

Rundschreiben zum risikookorientierten Ansatz

zur Prävention von
Geldwäscherei und
Terrorismusfinanzierung

3.1.1.1	Kredit- oder Finanzinstitut bzw. Versicherungsunternehmen aus einem EWR-Mitgliedstaat oder gleichwertigem Drittstaat (§ 40a Abs. 1 Z 1 BWG, § 98c Abs. 1 Z 1 lit. a und b VAG)	23
3.1.1.2	Börsennotierte Gesellschaft (§ 40a Abs. 1 Z 2 BWG, § 98c Abs. 1 Z 1 lit. c VAG)	24
3.1.1.3	Inländische Behörde (§ 40a Abs. 1 Z 3 BWG, § 98c Abs. 1 Z 1 lit. d VAG)	25
3.1.1.4	Behörde oder öffentliche Einrichtung der EU (§ 40a Abs. 1 Z 4 BWG, § 98c Abs. 1 Z 1 lit. e VAG)	25
3.1.2.	Beaufsichtigte Unternehmen gemäß BWG	26
3.1.2.1	E-Geld (§ 40a Abs. 2 Z 1 BWG)	26
3.1.2.2	Schulsparen (§ 40a Abs. 2 Z 2 BWG).....	26
3.1.3.	Versicherungsunternehmen.....	26
3.1.3.1	Bagatellverträge (§ 98c Abs. 1 Z 2 lit. a VAG).....	26
3.1.3.2	Rentenversicherungsverträge (§ 98c Abs. 1 Z 2 lit. b VAG).....	27
3.2.	Verstärkte Sorgfaltspflichten	27
3.2.1.	Gleichermaßen für beaufsichtigte Unternehmen nach BWG und Versicherungsunternehmen anwendbare Fälle	28
3.2.1.1	Ferngeschäft (§ 40b Abs. 1 Z 1 BWG, § 98d Abs. 1 Z 1 VAG).....	28
3.2.1.2	Transaktionen oder Geschäftsbeziehungen mit Bezug zu politisch exponierten Personen (§ 40b Abs. 1 Z 3 BWG, § 98d Abs. 1 Z 2 VAG). ...	28
3.2.2.	Beaufsichtigte Unternehmen gemäß BWG.....	30
3.2.2.1	Grenzüberschreitende Korrespondenzbankbeziehungen (§ 40b Abs. 1 Z 2 BWG)	30
3.2.2.2	Sonstige Anwendungsfälle.....	32
3.2.3.	Versicherungsunternehmen.....	33
3.2.3.1	Sonstige Anwendungsfälle.....	33
4.	Anhang	35
4.1.	Basler Ausschuss für Bankenaufsicht - Risikomatrix	35
4.2.	Basler Ausschuss für Bankenaufsicht - Verbindung der Risikobewertung zum AML-Managementprogramm	37
4.3.	Materialien.....	38

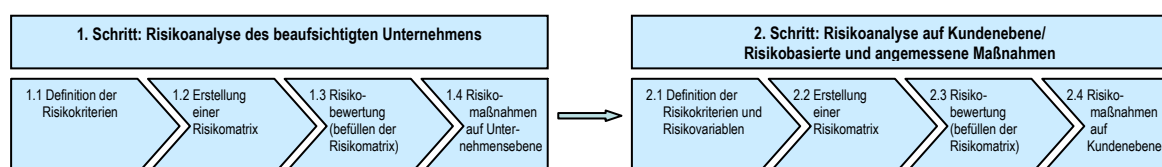
1. Einleitung

- 1 Der risikoorientierte Ansatz ist bedeutend für die Prävention von Geldwäscherei und Terrorismusfinanzierung. Er ermöglicht, beruhend auf Erfahrungen, den gezielten Einsatz von Ressourcen und Aktivitäten im Verhältnis zur Wahrscheinlichkeit, als Unternehmen zu Zwecken der Geldwäscherei oder Terrorismusfinanzierung missbraucht zu werden. Der risikoorientierte Ansatz berücksichtigt weiter den Grundsatz der Proportionalität, indem geeignete Maßnahmen im Verhältnis zum tatsächlich vorhandenen Risiko gesetzt werden.
- 2 Dieses Rundschreiben soll den beaufsichtigten Unternehmen, die Adressaten dieses Rundschreibens sind, helfen, jene Situationen festzustellen, in denen zusätzliche Maßnahmen und Kontrollen angemessen erscheinen, um wirksam den gesetzlichen Anforderungen zu entsprechen. Die Anwendung eines risikoorientierten Ansatzes verlangt kein Abstreifen von Geschäftsbeziehungen ausschließlich aufgrund der Zugehörigkeit zu einer höheren Risikoklasse.
- 3 Die gesetzliche Basis für den risikoorientierten Ansatz im Zusammenhang mit der Prävention von Geldwäscherei und Terrorismusfinanzierung findet sich insbesondere in den §§ 40 Abs. 2a und 2b, 40a, 40b und 41 Abs. 4 Z 1 Bankwesengesetz (BWG) bzw. §§ 98b Abs. 3 und 4, 98c, 98d und 98h Abs. 1 Z 1 Versicherungsaufsichtsgesetz (VAG) sowie § 6 Wertpapieraufsichtsgesetz 2007 (WAG 2007), § 19 Abs. 5 Zahlungsdienstegesetz (ZaDiG) und § 13 Abs. 1 E-Geldgesetz, welche jeweils auf die Bestimmungen des BWG verweisen. Der risikoorientierte Ansatz besteht im Wesentlichen aus der Verpflichtung der beaufsichtigten Unternehmen, eine Risikoanalyse durchzuführen sowie in bestimmten Fällen risikobasierte und angemessene Maßnahmen anzuwenden.
- 4 Generell gilt, dass risikobasierte und angemessene Maßnahmen anzuwenden sind, wenn Anhaltspunkte für ein erhöhtes Risiko bestehen. Damit beaufsichtigte Unternehmen feststellen können, ob ein erhöhtes Risiko vorliegt, ist es unerlässlich, über detaillierte Angaben zum Kunden und/oder der Transaktion zu verfügen. Je mehr Informationen beaufsichtigte Unternehmen besitzen, umso eher haben sie ein vollständiges Bild über eine Geschäftsbeziehung oder eine Transaktion und können Auffälligkeiten erkennen.
- 5 Dieses Rundschreiben beinhaltet Überlegungen der Aufsichtsbehörde, die von beaufsichtigten Unternehmen als hilfreich für die Anwendung des auf die konkreten Erfordernisse des einzelnen beaufsichtigten Unternehmens maßgeschneiderten risikoorientierten Ansatzes betrachtet werden mögen. Damit im Einklang sollen die Einzelheiten des unternehmensspezifischen risikoorientierten Ansatzes stehen, der entsprechend der Spezifika der ausgeübten Tätigkeiten des beaufsichtigten Unternehmens anzuwenden ist. Standards und andere Veröffentlichungen internationaler Organisationen und Initiativen fanden bei Erstellung des Rundschreibens entsprechende Berücksichtigung.

