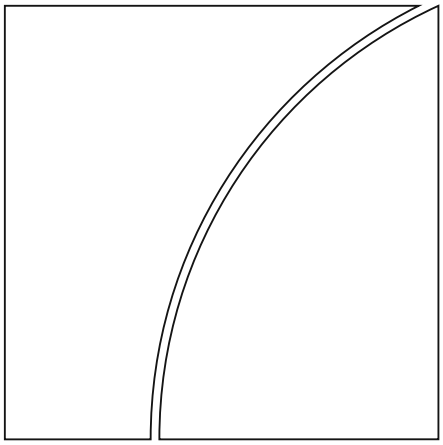
Basler Ausschuss für Bankenaufsicht



Solides Management der Risiken im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung

Januar 2014

BANK FÜR INTERNATIONALEN ZAHLUNGSAUSGLEICH

Dieses Papier wurde in englischer Sprache verfasst. In Zweifelsfällen wird auf die englische Fassung verwiesen.

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

ISBN 92-9131-303-3 (Druckversion)

ISBN 92-9197-303-3 (Online)

Inhalt

Solides Management der Risiken im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung

I. Einleitung

1. Angesichts der Bedeutung der Risiken, die dadurch entstehen, dass Banken – mit oder ohne Vorsatz – für das Begehen strafbarer Handlungen genutzt werden, hat sich der Basler Ausschuss für Bankenaufsicht entschlossen, diese Leitlinien herauszugeben, in denen beschrieben wird, wie Banken die Risiken der Geldwäsche und der Terrorismusfinanzierung im Rahmen ihres gesamten Risikomanagements berücksichtigen sollten.

2. Der Basler Ausschuss setzt sich seit Langem für solide Richtlinien und Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung ein, die im Hinblick auf die Wahrung der Sicherheit und Solidität von Banken sowie der Integrität des internationalen Finanzsystems von grosser Bedeutung sind. Nach einer ersten Erklärung im Jahre 1988[1] folgten mehrere Papiere des Ausschusses, in denen sein Engagement in dieser Sache zum Ausdruck kam. Im September 2012 machte er mit der Veröffentlichung der überarbeiteten Fassung der *Grundsätze für eine wirksame Bankenaufsicht* – die einen spezifischen Grundsatz (Grundsatz 29) enthalten, der auf den Missbrauch von Finanzdienstleistungen Bezug nimmt – nochmals seinen Standpunkt deutlich.

3. Der Basler Ausschuss spricht sich für die Annahme der Standards der Financial Action Task Force (FATF) aus.[2] Im Februar 2012 gab die FATF eine überarbeitete Fassung der *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (Internationale Standards zur Bekämpfung von Geldwäsche, Terrorismus- und Proliferationsfinanzierung* – die FATF-Standards) heraus, zu deren Entstehung der Ausschuss beigetragen hat.[3] Ferner hat die FATF im März 2013 die Leitlinien *Financial Inclusion Guidance* veröffentlicht, die der Ausschuss bei der Erarbeitung der vorliegenden Leitlinien ebenfalls berücksichtigt hat. Der Ausschuss verfolgt mit diesem Papier den Zweck, die Umsetzung der FATF-Standards auf nationaler Ebene zu unterstützen, indem er prüft, wo sich die Erfahrungen beider Organisationen ergänzen und wie diese am besten gemeinsam genutzt werden können. In die vorliegenden Leitlinien sind sowohl die FATF-Standards als auch die Basler Grundsätze für grenzüberschreitend tätige Banken eingeflossen, und sie passen in den Gesamtrahmen der Bankenaufsicht. Deshalb sind diese Leitlinien so gestaltet, dass sie im Hinblick auf die FATF-Standards kohärent sind und deren Zielsetzungen ergänzen; auf keinen Fall sollten sie als Änderungen der FATF-Standards verstanden werden – weder im Sinne einer Verschärfung noch einer Lockerung.

[1] Siehe BCBS, *Verhütung des Missbrauchs des Bankensystems für die Geldwäsche*, Dezember 1988, verfügbar auf www.bis.org/publ/bcbsc137de.pdf.

[2] Die FATF ist ein zwischenstaatliches Gremium, das internationale Standards entwickelt und sich für Richtlinien zum Schutz des globalen Finanzsystems vor Geldwäsche, Terrorismusfinanzierung und Finanzierung der Verbreitung von Massenvernichtungswaffen einsetzt. Die FATF definiert Geldwäsche als Weiterleitung von Erträgen aus strafbaren Handlungen, um deren illegale Herkunft zu verschleiern. Die FATF arbeitet eng mit anderen in diesem Bereich tätigen Einrichtungen und insbesondere mit assoziierten FATF-Mitgliedern und Beobachtern zusammen. Der Basler Ausschuss hat bei der FATF Beobachterstatus.

[3] Anhang 3 enthält eine Liste der wichtigsten FATF-Empfehlungen, an die sich die Banken und die Bankenaufsicht bei der Umsetzung ihrer Massnahmen gegen Geldwäsche und Terrorismusfinanzierung halten sollten. Die Aufzählung ist nicht vollständig, und weitere FATF-Empfehlungen, einschl. der Auslegungshinweise, können von Bedeutung sein. Das vollständige Papier ist unter www.fatf-gafi.org/recommendations verfügbar.

4. Im vorliegenden Papier hat der Ausschuss an bestimmten Stellen Querverweise auf FATF-Standards aufgenommen, um den Banken bei der Einhaltung nationaler Anforderungen, die auf die Umsetzung dieser Standards zurückgehen, Hilfestellung zu geben. Da es jedoch nicht die Absicht des Ausschusses ist, die bestehenden FATF-Standards einfach zu duplizieren, wird auf diese nicht systematisch Bezug genommen.

5. Das Engagement des Ausschusses im Zusammenhang mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung entspricht durchaus seinem Mandat: „die Bankenaufsicht mit Blick auf die Regelungen, Verfahren und Bankpraktiken weltweit zu stärken und dadurch die Finanzstabilität zu fördern".[4] Ein solides Management der Risiken der Geldwäsche und der Terrorismusbekämpfung ist für die Sicherheit und Solidität der Banken und des gesamten Bankensystems – das vorrangige Ziel der Bankenaufsicht – von grosser Bedeutung, weil

- es dazu beiträgt, den Ruf von Banken und nationalen Bankensystemen zu schützen, indem es verhindert bzw. davon abhält, dass Banken zum Waschen von unrechtmässig erzielten Erträgen oder zum Sammeln bzw. zum Weiterleiten von Finanzmitteln zur Unterstützung von Terrorismus genutzt werden
- es sowohl die Integrität des internationalen Finanzsystems schützt als auch die Bestrebungen der Regierungen im Hinblick auf die Bekämpfung von Korruption und Terrorismusfinanzierung unterstützt.

6. Ein unzulängliches bzw. nicht vorhandenes solides Management der Risiken der Geldwäsche und der Terrorismusfinanzierung führt dazu, dass sich Banken schwerwiegenden Risiken – insbesondere Reputations-, Geschäfts-, Compliance- und Konzentrationsrisiken – aussetzen. Entwicklungen in der letzten Zeit haben diese Risiken deutlich gemacht – dazu gehören sowohl strenge Zwangsmassnahmen seitens der Aufsichtsinstanzen als auch die den Banken aufgrund mangelnder Sorgfalt bei der Anwendung von geeigneten Richtlinien, Verfahren und Kontrollen des Risikomanagements entstandenen direkten und indirekten Kosten. Diese Kosten und Schäden wären wahrscheinlich vermeidbar gewesen, wenn die Banken über wirksame risikobasierte Richtlinien und Verfahren für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung verfügt hätten.

7. Es sei hier darauf hingewiesen, dass zwischen sämtlichen genannten Risiken Wechselwirkungen bestehen. Jedes einzelne Risiko kann jedoch neben der Verhängung von Geldstrafen und Sanktionen seitens der Aufsichtsinstanzen zu erheblichen finanziellen Kosten für die Banken führen (z.B. Abzug von Grosskundenmitteln und Kündigung von Fazilitäten, Forderungen an die Bank, Untersuchungskosten, Beschlagnahme und Einfrieren von Vermögenswerten sowie Kreditverluste); darüber hinaus muss das Management viel wertvolle und knappe Zeit sowie operative Ressourcen einsetzen, um Probleme zu lösen.

8. Deshalb sollte dieses Papier in Verbindung mit einer Reihe anderer einschlägiger Papiere des Ausschusses betrachtet werden, u.a.:

- *Grundsätze für eine wirksame Bankenaufsicht*, September 2012[5]
- *The internal audit function in banks*, Juni 2012[6]

[4] Siehe Basler Ausschuss für Bankenaufsicht, *Charta*, Januar 2013, verfügbar auf www.bis.org/bcbs/charter_de.pdf.

[5] Verfügbar auf www.bis.org/publ/bcbs230_de.pdf.

[6] Verfügbar auf www.bis.org/publ/bcbs223.pdf.

- *Principles for the sound management of operational risk*, Juni 2011[7]
- *Principles for enhancing corporate governance*, Oktober 2010[8]
- *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers*, Mai 2009[9]
- *Compliance and the compliance function in banks*, April 2005[10]

9. Mit der Absicht, die Veröffentlichungen des Ausschusses zum Thema Leitlinien für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung zu straffen, sind zwei der früheren Veröffentlichungen des Ausschusses in dieses Papier eingeflossen und werden durch dieses ersetzt: *Sorgfaltspflicht der Banken bei der Feststellung der Kundenidentität*, Oktober 2001 und *Consolidated KYC risk management*, Oktober 2004. Bei der Überarbeitung dieser Papiere hat der Ausschuss auch den Schwerpunkt verstärkt auf Risiken in Verbindung mit der Nutzung Dritter zur Anbahnung von Geschäften (s. Anhang 1) und bei der Bereitstellung von Korrespondenzbankdienstleistungen (s. Anhang 2) gelegt. Trotz ihrer Bedeutung und Relevanz wird auf andere spezifische Risikobereiche – wie politisch exponierte Personen (PEP), Privatbankgeschäfte sowie spezifische Rechtsstrukturen, die Gegenstand der früheren Papiere waren – im Zusammenhang mit diesen Leitlinien nicht speziell eingegangen, da sie Gegenstand von Veröffentlichungen der FATF sind.[11]

10. Hinsichtlich ihres Anwendungsbereichs sind die vorliegenden Leitlinien in Verbindung mit anderen Standards und Leitlinien des Ausschusses zur Förderung einer konsolidierten Aufsicht über Bankkonzerne zu sehen.[12] Dies gilt insbesondere im Kontext von Geldwäsche und Terrorismusfinanzierung, da Kunden häufig mehrfach Geschäftsbeziehungen zu ein und demselben Bankkonzern unterhalten und/oder Inhaber mehrerer Konten beim selben Konzern sind, wobei sich die jeweiligen Geschäftsstellen jedoch in verschiedenen Ländern befinden.

11. Diese Leitlinien gelten für alle Banken. Dabei müssen möglicherweise die Anforderungen im Hinblick auf kleine oder spezialisierte Institute angepasst werden, um deren spezifische Grösse bzw. deren Geschäftsmodellen Rechnung zu tragen. Es würde jedoch den Rahmen dieses Leitlinienpapiers sprengen, hier darauf einzugehen.

12. Diese Leitlinien richten sich speziell an Banken, Bankkonzerne (Teil II bzw. III) und an Aufsichtsinstanzen (Teil IV). Wie in Grundsatz 29 der *Grundsätze für eine wirksame Bankenaufsicht* ausgeführt, ist sich der Ausschuss bewusst, dass es eine Vielzahl unterschiedlicher einzelstaatlicher Regelungen hinsichtlich der Einhaltung der Anforderungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung gibt; dies gilt insbesondere für die funktionale aufsichtliche Arbeitsteilung zwischen Bankenaufsicht und anderen Stellen wie Financial Intelligence Units (FIU, Geldwäsche-Meldestellen).[13] Deshalb kann sich im Zusammenhang mit diesen Leitlinien der Begriff „Aufsichtsinstanz" auch auf diese Stellen beziehen. In Ländern mit geteilten aufsichtlichen Zuständigkeiten für Geldwäsche und

7 Verfügbar auf www.bis.org/publ/bcbs195.pdf.

8 Verfügbar auf www.bis.org/publ/bcbs176.pdf.

9 Verfügbar auf www.bis.org/publ/bcbs154.pdf.

10 Verfügbar auf: www.bis.org/publ/bcbs113.pdf.

11 Siehe insbesondere *FATF Guidance on Politically Exposed Persons* (Empfehlungen 12 und 22), verfügbar auf www.fatf-gafi.org/fr/documents/documents/peps-r12-r22.html.

12 Siehe z.B. Grundsatz 12 in *Grundsätze für eine wirksame Bankenaufsicht*, September 2012.

13 Financial Intelligence Units sind in der Empfehlung 26 der FATF Standards beschrieben.

Terrorismusfinanzierung arbeitet die Bankenaufsicht mit anderen Stellen zusammen, um die Einhaltung dieser Leitlinien erreichen.

13. Die FATF-Standards, die es Ländern vorschreiben, in ihren Finanzsektoren und anderen benannten Nichtfinanzsektoren weitere Massnahmen zu treffen oder Befugnisse und Zuständigkeiten für die zuständigen Behörden einzuführen, werden hier nicht behandelt.

II. Wesentliche Merkmale eines soliden Managements von Risiken der Geldwäsche und der Terrorismusfinanzierung

14. Entsprechend den überarbeiteten *Grundsätzen für eine wirksame Bankenaufsicht* (2012) sollten alle Banken über „angemessene Geschäftsgrundsätze und Verfahrensweisen, einschl. strenger Vorschriften für die Feststellung der Kundenidentität, verfügen, die hohe ethische Standards und Berufsstandsregeln im Finanzsektor fördern und verhindern, dass die Bank – mit oder ohne Vorsatz – für das Begehen strafbarer Handlungen genutzt wird .[14] Diese Anforderung ist als besonderer Teil der allgemeinen Pflichten von Banken zu sehen, wonach ein sachgerechtes Risikomanagement-Konzept vorhanden sein muss, das sämtliche Arten von Risiken, einschl. der Risiken der Geldwäsche und der Terrorismusfinanzierung, abdeckt. „Angemessene Geschäftsgrundsätze und Verfahrensweisen bedeutet in diesem Zusammenhang die Umsetzung weiterer Massnahmen zusätzlich zu wirksamen Sorgfaltspflichten bei der Feststellung der Kundenidentität. Diese Massnahmen sollten darüber hinaus angemessen und risikobasiert sein und sollten durch eine bankeigene Bewertung der Risiken der Geldwäsche und Terrorismusfinanzierung ergänzt werden. In diesem Papier sind Empfehlungen für derartige Massnahmen zusammengestellt. Ferner sind andere Richtlinien (s. Absatz 8 oben) zu befolgen oder zusätzlich zu berücksichtigen, wenn es keine spezifischen Empfehlungen für die Verhinderung von Geldwäsche und Terrorismusfinanzierung gibt.

1. Bewertung, Kenntnis, Management und Minderung von Risiken

a) Bewertung und Kenntnisse von Risiken

15. Voraussetzung für ein solides Risikomanagement[15] sind das Erkennen und die Analyse von in der Bank vorhandenen Risiken der Geldwäsche und der Terrorismusfinanzierung und die Entwicklung und wirksame Umsetzung von Richtlinien und Verfahren, die den festgestellten Risiken angemessen sind. Bei der Durchführung einer umfassenden Risikobewertung zur Einschätzung der Risiken der Geldwäsche und der Terrorismusfinanzierung sollte eine Bank sämtliche relevanten, damit verbundenen Risikofaktoren sowie die entsprechenden Restrisikofaktoren bezogen auf u.a. das Land[16], den Sektor, die Bank und ihre Geschäftsbeziehungen berücksichtigen, um ihr Risikoprofil und den geeigneten Umfang der anzuwendenden Minderungsmassnahmen zu bestimmen. Die Grundsätze und Verfahren für die Sorgfaltspflichten bei der Annahme von Kunden, der Identifizierung von Kunden und der Überwachung der Geschäftsbeziehungen und der Geschäfte (angebotene Produkte und Dienstleistungen) sind dann so zu

[14] Siehe Grundsatz 29 in *Grundsätze für eine wirksame Bankenaufsicht*, September 2012.

[15] Siehe insbesondere Grundsatz 15 in *Grundsätze für eine wirksame Bankenaufsicht,* September 2012 und Grundsatz 6 in *Principles for enhancing corporate governance*, Oktober 2010.

[16] Gegebenenfalls ist eine Bewertung der Risiken der Geldwäsche und der Terrorismusfinanzierung auf supranationaler Ebene in Erwägung zu ziehen.

gestalten, dass sie die Risikobewertung und das sich daraus ergebende Risikoprofil der Bank berücksichtigen. Eine Bank sollte über geeignete Verfahren für die Dokumentation und Weitergabe von Informationen zu Risikobewertungen an zuständige Behörden, z.B. die Aufsichtsinstanzen, verfügen.

