																												
28	Marktfolge Finanzierungen																																												
33	Firmenkunden																																												
37	Spezialfinanzierungen																																												
37	Leasing GmbH																																												
42	Privatkunden																																												
61	Financial Markets																																												
94	Personalrat / Gesamtpersonalrat																																												

* Das Kreuz an dieser Stelle stellt eine fiktiv ermittelte Risikoposition entsprechend der in der Legende aufgeführten Risikokategorien/-gruppen zwischen 0 – 5 dar.
Quelle: Mitgliedsinstitut des VÖB

Risiko	Risikogruppe
hoch	5
mittel-hoch (erhöht)	4
mittel	3
mittel-niedrig (reduziert)	2
niedrig	1
ohne Risiko	0

Risikomatrix „Betrügerische Handlungen extern“ zur Gefährdungsanalyse

Risikokategorien		Kd.an-nahme	Zahlungsverkehr (ZV)								Beleg-loser ZV		Kartenbetrug			Internet/Telekommunikation						Kreditbetrug					Korruption			Erpressung		Gw	sonst. Pflichtverl. durch Externe				
Betrugstypologien / Bereiche		Kontoeröffnungsbetrug	Wechselfalle	Falschgeld	Reisescheckbetrug	Scheckbetrug	Scheckreiterei	Wechselbetrug	Akkreditivbetrug	unautorisierte Vfg. am Schalter	Lastschriftbetrug (Lastschriftreiterei)	Überweisungsbetrug	EC- und Kreditkartenbetrug	Missbrauch durch Karteninhaber	Skimming	Hacking	Phishing/Pharming	Vishing	Finanzagent	Vorschussbetrug/ Nigeria-Connection	Podslurping	Beantragung mithilfe gefälschter Unterlagen	Zessionsbetrug	sonst. vermeintliche Sicherheiten	Traditionsnamensbetrug	gefälschte Gutachten, Bescheinigungen	Absprachen bei Ausschreibungen	Vorteilsannahme/ Bestechlichkeit	Vorteilsgewährung/ Bestechung	Erpressung zur Informationsherausgabe	Erpressung zur Auftragsvergabe	Geldwäsche	Verl. der Geheimhaltungspflicht durch Abschlussprüfer	Verl. der Geheimhaltungspflicht durch Lieferanten etc.	Überhöhte Lieferantenrechnungen	Kapitalanlagebetrug (Prospektbetrug)	Aktienspam
AR	Aufsichtsrat																																			
10	Vorstand																																			
10	Geldwäscheprävention																																x*			
10	Compliance																																			
10	Immobilien GmbH																																			
20	Stabsbereich Vorstand																																			
20a	*Unternehmensentwicklung/																																			
20b	Rechtsabteilung																																			
25	Kommunikation und Marketing																																			
21	Personalmanagement																																			
23	Interne Revision																																			
24	Organisation und Informatik																																			
26	Gesamtbanksteuerung																																			
27	Unternehmensservice																																			
28	Marktfolge Finanzierungen																																			
33	Firmenkunden																																			
37	Spezialfinanzierungen																																			
37	Leasing GmbH																																			
42	Privatkunden																																			
61	Financial Markets																																			
94	Personalrat / Gesamtpersonalrat																																			

* Das Kreuz an dieser Stelle stellt eine fiktiv ermittelte Risikoposition entsprechend der in der Legende aufgeführten Risikokategorien/-gruppen zwischen 0 – 5 dar.
Quelle: Mitgliedsinstitut des VÖB

Risiko	Risikogruppe
hoch	5
mittel-hoch (erhöht)	4
mittel	3
mittel-niedrig (reduziert)	2
niedrig	1
ohne Risiko	0