- 6 Dieses Rundschreiben richtet sich an alle österreichischen Kreditinstitute sowie an alle Kreditinstitute aus EWR-Mitgliedstaaten, wenn sie in Österreich im Wege der Dienstleistungsfreiheit oder im Rahmen der Niederlassungsfreiheit über Zweigstellen tätig sind.
- 7 Dieses Rundschreiben richtet sich weiters an alle österreichischen Wertpapierfirmen und Wertpapierdienstleistungsunternehmen (WPDLU) sowie an Wertpapierfirmen aus EWR-Mitgliedstaaten, wenn sie in Österreich im Wege der Dienstleistungsfreiheit oder im Rahmen der Niederlassungsfreiheit über Zweigstellen tätig sind.
- 8 Dieses Rundschreiben richtet sich auch an alle österreichischen Zahlungsinstitute und E-Geld-Institute sowie an Zahlungsinstitute und E-Geld-Institute aus EWR-Mitgliedstaaten, wenn sie in Österreich im Wege der Dienstleistungsfreiheit oder im Rahmen der Niederlassungsfreiheit über Zweigstellen tätig sind.
- 9 Dieses Rundschreiben richtet sich ebenso an alle Versicherungsunternehmen, die in Österreich die Lebensversicherung betreiben sowie an Versicherungsunternehmen aus EWR-Mitgliedstaaten, wenn sie in Österreich über eine Zweigniederlassung oder im Wege des Dienstleistungsverkehrs tätig sind, und Versicherungsunternehmen aus Drittländern, wenn sie in Österreich über eine Zweigniederlassung tätig sind. Das Rundschreiben ist darüber hinaus auch an Tochterunternehmen und Zweigniederlassungen österreichischer Versicherungsunternehmen in Drittländern adressiert.
- 10 Die Adressaten dieses Rundschreibens werden im Folgenden einheitlich als beaufsichtigte Unternehmen bezeichnet. Sofern eine Unterscheidung zwischen Instituten gemäß Rz 6, 7, 8 und 11 einerseits und Versicherungsunternehmen gemäß Rz 9 andererseits gemacht wird, wird dies für die ersteren durch die Formulierung „beaufsichtigte Unternehmen gemäß BWG“ und für letztere durch die Formulierung „Versicherungsunternehmen“ ausgedrückt.
- 11 Finanzinstitute gemäß § 1 Abs. 2 BWG sind ebenso von den im BWG normierten Sorgfaltspflichten zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung erfasst. Der Inhalt dieses Rundschreibens vermag daher auch Finanzinstituten Hilfestellung bei der Anwendung der einschlägigen gesetzlichen Bestimmungen zu leisten. Finanzinstitute gemäß § 1 Abs. 2 BWG sind vom Begriff „beaufsichtigte Unternehmen“ miterfaßt.
- 12 Die konkrete Umsetzung der Empfehlungen dieses Rundschreibens obliegt den einzelnen beaufsichtigten Unternehmen und hat sich insbesondere an deren Art, Größe, Geschäftsstruktur und Risikopotential zu orientieren.
- 13 Dieses Rundschreiben gibt die Rechtsansicht der FMA zu den gesetzlich festgelegten Sorgfaltspflichten zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung wieder. Die rechtlichen Grundlagen bleiben dadurch unberührt. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus dem Rundschreiben nicht abgeleitet werden.

2. Allgemeiner Teil: Der risikoorientierte Ansatz

- 14 Ein angemessen gestalteter risikoorientierter Ansatz gibt dem beaufsichtigten Unternehmen Mittel zur Identifizierung der für die Beurteilung der potentiellen Geldwäscherei- und Terrorismusfinanzierungsrisiken heranzuziehenden Kriterien in die Hand. Ein angemessen umgesetztes risikoorientiertes Verfahren stellt auch ein Regelwerk zur Identifizierung der Höhe des mit Kunden und Transaktionen potenziell verbundenen Geldwäscherei- und Terrorismusfinanzierungsrisikos bereit, sodass sich das beaufsichtigte Unternehmen auf die Kunden und Transaktionen konzentrieren kann, die potentiell das größte Geldwäscherei- und Terrorismusfinanzierungsrisiko darstellen.
- 15 Die Einzelheiten des unternehmensspezifischen risikoorientierten Verfahrens sollten auf Grundlage der Geschäftstätigkeit des jeweiligen beaufsichtigten Unternehmens festgelegt werden. Falls angemessen und durchführbar, sollte das Regelwerk (z.B. Richtlinien, Verfahren und Kontrollen), in denen niedergelegt ist, wie das beaufsichtigte Unternehmen seine Geldwäscherei- und Terrorismusfinanzierungsrisiken steuert und mindert, konzernweit bekannt gemacht werden.
- 16 Es wird jedoch darauf hingewiesen, dass sich die Merkmale der Terrorismusfinanzierung von denen der Geldwäscherei unterscheiden und daher die damit verbundenen Risiken ohne umfassendere Indikatoren der zur Terrorismusfinanzierung eingesetzten Methoden und Techniken möglicherweise schwer zu beurteilen sind.
- 17 Während im ersten Schritt der Risikoanalyse das abstrakte Risiko des beaufsichtigten Unternehmens durch Erfassung und Auswertung der Risikokriterien ermittelt wird, erfolgt im zweiten Schritt die kunden- bzw. transaktionsspezifische Betrachtung und Analyse. Es sollte besonders darauf geachtet werden, die Risikoeinstufung erst nach einer sorgfältigen Ermittlung der Risikokriterien vorzunehmen und nicht versehentlich die Risikoeinstufung bei Bewertung der Risikokriterien einfließen zu lassen. Ebenso wenig sollte die Risikoanalyse des beaufsichtigten Unternehmens mit der kunden- bzw. transaktionsspezifischen Analyse vermengt werden.