16. Eine Bank sollte über umfassende Kenntnis der Risiken verfügen, die mit ihrem Kundenstamm, ihren Produkten, Vertriebswegen und angebotenen Dienstleistungen (einschl. Produkte in Entwicklung oder Produkte vor der Markteinführung) sowie den Ländern, in denen sie oder ihre Kunden geschäftlich tätig sind, verbunden sind. Spezifische Geschäfts- und Transaktionsdaten und andere von der Bank intern erhobene Informationen, aber auch externe Informationsquellen wie nationale Risikobewertungen und Länderberichte internationaler Organisationen sollten die Grundlage dieser Kenntnis bilden. Richtlinien und Verfahren für die Annahme von Kunden, die Feststellung der Kundenidentität und die laufende Überwachung sind so auszugestalten und umzusetzen, dass die festgestellten inhärenten Risiken angemessen kontrolliert werden können. Eventuell bestehende Restrisiken sollten entsprechend dem sich aus der Risikobewertung ergebenden Risikoprofil der Bank behandelt werden. Diese Bewertung und diese Kenntnisse sollten auf Verlangen der Aufsichtsinstanz der Bank nachgewiesen werden können und sollten von dieser anerkannt werden.

b) Funktionierende Führungsmechanismen

17. Ein wirksames Management der Risiken von Geldwäsche und der Terrorismusfinanzierung setzt geeignete Führungsmechanismen voraus, die in früheren einschlägigen Veröffentlichungen des Ausschusses dargestellt sind.[17] Insbesondere die Anforderung an das oberste Verwaltungsorgan der Bank, die Richtlinien für Risiken, Risikomanagement und Compliance zu genehmigen und zu überwachen, ist im Zusammenhang mit diesen Risiken von grosser Bedeutung. Das oberste Verwaltungsorgan sollte die Risiken im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung genau kennen. Informationen über Bewertungen dieser Risiken sollten dem obersten Verwaltungsorgan zeitnah, vollständig, verständlich und korrekt mitgeteilt werden, damit dieses in der Lage ist, Entscheidungen in Kenntnis der Sachlage zu treffen.

18. Das oberste Verwaltungsorgan sollte explizite Zuständigkeiten unter Berücksichtigung der Führungsstruktur der Bank zuteilen, um sicherzustellen, dass die bankinternen Richtlinien und Verfahren wirksam gehandhabt werden. Das oberste Verwaltungsorgan und die Geschäftsleitung sollten einen entsprechend qualifizierten Chief AML/CFT Officer (Geldwäschebeauftragten) ernennen, der die Gesamtverantwortung für die Funktion Verhinderung von Geldwäsche (AML, Anti-Money Laundering) und Terrorismusfinanzierung (CFT, Countering Financing of Terrorism) trägt; diese leitende Person muss in der Bank über die notwendige Statur und Autorität verfügen, damit von ihr auf den Tisch gebrachte Probleme beim obersten Verwaltungsorgan, bei der Geschäftsleitung und in den Geschäftsbereichen die erforderliche Aufmerksamkeit erhalten.

c) Drei Verteidigungslinien

19. Im Allgemeinen und im Zusammenhang mit den Risiken von Geldwäsche und Terrorismusfinanzierung bilden die Geschäftseinheiten (z.B. Handelsabteilung und Abteilungen mit Kundenkontakt) die erste Verteidigungslinie, die die Aufgabe hat, die Risiken der getätigten Geschäfte zu identifizieren, zu bewerten und zu steuern. Die Mitarbeiter der betreffenden Geschäftseinheiten sollten die Richtlinien und Verfahren kennen und umsetzen; für eine wirksame Umsetzung sollten ausreichend Mittel zur Verfügung stehen. Zur zweiten Verteidigungslinie gehören das für Geldwäsche und Terrorismus verantwortliche Mitglied der Geschäftsleitung (Chief Officer in charge of AML/CFT), die Compliance-Funktion, aber

[17] Siehe insbesondere *The internal audit function in banks*, Juni 2012; *Principles for enhancing corporate governance*, Oktober 2010*; Compliance and the compliance function in banks*, April 2005.

auch die Bereiche Personalmanagement oder Technologie. Die dritte Verteidigungslinie bildet die Funktion Interne Revision.

20. Richtlinien und Verfahren sind Teil **der ersten Verteidigungslinie** und sollten klar definiert sein, in schriftlicher Form vorliegen und allen Mitarbeitern bekannt gemacht werden. Sie sollten eine klare Beschreibung der für Mitarbeiter geltenden Pflichten und Vorschriften enthalten sowie Anweisungen und Leitlinien dazu, wie sichergestellt ist, dass im Rahmen der Geschäftstätigkeit der Bank geltende Vorschriften eingehalten werden. Es sollten interne Verfahren bestehen, die es ermöglichen, verdächtige Transaktionen festzustellen und zu melden.

21. Eine Bank sollte über angemessene Grundsätze und Verfahren für die Überprüfung neuer und bestehender Mitarbeiter verfügen, um die Einhaltung hoher ethischer Standards und Berufsstandsregeln zu gewährleisten. Alle Banken sollten ihre Mitarbeiter laufend aus- und fortbilden, damit diese fähig sind, die Richtlinien und Verfahren für die Verhinderung von Geldwäsche und Terrorismusfinanzierung umzusetzen. Zeitpunkt und Inhalt der Bildungsmassnahmen für die verschiedenen Mitarbeitergruppen sind, ausgehend vom jeweiligen Bedarf und dem Risikoprofil der Bank, entsprechend anzupassen. Der Fortbildungsbedarf wird unterschiedlich sein und von der bankinternen Funktion, der Zuständigkeit und der Dauer der Betriebszugehörigkeit der betreffenden Person abhängen. Die Durchführung der Fortbildungskurse und die verwendeten Materialien sollten auf die besonderen Zuständigkeiten bzw. Funktionen des Mitarbeiters zugeschnitten sein, damit sichergestellt ist, dass der Mitarbeiter über ausreichend Kenntnisse und Informationen verfügt, um die Richtlinien und Verfahren der Bank zur Verhinderung von Geldwäsche und Terrorismusfinanzierung wirksam umsetzen zu können. Aus diesen Gründen sollten neu eingestellte Mitarbeiter so bald wie möglich nach der Einstellung an einer Fortbildungsmassnahme teilnehmen. Im Rahmen von Auffrischungslehrgängen sollten die Mitarbeiter an ihre Pflichten erinnert und ihr Wissen und ihre Sachkenntnisse auf den letzten Stand gebracht werden. Umfang und Häufigkeit derartiger Ausbildungsprogramme sollten auf die Risikofaktoren, denen die Mitarbeiter im Rahmen ihrer Zuständigkeiten ausgesetzt sind, und auf die Art und Höhe der bankinternen Risiken zugeschnitten sein.

22. Als Teil **der zweiten Verteidigungslinie** sollte das für Geldwäsche und Terrorismusbekämpfung zuständige Mitglied der Geschäftsleitung (Chief Officer in charge of AML/CFT) für die laufende Überwachung der Einhaltung sämtlicher einschlägiger Auflagen der Bank verantwortlich sein. Dazu gehören Stichproben-Compliance-Kontrollen und die Prüfung von Meldungen über Abweichungen an die Geschäftsleitung bzw. das oberste Verwaltungsorgan, wenn anzunehmen ist, dass das Management mit den Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung nicht verantwortungsvoll umgeht. Der Chief AML/CFT Officer sollte für alle Angelegenheiten, die mit Geldwäsche und Terrorismusbekämpfung zu tun haben, der Ansprechpartner für interne und externe Stellen sein, einschl. der Aufsichtsinstanzen oder der FIU.

23. Die Geschäftsinteressen einer Bank sollten auf keinen Fall im Widerspruch zu einer wirksamen Ausübung der oben genannten Zuständigkeiten des Chief AML/CFT-Officers stehen. Unabhängig von der Grösse der Bank oder ihrer Führungsstruktur sollten potenzielle Interessenkonflikte vermieden werden. Um neutrale Beurteilungen und eine unparteiische Beratung des Managements zu ermöglichen, sollte der AML/CFT-Officer deshalb z.B. keine Führungsverantwortung in einem Geschäftsbereich haben und sollte nicht mit Aufgaben betraut werden, die mit dem Datenschutz oder der Funktion Interne Revision zu tun haben. Für Fälle von Konflikten zwischen den Geschäftsbereichen und den Zuständigkeiten des AML/CFT-Officers sollten Regelungen bestehen, die gewährleisten, dass Aspekte der Verhinderung von Geldwäsche und Terrorismusfinanzierung auf höchster Ebene objektiv berücksichtigt werden.

24. Der Chief AML/CFT-Officer kann daneben noch mit der Funktion des Chief Risk Officers oder des Chief Compliance Officers oder ähnlichen Aufgaben betraut werden. Diese Person sollte direkt an die Geschäftsleitung oder das oberste Verwaltungsorgan berichten. Im Falle getrennter Zuständigkeiten müssen die Beziehungen zwischen den oben genannten Chief Officers bzw. deren jeweilige Rollen klar definiert und verstanden werden.

25. Der Chief AML/CFT-Officer sollte auch für die Meldung verdächtiger Transaktionen verantwortlich sein. Der Chief AML/CFT-Officer sollte über ausreichend Ressourcen verfügen, um sämtliche ihm übertragenen Aufgaben wirksam ausführen und im bankinternen System zur Verhinderung von Geldwäsche und Terrorismusfinanzierung eine zentrale und proaktive Rolle spielen zu können. Die Voraussetzung dafür ist, dass die Person mit diesem vollständig vertraut ist; das Gleiche gilt in Bezug auf gesetzliche und aufsichtliche Anforderungen sowie für die mit den Geschäften der Bank verbundenen Risiken von Geldwäsche und Terrorismusfinanzierung.

26. **Die interne Revision, die dritte Verteidigungslinie,** spielt im Hinblick auf eine unabhängige Bewertung des Risikomanagements und des Kontrollsystems eine wichtige Rolle; sie bewertet regelmässig die Wirksamkeit der Richtlinien und Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung und berichtet darüber an den Revisionsausschuss des obersten Verwaltungsorgans oder an eine vergleichbare Überwachungsinstanz. Eine Bank sollte über Richtlinien für die Durchführung von Prüfungen der internen Revision hinsichtlich folgender Aspekte verfügen: i) Angemessenheit der bankinternen Richtlinien und Verfahren für identifizierte Risiken; ii) Wirksamkeit der Umsetzung der Richtlinien und Verfahren durch die Mitarbeiter der Bank; iii) Wirksamkeit der Kontrolle der Einhaltung der Vorschriften und der Qualitätskontrolle, einschl. der Kriterien für das Auslösen automatischer Warnmeldungen; iv) Effizienz der bankinternen Aus- und Fortbildung für bestimmte Mitarbeiter. Die Geschäftsleitung stellt sicher, dass die Revisionsfunktion durch Mitarbeiter wahrgenommen wird, die über das entsprechende Fachwissen und über eine angemessene Erfahrung verfügen, um solche Prüfungen durchzuführen. Weiter stellt sie sicher, dass der Prüfungsumfang und die Prüfungsmethode dem Risikoprofil der Bank entsprechen und dass die Frequenz solcher Prüfungen ebenfalls ausgehend vom Risiko bestimmt wird. In regelmässigen Abständen sollte die interne Revision bankweit die Massnahmen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung prüfen. Darüber hinaus sollte die interne Revision die Prüfungsfeststellungen und -empfehlungen proaktiv weiterverfolgen.[18] In der Regel sollten die Prüfverfahren dem allgemeinen Prüfmandat der internen Revision entsprechen, vorbehaltlich bestimmter vorgeschriebener Prüfungsanforderungen für Massnahmen in den Bereichen Geldwäsche und Terrorismusfinanzierung.

27. In vielen Ländern spielen auch **externe Revisoren** eine wichtige Rolle, wenn es darum geht, die internen Kontrollen und Verfahren von Banken im Zusammenhang mit Abschlussprüfungen zu bewerten und zu prüfen, ob diese den Richtlinien zur Verhinderung von Geldwäsche und Terrorismusfinanzierung und der aufsichtlichen Praxis entsprechen. Falls Banken zur Bewertung der Effizienz ihrer Richtlinien und Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung auf externe Prüfer zurückgreifen, sollte sichergestellt sein, dass der Prüfungsumfang die bei der Bank gegebenen Risiken abdeckt und dass die mit der Durchführung beauftragten Prüfer über das notwendige Fachwissen und die erforderliche Erfahrung verfügen. Eine Bank sollte ferner sicherstellen, dass sie derartige Einsätze angemessen beaufsichtigt.

d) Angemessenes Transaktionsüberwachungssystem

28. Eine Bank sollte über ein Überwachungssystem verfügen, das ihrer Grösse, ihren Aktivitäten und ihrer Komplexität sowie den in der Bank gegebenen Risiken angemessen ist. Bei den meisten Banken, insbesondere bei international tätigen, dürfte davon auszugehen sein, dass eine wirksame Überwachung die Automatisierung des Überwachungsprozesses erforderlich macht. Ist die Bank der Auffassung, dass ein IT-Überwachungssystem für ihre spezifische Situation nicht notwendig ist, sollte sie diese Entscheidung dokumentieren und in der Lage sein, ihrer Aufsichtsinstanz oder externen Revisoren nachzuweisen, dass die Bank über eine wirksame Alternative verfügt. Bei Verwendung eines IT-Systems sollte dieses

[18] Siehe BCBS, *The internal audit function in banks*, Juni 2012.

sämtliche Konten und Transaktionen der Kunden der Bank – zugunsten bzw. im Auftrag dieser Kunden – erfassen. Dieses System muss es der Bank ermöglichen, Trendanalysen der Transaktionsaktivitäten zu erstellen und ungewöhnliche Geschäftsbeziehungen und Transaktionen zu identifizieren, um Geldwäsche oder Terrorismusfinanzierung zu verhindern.

29. Im Einzelnen sollte dieses System der Geschäftsleitung korrekte Informationen zu mehreren wichtigen Aspekten liefern, einschl. Änderungen des Transaktionsprofils von Kunden. Bei der Erstellung des Kundenprofils sollte die Bank die aktualisierten, vollständigen und korrekten Informationen verwenden, die der Kunde im Rahmen der Feststellung der Kundenidentität angegeben hat. Das IT-System sollte es der Bank und gegebenenfalls dem Bankkonzern erlauben, sich nach bestimmten Kriterien (d.h. nach Kunden, Produkten, Geschäftseinheiten, Transaktionen innerhalb eines gewissen Zeitraums usw.) geordnete Informationen zu verschaffen. Auch ohne die Verpflichtung, ein einheitliches Kundenbestandsverzeichis zu führen, sollten die Banken in der Lage sein, ihre Kunden Risikogruppen zuzuordnen und bei Warnmeldungen unter Verwendung sämtlicher ihr zur Verfügung stehenden Informationen zu reagieren. Ein IT-Überwachungssystem muss geeignete Parameter verwenden, die von nationalen und internationalen Erfahrungen mit den Methoden der Geldwäsche und Terrorismusfinanzierung und deren Prävention ausgehen. Eine Bank kann die Standardparameter des Entwicklers des IT-Überwachungssystems verwenden; die verwendeten Parameter müssen aber die bankspezifische Risikosituation abbilden und berücksichtigen.

30. Das IT-Überwachungssystem sollte es einer Bank erlauben, eigene Kriterien für zusätzliche Überwachungsmassnahmen, die Meldung verdächtiger Transaktionen oder andere Massnahmen zur Minderung von Risiken festzulegen. Der Chief AML/CFT Officer sollte Zugang zum IT-System haben und dieses nutzen können, soweit dies für seine Funktion relevant ist (selbst dann, wenn das System von anderen Geschäftsbereichen verwaltet oder verwendet wird). Die Parameter des IT-Systems sollten es zulassen, dass bei ungewöhnlichen Transaktionen Warnmeldungen generiert werden, die in der Folge durch den Chief AML/CFL-Officer auszuwerten sind. Sämtliche in diesem Zusammenhang verwendeten Risikokriterien sollten der Risikobewertung der Bank entsprechen.

31. Um sicherzustellen, dass das IT-System angemessen ist und in der ersten und zweiten Verteidigungslinie wirksam eingesetzt werden kann, sollte auch die interne Revision das System prüfen.

2. Richtlinien für die Annahme von Kunden

32. Eine Bank sollte klare Richtlinien und Verfahren für die Annahme von Kunden und die Identifikation von Kundentypen, die aufgrund der Risikobewertung der Bank bezüglich Geldwäsche und Terrorismusfinanzierung ein höheres Risiko darstellen dürften, entwickeln und umsetzen.[19] Im Zuge der Risikoeinschätzung berücksichtigt eine Bank bei der Bestimmung des Gesamtrisikos und der geeigneten Massnahmen zum Management dieser Risiken die Faktoren, die für die jeweilige Situation von Bedeutung sind, wie Hintergrund des Kunden, berufliche Tätigkeit (einschl. öffentliche Ämter oder hochrangige Stellung), Herkunft des Einkommens und Vermögens, Herkunftsland und Wohnsitz (falls nicht identisch), genutzte Produkte, Art und Zweck der Konten, verbundene Konten, Geschäftstätigkeit und andere kundenbezogene Risikoindikatoren.