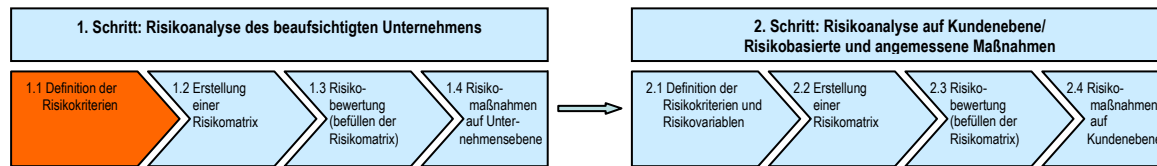


2.1. Risikoanalyse

- 18 Zur Risikoanalyse führt das Gesetz aus (§ 40 Abs. 2b BWG bzw. § 98b Abs. 4 VAG):
- 19 „Die [beaufsichtigten Unternehmen] haben ihr Geschäft anhand geeigneter Kriterien (insbesondere Produkte, Kunden, Komplexität der Transaktionen, Geschäft der Kunden, Geographie) einer Risikoanalyse betreffend ihres Risikos, für Zwecke der Geldwäscherei und Terrorismusfinanzierung missbraucht zu werden, zu unterziehen. Die [beaufsichtigten Unternehmen] müssen gegenüber der FMA nachweisen können, dass der Umfang der auf Grund der Analyse gesetzten Maßnahmen im Hinblick auf die Risiken der Geldwäscherei und der Terrorismusfinanzierung als angemessen anzusehen ist.“
- 20 Mit dieser gesetzlichen Regelung wird anerkannt, dass eine Risikoanalyse die Grundlage zur Anwendung des europarechtlich und nationalstaatlich vorgesehenen risikoorientierten Ansatzes darstellt. Die Einzelheiten des unternehmensspezifischen risikoorientierten Ansatzes sollten auf Grundlage der Geschäftstätigkeit des jeweiligen beaufsichtigten Unternehmens festgelegt werden (siehe dazu die Ausführungen zu den Risikokriterien, Abschnitt 2.1.1). Dieses Verfahren, angemessen für den konkreten Einzelfall umgesetzt, stellt in weiterer Folge eine Methode zur Identifizierung des mit dem Kunden und der Transaktionen potentiell verbundenen Geldwäscherei- und Terrorismusfinanzierungsrisikos dar, und versetzt das beaufsichtigte Unternehmen in die Lage, dem Risiko entsprechende Maßnahmen zielgerichtet einzusetzen (siehe dazu die Ausführungen zum Prozess der Risikoanalyse, Abschnitt 2.1.2). Ein Element zur Umsetzung des risikoorientierten Ansatzes ist die Etablierung von Systemen und Maßnahmen zwecks laufenden Monitoring der Geschäftstätigkeit der beaufsichtigten Unternehmen im Hinblick auf Aktivitäten der Geldwäscherei und Terrorismusfinanzierung. Ein anderes Element ist die verstärkte Konzentration auf Kunden und Transaktionen, die potentiell ein größeres Risiko der Geldwäscherei und Terrorismusfinanzierung darstellen (siehe dazu jeweils Abschnitt 2.2).
- 21 Die Einführung und Etablierung „angemessene[r] und geeignete[r] Strategien für [...] die Risikobewertung [und] das Risikomanagement [...]“ wird von § 41 Abs. 4 Z 1 BWG und § 98h Abs. 1 Z 1 VAG verlangt.

2.1.1. Risikokriterien

- 22 Erster Schritt einer Risikoanalyse ist die Identifizierung potentieller Risiken. Das BWG und das VAG nennen hierzu einige Risikokriterien, wobei diese Liste nicht abschließend ist. Dabei wird bei einer generellen Risikoanalyse ermittelt, welche Risikokriterien durch die Geschäftstätigkeit, die durch die Geschäftspolitik vorgegeben wird, für das beaufsichtigte Unternehmen gegeben sind. Nachfolgend sind in den einzelnen Risikokriterien Anhaltspunkte für ein erhöhtes Risiko angeführt, wobei das Vorliegen eines einzelnen Anhaltspunktes nicht automatisch zu einer Qualifizierung als erhöhtes Risiko führt, sondern vielmehr im Rahmen einer Gesamtbetrachtung Berücksichtigung finden sollte.



2.1.1.1 Produkte

- 23 In die Bewertung des Gesamt-Geldwäscherei und Terrorismusfinanzierungsrisikos sollten die Risiken einfließen, die sich aus den vom beaufsichtigten Unternehmen angebotenen Produkten und Dienstleistungen ergeben. Die maßgeblichen Geschäftszweige eines beaufsichtigten Unternehmens sind daher wesentlicher Anknüpfungspunkt für die Risikokategorisierung. Bei der Bestimmung der von Produkten und Dienstleistungen ausgehenden Risiken sollten Faktoren berücksichtigt werden wie: Ausmaß des Kundenkontakts, internationaler Bezug, direkte Kundenbeziehung erfolgt durch ein anderes beaufsichtigtes Unternehmen etc.
- 24 Die Produktkriterien sind nach Geschäftsfeld des beaufsichtigten Unternehmens unterschiedlich.
- 25 Für beaufsichtigte Unternehmen gemäß BWG gilt insbesondere:
- Vermögensverwaltung vermögender Privatkunden („private banking“): Aufgrund der Kundenstruktur und der hohen Beträge, die im Privatkundengeschäft typischerweise zum Einsatz kommen, kann ein erhöhtes Risiko bestehen.
 - Das Risiko kann weiters erhöht werden, wenn bei der Kundenstruktur Unternehmensstrukturen wie Off-Shore Unternehmen, Stiftungen, Treuhandschaften, Trusts oder andere Formen vorliegen (z.B. nominee shareholder), die den wirtschaftlichen Eigentümer nicht klar erkennen lassen.
 - Grenzüberschreitende Korrespondenzbankbeziehungen mit Drittländern sind gesetzlich verpflichtend als Anwendungsfall der verstärkten Sorgfaltspflichten vorgeschrieben. Für weitere Ausführungen siehe Abschnitt 3.2.2.1.
 - Dienstleistungen, die ohne persönlichen Kontakt zwischen dem beaufsichtigten Unternehmen und dem Kunden und leicht grenzüberschreitend erfolgen können, wie
 - Online-Banking;
 - elektronischer Zahlungsverkehr und Kreditkartenzahlungen;
 - neue Technologien;
 - Begründung der Geschäftsbeziehung über das Internet;
 - Durchführung von Transaktionen (meistens im Rahmen einer Geschäftsbeziehung) über das Internet, inklusive Auftragsorder für Wertpapiere;
 - Verwendung von Geldausgabeautomaten und Geldeinzahlungsautomaten;
 - Auftragserteilung via Fax oder Email.
 - Abwicklung von Akkreditiven.

- Export-/Importfinanzierung von Hochrisikogütern bzw. in Länder, die Sanktionen, Embargos oder ähnlichen Maßnahmen internationaler Organisationen im Bereich der Bekämpfung der Geldwäscherei und Terrorismusfinanzierung unterworfen sind.
- Spareinlagen gemäß § 31 Abs. 3 in Verbindung mit § 32 Abs. 4 Z 1 BWG, die nicht auf den Namen des identifizierten Kunden lauten und über die gegen Angabe eines Lösungswortes verfügt werden kann.
- Produkte mit überwiegenden Bargeldtransfers und Bargeldauszahlungen.
- Non-resident Konten, Nummernkonten, Geschäftsbeziehungen zu Kunden, auf deren ausdrücklichen Wunsch Korrespondenz ausschließlich zur Abholung bereit gehalten wird („schalterlagernd“).

26 Für Versicherungsunternehmen gilt insbesondere:

- Einmalerläge stellen ein höheres Risiko als laufende Prämienzahlungen dar.
- Verträge mit Kapitalauszahlung stellen ein höheres Risiko dar als solche mit Rentenauszahlung.
- Kapitalversicherung stellt ein höheres Risiko dar als Risikoversicherung.
- Unübliche Vertragsgestaltung stellt ein höheres Risiko dar als Standardverträge.
- Produkte mit langfristiger Veranlagung, nach Standardvertragsmustern („traditionelle Lebensversicherung“ als Massengeschäft) und relativ niedrigen Rückkaufswerten werden typischerweise ein geringeres Risiko mit sich tragen.

27 Zu den Produktrisiken zählen auch jene Risiken, welche mit Dienstleistungen verbunden sind, die als Nebenleistung zur vertraglich vereinbarten Leistung angeboten werden.

2.1.1.2 Kunden

28 Bei der Analyse des Risikokriteriums „Kunden“ sollte die Kundenstruktur erfasst und betrachtet werden. Dazu gehören insbesondere:

- Kunden, die ihre Geschäftsbeziehungen oder Transaktionen unter ungewöhnlichen Umständen durchführen, wie
 - erhebliche und nicht plausible geographische Distanz zwischen beaufsichtigtem Unternehmen und Wohnsitz/Hauptsitz des Kunden;
 - häufige und nicht erklärte Übertragung von Konten auf verschiedene beaufsichtigte Unternehmen bzw. Umschichtung auf neue Verträge;
 - häufige und nicht geklärte Mittelbewegung zwischen beaufsichtigten Unternehmen verschiedener Standorte;
 - ungewöhnliche Barbewegungen;
 - Zuhilfenahme von komplexen Firmenkonstrukten („off-shore“) oder solchen, die den wirtschaftlichen Eigentümer nicht klar erkennen lassen (siehe auch oben Abschnitt 2.1.1.1.);
 - Mittelbewegungen, die nicht mit dem wirtschaftlichen Hintergrund in Einklang stehen.
- Kunden aus Ländern oder Regionen, die als hohes Risiko einzuschätzen sind, und Kunden, die in Ländern oder Regionen, die als hohes Risiko einzuschätzen sind, Einkommen bzw. Vermögen erwirtschaftet haben (siehe auch Abschnitt 2.1.1.5).

- Kunden, bei denen die Überprüfung der Identität des wirtschaftlichen Eigentümers oder des beherrschenden Anteils durch die Struktur oder die gesellschaftsrechtliche Gestaltung erschwert sein kann (Off-Shore Unternehmen, Stiftungen, Treuhandschaften, Trusts oder andere Formen wie z.B. nominee Shareholder).
- Kunden, die keine berufsmäßigen Parteienvertreter sind und auf fremde Rechnung bzw. im fremden Auftrag handeln.
- Nicht auf Gewinn ausgerichtete Vereinigungen unter Berücksichtigung des Organisationszwecks, des Herkunftslandes bzw. Registrierungslandes und der Tätigkeit, sowohl einnahmen- als auch ausgabenseitig.
- Politisch exponierte Personen (PEP) sind gesetzlich verpflichtend als Anwendungsfall der verstärkten Sorgfaltspflichten vorgeschrieben. Für weitere Ausführungen siehe Abschnitt 3.2.1.2.

2.1.1.3 Komplexität der Transaktionen

- 29 Bei der Analyse des Risikos sollte die Art und Weise der Durchführung der Transaktion erfasst werden.
- 30 Beurteilungskriterien sind dabei für beaufsichtigte Unternehmen gemäß BWG insbesondere:
- Betrag und Häufigkeit der Transaktionen;
 - Grenzüberschreitung;
 - Auftraggeber bzw. Empfänger der Transaktionen;
 - Transaktionen, die vordergründig eines wirtschaftlichen Zwecks entbehren;
 - Transaktionen, die nicht mit dem im Kundenprofil angegebenen Zweck der Geschäftsbeziehung übereinstimmen;
 - Trennung von Transaktionen zum Unterschreiten der zur Identifizierung verpflichtenden Betragsgrenze („smurfing“);
 - Vollständigkeit der Daten des Auftraggebers im Sinne der sogenannten Auftraggeber-Verordnung (Verordnung (EG) Nr. 1781/2006 des Europäischen Parlaments und des Rates vom 15. November 2006 über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers).
- 31 Für Versicherungsunternehmen gilt insbesondere:
- Verhältnis zwischen Versicherungsvertrag und dem damit verbundenen Darlehen;
 - Treuhänderkonstruktion;
 - Fremdfinanzierung;
 - Grenzüberschreitung;
 - Abschluss von mehreren Versicherungsverträgen zum Unterschreiten der zur Identifizierung verpflichtenden Betragsgrenze („smurfing“).