33. Derartige Richtlinien und Verfahren sollten elementare Sorgfaltspflichten für alle Kunden vorsehen sowie Sorgfaltspflichten, die den unterschiedlichen Risiken von Kunden Rechnung tragen. Für Situationen mit nachweislich geringeren Risiken können vereinfachte Massnahmen zulässig sein, soweit

[19] Die FATF-Empfehlungen enthalten ebenfalls nützliche Hinweise dazu, wie die Bank einen risikobasierten Ansatz wirksam umsetzen kann (s. insbesondere Empfehlung 1).

dies gesetzlich erlaubt ist. Im Falle einer Einzelperson, die ein Bankkonto einrichten möchte, um als Privatkunde geringe Beträge zu halten und kleinere Routinegeschäfte abzuwickeln, dürfte z.B. die Anwendung von Standardverfahren für die Eröffnung von Konten angemessen sein. Es ist wichtig, dass die Regeln für die Annahme von Kunden nicht so restriktiv gehandhabt werden, dass der Allgemeinheit dadurch die Inanspruchnahme von Bankdienstleistungen verwehrt wird, vor allem finanziell oder sozial benachteiligten Personen. Die FATF *Financial Inclusion Guidance*[20] enthalten nützliche Hinweise für die Gestaltung von Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung, die für finanziell oder sozial Benachteiligte nicht übermässig restriktiv sind.

34. Im Falle höherer Risiken sollten Banken verstärkte Massnahmen treffen, um diese Risiken zu mindern und zu steuern. Erhöhte Sorgfalt kann bei einer Einzelperson angezeigt sein, die beabsichtigt, grössere Beträge auf dem Konto zu halten, und die regelmässig am grenzüberschreitenden elektronischen Zahlungsverkehr teilnimmt, oder bei jemandem, der als politisch exponierte Person (PEP) zu betrachten ist. Erhöhte Sorgfalt ist insbesondere bei ausländischen PEP angezeigt. Entscheidungen in Bezug auf die Aufnahme bzw. die Fortführung von Geschäftsbeziehungen mit Kunden mit höherem Risiko sollten unter Ansatz verstärkter Sorgfaltspflichten – wie Genehmigung der Aufnahme bzw. Fortführung der Beziehung durch die Geschäftsleitung – getroffen werden. In den Richtlinien der Bank für die Annahme von Kunden sollten auch die Umstände festgelegt sein, unter denen die Bank nicht bereit ist, eine neue Geschäftsbeziehung zu begründen bzw. eine bestehende fortzuführen.

3. Identifizierung und Überprüfung von Kunden und wirtschaftlich Berechtigten, Erstellen von Risikoprofilen

35. Für den Zweck dieses Leitlinienpapiers bezieht sich der Begriff „Kunde" entsprechend der FATF-Empfehlung 10 auf jede Person[21], die in Geschäftsbeziehungen mit einer Bank eintritt oder die gelegentlich Finanztransaktionen bei der Bank tätigt. Die Vorschriften für die Feststellung der Kundenidentität sollten nicht nur für Kunden gelten, sondern auch für Personen, die in ihrem Auftrag handeln, sowie für wirtschaftlich Berechtigte[22]. Entsprechend den FATF-Standards sollten Banken die Identität ihrer Kunden feststellen und überprüfen.[23]

36. Eine Bank sollte über ein systematisches Verfahren zur Identifizierung und Überprüfung der Kunden der Bank und gegebenenfalls der Personen, die im Auftrag von Kunden handeln, und des/der wirtschaftlich Berechtigten verfügen. Im Allgemeinen sollte eine Bank keine Bankgeschäftsbeziehungen begründen oder Transaktionen durchführen, solange die Identität des Kunden nicht entsprechend der FATF-Empfehlung 10 zufriedenstellend festgestellt und überprüft worden ist. Die Verfahren sollten nach

[20] Siehe FATF, *Guidance on Anti-Money Laundering and Terrorist Financing and Financial Inclusion*, Februar 2013, verfügbar auf http://www.fatf-gafi.org/topics/financialinclusion/.

[21] Der Begriff „Person" bezieht sich hier auf natürliche und juristische Personen oder Rechtsgestaltungen.

[22] Der Begriff „wirtschaftlich Berechtigter" wird hier entsprechend der Definition und den Erläuterungen in den FATF-Standards verwendet. Zur Erinnerung: Die FATF definiert „wirtschaftlich Berechtigter" als eine oder mehre natürliche Personen, in deren Eigentum oder unter deren Kontrolle der Kunde letztlich steht, und/oder eine natürliche Person, auf deren Veranlassung eine Transaktion letztendlich durchgeführt wird. Dazu gehören auch die Personen, die letztlich die effektive Kontrolle über eine juristische Person oder Rechtsgestaltung innehaben.

[23] Siehe Auslegungshinweis zur FATF-Empfehlung 1. Diese Anforderung gilt nur insofern, als das Land nicht im Zuge einer Risikobewertung festgestellt hat, dass bestimmte Arten von Aktivitäten (und mit diesen verbundene Kunden) in begrenztem Umfang ausgenommen werden können, weil gem. Auslegungshinweis zu Empfehlung 1 ein nachweislich geringes Geldwäsche- und Terrorismusfinanzierungsrisiko besteht.

dem Basler Grundsatz 29[24] und den FATF-Standards auch beinhalten, dass zumutbare Massnahmen ergriffen werden, um die Identität des wirtschaftlich Berechtigten zu überprüfen. Ferner sollte eine Bank überprüfen, ob Personen, die im Namen von Kunden handeln, tatsächlich dazu berechtigt sind, und sollten die Identität dieser Personen überprüfen.

37. Die Identität der Kunden, der wirtschaftlich Berechtigten und der in ihrem Namen handelnden Personen ist anhand von verlässlichen, unabhängigen Ausgangsdokumenten, Daten und Informationen zu überprüfen. Bei der Verwendung von Dokumenten sollte sich eine Bank im Klaren sein, dass die für eine Überprüfung der Identität am besten geeigneten Dokumente diejenigen sind, die am schwierigsten auf illegalem Weg zu bekommen bzw. zu fälschen sind. Werden andere Quellen als Dokumente herangezogen, muss die Bank sicherstellen, dass die Methoden der Informationsbeschaffung (dazu können gehören: Rücksprache bei anderen Finanzinstituten, Vorlage von Jahresabschlüssen) und die Informationsquellen geeignet sind und den bankinternen Richtlinien und Verfahren sowie dem Risikoprofil des Kunden entsprechen. Eine Bank kann von ihren Kunden eine schriftliche Erklärung verlangen, aus der sich die Identität und nähere Angaben zum wirtschaftlich Berechtigten ergeben; allerdings sollte sich die Bank nicht ausschliesslich auf derartige Erklärungen verlassen. Wie bei sämtlichen Aspekten im Zusammenhang mit der Feststellung und Überprüfung der Kundenidentität sollte eine Bank auch bei der Festlegung des Umfangs der zur Einhaltung der Sorgfaltspflichten notwendigen Massnahmen die Art und die Höhe des Risikos, das ein Kunde darstellt, berücksichtigen.[25] Auf keinen Fall sollte eine Bank von ihren Massnahmen zur Kundenidentifizierung und -überprüfung absehen, nur weil der Kunde nicht in der Lage ist, zu einem persönlichen Gespräch in die Bank zu kommen (Fernkunden). Die Bank sollte auch diese Risikofaktoren prüfen: Warum möchte der Kunde weit entfernt von seinem Wohnsitz/Gesellschaftssitz ein Konto – und dann noch im Ausland – eröffnen? Zu berücksichtigen sind auch die einschlägigen Risiken im Zusammenhang mit Kunden aus Ländern, die für ihre strategischen Defizite bei der Verhinderung von Geldwäsche und Terrorismusfinanzierung bekannt sind, und die Sorgfaltspflichten sind zu verschärfen, wenn dies die FATF, andere internationale Gremien oder nationale Behörden verlangen.

38. Auch wenn das Verfahren zur Identifizierung und Überprüfung der Kunden bei Beginn der Geschäftsbeziehung oder vor der Durchführung gelegentlicher Transaktionen anzuwenden ist, sollte eine Bank diese Informationen nutzen, um sich ein Bild vom Profil und Verhalten des Kunden zu machen. Der Zweck der Beziehung oder der gelegentlich vorgenommenen Bankgeschäfte, die Höhe des Vermögens oder der Umfang der Transaktionen und die Regelmässigkeit oder die Dauer der Beziehung sind Beispiele von Informationen, die in der Regel erfasst werden. Deshalb sollte es in einer Bank auch Richtlinien und Verfahren zur Identifizierung und Überprüfung von Kunden geben, die es ermöglichen, Risikoprofile von Kunden – entweder für bestimmte Kunden oder für Kundenkategorien – zu erstellen. Was zu diesem Zweck an Informationen zu sammeln ist, sollte von der Höhe der mit dem Geschäftsmodell und den Aktivitäten des Kunden verbundenen Risiken sowie den vom Kunden nachgefragten Produkten oder Dienstleistungen abhängen. Diese Risikoprofile erleichtern die Identifizierung von Kontenbewegungen, die von Aktivitäten oder Verhaltensweisen, die für einen bestimmten Kunden oder eine bestimmte Kundenkategorie „normal" sind, abweichen und die als ungewöhnlich oder sogar als verdächtig eingestuft werden könnten. Risikoprofile von Kunden sind für eine Bank hilfreich, wenn es darum geht zu entscheiden, ob ein Kunde oder eine Kundenkategorie ein höheres Risiko aufweist, das die Anwendung verstärkter Sorgfaltspflichten erforderlich macht. In den Risikoprofilen sollte sich auch das Wissen der Bank über den beabsichtigten Zweck und die Art der Geschäftsbeziehung bzw. der gelegentlichen Banktransaktionen, der erwartete Umfang der Aktivitäten, die Art der Transaktionen und

[24] Siehe Grundsatz 29, zentrales Kriterium 5. b) in *Grundsätze für eine wirksame Bankenaufsicht*, September 2012.

[25] Siehe Weltbank, *Politically Exposed Persons, Preventive Measures for the Banking Sector,* 2010.

gegebenenfalls die Herkunft der Mittel, des Einkommens oder Vermögens und andere ähnliche Aspekte niederschlagen. Wichtige Informationen betreffend die Aktivitäten oder das Verhalten von Kunden sollten zur Aktualisierung der Risikobewertung des Kunden verwendet werden.

39. Eine Bank sollte vom Kunden ein Ausweispapier verlangen sowie jegliche Informationen und Unterlagen einholen, die im Zuge der Feststellung und Überprüfung der Kundenidentität anfallen. Dazu können gehören: Kopien oder Aufzeichnungen amtlicher Dokumente (z.B. Pass, Personalausweis/Identitätskarte, Führerschein), Kontounterlagen (z.B. Aufzeichnungen von Finanztransaktionen) und Geschäftskorrespondenz, einschl. Ergebnisse durchgeführter Prüfungen wie Risikobewertungen und Nachforschungen zur Ermittlung des Hintergrunds und Zwecks der Geschäftsbeziehung bzw. der Aktivitäten.

40. Eine Bank sollte auch sämtliche Informationen einholen, die notwendig sind, um die Identität ihrer Kunden, die Identität der im Namen der Kunden handelnden Vertreter und die Identität der wirtschaftlich Berechtigten zu ihrer vollen Zufriedenheit feststellen zu können. Während eine Bank verpflichtet ist, die Identität ihrer Kunden festzustellen und zu überprüfen, hängen Art und Umfang der für eine Überprüfung notwendigen Informationen von einer Risikobewertung ab, bei der die Art des Antragstellers (Einzelperson, Unternehmen usw.), das erwartete Kontovolumen und die erwartete Verwendung des Kontos Berücksichtigung finden. Die spezifischen Pflichten hinsichtlich der Feststellung der Identität natürlicher Personen sind gewöhnlich im Landesrecht geregelt. Bei Kunden mit höheren Risiken gelten für die Überprüfung der Identität verstärkte Sorgfaltspflichten. Bei Vorliegen einer komplexen Beziehung oder bei einem erheblichen Kontovolumen kann es ratsam sein, zusätzliche Identifizierungsmassnahmen zu treffen; dabei sollte von der Höhe des Gesamtrisikos ausgegangen werden.

41. Ist die Bank nicht in der Lage, die Massnahmen zur Identifizierung von Kunden abzuschliessen, sollte das Konto nicht eröffnet, die Geschäftsbeziehung nicht aufgenommen bzw. die Transaktion nicht durchgeführt werden. Es kann jedoch Umstände geben, unter denen es zulässig ist, die Überprüfung nach Aufnahme der Geschäftsbeziehung abzuschliessen, weil es wesentlich ist, die Abwicklung normaler Geschäftsvorgänge nicht zu unterbrechen. Für solche Fälle sollte die Bank über angemessene Verfahrensregelungen des Risikomanagements verfügen, in denen festgelegt ist, unter welchen Bedingungen und mit welchen Einschränkungen ein Kunde die Geschäftsbeziehung zur Bank vor Abschluss der Überprüfung nutzen kann. In Fällen, in denen sich nach der Kontoeröffnung bei der Aufnahme der Geschäftsbeziehungen nicht zu lösende Schwierigkeiten hinsichtlich der Identitätsüberprüfung ergeben, sollte die Bank das Konto schliessen oder den Zugang dazu sperren. Auf jeden Fall sollte die Bank prüfen, ob im Zusammenhang mit Problemen beim Abschluss der Überprüfungen zur Feststellung der Identität nicht eine Verdachtsmeldung erfolgen sollte.[26] Ergeben sich bei Identitätsprüfungen darüber hinaus Verdachtsmomente bzw. vertretbare Gründe für die Annahme, dass die Vermögenswerte oder die finanziellen Mittel des potenziellen Kunden aus den Erträgen aus Vortaten und Straftaten in Verbindung mit Geldwäsche und Terrorismusfinanzierung stammen, sollten Banken von sich aus für diese Kunden keine Konten eröffnen. In diesen Fällen sollten Banken den zuständigen Stellen eine entsprechende Verdachtsmeldung machen und dabei sicherstellen, dass der Kunde keine Kenntnis davon erhält – auch nicht mittelbar – , dass eine solche Meldung erfolgt ist, gerade erfolgt bzw. erfolgen wird.

42. Eine Bank sollte über Verfahren und materielle Kapazitäten verfügen, die es den Mitarbeitern in der Handelsabteilung und den Mitarbeitern mit Kundenkontakt ermöglichen, benannte Organisationen oder Einzelpersonen (z.B. Terroristen, Terrororganisationen) entsprechend den nationalen gesetzlichen

[26] Vorbehaltlich einzelstaatlicher gesetzlicher Regelungen zum Vorgehen bei verdächtigen Transaktionen.

Bestimmungen und den einschlägigen Entschliessungen des Sicherheitsrats der Vereinten Nationen zu identifizieren.

43. Beim Transfer von Mitteln von einem auf den Namen des Inhabers lautenden Kontos bei einer anderen Bank, für die die gleichen Auflagen für die Feststellung der Identität gelten, dürfte eine gewisse Sicherheit gegeben sein, doch sollten Banken trotzdem eigene Sorgfaltspflichten ausüben und prüfen, ob nicht der vorherige Kundenbetreuer veranlasst hat, das Konto aufgrund von Bedenken wegen illegaler Aktivitäten zu schliessen. Selbstverständlich haben Kunden das Recht, ihre Geschäfte von einer Bank auf eine andere zu übertragen. Wenn eine Bank jedoch Grund zur Annahme hat, dass der Antrag einer Person auf Eröffnung eines Bankkontos von einer anderen Bank aufgrund von Bedenken wegen illegaler Aktivitäten des Kunden abgelehnt worden ist, sollte sie prüfen, ob dieser Antragsteller nicht ein höheres Risiko darstellt und verschärfte Sorgfaltspflichten anzuwenden sind, ob eine Verdachtsmeldung erfolgen soll und/oder ob der Kunde nach den eigenen Risikobewertungen und Risikoverfahren abzulehnen ist.

44. Eine Bank sollte für Kunden, die auf Anonymität bestehen oder einen offensichtlich falschen Namen angeben, keine Konten eröffnen oder Geschäftsbeziehungen unterhalten. Auch vertrauliche Nummernkonten[27] sollten nicht als anonyme Konten geführt werden; für sie gelten genau dieselben Sorgfaltspflichten wie für alle anderen Kundenkonten, selbst dann, wenn diese Verfahren von ausgewählten Mitarbeitern durchgeführt werden. Ein Nummernkonto darf den Kontoinhaber zwar ein Mehr an Vertraulichkeit bieten, doch muss seine Identität von der Bank überprüft werden und einer ausreichenden Zahl von Mitarbeitern bekannt sein, um der Sorgfaltspflicht wirksam nachzukommen, insbesondere wenn weitere Risikofaktoren darauf hindeuten, dass der Kunde ein höheres Risiko darstellt. Eine Bank sollte gewährleisten, dass die Funktionen Interne Kontrolle, Compliance, Revision und Überwachung, insbesondere der Chief AML/CFT-Officer und die Aufsichtsinstanz der Bank bei Bedarf uneingeschränkten Zugang zu diesen Informationen haben.

4. Laufende Überwachung

45. Die laufende Überwachung ist ein wesentliches Merkmal eines wirksamen und soliden Managements der Risiken von Geldwäsche und Terrorismusfinanzierung. Eine Bank kann ihre Risiken nur wirksam steuern, wenn sie ein Bild von den normalen und angemessenen Bankgeschäften ihrer Kunden hat, das es ihr ermöglicht, Transaktionsversuche und ungewöhnliche Transaktionen zu erkennen, die vom üblichen Muster abweichen. Sind derartige Kenntnisse nicht vorhanden, dürfte die Bank ihrer Pflicht, verdächtige Transaktionen zu identifizieren und den zuständigen Stellen zu melden, nicht nachkommen können. Alle Geschäftsbeziehungen und Transaktionen sind laufend zu überwachen, doch der Umfang der Überwachung sollte von den Risiken ausgehen, die der Risikobewertung der Bank und ihren Massnahmen im Rahmen der Sorgfaltspflichten zugrunde liegen. Für Kunden bzw. Transaktionen mit höheren Risiken ist eine verstärkte Überwachung durchzuführen. Eine Bank sollte nicht nur ihre Kunden und deren Transaktionen überwachen, sondern sollte auch eine querschnittsbezogene Überwachung von Produkten bzw. Dienstleistungen vornehmen, um sich abzeichnende Risikomuster erkennen und mindern zu können.

46. Alle Banken sollten über Systeme verfügen, mit deren Hilfe ungewöhnliche oder verdächtige Transaktionen bzw. Muster erkannt werden können. Bei der Entwicklung von Szenarien zur Identifizierung derartiger Aktivitäten ist das Risikoprofil des Kunden zu berücksichtigen, das auf der Grundlage der Risikobewertung der Bank sowie unter Verwendung von Informationen, die im Zuge der Feststellung der Kundenidentität gesammelt worden sind, und anderen Informationen von Strafverfolgungsbehörden

[27] Bei einem Nummernkonto kennt die Bank die Namen des Kunden und des wirtschaftlich Berechtigten; die Namen werden aber danach in den Unterlagen durch eine Kontonummer oder einen Codenamen ersetzt.

oder anderen öffentlichen Stellen im Land der Bank erstellt worden ist. Eine Bank hat z.B. Kenntnis von bestimmten Methoden oder von Vorkehrungen zum Waschen von Erträgen aus Straftaten, die von den Behörden im Land der Bank festgestellt worden sind. Im Rahmen ihrer Risikobewertung schätzt die Bank dann ein, wie gross das Risiko ist, dass Aktivitäten in Verbindung mit derartigen Methoden oder Vorkehrungen innerhalb der Bank bei einer bestimmten Kategorie von Kunden, Kontengruppen, Transaktionsmustern oder Produktverwendungen vorkommen. Ausgehend von diesem Wissen sollte die Bank geeignete Überwachungs- und Kontrollinstrumente entwickeln und anwenden, mit denen derartige Aktivitäten ausgemacht werden können. Beispiele hierfür sind die Verwendung computergestützter Überwachungssysteme mit Schnellwarnfunktion oder die Festlegung von Grenzwerten für eine bestimmte Klasse oder Kategorie von Aktivitäten.

47. Unter Verwendung der im Zuge der Sorgfaltspflichten gewonnen Informationen sollte eine Bank in der Lage sein, Transaktionen zu bestimmen, die wirtschaftlich nicht sinnvoll erscheinen, die grosse Bareinzahlungen beinhalten oder die nicht mit den üblichen und erwarteten Transaktionen des Kunden übereinstimmen.

48. Eine Bank sollte für Kunden, die von der Bank als Kunden mit höheren Risiken eingestuft worden sind, über verstärkte Sorgfaltspflichten verfügen. Zusätzlich zu den bestehenden Richtlinien und Verfahren für die Genehmigung von Konteneröffnungen sollte eine Bank auch über besondere Richtlinien hinsichtlich der Art und des Umfangs der Massnahmen zur vorgeschriebenen Feststellung der Kundenidentität verfügen; das Gleiche gilt in Bezug auf die Häufigkeit von laufenden Kontoüberwachungen und Aktualisierungen der Informationen zur Kundenidentität und anderen Daten. Die Fähigkeit der Bank, verdächtige Aktivitäten wirksam festzustellen und zu überwachen, setzt den Zugang zu aktuellen, umfassenden und korrekten Kundenprofilen und Kundendaten voraus.

49. Eine Bank sollte sicherstellen, dass geeignete integrierte Management-Informationssysteme bestehen, die der Grösse der Bank, ihrer Organisationsstruktur oder Komplexität angemessen sind, auf dem Wesentlichkeitsprinzip und den Risiken basieren und die den Geschäftseinheiten (d.h. den Kundenbetreuern) und den Risiko- und Compliance-Beauftragten (einschl. Mitarbeiter der Kundenprüfung) zeitnah die Informationen zur Verfügung stellen, die für eine Identifizierung, Analyse und wirksame Überwachung der Kundenkonten notwendig sind. Die verwendeten Systeme und die verfügbaren Informationen sollten die Überwachung der Kundenbeziehungen geschäftsbereichsübergreifend erleichtern und sämtliche Informationen über diese Kundenbeziehung beinhalten, einschl. Transaktionsverlauf, fehlende Kontoeröffnungsunterlagen sowie wesentliche Veränderungen im Kundenverhalten oder Geschäftsprofil und ungewöhnliche Transaktionen auf einem Kundenkonto.

50. Bei Änderungen der Sanktionslisten sollte die Bank ihre Kundendatenbank(en) überprüfen. Die Bank sollte ihre Kundendatenbank(en) auch regelmässig auf ausländische PEP und andere risikoreiche Konten überprüfen und für diese verstärkte Sorgfaltspflichtverfahren in Ansatz bringen.

5. Umgang mit den Informationen

a) Aufzeichnen und Aufbewahren von Unterlagen

51. Eine Bank sollte sicherstellen, dass sämtliche im Zusammenhang mit der Feststellung der Kundenidentität eingeholten Informationen aufgezeichnet werden. Dazu gehören i) die Aufzeichnung der Dokumente, die der Bank bei der Überprüfung der Kundenidentität bzw. der Identität des wirtschaftlich Berechtigten vorgelegt werden, und ii) das Übertragen der relevanten Identitätsdaten dieser Dokumente in das bankeigene IT-System; Entsprechendes gilt für anderweitig gewonnene Daten.

52. Eine Bank sollte ferner klare Regelungen zur Aufbewahrungspflicht von Aufzeichnungen erstellen und anwenden, die dem Nachweis der erfüllten Sorgfaltspflicht betreffend Kunden und einzelne Transaktionen dienen. Diese Regelungen sollten soweit möglich Vorschriften zum Datenschutz berücksichtigen. Zu definieren ist dabei, welche Arten von Informationen und Dokumentationen aufzubewahren sind. Darüber hinaus ist die Dauer der Aufbewahrung festzulegen; die Aufbewahrungsfrist sollte

mindestens fünf Jahre nach Beendigung der Geschäftsbeziehung bzw. der gelegentlichen Transaktion betragen.[28] Auch wenn Konten geschlossen werden, sind bei laufenden Untersuchungen bzw. Streitfällen sämtliche Aufzeichnungen bis zum Abschluss des Falls aufzubewahren. Vollständige und aktuelle Aufzeichnungen sind für eine Bank von wesentlicher Bedeutung und sind Voraussetzung für eine angemessene Überwachung der Kundenbeziehung, das Verständnis der laufenden Geschäfte und Aktivitäten von Kunden und – falls notwendig – für das Anlegen eines Prüfungspfads im Fall von Streitigkeiten, Gerichtsverfahren oder Untersuchungen bzw. Ermittlungen, die zu aufsichtsrechtlichen Massnahmen oder zu einer Strafverfolgung führen könnten.

53. Der Bewertungsprozess im Rahmen der laufenden Überwachung und Überprüfung sowie die sich dabei ergebenden Feststellungen sind angemessenen zu dokumentieren und aufzuzeichnen; diese Aufzeichnungen helfen dabei, den Nachweis zu erbringen, dass die Bank ihre Sorgfaltspflichten erfüllt hat und in der Lage ist, die Risiken von Geldwäsche und Terrorismusfinanzierung zu steuern.

b) Aktualisierung der Informationen

54. Nur wenn Banken durch regelmässige Überprüfungen der bestehenden Aufzeichnungen und durch Aktualisierungen der Identitätsdaten sicherstellen, dass die Aufzeichnungen korrekt, aktuell und zweckdienlich sind, können andere zuständige Behörden, Vollzugsorgane oder FIU diese Informationen im Rahmen ihrer jeweiligen Zuständigkeit bei der Bekämpfung von Geldwäsche und Terrorismusbekämpfung wirksam nutzen. Aktuelle Informationen helfen der Bank darüber hinaus dabei, Konten auf ungewöhnliche oder verdächtige Aktivitäten wirksam zu kontrollieren.

c) Weitergabe von Informationen an die Aufsichtsinstanzen

55. Eine Bank sollte auf Anfrage ihrer Aufsichtsinstanz in der Lage sein, in folgenden Punkten ein angemessenes Vorgehen nachzuweisen: Bewertung, Management und Minderung von Risiken im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung; Regelungen für die Annahme von Kunden; Verfahren und Richtlinien zur Feststellung und Überprüfung der Kundenidentität; laufende Überwachung und Verfahren für die Meldung verdächtiger Transaktionen; betreffend sämtliche Massnahmen in Verbindung mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung.

6. Meldung verdächtiger Transaktionen und Einfrieren von Vermögenswerten

a) Meldung verdächtiger Transaktionen

56. Eine laufende Überwachung und Überprüfung von Konten und Transaktionen macht es den Banken möglich, „falsch-positive" Anzeigen zu eliminieren und wirklich verdächtige Transaktionen unverzüglich zu melden. Das Verfahren, mit dem verdächtige Transaktionen festgestellt, untersucht und an die FIU gemeldet werden, ist in den bankinternen Richtlinien und Verfahren klar zu beschreiben und allen Mitarbeitern über regelmässige Weiterbildungsmassnahmen zu vermitteln. In diesen Richtlinien und Verfahren sollten die für die Mitarbeiter geltenden Pflichten und Anweisungen bei der Analyse, Untersuchung und Meldung solcher Aktivitäten innerhalb der Bank klar beschrieben sein; entsprechendes gilt für Leitlinien zur Erstellung derartiger Meldungen.

57. Daneben sind feste Verfahren für die Beurteilung zu entwickeln, ob es nach den gesetzlichen Meldepflichten der Bank im Falle festgestellter verdächtiger Aktivitäten notwendig ist, die Transaktion der zuständigen Strafverfolgungsbehörde oder FIU und/oder gegebenenfalls der Aufsichtsinstanz zu melden. Auch diese Verfahren sollten den Grundsatz der Vertraulichkeit beachten und gewährleisten,

[28] Siehe Grundsatz 29, zentrales Kriterium 5. f) in *Grundsätze für eine wirksame Bankenaufsicht*, September 2012.

dass die Untersuchungen zügig vorgenommen werden und die Meldungen zweckdienliche Angaben enthalten und zeitnah erstellt und vorgelegt werden. Der Chief AML/CFT-Officer sollte in Fällen, in denen Gelder oder andere Vermögensgegenstände, die vermutlich Erträge aus Straftaten sind, noch auf einem Konto ausgewiesen werden, für eine schnelle Offenlegung sorgen.

58. Besteht ein Verdacht in Bezug auf ein Konto oder eine Geschäftsbeziehung, sollte die Bank neben der Meldung der verdächtigen Aktivität sicherstellen, dass angemessene Massnahmen zur Minderung des Risikos, dass die Bank für das Begehen strafbarer Handlungen genutzt wird, ergriffen werden. Dazu kann eine Überprüfung der Risikoeinstufung des Kunden oder des Kontos bzw. der gesamten Geschäftsbeziehung gehören. Eine angemessene Massnahme kann die Heraufstufung der Entscheidung über die Fortführung der Geschäftsbeziehung unter Berücksichtigung anderer relevanter Faktoren wie Zusammenarbeit mit Strafverfolgungsbehörden oder der FIU auf die entsprechende Hierarchieebene erforderlich machen.

b) Einfrieren von Vermögenswerten

59. Terrorismusfinanzierung und Geldwäsche weisen Gemeinsamkeiten auf, haben aber auch ihre besonderen Merkmale, die Banken gebührend berücksichtigen sollten: Gelder, die zur Finanzierung terroristischer Aktivitäten verwendet werden, können entweder aus strafbaren Handlungen oder aus legalen Quellen stammen, und die Finanzquellen können je nach Art der terroristischen Organisation variieren. Zusätzlich ist zu beachten, dass Transaktionen in Verbindung mit der Finanzierung von Terroristen auch auf sehr kleine Beträge lauten können.

60. Eine Bank sollte in der Lage sein, Entscheidungen zuständiger Stellen über das Einfrieren von Geldern zuzuordnen und durchzusetzen und sollte im Übrigen entsprechend den nationalen gesetzlichen Bestimmungen und den Entschliessungen des Sicherheitsrats der Vereinten Nationen mit den dort benannten Einrichtungen oder Einzelpersonen (z.B. Terroristen, Terrororganisationen) keine Verbindung pflegen.

61. Die Sorgfaltspflichten bei der Feststellung der Kundenidentität helfen der Bank dabei, potenzielle Transaktionen zur Terrorismusfinanzierung aufzudecken und zu identifizieren; sie tragen wesentlich dazu bei, die Kenntnisse über die Kunden der Bank und deren Transaktionen zu erweitern. Bei der Gestaltung der Richtlinien und Verfahren für die Annahme von Kunden sollte die Bank die spezifischen Risiken einer Aufnahme bzw. Fortführung von Geschäftsbeziehungen mit Einzelpersonen oder Einrichtungen, die mit terroristischen Gruppen verbunden sind, angemessen berücksichtigen. Vor Aufnahme von Geschäftsbeziehungen bzw. vor der Durchführung gelegentlicher Transaktionen für neue Kunden sollte die Bank die Kundendaten mit einer von zuständigen (nationalen und internationalen) Stellen herausgegebenen Liste bekannter oder mutmasslicher Terroristen abgleichen. Ebenso sollte im Zuge der laufenden Überprüfung darauf geachtet werden, dass keine Bestandskunden auf diesen Listen stehen.

62. Alle Banken sollten über Systeme verfügen, die verbotene Transaktionen (z.B. Transaktionen mit Organisationen, die Gegenstand einschlägiger Resolutionen des UN-Sicherheitsrats oder nationaler Sanktionen sind) aufdecken. Eine Überprüfung auf Verbindungen zu Terroristen stellt keine risikogerechte Massnahme zur Wahrung der Sorgfaltspflichten bei der Kundenidentifizierung dar und sollte unabhängig vom Risikoprofil des Kunden durchgeführt werden. Zum Zweck der Überprüfung auf Verbindungen zu Terroristen kann eine Bank automatische Prüfsysteme einsetzen, sollte jedoch sicherstellen, dass diese zweckentsprechend arbeiten. Eine Bank sollte Gelder oder andere Vermögenswerte benannter Personen oder Organisationen entsprechend geltenden Gesetzen und Vorschriften unverzüglich und ohne vorherige Ankündigung einfrieren.

III. Bekämpfung von Geldwäsche und Terrorismusfinanzierung in Bankkonzernen und im grenzüberschreitenden Kontext

63. Ein solides Management der Risiken von Geldwäsche und Terrorismusfinanzierung in Banken, die im Ausland tätig sind, berücksichtigt die gesetzlichen Anforderungen des Aufnahmelandes. Angesichts der Risiken sollte jeder Bankkonzern konzernweit geltende Richtlinien und Verfahren für die Verhinderung von Geldwäsche und Terrorismusfinanzierung entwickeln, die innerhalb des Konzerns einheitlich anzuwenden und zu überwachen sind. Umgekehrt müssen die Richtlinien und Verfahren auf Ebene der Niederlassungen oder der Tochterunternehmen, auch wenn sie lokale Aspekte des Bankgeschäfts und die Anforderungen des Aufnahmelandes abbilden, mit den übergeordneten Richtlinien und Verfahren des Konzerns übereinstimmen und diese unterstützen.[29] In Fällen, in denen die Anforderungen des Aufnahmelandes strenger als die des Konzerns sind, sollten es die Richtlinien des Konzerns zulassen, dass die jeweilige Niederlassung bzw. das jeweilige Tochterunternehmen die lokalen Anforderungen übernimmt und umsetzt.