2.1.1.4 Geschäft der Kunden

- 32 Bei der Analyse des Risikokriteriums „Geschäft der Kunden“ sollte der Unternehmensgegenstand der Kunden erfasst werden.
- 33 Sowohl berufsmäßige Parteienvertreter wie Rechtsanwälte, Notare, Wirtschaftstreuhänder, Steuerberater etc., die Konten bei einem beaufsichtigten Unternehmen unterhalten und im Namen ihrer Mandanten handeln, als auch Vermittler, sofern sie eine Handlungsvollmacht für ihre Klienten besitzen, können ein erhöhtes Risiko bedeuten.
- 34 Ebenso können Unternehmen, deren Geschäftstätigkeit verstärkt auf Bargeld ausgerichtet ist, ein erhöhtes Risiko darstellen.

2.1.1.5 Geographie

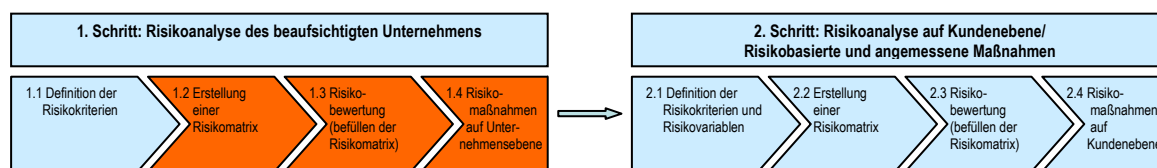
- 35 Zu den Kriterien, die zu der Feststellung führen könnten, dass Transaktionen innerhalb oder mit einer geographischen Region ein höheres Risiko darstellen¹, zählen insbesondere:
- der Standort des beaufsichtigten Unternehmens, seiner Filiale oder Zweigstelle im In- und Ausland.
 - Länder, die Sanktionen, Embargos oder ähnlichen Maßnahmen internationaler Organisationen im Bereich der Bekämpfung der Geldwäscherei und Terrorismusfinanzierung unterworfen sind. Geschäftsbeziehungen mit Kunden aus diesen Ländern bedeuten jedenfalls ein höheres Risiko. Darunter fallen solche Länder, die Gegenstand einer Verordnung der Bundesregierung gemäß § 78 Abs. 8 BWG sind, sogenannte Nicht-Kooperationsstaaten.
 - Länder, über die Informationen im Bereich der Geldwäscherei und Terrorismusfinanzierung durch Mitteilungen des BMF oder der WKÖ veröffentlicht wurden, und die auf der Homepage der FMA angeführt sind.
 - Länder, mit denen das beaufsichtigte Unternehmen noch keine Erfahrungen hat und die laut glaubwürdiger Quellen nicht über angemessene Gesetze, Vorschriften und andere Maßnahmen zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung verfügen oder Mittel zur Unterstützung terroristischer Handlungen bereitstellen oder auf ihrem Gebiet terroristische Organisationen operieren lassen.
 - Länder, mit denen das beaufsichtigte Unternehmen noch keine Erfahrungen hat und in denen laut glaubwürdiger Quellen ein erhebliches Maß an Korruption herrscht.
 - Länder, die über keine offiziellen Firmenbuchregister verfügen, bzw. in denen der im Firmenbuchregister bereitgestellte Informationsgehalt nicht dem des österreichischen Firmenbuchs entspricht und in denen laut glaubwürdiger Quellen ein erhöhtes Risiko der Geldwäscherei und Terrorismusfinanzierung besteht, z.B. mangels Angaben über die organschaftlichen Vertreter oder über die Eigentümer.

¹ Siehe auch die von der FMA erlassene Geldwäscherei- und Terrorismusfinanzierungsrisiko-Verordnung – GTV, BGBl. II Nr. 377/2011. In den in dieser Verordnung angeführten Fällen sind jedenfalls verstärkte Sorgfaltspflichten anzuwenden.

- Länder, die gesellschaftsrechtliche Konstruktionen anbieten, die die Feststellung und Überprüfung der Mittelherkunft erschweren und in denen laut glaubwürdiger Quellen ein erhöhtes Risiko der Geldwäscherei und Terrorismusfinanzierung besteht.

36 Der Ausdruck "glaubwürdige Quellen" bezieht sich auf Informationen, die von bekannten Stellen ausgegeben werden, die als seriös gelten, und die diese Informationen veröffentlichen und weithin zugänglich machen. Neben der Financial Action Task Force (FATF) und regionalen FATF-ähnlichen Organisationen („FATF-style regional bodies“ (FSRBs), wie etwa Moneyval), können diese Quellen u.a. folgende umfassen: supranationale oder internationale Organisationen wie Internationaler Währungsfonds, Weltbank, Egmont Group of Financial Intelligence Units sowie die Staatengruppe gegen Korruption (GRECO) beim Europarat, sowie maßgebliche nationale Regierungsstellen. Die von diesen glaubwürdigen Quellen bereitgestellten Informationen haben informativen Charakter und sollten nicht als automatische Feststellung erachtet werden, dass ein höheres Risiko besteht.

2.1.2. Der Prozess der Risikoanalyse



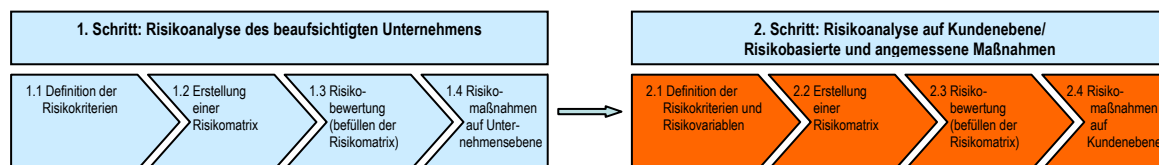
- 37 Die Analyse des Umfelds, in dem ein beaufsichtigtes Unternehmen agiert, gibt grundsätzlichen Aufschluss über die Bedrohung und Anfälligkeit dieses beaufsichtigten Unternehmens gegenüber Geldwäscherei und Terrorismusfinanzierung. Am Ende der Analyse des Umfelds des beaufsichtigten Unternehmens soll dieses wissen, welchem abstrakten Risiko der Geldwäscherei und Terrorismusfinanzierung es aufgrund seiner Geschäftspolitik ausgesetzt ist. Die Bedrohung ergibt sich aus der Wahrscheinlichkeit, dass das beaufsichtigte Unternehmen tatsächlich Teil eines Versuchs zur Geldwäscherei und/oder Terrorismusfinanzierung wird, und ist durch die einzelne Geschäftsbeziehung oder Transaktion beeinflusst. Die daraus entstehenden Folgen sind die Auswirkungen, die zu einem Großteil im Reputationsrisiko manifest werden.
- 38 Diese drei Elemente – Bedrohung, Wahrscheinlichkeit und Auswirkungen – sind maßgeblich für die Einstufung in eine Risikokategorie. Zur Bewertung des Risikos erweist sich die Verwendung einer Risikomatrix als hilfreich. In ihr sind die Risikokategorien aufgelistet, die mindestens drei Stufen, wie geringes, mittleres und hohes Risiko, enthalten. Eine dreistufige Matrix wird dann als ausreichend erachtet, wenn sichergestellt ist, dass hinter den Stufen Handlungsmechanismen stehen, die für die jeweilige Kundengruppe differenziert ablaufen.
- 39 Aus der Verknüpfung verschiedener Faktoren ergibt sich in der ersten Phase das Risiko der Geschäftstätigkeit des beaufsichtigten Instituts im Allgemeinen und die daraus resultierenden Risikomaßnahmen (u.a. Kundenakzeptanzvorgaben, Monitoringvorgaben, Mitarbeiter-

Training und interne Prozesse). In der zweiten Phase erfolgt die Einstufung der konkreten einzelnen Geschäftsbeziehung oder Transaktion in die festgelegten Risikokategorien und die Anwendung der dafür festgelegten Maßnahmen. Die Einstufung kann für Gruppen vergleichbarer Kunden pauschal erfolgen. Faktoren mit keinem Risiko sollten nicht verwendet werden. Je mehr Stufen bestehen, umso feiner kann unterschieden werden. Im Prozess des Zusammenfügens von verschiedenen Risikokategorien (z.B. der Kunde ist eine politisch exponierte Person mit Geschäftspartner in einem Land erhöhter Korruptionsanfälligkeit) können so risikomindernde und risikoe erhöhende Faktoren miteinander in Relation gesetzt werden und es ergibt sich ein differenziertes Gesamtbild (siehe dazu auch die Risikomatrix des Basler Ausschusses für Bankenaufsicht in Abschnitt 4.1.).

- 40 Beaufsichtigte Unternehmen können überdies erwägen, bestimmte Geschäfte aufgrund ihrer besonders stark ausgeprägten Risikoeinstufung grundsätzlich nicht durchzuführen. In jedem Fall soll dem beaufsichtigten Unternehmen das Risiko bewusst sein und entsprechende Maßnahmen gesetzt werden, um das Risiko, das sich aus einer Geschäftsbeziehung oder einer Transaktion ergibt, auszugleichen.
- 41 Ziel der Risikoanalyse ist es, ein umfassendes Bild und die abstrakte Kenntnis über die Anfälligkeit der Geschäftstätigkeit eines beaufsichtigten Unternehmens im Bereich der Geldwäscherei und Terrorismusfinanzierung zu bekommen. Während im ersten Schritt auf abstrakter Ebene Risiken ermittelt werden und ihnen Risikokategorien zugeordnet wurden, gilt es im nächsten Schritt, die Risikokategorien auf die konkrete Geschäftstätigkeit des Kunden umzulegen und in Verbindung zu bringen.

2.2. Risikobasierte und angemessene Maßnahmen

- 42 In der zweiten Phase der Risikoanalyse liegt der Fokus auf dem einzelnen Kunden oder der einzelnen Transaktion des beaufsichtigten Unternehmens, wobei oftmals Systeme verwendet werden, die die Kunden weitgehend automationsunterstützt mit Hilfe von Computerprogrammen erfassen.



- 43 Jedem Kunden sollte eine Risikoeinstufung zugeteilt werden. Zur Risikoeinstufung können die Risikokriterien, wie in Abschnitt 2.1.1 dargestellt, zur Orientierung herangezogen werden. Die Einstufung kann für Gruppen vergleichbarer Kunden pauschal erfolgen. Diese Risikoeinstufung ist für das Ausmaß der Anwendung von Maßnahmen auf risikoorientierte Grundlage maßgeblich.