1. Globales Management von Kundenrisiken

64. Ein konsolidiertes Risikomanagement heisst, einen Prozess zu entwickeln und zu steuern, mit dem auf Konzernebene Richtlinien und Verfahren abgestimmt und angewandt werden, um eine kohärente und umfassende Grundlage für das Management der Risiken der Bank in ihren internationalen Geschäften zu schaffen. Die Richtlinien und Verfahren sollten nicht lediglich den Zweck verfolgen, eine strikte Einhaltung aller einschlägigen Gesetze und Vorschriften zu erreichen, sondern sollten darüber hinaus so gestaltet sein, dass konzernweit bestehende Risiken aufgedeckt, überwacht und gemindert werden können. Es ist alles vorzukehren, um sicherzustellen, dass der Konzern die in seinen globalen Richtlinien und Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung aufgeführten Informationen einholen und prüfen kann, ohne dabei durch lokale Richtlinien und Verfahren, die aufgrund veränderter gesetzlicher Anforderungen vor Ort notwendig sind, eingeschränkt zu werden. Diesbezüglich sollte der Informationsaustausch zwischen dem Hauptsitz und sämtlichen Niederlassungen und Tochterunternehmen der Bank zuverlässig funktionieren. Unterscheiden sich die aufsichtlichen oder gesetzlichen Mindestanforderungen im Herkunftsland von denen im Aufnahmeland, sollten im Aufnahmeland die strengeren Anforderungen gelten.

65. Wenn das Aufnahmeland die angemessene Umsetzung von FATF-Standards[30] nicht zulässt, sollte der Chief AML/CFT-Officer gemäss diesen Standards die Aufsichtsinstanz des Herkunftslandes informieren. Zusätzliche Massnahmen sollten geprüft werden; dazu gehört gegebenenfalls die Einstellung der Geschäftstätigkeit des Finanzkonzerns im Aufnahmeland.

66. Der Ausschuss erkennt an, dass eine Umsetzung konzernweit geltender Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung im Vergleich zu vielen anderen Aufgaben des Risikomanagements eine grössere Herausforderung darstellt, weil einige Länder es weiterhin nicht zulassen, dass Banken die Namen von Kunden und Kontostände über nationale Grenzen hinweg weitergeben. Für eine wirksame konzernweite Überwachung und für Zwecke des Managements der Risiken von Geld-

[29] Der Begriff „Konzern" bezeichnet hier eine oder mehrere Banken eines Verbunds sowie die Niederlassungen und Tochterunternehmen dieser Banken. Der Begriff „Hauptsitz" bezeichnet hier auch die Mutterbank oder die Geschäftseinheit, in der das Management der Risiken von Geldwäsche und Terrorismusfinanzierung auf Ebene der verschiedenen Geschäftsbereiche erfolgt.

[30] Siehe Auslegungshinweis zu Empfehlung 18 (Internal controls and foreign branches and subsidiaries) in den FATF-Standards.

wäsche und Terrorismusfinanzierung ist es von Bedeutung, dass Banken befugt sind, Informationen über ihre Kunden mit dem Hauptsitz oder der Mutterbank auszutauschen, vorbehaltlich eines angemessenen Rechtsschutzes. Dies gilt für Niederlassungen und Tochterunternehmen.

2. Risikobewertung und -management

67. Die Bank sollte umfassende Kenntnisse über alle mit ihren Kunden – Einzelkunden und Kundenkategorien – verbundenen Risiken im gesamten Konzern haben und sollte diese entsprechend der Höhe und Art der Risiken innerhalb des Konzerns regelmässig dokumentieren und aktualisieren. Bei der Bewertung von Kundenrisiken sollte eine Bank sämtliche relevanten Risikofaktoren wie Standort, Muster von (vom Kunden angekündigten oder von der Bank selbst beobachteten) Aktivitäten/Transaktionen und Nutzung von Bankprodukten und -dienstleistungen berücksichtigen und Kriterien zur Identifizierung von Kunden mit höherem Risiko festlegen. Diese Kriterien sind in der Bank, in ihren Niederlassungen und Tochterunternehmen sowie bei der Auslagerung von Tätigkeiten (s. Anhang 1) anzuwenden. Kunden, die für die Bank ein höheres Risiko von Geldwäsche und Terrorismusfinanzierung darstellen, sollten unter Verwendung dieser Kriterien konzernweit identifiziert werden. Risikobewertungen von Kunden sollten auf Konzernebene angewandt werden bzw. sollten mindestens mit der konzernweiten Risikobewertung übereinstimmen. Im Hinblick auf die Unterschiede der mit bestimmten Kundenkategorien verbundenen Risiken sollten die Richtlinien des Konzerns berücksichtigen, dass Kunden derselben Kategorie in verschiedenen Ländern unterschiedliche Risiken darstellen können. Die im Zuge des Bewertungsprozesses erfassten Informationen sollten in der Folge dazu verwendet werden, die Höhe und Art des Risikos des gesamten Konzerns zu bestimmen und sollten bei der Gestaltung angemessener Kontrollen auf Konzernebene zur Minderung dieser Risiken berücksichtigt werden. Zu den Minderungsfaktoren können zusätzliche Kundeninformationen, verstärkte Überwachung, häufigere Aktualisierung personenbezogener Daten und Besuch der Kunden vor Ort durch Bankangestellte gehören.

68. Mitarbeiter der Bank in den Funktionsbereichen Compliance und Interne Revision, insbesondere der Chief AML/CFT-Officer, oder auch die externen Revisoren sollten prüfen, ob sämtliche Aspekte der Konzernrichtlinien und -verfahren eingehalten werden – einschl. der Wirksamkeit der zentralen Richtlinien für die Kundenidentifizierung, der Anforderungen für den Informationsaustausch mit anderen Konzerneinheiten und der Beantwortung von Anfragen des Hauptsitzes. International tätige Bankkonzerne sollten sicherstellen, dass sie über starke Funktionen Interne Revision und Global Compliance verfügen, weil diese im Hinblick auf die Überwachung der Anwendung der Sorgfaltspflichten insgesamt und der Wirksamkeit der Richtlinien und Verfahren zum Austausch von Informationen innerhalb des Konzerns die wichtigsten Instrumente darstellen. Dazu sollte gehören, dass der Chief AML/CFT-Officer für die konzernweite Einhaltung sämtlicher Richtlinien, Verfahren und Kontrollen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung im In- und Ausland zuständig ist (s. Absätze 75 und 76).

3. Konsolidierte Richtlinien und Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung

69. Eine Bank sollte sicherstellen, dass sie Kenntnis davon hat, in welchem Umfang es im Rahmen der Gesetze zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung zulässig ist, sich bei der Vermittlung von Geschäften bzw. Kunden auf von anderen Banken (z.B. Banken desselben Konzerns) bereits durchgeführte Verfahren zu verlassen. Die Bank sollte sich nicht auf Vermittler verlassen, die mit weniger strikten Standards zur Verhinderung von Geldwäsche und Terrorismusfinanzierung arbeiten als die Bank selbst. Das bedeutet, dass die Bank die im Land der vermittelnden Bank bestehenden Standards für Geldwäsche und Terrorismusfinanzierung überwachen und bewerten muss. Sie kann auf einen Vermittler zurückgreifen, der demselben Finanzkonzern angehört, und kann die von diesem gemachten Angaben als zuverlässiger einstufen, wenn für diesen Vermittler dieselben Standards gelten wie für die Bank selbst und die Anwendung dieser Anforderungen auf Konzernebene überwacht wird. Eine Bank, die nach diesem Ansatz vorgeht, sollte jedoch sicherstellen, dass sie von der vermittelnden Bank die Anga-

ben zum Kunden erhält (wie in Anhang 1 im Einzelnen ausgeführt), da diese Informationen möglicherweise an die FIU weitergegeben werden müssen, falls sich Transaktionen, an denen der vermittelte Kunde beteiligt ist, als verdächtig herausstellen.

70. Der Hauptsitz des Bankkonzerns sollte zum Zweck der Durchsetzung der konzernweiten Richtlinien und Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung Zugang zu relevanten Informationen haben. Jede Geschäftsstelle des Bankkonzerns sollte in der Lage sein, die Mindestanforderungen der vom Hauptsitz auf der Grundlage der Leitlinien des Basler Ausschusses festgelegten Richtlinien und Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung und betreffend den Zugang zu Informationen einzuhalten.

71. Die Richtlinien und Verfahren für die Annahme und Identifizierung von Kunden und die Aufzeichnung von Informationen sind durch eine einheitliche Anwendung innerhalb des gesamten Konzerns – mit den eventuell notwendigen Anpassungen zur Berücksichtigung unterschiedlicher Risiken bestimmter Geschäftsbereiche oder geografischer Gebiete – umzusetzen. Darüber hinaus wird anerkannt, dass in den einzelnen Ländern unterschiedliche Vorgehensweisen zum Einholen und zur Aufbewahrung von Informationen erforderlich sein können, um den aufsichtlichen Anforderungen vor Ort zu genügen oder bestimmten Risikofaktoren Rechnung zu tragen. Diese Vorgehensweisen sollten jedoch mit den oben dargestellten konzernweit gültigen Standards übereinstimmen.

72. Unabhängig von ihrem Standort sollte jede Geschäftsstelle wirksame Überwachungsrichtlinien und -verfahren einführen und pflegen, die den im betreffenden Land und in der betreffenden Bank bestehenden Risiken angemessen sind. Diese Überwachung auf lokaler Ebene sollte durch einen zuverlässig funktionierenden Austausch von Informationen über Konten und Aktivitäten, die ein erhöhtes Risiko darstellen können, mit dem Hauptsitz und – wenn zweckdienlich – mit anderen Niederlassungen und Tochterunternehmen ergänzt werden.

73. Um die sich aus derartigen Konten ergebenden Risiken von Geldwäsche und Terrorismusfinanzierung wirksam zu steuern, sollte eine Bank diese Informationen nicht nur durch eigene Kenntnisse über den Kunden ergänzen, sondern auch durch Informationen über die wirtschaftlich Berechtigten des Kunden und die fraglichen Finanzmittel. Eine Bank sollte die bedeutendsten Kundenbeziehungen, Kontostände und Aktivitäten auf konsolidierter Basis überwachen – unabhängig davon, ob die Konten in der Bilanz erscheinen oder ausserbilanziell geführt, mit einem Vermögensverwaltungsauftrag oder treuhänderisch verwaltet werden, und unabhängig davon, wo sie bestehen. Auch in den FATF-Standards finden sich nunmehr nähere Angaben zur Überwachung der Funktionen Compliance, Interne Revision und/oder Bekämpfung von Geldwäsche und Terrorismusfinanzierung im Konzern durch den Hauptsitz.[31] Diese Leitlinien sind zwar hauptsächlich für Banken entwickelt worden, dürften aber darüber hinaus auch für Konglomerate (einschl. Banken) von Interesse sein.

74. Viele grosse Banken, die dazu in der Lage sind, zentralisieren bestimmte Verarbeitungssysteme und Datenbanken, um die Wirksamkeit des Managements oder die Wirtschaftlichkeit zu verbessern. Bei der Umsetzung eines solchen Ansatzes sollte eine Bank die lokalen und zentralen Funktionen zur Überwachung von Transaktionen/Konten angemessen dokumentieren und zusammenfassen, um sicherzustellen, dass die Möglichkeit besteht, im gesamten Konzern – und nicht nur entweder lokal oder zentral – nach bestimmten Mustern potenziell verdächtiger Aktivitäten zu suchen.

75. Eine Bank, die im In- und Ausland tätig ist, sollte einen Chief AML/CFT-Officer ernennen, der für den gesamten Konzern zuständig ist (Group AML/CFL-Officer). Als Bestandteil des globalen Risikomanagements hat der Group AML/CFL-Officer die Aufgabe, eine einheitlichen Strategie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (einschl. verbindlicher Richtlinien und Verfahren sowie der

[31] Siehe insbesondere Empfehlung 18 in den FATF-Standards.

Befugnis, allen Niederlassungen, Tochterunternehmen und nachgeordneten Geschäftsstellen im In- und Ausland Anweisungen zu erteilen) zu schaffen, zu koordinieren und deren Umsetzung auf Konzernebene zu bewerten.

76. Zur Funktion des Group AML/CFL-Officers gehört die laufende Überwachung der Einhaltung sämtlicher Vorgaben hinsichtlich der Verhinderung von Geldwäsche und Terrorismusbekämpfung auf Ebene des Konzerns im In- und Ausland. Dazu sollte sich der Group AML/CFL-Officer selbst vergewissern (auch mittels regelmässiger Besuche vor Ort), dass die einschlägigen Anforderungen konzernweit eingehalten werden. Falls notwendig, sollte er befugt sein, Anweisungen zu erteilen oder die für den gesamten Konzern notwendigen Massnahmen zu treffen.

4. Konzernweiter Informationsaustausch

77. Banken sollten die Koordinierung des Informationsaustauschs beaufsichtigen. Tochterunternehmen und Niederlassungen sind aufzufordern, den Hauptsitz proaktiv über Kunden und Aktivitäten mit höherem Risiko, die im Hinblick auf die globalen Standards für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung von Bedeutung sind, zu informieren und auf Anfragen zu Konteninformationen des Hauptsitzes oder der Mutterbank zeitnah zu antworten. Die konzernweit geltenden Standards der Bank sollten eine Beschreibung der Verfahren enthalten, die an allen Standorten bei der Identifizierung, Überwachung und Untersuchung von potenziell ungewöhnlichen Umständen und bei der Meldung verdächtiger Aktivitäten einzuhalten sind.

78. Die konzernweit geltenden Richtlinien und Verfahren der Bank sollten Aspekte und Vorschriften im Zusammenhang mit lokalen Datenschutzbestimmungen und Gesetzen zum Schutz der Persönlichkeitsrechte berücksichtigen. Ferner sind die unterschiedlichen Arten von Informationen, die innerhalb des Konzerns ausgetauscht werden können, sowie die Vorschriften für das Aufzeichnen, die Abfrage, den Austausch bzw. die Weitergabe und die Löschung dieser Informationen zu berücksichtigen.

79. Die Gesamtkonzernfunktion Management der Risiken von Geldwäsche und Terrorismusfinanzierung sollte potenzielle Risiken bewerten, die aus den von den Niederlassungen und Tochterunternehmen gemeldeten Aktivitäten resultieren, und gegebenenfalls die konzernweiten Risiken, die sich durch einen bestimmten Kunden bzw. eine bestimmte Kundenkategorie ergeben, einschätzen. Sie sollte über Richtlinien und Verfahren verfügen, um beurteilen zu können, ob bei anderen Niederlassungen oder Tochterunternehmen Konten desselben Kunden (einschl. mit diesem verbundener bzw. ihm nahestehender Parteien) geführt werden. Die Bank sollte ferner über Richtlinien und Verfahren zur Regelung globaler Kontobeziehungen verfügen, bei denen von einem höheren Risiko auszugehen ist bzw. bei denen Verbindungen zu potenziell verdächtigen Aktivitäten bestehen; dazu gehören auch Eskalationsverfahren und Leitlinien zur Einschränkung von Kontenaktivitäten, einschl. nötigenfalls der Schliessung des Kontos.

80. Darüber hinaus sollten eine Bank sowie ihre Niederlassungen und Tochterunternehmen entsprechend den einschlägigen nationalen Gesetzen den Ersuchen von Strafverfolgungsbehörden, Aufsichtsinstanzen oder FIU um Kundeninformationen, die diese für die Bekämpfung der Geldwäsche und Terrorismusfinanzierung für notwendig erachten, nachkommen. Der Hauptsitz einer Bank sollte in der Lage sein, alle Niederlassungen und Tochterunternehmen aufzufordern, ihre Unterlagen nach Einzelpersonen oder Organisationen zu durchsuchen, die in speziellen Listen geführt werden oder Gegenstand von Anfragen sind und die im Verdacht stehen, Beihilfe zur Geldwäsche und Terrorismusfinanzierung zu leisten, und die dabei festgestellten Treffer zu melden.

81. Eine Bank sollte in der Lage sein, ihre Aufsichtsinstanz auf deren Verlangen über ihre globalen Prozesse zum Management von Kundenrisiken, ihre Risikobewertung und ihr Management der Risiken von Geldwäsche und Terrorismusfinanzierung, ihre konsolidierten Richtlinien und Verfahren zur Verhinderung von Geldwäsche und Terrorismusfinanzierung und ihre Regelungen betreffend den konzernweiten Informationsaustausch zu unterrichten.

5. Gemischte Finanzkonzerne

82. Viele Bankkonzerne sind auch im Wertpapier- und im Versicherungsgeschäft tätig. Bei der Anwendung von Risikomanagementkontrollen in Bezug auf die Risiken von Geldwäsche und Terrorismusfinanzierung stellen sich im Falle gemischter Finanzkonzerne zusätzliche Probleme, die im Einlagen- und Kreditgeschäft vielleicht nicht vorhanden sind. Gemischte Konzerne sollten in der Lage sein, die Identität ihrer Kunden, deren Geschäfte und Kontobewegungen innerhalb des gesamten Konzerns zu überwachen und diesbezügliche Informationen auszutauschen; ferner sollten sie auf Kunden achten, die ihre Dienstleistungen in verschiedenen Sektoren – wie oben in Absatz 79 beschrieben – nutzen.