- 44 In Fällen, die hochautomatisiert erfolgen, wird die Anwendung risikobasierter Maßnahmen zur Prävention von Geldwäscherei und Terrorismusfinanzierung damit beginnen, dass jene Kunden und Transaktionen laufend gefiltert werden, die erhöhter Beobachtung und Sorgfalt bedürfen. Das beaufsichtigte Unternehmen hat jedenfalls jene Kunden zu kennen, die einem erhöhten Risiko unterliegen. Zur Bewertung des Risikos erweist sich auch hier die Verwendung einer mindestens dreistufigen Risikomatrix als hilfreich, wobei vier Stufen aufgrund der besseren Kategorisierung empfohlen werden. Der Grad der Überwachung des Kunden soll danach gewählt werden, ob er zu einer erhöhten Risikokategorie zählt, abhängig von der Bewertung der vorgenannten Kriterien, wie z.B. Art der Geschäfte oder Transaktionen des Kunden sowie seinem Standort und der Destination einer Dienstleistung.
- 45 Die Überwachung einer Kundenbeziehung sollte nicht statisch erfolgen, sondern Erfahrungen des beaufsichtigten Unternehmens mit dem Kunden und allgemeiner Art berücksichtigen, die gegebenenfalls eine Neubewertung der Monitoringkriterien erfordern können. Aus diesem Grund kann es sich als sinnvoll erweisen, die Evaluierung in regelmäßigen Abständen vorzusehen. Diese Evaluierung der Kundeneinstufung kann im Rahmen der regelmäßigen Kontakte vorgesehen sein.
- 46 Die Anwendung eines risikoorientierten Ansatzes erlaubt dem beaufsichtigten Unternehmen, quantitative oder qualitative Schranken zu ziehen, unter denen eine Beziehung standardmäßig erhöhten Sorgfaltspflichten unterliegt. Diese Schranken sollten ebenfalls regelmäßig evaluiert werden, um die Angemessenheit der Risikokategorie zu rechtfertigen.
- 47 Es wird darauf hingewiesen, dass nicht in allen Fällen die Anwendung von risikobasierten Maßnahmen zulässig ist. So werden im Gesetz z.B. die Fälle, in denen eine Verdachtsmeldung an die Geldwäschemeldeinstelle (§ 4 Abs. 2 Z 1 und 2 des Bundeskriminalamt-Gesetzes, BGBl. I Nr. 22/2002) zu erstatten ist, aufgelistet. Die Entscheidung über die Erstattung einer Verdachtsmeldung ist somit eine gesetzliche Verpflichtung und darf nicht nach Risikogesichtspunkten erfolgen. Das Einfrieren von Vermögenswerten ist ebenfalls kein Anwendungsfall des risikoorientierten Ansatzes.
- 48 Im Umgang mit Kunden oder Transaktionen aus Nicht-Kooperationsstaaten gelten die Bestimmungen des § 78 Abs. 9 Z 4 und 5 BWG. Darüber hinaus können weitere verstärkte Sorgfaltsmaßnahmen erforderlich sein.

2.2.1. Variablen mit möglichem Einfluss auf das Risiko

- 49 Die von einem beaufsichtigten Unternehmen gewählten Verfahren zur Umsetzung des risikoorientierten Ansatzes können kundenspezifische oder transaktionsspezifische Risikovariablen berücksichtigen. Durch diese Variablen kann sich das in Bezug auf einen bestimmten Kunden oder eine bestimmte Transaktion wahrgenommene Risiko erhöhen oder vermindern. Zu diesen Variablen gehören beispielsweise die im Folgenden angeführten Variablen.

2.2.1.1 Zweck und Art eines Kontos oder Geschäftsbeziehung

- 50 Der Zweck und die Art eines Kontos oder einer Geschäftsbeziehung kann das bewertete Risiko beeinflussen. Konten, die vorwiegend für herkömmliche Kleinbetragsgeschäfte von Verbrauchern eröffnet werden, stellen im Allgemeinen ein geringeres Risiko dar als ein Konto, das für große Bargeldtransaktionen eines zuvor unbekanntem gewerblichen Unternehmens eröffnet wird. Der Zweck der Geschäftsbeziehung ist vom beaufsichtigten Unternehmen zu erheben (§ 40 Abs. 2a Z 2 BWG, § 98b Abs. 3 Z 2 VAG).

2.2.1.2 Höhe des Betrages

- 51 Die Höhe der von einem bestimmten Kunden eingezahlten Vermögenswerte oder das Volumen der getätigten Geschäfte kann auf das bewertete Risiko Auswirkungen haben. Vermögenswerte in ungewöhnlicher Höhe oder ungewöhnlich große Transaktionen im Vergleich zu jenen, die von Kunden mit ähnlichem Profil erwartet werden können, deuten möglicherweise darauf hin, dass ein Kunde, der anderweitig nicht als Kunde höheren Risikos gilt, als solcher behandelt werden sollte. Im Bereich der Terrorismusfinanzierung werden erfahrungsgemäß allerdings auch Kleinstbeträge im Zusammenhang mit den übrigen Risikoindikatoren eingesetzt. Dieser Anhaltspunkt ist im Rahmen einer Gesamtbetrachtung im Zusammenhang mit anderen Risikofaktoren zu beurteilen.

2.2.1.3 Aufsicht über den Kunden

- 52 Der Grad der Regulierung oder der sonstigen Aufsicht oder Grundsätze der Unternehmensführung, denen ein Kunde unterliegt, hat Einfluss auf seine Risikobeurteilung. Handelt es sich bei einem Kunden um ein Unternehmen, das in einem Land mit zufriedenstellenden Regelungen zur Bekämpfung von Geldwäscherei ansässig ist, stellt dieses aus Geldwäscherperspektive ein geringeres Risiko dar, als ein nicht regulierter Kunde, der nur minimalen Regelungen zur Bekämpfung von Geldwäscherei unterliegt. Zudem stellen Unternehmen und deren hundertprozentige Tochtergesellschaften, die sich im Eigentum von EWR-Mitgliedsstaaten oder anerkannten Drittländern befinden, und deren Wertpapiere am geregelten Markt einer anerkannten Börse gehandelt werden, im Allgemeinen geringere Geldwäscherisiken dar. Diese Unternehmen stammen gewöhnlich aus Ländern mit einem angemessenen, anerkannten Aufsichtssystem und bergen daher aufgrund der von ihnen ausgeübten Geschäftstätigkeit und der weiter reichenden Unternehmensführung, der sie unterworfen sind, unter normalen Umständen ein geringeres Risiko. Ebenso sind diese Unternehmen während der Dauer der Beziehung möglicherweise geringeren Maßnahmen bei der Kontoeröffnung oder Überwachungsverfahren bezüglich der Transaktionen zu unterstellen. Im Gegensatz dazu können hinsichtlich Kunden aus Ländern, die Sanktionen, Embargos oder ähnlichen Maßnahmen internationaler Organisationen im Bereich der Bekämpfung der Geldwäscherei und Terrorismusfinanzierung unterliegen, erhöhte Maßnahmen bei der Kontoeröffnung oder Überwachungsverfahren bezüglich der Transaktionen erfordern.

2.2.1.4 Regelmäßigkeit oder Dauer der Beziehung

- 53 Lange bestehende Beziehungen mit häufigen Kundenkontakten im Laufe der Beziehung stellen aus Geldwäscherperspektive möglicherweise ein geringeres Risiko dar.