83. Die Unterschiede hinsichtlich der Art von Aktivitäten und der Muster von Geschäftsbeziehungen zwischen Banken und Kunden in den einzelnen Sektoren können eine Anpassung bzw. Begründung der Anforderungen für die Verhinderung von Geldwäsche und Terrorismusfinanzierung in den einzelnen Sektoren erforderlich machen. Der Konzern sollte beim Cross-Selling von Produkten und Dienstleistungen an Kunden aus unterschiedlichen Geschäftssparten auf diese Unterschiede achten und geeignete Anforderungen für die Verhinderung von Geldwäsche und Terrorismusfinanzierung in den betreffenden Sektoren anwenden.

IV. Die Rolle der Bankenaufsicht

84. Von den Bankenaufsichtsinstanzen wird erwartet, dass sie sich an die FATF-Empfehlung 26 halten, die u.a. lautet: „Finanzinstitute, für die die Basler Grundsätze gelten, sollten die Regulierungs- und Aufsichtsmassnahmen, die sie für aufsichtliche Zwecke anwenden und die auch im Hinblick auf Geldwäsche und Terrorismusfinanzierung relevant sind, in ähnlicher Weise für Zwecke der Bekämpfung von Geldwäsche und Terrorismusfinanzierung anwenden. Dazu sollte eine konsolidierte Aufsicht über die Gruppe zu Zwecken der Bekämpfung der Geldwäsche und Terrorismusfinanzierung gehören." Der Basler Ausschuss erwartet, dass die Aufsichtsinstanzen die *Grundsätze einer wirksamen Bankenaufsicht* auf das Management der Risiken von Geldwäsche und Terrorismusfinanzierung der Banken auf eine Weise anwenden, die mit der Gesamtbeaufsichtigung von Banken durch die Aufsichtsinstanzen übereinstimmt und dieser förderlich ist. Die Aufsichtsinstanzen sollten in der Lage sein, eine Reihe von wirksamen, angemessenen und abschreckenden Sanktionen zu verhängen, wenn Banken die Anforderungen im Hinblick auf die Bekämpfung von Geldwäsche und Terrorismusfinanzierung nicht einhalten.

85. Die Aufsichtsinstanzen sollten ihre Vorstellungen in Bezug auf Richtlinien und Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung von Banken darlegen. Die in diesem Papier behandelten wesentlichen Aspekte sollten den Aufsichtsinstanzen bei ihren weiteren Bemühungen, die nationale Aufsichtspraxis zu gestalten oder zu verbessern, klare Anhaltspunkte liefern. Nationale Aufsichtsinstanzen werden dazu angehalten, den Banken bei der Gestaltung eigener Richtlinien und Verfahren zur Kundenidentifizierung Hilfestellung zu geben. Der Ausschuss hat dazu in den Anhängen 1 und 2 zwei gesonderte, themenbezogene Leitfäden erstellt, die von den Aufsichtsinstanzen für diese Zwecke verwendet werden können.

86. Die Aufsichtsinstanzen sollten bei der Überwachung des Risikomanagements der Banken in Bezug auf Geldwäsche und Terrorismusfinanzierung nach einem risikobasierten Ansatz vorgehen.[32] Ein

[32] Die Aufsichtsinstanzen sollten auch den im Auslegungshinweis 26 in den FATF-Standards beschriebenen risikobasierten Ansatz berücksichtigen.

solcher Ansatz setzt voraus, dass die Aufsichtsinstanz: i) sich umfassende Kenntnisse über die in dem Land gegebenen Risiken und deren potenzielle Auswirkungen auf die beaufsichtigten Institute verschafft;[33] ii) die Angemessenheit der Risikobewertung der Bank auf der Grundlage der nationalen Risikobewertung des Landes beurteilt;[34] iii) die bei dem zu beaufsichtigenden Institut vorhandenen Risiken bewertet, um sich Kenntnis über Art und Umfang der Risiken des Kundenstamms des Instituts, der Produkte und Dienstleistungen sowie der Standorte, an denen die Bank und deren Kunden ihre Geschäftstätigkeit ausüben, zu verschaffen; iv) die Angemessenheit und Effizienz bei der Umsetzung der von der Bank konzipierten Kontrollen (einschl. Massnahmen zur Kundenidentifizierung) im Hinblick auf die Einhaltung ihrer Pflichten im Zusammenhang mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung sowie auch die Risikominderung bewertet; v) diese Informationen für die Zuteilung der Ressourcen, für die Festlegung des Prüfungsumfangs, für die Bestimmung des Fachwissens und der Erfahrung verwendet, die aufsichtsseitig für eine wirksame Prüfung nötig sind, und diese Ressourcen entsprechend den festgestellten Risiken einsetzt.

87. Geschäftsbereiche oder Kundenkategorien mit grösseren Risiken können im Sinne einer wirksamen Prüfung spezielle Fachkenntnisse und zusätzliche Verfahren erforderlich machen. Bei der Festlegung des Aufsichtszyklus sollte im Hinblick auf Häufigkeit und Terminierung der Prüfungen auch das Risikoprofil der Bank berücksichtigt werden. Auch hier wieder kann es erforderlich sein, Banken mit einem höheren Risikoprofil häufiger zu prüfen als andere. Die Aufsichtsinstanzen sollten überdies prüfen, ob Banken ihren Ermessensspielraum hinsichtlich der Anwendung von Massnahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung auf der Grundlage eines risikobasierten Ansatzes angemessen genutzt haben. Sie sollten ferner die vorhandenen internen Kontrollen bewerten und beurteilen, wie Banken bestimmen, ob sie die aufsichtsrechtlichen und regulatorischen Leitlinien bzw. die Vorschriften einhalten. Der Aufsichtsprozess sollte nicht nur eine Prüfung der Richtlinien und Verfahren beinhalten, sondern auch – wenn angezeigt – eine Prüfung der Kundendokumentation und Stichprobenprüfungen von Konten und Transaktionen, internen Berichten und Meldungen verdächtiger Transaktionen umfassen. Die Aufsichtsinstanz sollte jederzeit berechtigt sein, Einblick in sämtliche Dokumentationen im Zusammenhang mit den im jeweiligen Land durchgeführten Transaktionen oder geführten Konten – einschl. der von der Bank durchgeführten Analysen zur Feststellung von ungewöhnlichen oder verdächtigen Transaktionen – zu nehmen.

88. Die Aufsichtsinstanzen sind verpflichtet, sicherzustellen, dass ihre Banken über ein solides Management der Risiken von Geldwäsche und Terrorismusfinanzierung verfügen, nicht nur, um die eigene Sicherheit und Solidität zu schützen, sondern auch die Integrität des Finanzsystems.[35] Die Aufsichtsinstanzen sollten deutlich machen, dass sie gegen Banken und deren leitende Mitarbeiter, die sich nachweislich nicht an ihre eigenen internen Verfahren und an aufsichtlichen Anforderungen halten, geeignete Massnahmen ergreifen, die – wenn die Umstände es erfordern – hart ausfallen und öffentlich gemacht werden können. Darüber hinaus sollten die Aufsichtsinstanzen (oder andere entsprechende nationale Stellen) in der Lage sein, geeignete Gegenmassnahmen anzuwenden und sicherzustellen, dass Banken verstärkte Sorgfaltspflichten im Zusammenhang mit Geschäftsbeziehungen und Transaktionen kennen und anwenden, wenn sie von der FATF dazu aufgefordert werden oder wenn die Geschäftsbeziehungen und Transaktionen einen Bezug zu Ländern aufweisen, deren Standards hinsichtlich Geldwäsche und Terrorismusfinanzierung als unzulänglich betrachtet werden. Diesbezüglich haben die FATF

[33] Dabei sollten die Aufsichtsinstanzen, wie im Auslegungshinweis zu Empfehlung 1 der FATF-Standards beschrieben, von den Länderbewertungen ausgehen.

[34] Gegebenenfalls auch supranationale Risikobewertungen.

[35] Viele Aufsichtsinstanzen sind auch verpflichtet, z.B. im Rahmen von Prüfungen vor Ort festgestellte verdächtige, ungewöhnliche oder illegale Transaktionen zu melden.

und einige nationale Behörden eine Liste der Länder und Gebiete erstellt, die im Hinblick auf die Bekämpfung von Geldwäsche und Terrorismusfinanzierung ein strategisches Defizit aufweisen oder die die einschlägigen internationalen Standards nicht einhalten;[36] derartige Erkenntnisse sollten in das bankinterne Management der Risiken von Geldwäsche und Terrorismusfinanzierung Eingang finden.

89. Die Aufsichtsinstanzen sollten ferner berücksichtigen, wie die Bank die Compliance auf Ebene der Niederlassungen und der Tochterunternehmen insgesamt überwacht und beaufsichtigt, und ob der Konzern in der Lage ist, lokale aufsichtsrechtliche Anforderungen in seine Richtlinien einfliessen zu lassen und zu gewährleisten, dass bei Unterschieden zwischen den Anforderungen auf Ebene des Konzerns und der lokalen Ebene die strengeren Anwendung finden. Die Aufsichtsinstanzen sollten auch sicherstellen, dass in Fällen, in denen die Niederlassung oder das Tochterunternehmen eines Konzerns den strengeren der beiden Standards nicht anwenden kann, die Gründe dafür und die Unterschiede zwischen den beiden dokumentiert werden und angemessene Massnahmen zur Minderung der sich aus diesen Unterschieden ergebenden Risiken getroffen werden.

90. Im Zusammenhang mit grenzüberschreitenden Tätigkeiten sollten die Aufsichtsinstanzen des Herkunftslandes[37] im Rahmen von Einsätzen vor Ort unbehindert prüfen können, ob die Bank sich an konzernweit geltende Richtlinien und Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung hält. Dies kann durchaus eine Prüfung der Kundenunterlagen und Stichprobenprüfungen von Konten oder Transaktionen im Aufnahmeland erforderlich machen. Die Aufsichtsinstanzen des Herkunftslandes sollten Zugang zu Informationen über ausgewählte Einzelkonten und Transaktionen und über spezifische Risiken solcher Kunden im In- und Ausland bekommen, soweit dies für eine angemessene Bewertung der Anwendung der Standards für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung und eine Beurteilung des Risikomanagements notwendig ist. Diese Art der Nutzung von Informationen für rechtmässige aufsichtliche Zwecke, bei der die Aufsichtsinstanzen sich an geltende Bestimmungen zum Schutz der Vertraulichkeit zu halten haben, sollte durch lokale gesetzliche Bestimmungen zur Wahrung des Bankgeheimnisses oder zum Datenschutz nicht beeinträchtigt werden. Obwohl die Aufsichtsinstanzen des Aufnahmelandes und/oder andere Stellen für die Einhaltung der lokalen Anforderungen für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung verantwortlich sind (dazu gehört eine Beurteilung der Angemessenheit der Verfahren), sollten die Aufsichtsinstanzen des Aufnahmelandes eng mit den Instanzen des Herkunftslandes – die unter Umständen zu bewerten haben, wie die Bank die Einhaltung konzernweiter Richtlinien und Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung überwacht – zusammenarbeiten und diese unterstützen.

91. Die Rolle der (internen oder externen) Revision auf Konzernebene ist im Hinblick auf die Bewertung der Wirksamkeit von Richtlinien und Verfahren für die Bekämpfung von Geldwäsche und

[36] Länder können z.B. wie folgt offiziell identifiziert werden:

- In der Erklärung (*Public Statement*) der FATF wird unterschieden zwischen:
  - i) Ländern mit strategischen Defiziten bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung, für die Gegenmassnahmen getroffen wurden;
  - ii) Ländern mit strategischen Defiziten bei der Bekämpfung von Geldwäsche und Terorismusbekämpfung, die beim Abbau der Defizite keine wesentlichen Fortschritte gemacht haben oder die sich nicht zu einem gemeinsam mit der FATF entwickelten Aktionsplan zum Abbau der Defizite verpflichtet haben.
- Im Dokument *Improving Global AML/CFT Compliance: On-going Process*, das von der FATF veröffentlicht wurde, sind Länder mit strategischen Defiziten bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung aufgeführt, die sich auf hoher politischer Ebene verpflichtet haben, die Defizite durch die Umsetzung eines gemeinsam mit der FATF entwickelten Aktionsplans abzubauen.

[37] In Ländern, in denen die Prüfungen durch externe Revisoren vorgenommen werden, sollte diese Ausnahme auch für die zuständigen Revisoren gelten.

Terrorismusfinanzierung von besonders grosser Bedeutung. Die Aufsichtsinstanzen des Herkunftslandes sollten sicherstellen, dass geeignete risikoorientierte Grundsätze bestehen und dass, ausgehend von Umfang und Häufigkeit der Überprüfung der Massnahmen des Konzerns zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, angemessene Ressourcen bereitgestellt werden. Sie sollten ferner sicherstellen, dass die Revisoren bei der Durchführung der Rechnungsrevision uneingeschränkten Zugang zu sämtlichen relevanten Berichten haben.

92. Die Aufsichtsinstanzen sollten sicherstellen, dass Informationen über Bankkunden und -transaktionen denselben Regelungen zum Schutz der Vertraulichkeit unterliegen wie die meisten Informationen über Bankaktivitäten, die die Aufsichtsinstanzen untereinander austauschen.

93. Wichtig ist, dass alle Länder, in denen ausländische Banken tätig sind, einen geeigneten Rechtsrahmen bieten, der die Weitergabe von Informationen erleichtert, die für das Management von Kundenrisiken am Hauptsitz oder in der Mutterbank bzw. seitens der Aufsichtsinstanzen des Herkunftslandes notwendig sind. Ebenso sollten hinsichtlich Besuchen von Revisoren der Zentrale, Risikomanagern und Compliance-Beauftragten (einschl. des Chief AML/CFT-Officers und/oder des AML/CFT-Group-Officers) des Hauptsitzes oder von Vertretern der Aufsichtsinstanz des Herkunftslands vor Ort bei den Tochtergesellschaften und Niederlassungen im Aufnahmeland keine Einschränkungen bestehen; ferner sollten die Möglichkeiten des Zugangs zu Unterlagen der Bank, einschl. Kundennamen und Kontostände, im Aufnahmeland nicht eingeschränkt sein. Diese Zugangsmöglichkeiten sollten bei Niederlassungen und Tochterunternehmen identisch sein. Erweisen sich die Hindernisse beim Informationsaustausch als unüberwindbar und bestehen keine zufriedenstellenden Alternativen, sollte die Aufsichtsinstanz des Herkunftslands der Aufsichtsinstanz des Aufnahmelands gegenüber deutlich zum Ausdruck bringen, dass gegen die Bank zusätzliche aufsichtliche Massnahmen verhängt werden können, wie verstärkte Überwachung des Konzerns einschliesslich wenn angezeigt der Aufforderung an den Mutterkonzern, seinen Geschäftsbetrieb im Aufnahmeland einzustellen.

94. Wenn Mitarbeiter des Hauptsitzes Zugang zu Informationen über lokale Kunden haben, sollten keine Einschränkungen bei der Weitergabe dieser Informationen an den Hauptsitz bestehen. Für Informationen dieser Art sollten hinsichtlich des Vertraulichkeitsschutzes und der Verwendung angemessene Regelungen bestehen; sie können im Herkunftsland gesetzlichen Bestimmungen zum Schutz von Persönlichkeitsrechten und Vorrechten unterworfen sein.

95. Der Basler Ausschuss ist der Ansicht, dass es keine Rechtfertigung für lokale gesetzliche Bestimmungen gibt, die die Weitergabe von Kundeninformationen von einer Bankniederlassung oder einem Tochterunternehmen der Bank im Aufnahmeland an den Hauptsitz oder die Mutterbank im Herkunftsland für Zwecke des Risikomanagements, einschl. der Risiken von Geldwäsche und Terrorismusfinanzierung, einschränken. Sehen die Gesetze im Aufnahmeland Einschränkungen bei der Offenlegung derartiger Informationen gegenüber „Dritten" vor, ist es von entscheidender Bedeutung, dass der Hauptsitz oder die Mutterbank sowie die Aufsichtsinstanz im Herkunftsland eindeutig nicht unter diese Begriffsbestimmung fallen. Länder mit gesetzlichen Bestimmungen, die eine Behinderung eines derartigen Informationsaustausch zu Zwecken des Managements der Risiken von Geldwäsche und Terrorismus darstellen bzw. die als Behinderung ausgelegt werden können, sind eindringlich aufgefordert, derartige Einschränkungen zu beseitigen und dazu spezifische Lösungswege aufzuzeigen.

Anhang 1

Nutzung von anderen Banken, Finanzinstituten oder Dritten zur Durchführung der Kundenidentifizierung

I. Einleitung

1. In einigen Ländern können Banken für die Durchführung der Feststellung und Überprüfung von Kundenidentität andere Banken, Finanzinstitute oder sonstige Stellen einsetzen. Die entsprechenden Regelungen sind unterschiedlich, doch sind sie im Wesentlichen einer der beiden folgenden Situationen zuzuordnen:

Delegierung an Dritte

2. In einigen Ländern können Banken die Identifizierung von Kunden durch andere Finanzinstitute oder entsprechende, nicht dem Finanzsektor angehörende Unternehmen oder Berufsangehörige vornehmen lassen,[38] die ihrerseits zu Zwecken der Bekämpfung von Geldwäsche und Terrorismusfinanzierung beaufsichtigt oder überwacht werden. In diesen Fällen besteht in der Regel bereits eine Geschäftsbeziehung zwischen dem Dritten und dem Kunden, und die Banken sind von der Pflicht befreit, zu Beginn einer Geschäftsbeziehung eigene Massnahmen zur Identifizierung der Kunden durchzuführen. Nach den FATF-Standards[39] ist die Delegierung an Dritte zulässig für:

a) die Feststellung der Identität des Kunden und die Überprüfung derselben anhand von verlässlichen, unabhängigen Ausgangsdokumenten, Daten und Informationen

b) die Feststellung der Identität des wirtschaftlich Berechtigten und das Ergreifen zumutbarer Massnahmen zur Überprüfung der Identität des wirtschaftlich Berechtigten, in der Weise, dass für das Finanzinstitut die Identität des wirtschaftlich Berechtigten feststeht. Bei juristischen Personen und bestimmten Rechtsgestaltungen sollten die Finanzinstitute die Eigentümer- und Kontrollstruktur des Kunden kennen

c) Kenntnisse über den vorgesehenen Zweck und die Art der Geschäftsbeziehungen und gegebenenfalls das Einholen von Angaben dazu.

Die FATF-Standards fordern darüber hinaus, dass Finanzinstitute, die auf Dritte zurückgreifen, die Informationen, die bei der Durchführung der drei genannten Identifizierungsmassnahmen gewonnen werden, unverzüglich erhalten.

3. Einige Länder schränken die Ausführung durch Dritte auf unterschiedliche Weise ein, z.B. durch eine Begrenzung auf Finanzinstitute, oder durch eine Einschränkung auf bereits bei Dritten bestehende Beziehungen (und ein Verbot von Übertragungsketten) oder durch ein Verbot der Delegierung an ausländische Dritte.

[38] Siehe Empfehlung 17 der FATF-Standards und den entsprechenden Auslegungshinweis.

[39] Siehe Empfehlung 17 und Empfehlung 10 zur Kundenidentifizierung in den FATF-Standards.

Outsourcing/Auftragsverhältnis

4. Banken können auch auf Dritte zurückgreifen, die auf Grundlage einer vertraglichen Vereinbarung verschiedene Aspekte der Sorgfaltspflichten im Zusammenhang mit der Identifizierung von Kunden erfüllen; oft erfolgt dies in Form einer Outsourcing-/Auftragsbeziehung (d.h., die ausgelagerte Stelle erfüllt die Sorgfaltspflichten im Namen der delegierenden Bank). In der Regel gibt es weniger Beschränkungen dazu, wer als Beauftragter einer Bank fungieren kann; allerdings bestehen zumeist Vorschriften und Aufzeichnungspflichten.

5. In Bezug auf die Delegierung an Dritte und Outsourcing können Banken Beschränkungen hinsichtlich der Höhe, des Umfangs und der Art der Transaktionen vornehmen. In allen Fällen sollten die Aufsichtsinstanzen auf Verlangen zeitnah Zugang zu Kundeninformationen haben. Obwohl diese beiden Kategorien sich ähnlich sind und Gemeinsamkeiten aufweisen, bestehen wesentliche Unterschiede, und Banken sollten sicherstellen, dass sie mit diesen Unterschieden vertraut sind und dass sie diese in ihren Richtlinien und Verfahren entsprechend berücksichtigen.

II. Ausführung durch Dritte

6. Banken sollten über klare Richtlinien und Verfahren verfügen, die eine Beurteilung ermöglichen, ob und wann es zulässig und angemessen ist, auf andere Banken oder Finanzinstitute zurückzugreifen. Ein solcher Rückgriff auf Dritte befreit die Bank auf keinen Fall von ihrer Verantwortung dafür, dass angemessene Richtlinien und Verfahren hinsichtlich der Identifizierung von Kunden und der sonstigen Sorgfaltspflichten betreffend Kunden in Bezug auf die Verhinderung von Geldwäsche und Terrorismusfinanzierung – wie Kenntnisse über die erwarteten Aktivitäten, Kenntnisse darüber, ob Kunden ein höheres Risiko darstellen und ob Transaktionen verdächtig sind – bestehen.

7. Bei der Durchführung bestimmter Sorgfaltspflichten durch eine andere Bank oder ein anderes Finanzinstitut sollten Banken prüfen, ob diese Abhängigkeit vertretbar ist. Neben der Prüfung, ob eine Delegierung an Dritte rechtlich möglich ist, sollten u.a. folgende wichtige Kriterien zur einer Bewertung einer solchen Delegierung herangezogen werden:

a) Die Bank, das Finanzinstitut oder sonstige Stelle (soweit nach nationalen Gesetzen zulässig) die/das mit der Durchführung betraut wird, sollte so umfassend reguliert und beaufsichtigt werden wie die Bank selbst, sollte in Bezug auf die Eröffnung eines Kontos vergleichbare Anforderungen für die Identifizierung von Kunden haben und sollte mit dem Kunden, der bei der Bank ein Konto eröffnen möchte, eine bereits bestehende Geschäftsbeziehung haben. In Fällen, in denen diese Standards nicht erfüllt sind, können alternativ dazu nationale gesetzliche Bestimmungen Ersatzmassnahmen oder -kontrollen vorschreiben.

b) Zwischen der Bank und dem betreffenden Institut sollte eine schriftliche Vereinbarung oder Abmachung bestehen, aus der hervorgeht, dass die Bank die Durchführung der Verfahren zur Kundenidentifizierung an das andere Finanzinstitut delegiert.

c) Die Richtlinien und Verfahren der Bank sollten diese Delegierung dokumentieren und für diese Art der Beziehung angemessene Kontrollen und Überprüfungen vorsehen.

d) Von der Drittpartei kann verlangt werden, der Bank zu bestätigen, dass sie ihre Massnahmen zur Bekämpfung von Geldwäsche umgesetzt hat und dass sie die Kundenidentifizierung im Wesentlichen entsprechend den Vorgaben durchführt bzw. diese einhält.

e) Die Bank sollte in der Öffentlichkeit verbreitete negative Nachrichten über die Drittpartei – wie das Verhängen von Zwangsmassnahmen wegen Mängeln bzw. Verstössen im Bereich der Geldwäschebekämpfung – angemessen berücksichtigen.

f) Die Bank sollte etwaige zusätzliche Risiken, die sich aus der Delegierung der Durchführung an mehrere Parteien (Delegierungskette) anstatt unmittelbar an eine einzige Partei ergeben, identifizieren und mindern.

g) In der Risikobewertung der Bank sollte die Ausführung durch Dritte als potenzieller Risikofaktor ausgewiesen sein.

h) Die Bank sollte die andere Partei in regelmässigen Abständen überprüfen, um sicherzustellen, dass diese die Kundenidentifizierung auch weiterhin so umfassend wie die Bank selbst durchführt. Dazu sollte die mit der Durchführung der Kundenidentifizierung beauftragte Stelle – Bank, Finanzinstitut oder Drittpartei – sämtliche bei der Durchführung der Kundenidentifizierung erlangten Informationen und Unterlagen an die Bank übermitteln, und die Bank sollte die vorgenommene Identifizierung bewerten, u.a. durch Abgleich mit lokalen Datenbanken, um die Einhaltung lokaler aufsichtlicher Anforderungen sicherzustellen.

i) Bei Stellen, die die Identität ihrer Kunden nicht angemessen feststellen und überprüfen bzw. sonstige bestehende Anforderungen und Erwartungen nicht erfüllen, sollten Banken die Beendigung der Zusammenarbeit erwägen.

8. Banken mit Tochterunternehmen oder Niederlassungen im Ausland nutzen in vielen Fällen ihren Finanzkonzern, um ihre Kunden bei anderen Konzerngesellschaften einzuführen. In Ländern, in denen eine grenzüberschreitende Inanspruchnahme von Konzerngesellschaften möglich ist, sollten Finanzinstitute, die die Durchführung der Kundenidentifizierung an andere Konzerngesellschaften delegieren, sicherstellen, dass die oben genannten Bewertungskriterien gelten. Nach den FATF-Standards[40] ist es zulässig, dass Länder bei dieser Bewertung die Länderrisiken unberücksichtigt lassen, wenn für das Finanzinstitut konzernweit geltende Standards für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung bestehen und es auf Konzernebene durch seine Aufsichtsinstanz überwacht wird.

III. Outsourcing/Auftragsverhältnis

9. Eine Bank kann nach ihrem Ermessen die Massnahmen zur Feststellung und Überprüfung der Kundenidentität – und entsprechende sonstige Massnahmen – unmittelbar selbst durchführen oder die Ausführung derselben einer oder mehreren Drittparteien übertragen, die diese dann im Namen der Bank ausführen, zum Teil in Form eines Auftragsverhältnisses. Die Funktion der Einhaltung der Anforderungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung kann zwar durch Dritte wahrgenommen werden, aber die Verantwortung für die Erfüllung der Pflichten hinsichtlich Kundenidentifizierung, Geldwäsche und Terrorismusfinanzierung verbleibt bei der Bank. Der Umfang, in dem auf Dritte zurückgegriffen wird, hängt in der Regel vom Geschäftsmodell der Bank ab; Banken, die ihre Geschäfte über Telefon oder im Internet abwickeln oder die nur wenige physische Niederlassungen haben, greifen normalerweise tendenziell stärker auf Dritte zurück. Banken können Dritte einsetzen, um ihre Kundenbasis auszubauen oder den Kundenservice sowie den Zugang zu den angebotenen Dienstleistungen zu verbessern.

10. Banken, die auf Dritte zurückgreifen, sollten sicherstellen, dass eine schriftliche Vereinbarung besteht, in der die Pflichten der Bank im Hinblick auf die Bekämpfung von Geldwäsche und Terrorismus-

[40] Siehe Empfehlung 17 in den FATF-Standards.

finanzierung aufgeführt sind und in der dargelegt ist, wie diese von der Drittpartei zu erfüllen sind. In einigen Ländern sind die Beziehungen zwischen Banken und Drittparteien reguliert.

11. Wie oben ausgeführt ist es für Banken wichtig, die Unterschiede zwischen der Nutzung einer Drittpartei im Auftragsverhältnis und dem Rückgriff auf andere Banken und deren Verfahren zur Identifizierung und Überprüfung von Kunden zu kennen. Ein Beauftragter ist in der Regel nach den für Auftragsverhältnisse geltenden gesetzlichen Bestimmungen juristisch gesehen der verlängerte Arm der Bank. Wenn ein Bankkunde oder ein potenzieller Kunde mit einem Beauftragten der Bank in Geschäftsbeziehungen tritt, ist das rechtlich wie eine Beziehung mit der Bank selbst zu bewerten. Der Dritte ist deshalb dazu verpflichtet, die bei der Bank geltenden Richtlinien und Verfahren zur Feststellung und Überprüfung von Kundenidentitäten anzuwenden.

12. In der Praxis müssen die von Banken eingesetzten Dritten über die notwendigen Sach- und Fachkenntnisse sowie über eine entsprechende Schulung verfügen, um die Massnahmen der Bank zur Identifizierung und Überprüfung von Kunden anwenden zu können. In einigen Fällen, in denen das Geschäftsmodell der beauftragten Drittpartei auf der Vertretung mehrerer Banken beruht, entsteht in der Regel ein beachtliches eigenes Know-how. Allerdings unterliegen solche Drittparteien nicht immer selbst den Anforderungen im Hinblick auf die Bekämpfung von Geldwäsche und Terrorismusfinanzierung, viele jedoch schon. Unabhängig davon, ob dies der Fall ist oder nicht, wenden Dritte bei der Identifizierung und Überprüfung von Kunden immer die Anforderungen ihres Auftraggebers an (die wiederum den gesetzlichen Anforderungen genügen müssen).

13. Beispiele für Drittparteien, die regelmässig von Banken zur Erfüllung ihrer Sorgfaltspflichten im Zusammenhang mit der Identifizierung von Kunden herangezogen werden, sind u.a. Vermittler im Einlagengeschäft mit Privatkunden, Hypothekenmakler und Anwälte. Die Minderung von Risiken im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung kann gefährdet sein, wenn Banken nicht sicherstellen, dass ihre Drittparteien die geltenden Anforderungen für die Identifizierung und Überprüfung von Kunden anwenden.

14. Wie oben erwähnt, sollte eine schriftliche Vereinbarung oder Abmachung bestehen, in der die Pflichten der Drittpartei festgehalten sind; dazu sollten gehören:

a) die Pflicht zur Einhaltung der für die Bank geltenden Anforderungen für die Identifizierung und Überprüfung von Kunden (einschl. gegebenenfalls Einholen von Angaben zur Herkunft der Gelder und des Vermögens)

b) Sicherstellen, dass in Fällen, in denen der Kunde zum Zeitpunkt der Durchführung der Identifizierung und/oder Überprüfung persönlich anwesend ist, die Drittpartei die Massnahmen zur Identifizierung anwendet, einschl. der Vorlage des Originals des Identifizierungsdokuments, wenn dies vorgeschrieben ist oder von der Bank verlangt wird

c) Sicherstellen, dass in Fällen, in denen der Kunde zum Zeitpunkt der Feststellung der Identität nicht anwesend ist, die Drittpartei sämtliche vorgeschriebenen bzw. von der Bank festgelegten Anforderungen hinsichtlich der Identifizierung von Fernkunden erfüllt

d) Sicherstellen, dass die Drittpartei die Kundeninformationen vertraulich behandelt.

15. Darüber hinaus sollten Banken:

a) wenn eine Drittpartei für die Bestimmung und/oder Identifizierung der wirtschaftlich Berechtigten oder von PEP verantwortlich ist, sicherstellen, dass diese Verantwortung dokumentiert ist

b) sicherstellen, dass die Drittpartei die bei der Identifizierung der Kunden erlangten Informationen in der vorgeschriebenen Zeit an die Bank übermittelt, und

c) die Qualität der von der Drittpartei eingeholten und aufgezeichneten Kundeninformationen regelmässig und systematisch prüfen bzw. überprüfen, um sicherzustellen, dass diese weiterhin den Anforderungen der Bank genügen

d) die Fälle eindeutig festlegen, die die Bank als Nichterfüllung der vertraglichen Pflichten seitens der Drittpartei betrachtet, und ein Verfahren bestimmen, das die Anwendung geeigneter Massnahmen erlaubt – wie die Beendigung der Zusammenarbeit angesichts festgestellter Pflichtverletzungen.

16. Die Bank sollte sämtliche wichtigen Informationen von der Drittpartei zeitnah übermittelt bekommen und sicherstellen, dass die Kundenstammdaten der Bank vollständig und auf dem neusten Stand sind.

17. Die Verträge mit Drittparteien sind gegebenenfalls zu überprüfen und zu aktualisieren, um sicherzustellen, dass die Rolle der Drittpartei darin weiterhin korrekt beschrieben ist und die zu erfüllenden Aufgaben dem letzten Stand entsprechen.

Anhang 2

Korrespondenzbankgeschäfte

I. Allgemeines zu Korrespondenzbankgeschäften

1. Nach dem Glossar der FATF besteht das Korrespondenzbankgeschäft darin, dass eine Bank (die „Korrespondenzbank“) einer anderen Bank (der „Respondenzbank“) Bankdienstleistungen zur Verfügung stellt.

2. Korrespondenzbankgeschäfte werden von Banken weltweit getätigt, und Korrespondenzkonten erlauben es Banken, Geschäfte abzuwickeln und Dienstleistungen[41] anzubieten, die sie nicht unmittelbar selbst anbieten (weil ein internationales Netz fehlt). Korrespondenzkonten, die besondere Aufmerksamkeit verdienen, sind die Konten, die in Ländern geführt werden, in denen die Respondenzbanken nicht physisch präsent sind.

3. Die Korrespondenzbank wickelt Transaktionen für Kunden der Respondenzbank ab bzw. führt diese aus. Die Korrespondenzbank hat im Allgemeinen keine direkten Geschäftsbeziehungen mit den Kunden der Respondenzbank, bei denen es sich um Einzelpersonen, Unternehmen oder Finanzinstitute handeln kann. Der Kunde der Korrespondenzbank ist die Respondenzbank.

4. Aufgrund der Struktur dieser Aktivitäten und wegen der begrenzt verfügbaren Informationen über Art und Zweck der zugrundeliegenden Transaktionen können Korrespondenzbanken spezifischen Risiken von Geldwäsche und Terrorismusfinanzierung ausgesetzt sein.

II. Bewertung der Risiken von Geldwäsche und Terrorismusfinanzierung im Korrespondenzbankgeschäft – Einholen von Informationen

5. Banken, die Korrespondenzbankgeschäfte tätigen, sollten eine angemessene Bewertung der Risiken von Geldwäsche und Terrorismusfinanzierung in Verbindung mit dem Korrespondenzbankgeschäft durchführen und dementsprechend geeignete Massnahmen zur Identifizierung von Kunden anwenden.

6. Korrespondenzbanken sollten bei Aufnahme der Geschäftsbeziehung und danach fortlaufend ausreichend Informationen über ihre Respondenzbanken einholen, um in der Lage zu sein, die Art der Geschäfte der Respondenzbank vollständig zu verstehen und die Risiken von Geldwäsche und Terrorismusfinanzierung jederzeit kontinuierlich korrekt zu bewerten.

7. Zu den Faktoren, die Korrespondenzbanken berücksichtigen sollten, gehören:

a) das Land, in dem die Respondenzbank ihren Sitz hat

[41] Beispiele im FATF-Glossar sind: Cash-Management (z.B. verzinsliche Konten unterschiedlicher Währungen), internationale elektronische Zahlungen, Scheckverrechnung, Durchleitungskonten und Devisenhandelsdienstleistungen.

b) der Konzern, zu dem die Respondenzbank gehört, und die Länder, in denen der Konzern Tochterunternehmen und Niederlassungen hat

c) Informationen über Geschäftsleitung und Eigentümer der Respondenzbank (insbesondere wirtschaftlich Berechtigte oder etwaige PEP), über ihren Ruf[42], ihre wichtigsten Geschäftstätigkeiten, ihre Kunden und deren Wohn-/Standorte

d) der Zweck der für die Respondenzbank erbrachten Leistungen

e) die Geschäfte der Respondenzbank, einschl. Zielmärkte und Kundenkreis

f) Stellenwert und Qualität der Bankenregulierung und Bankenaufsicht im Land der Respondenzbank (insbesondere Gesetze und Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung)

g) Richtlinien und Verfahren der Respondenzbank zur Prävention und Erkennung von Geldwäsche, einschl. einer Beschreibung der von der Bank angewandten Massnahmen zur Identifizierung von Kunden

h) Verfügbarkeit von Angaben zur Identität von Dritten, die berechtigt sind, Korrespondenzbankdienstleistungen in Anspruch zu nehmen

i) mögliche Nutzung des Kontos durch andere Respondenzbanken im Rahmen von „verschachtelten" Korrespondenzbank-Beziehungen.[43]

8. Die Informationen hinsichtlich der Richtlinien und Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung können aus Fragebögen stammen, die von der Respondenzbank ausgefüllt werden; es kann sich auch um Informationen der Respondenzbank handeln, die öffentlich verfügbar sind (wie Finanzinformationen oder aufsichtsrechtliche Pflichtangaben).

III. Sorgfaltspflichten bei der Feststellung der Kundenidentität

9. Wenn Korrespondenzbanken bei ihren Korrespondenzbankbeziehungen keine angemessenen Sorgfaltspflichten zur Kundenüberprüfung anwenden, ist es möglich, dass sie Gelder halten und/oder weiterleiten, die in Verbindung mit strafbaren Handlungen stehen.

10. Für alle Korrespondenzbankbeziehungen sollte die Anforderung angemessener Sorgfaltspflichten gelten. Banken sollten die dazu durchgeführten Verfahren nicht als „Papiersammelaktion" betrachten, sondern als ernstzunehmende Bewertung der Geldwäscherisiken. Das Einholen von Informationen sollte gegebenenfalls in Form einer Sitzung mit dem lokalen Management und dem Compliance-Beauftragten der Respondenzbank sowie mit Vertretern der Regulierungsstellen bzw. Aufsichtsinstanzen, der Financial Intelligence Units und der zuständigen staatlichen Stellen abgeschlossen werden.

[42] Hier können von Gerichten oder Aufsichtsinstanzen verhängte zivil-, verwaltungs- oder strafrechtliche Massnahmen/Sanktionen (Bussgelder, Rügen/Kritik usw.) mitberücksichtigt werden.

[43] Der Begriff verschachtelte Korrespondenzbankgeschäfte bezieht sich auf die Nutzung der Korrespondenzbankbeziehung einer Bank durch eine Reihe von Respondenzbanken über deren Beziehungen zu der unmittelbaren Respondenzbank der Bank zur Durchführung von Transaktionen und zum Zweck des Zugangs zu anderen Finanzdienstleistungen.

11. Die im Rahmen der Durchführung der Sorgfaltspflichten erlangten Informationen sollten auf der Grundlage eines risikoorientierten Ansatzes regelmässig aktualisiert werden. Die Informationen sollten zur Aktualisierung des Risikobewertungsprozesses der Bank verwendet werden.

IV. Annahme von Kunden

12. Die Entscheidung, Korrespondenzbankbeziehungen aufzunehmen (oder zu beenden), sollte auf oberster Ebene der Korrespondenzbank getroffen werden.

13. Informationen finden sich auch in den Berichten über die Länderprüfungen der FATF und den Erklärungen der FATF zu bestimmten Ländern, gegen die Massnahmen ergriffen wurden bzw. die strategische Defizite bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung aufweisen. Auch die Berichte über gegenseitige Evaluierungen der FATF-ähnlichen Regionalgruppen (FATF-style regional bodies, FSRB) enthalten derartige Informationen. Banken können ebenfalls öffentlich verfügbare Informationen von zuständigen nationalen Stellen verwenden. Die Tatsache, dass gegen ein Land Massnahmen verhängt worden sind – insbesondere wenn das Verbot besteht, Korrespondenzbankdienstleistungen anzubieten –, sollte berücksichtigt werden. Korrespondenzbanken sollten besonders vorsichtig sein, wenn sie Geschäftsbeziehungen mit Respondenzbanken in Ländern aufnehmen bzw. fortführen, die Defizite bezüglich ihrer Standards für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung aufweisen oder die diesbezüglich als „nicht kooperierend" eingestuft wurden.

14. Eine Korrespondenzbank sollte keine Korrespondenzbankbeziehung zu einer Bank aufnehmen oder weiterführen, die ihren Sitz in einem Land hat, in dem sie nicht physisch präsent ist, und die keinem regulierten Finanzkonzern angehört (d.h. die ein reines Buchungszentrum ist).

V. Laufende Überwachung

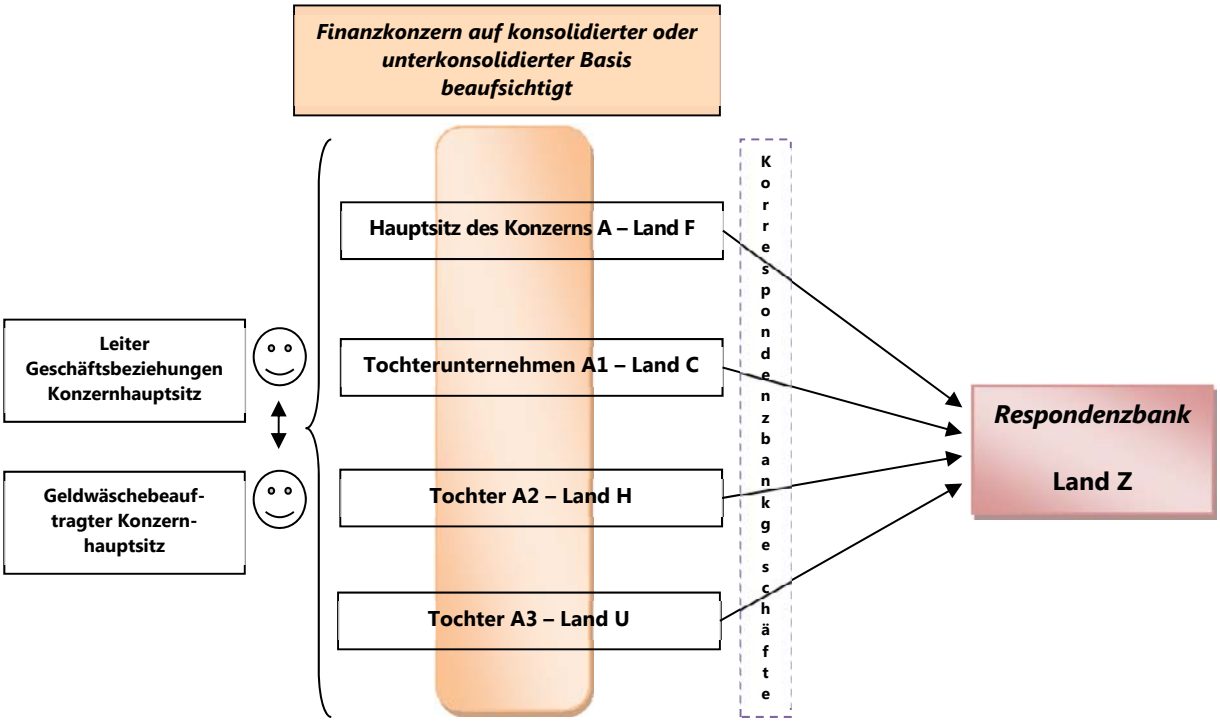
15. Eine Korrespondenzbank sollte angemessene Richtlinien und Verfahren einführen, die es ermöglichen, Aktivitäten aufzudecken, die nicht dem Zweck der für die Respondenzbank erbrachten Dienstleistungen entsprechen, ebenso Aktivitäten, die im Widerspruch zu den zwischen der Korrespondenz- und Respondenzbank vereinbarten Verpflichtungen stehen.

16. Lässt es eine Korrespondenzbank zu, dass Korrespondenzkonten unmittelbar durch Dritte zur Durchführung von Geschäften in eigenem Namen genutzt werden (z.B. Durchleitungskonten), sollte sie diese Aktivitäten, ausgehend von deren spezifischen Risiken, verstärkt überwachen. Die Korrespondenzbank sollte prüfen, ob die Respondenzbank bei Kunden, die direkten Zugang zu den Konten der Korrespondenzbank haben, eine angemessene Kundenidentifizierung vorgenommen hat und ob sie auf Verlangen entsprechende Informationen zur Identität von Kunden vorlegen kann.

17. Die Geschäftsleitung sollte regelmässig über risikoreiche Korrespondenzbeziehungen und darüber, wie diese überwacht werden, unterrichtet werden.

VI. Überlegungen zu Konzernen und grenzüberschreitenden Geschäften

18. Unterhält eine Respondenzbank Geschäftsbeziehungen zu mehreren Korrespondenzbanken, die zum selben Konzern[44] gehören (Fall 1), sollte der Konzernhauptsitz besonders darauf achten, dass die Risikobewertung durch die einzelnen Konzerngesellschaften in Übereinstimmung mit den entsprechenden konzernweiten Richtlinien erfolgt. Der Konzernhauptsitz sollte die Überwachung der Beziehungen zu der Respondenzbank koordinieren – insbesondere bei Beziehungen mit hohen Risiken – und sicherstellen, dass geeignete Mechanismen für den Informationsaustausch auf Konzernebene bestehen.

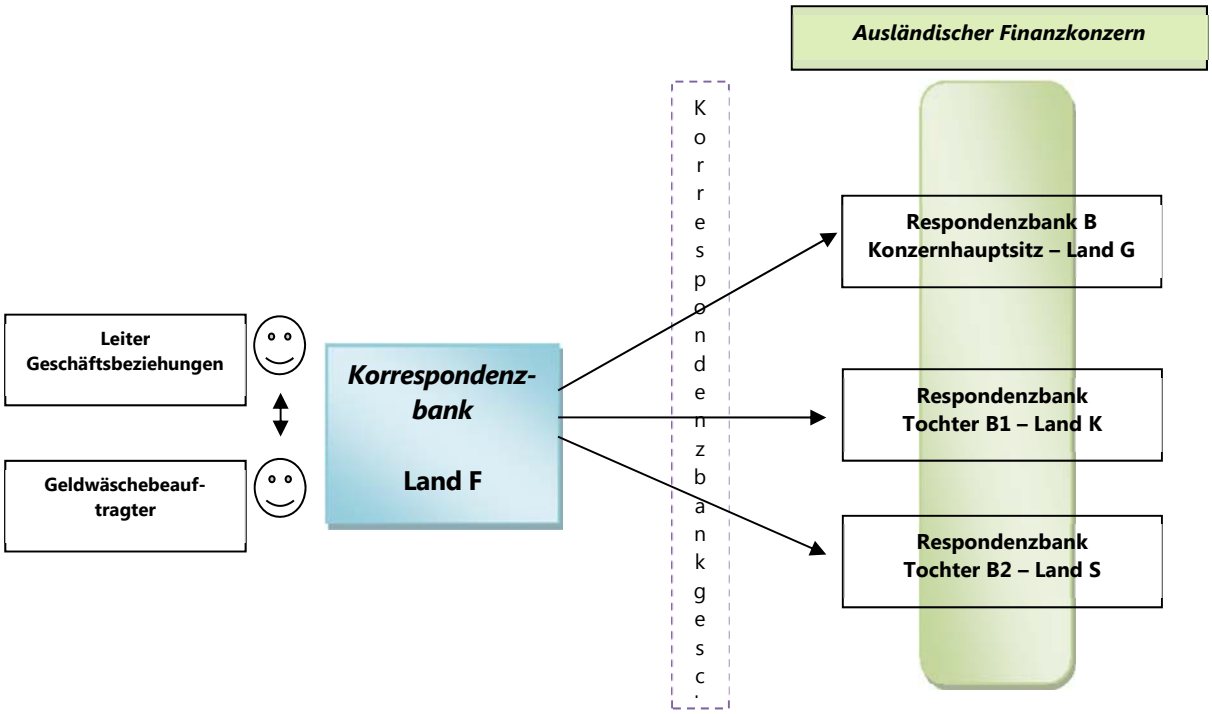


Fall 1

19. Unterhält eine Korrespondenzbank Geschäftsbeziehungen zu mehreren Instituten, die demselben Konzern angehören, aber in verschiedenen Aufnahmeländern niedergelassen sind (Fall 2), sollte die Korrespondenzbank die Tatsache berücksichtigen, dass diese Institute zum selben Konzern gehören. Dennoch sollte die Korrespondenzbank jeweils auch die Risiken von Geldwäsche und Terrorismusfinanzierung in jeder einzelnen Beziehung bewerten.

[44] Jede Konzerngesellschaft erbringt im jeweiligen Aufnahmeland Korrespondenzbankdienstleistungen.

Fall 2



VII. Risikomanagement

20. Eine Bank sollte über spezifische Verfahren für die Handhabung der Korrespondenzbankbeziehungen verfügen. Die Geschäftsbeziehungen sollten Gegenstand einer schriftlichen Vereinbarung sein, in der die Aufgaben und Zuständigkeiten der Partnerbanken klar festgelegt sind.

21. Die Geschäftsleitung sollte im Hinblick auf Aktivitäten des Korrespondenzbankgeschäfts auch die Zuständigkeiten und die Aufgaben der verschiedenen bankinternen Einheiten (Geschäftsbereiche, Compliance-Beauftragte – einschl. Chief AML/CFT-Officer oder Group AML/CFT-Officer –, Revision usw.) berücksichtigen.

22. Die Funktionsbereiche Interne Revision und Compliance[45] tragen bei einer Bank grosse Verantwortung, wenn es darum geht, die Einhaltung der Verfahren für Aktivitäten im Bereich Korrespondenzbankgeschäfte zu bewerten und zu sichern. Die Massnahmen der Respondenzbanken zur Feststellung der Identität, das Einholen von Informationen, die Verfahren zur Bewertung der Risiken von Geldwäsche und Terrorismusfinanzierung und die laufende Überwachung der Korrespondenzbankbeziehungen sollten Gegenstand interner Kontrollen sein.

[45] Siehe *The internal audit function in banks*, Juni 2012 und Grundsatz 26 zu interner Kontrolle und Prüfung in *Grundsätze für eine wirksame Bankenaufsicht*, September 2012.

Anhang 3

Liste wichtiger FATF-Empfehlungen

Neue FATF-Empfehlungen (einschl. ihrer Auslegungshinweise)
• R. 1: Bewertung von Risiken und Anwendung eines risikobasierten Ansatzes
• R. 2: Nationale Zusammenarbeit und Koordination
• R. 9: Finanzinstitute und Bankgeheimnis
• R. 10: Sorgfaltspflichten bei der Feststellung der Kundenidentität
• R. 11: Führen von Aufzeichnungen
• R. 12: Politisch exponierte Personen
• R. 13: Korrespondenzbankgeschäfte
• R. 15: Neue Technologien
• R. 16: Elektronischer Zahlungsverkehr
• R. 17: Delegierung an Dritte
• R. 18: Interne Kontrollen und ausländische Niederlassungen und Tochterunternehmen
• R. 20: Meldung verdächtiger Transaktionen
• R. 26: Regulierung und Beaufsichtigung von Finanzinstituten
• R. 40: Internationale Zusammenarbeit