2.2.1.5 Erfahrungen mit einem Land

- 54 Vorhandene Erfahrungen mit einem Land können das aus Geldwäscherperspektive wahrgenommene Risiko vermindern. Dazu gehören die Kenntnisse nationaler Gesetze, Vorschriften und Regeln, sowie die Kenntnis von Struktur und Umfang der Aufsicht, über die ausgeübte Geschäftstätigkeit des beaufsichtigten Unternehmens in diesem Land.

2.2.1.6 Komplexe Strukturen

- 55 Die Nutzung zwischengeschalteter Unternehmensvehikel oder anderer Strukturen, für die es keine offenkundige kommerzielle oder sonstige Begründung gibt, oder die die Komplexität unnötig erhöhen oder anderweitig zu einem Transparenzmangel führen, erhöhen das Risiko.

2.2.2. Kontrollen für Situationen höheren Risikos

- 56 Die beaufsichtigten Unternehmen sollten angemessene Maßnahmen und Kontrollen zur Handhabung der potentiellen Geldwäschereirisiken jener Kunden implementieren, die aufgrund des risikoorientierten Ansatzes des beaufsichtigten Unternehmens als Kunden höheren Risikos identifiziert werden.
- 57 Zu den Maßnahmen und Kontrollen, um potentiellen Geldwäschereirisiken entgegenzutreten, gehören u.a.:
- höhere Wachsamkeit seitens des beaufsichtigten Unternehmens gegenüber Hochrisikokunden und Transaktionen, die über den Rahmen des Geschäftszweiges hinausgehen;
 - höhere Standards bei den Verfahrensweisen für die Feststellung der Kundenidentität ("know your customer", KYC) und/oder verstärkte Sorgfaltspflichten;
 - Erhebung zusätzlicher Angaben zur Identität. Siehe dazu das FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Kreditinstitute vom 01.12.2011 (Rz 18 und 20) und das FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Versicherungsunternehmen vom 01.12.2011 (Rz 17 und 19).
 - höhere Standards bei der Überprüfung der Herkunft der Geld- oder Finanzmittel und deren Dokumentation;
 - Einholung der Zustimmung von nächsthöheren Führungsebenen, damit Kontoeröffnung und neue Geschäftsbeziehungen genehmigt werden;
 - stärkere, laufende und institutionalisierte Überwachung von Transaktionen;
 - vermehrte, laufende Kontrollen und häufigere, institutionalisierte Überprüfungen bzw. Beobachtung der Geschäftsbeziehungen;
 - verstärkte und intensiviertere Schulung der Mitarbeiter.

- 58 Kundendaten sind zu aktualisieren und Transaktionen sind zu überwachen (vgl. § 40 Abs. 2a Z 3 und Abs. 2e BWG bzw. § 98b Abs. 3 Z 3 und Abs. 7 VAG); für die Intervalle siehe Abschnitt 2.2.3.3, Rz 75 und 76. Die Evaluierung erfolgt auf der Ebene des beaufsichtigten Unternehmens, und schließt Zweigstellen und Tochterunternehmen mit ein. Über die Ergebnisse dieser konzernweit durchgeführten Evaluierung ist dem Vorstand Bericht zu erstatten.
- 59 Generell gilt, dass es keine Risikokategorie „kein Risiko“ gibt. Die Einstufung in eine Risikokategorie sollte jedenfalls bei Anhaltspunkten, die ein Abweichen von der einmal getroffenen Risikokategorisierung indizieren, evaluiert werden. Anhaltspunkte für ein Abweichen können z.B. sein:
- Änderungen des Kundenverhaltens;
 - Änderungen im typischen Kontoablauf bzw. Transaktionsschemas;
 - Änderungen des wirtschaftlichen Eigentümers (inkl PEP-Eigenschaft, siehe Abschnitt 3.2.1.2).
- 60 Unter den Dokumenten, Daten oder Informationen, die im Zuge der Überwachung der Geschäftsbeziehung mit dem Kunden stets zu aktualisieren sind, sind jene zu verstehen, die bei der Identifizierung des Kunden, der vertretungsbefugten Personen, der Treugeber und wirtschaftlichen Eigentümer zur Erfüllung der Identifizierungspflichten gemäß den §§ 40 Abs. 1, 2 und 2a Z 1, 40a und 40b BWG bzw. §§ 98b Abs. 1, 2 und 3 Z 1, 98c und 98d VAG vorzulegen sind. Zu den Identifizierungspflichten und der Aktualisierung der Angaben siehe das FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Kreditinstitute vom 01.12.2011 und das FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Versicherungsunternehmen vom 01.12.2011.
- 61 Im beaufsichtigten Unternehmen ist jedenfalls eine vom Marktbereich unabhängige Stelle zu implementieren, der für die Aufgabe der laufenden Überwachung umfassende Einschau-, Kontroll- und Weisungsrechte zugestanden werden. Im Regelfall sollte das der besondere Beauftragte gemäß § 41 Abs. 4 Z 6 BWG bzw. § 98h Abs. 1 Z 6 VAG sein.²

2.2.3. Entscheidung über Maßnahmen durch das beaufsichtigte Unternehmen

- 62 Die Entscheidung über die Art und Weise der risikobasierten und angemessenen Maßnahmen sollte vom beaufsichtigten Unternehmen abhängig von den Ergebnissen der risikosteigernden und risikomindernden Faktoren der Risikoanalyse getroffen werden. Die allgemeinen Kriterien können als Anhaltspunkte für die Ausgestaltung der Maßnahmen im Hinblick auf eine konkrete Geschäftsbeziehung oder Transaktion herangezogen werden.
- 63 Bestehen in einer Geschäftsbeziehung oder Transaktion risikoerhöhende Faktoren, so sollte dies verstärkte Maßnahmen und Kontrollen nach sich ziehen. Für verstärkte Maßnahmen

²

Siehe auch das geplante FMA-Rundschreiben zum Geldwäschereibeauftragten.

und Kontrollen siehe Abschnitt 2.2.2, insbesondere Rz 57. Zum Beispiel wird ein Kunde mit Wohnsitz in einem nicht gleichwertigen Drittland, der sich zusätzlich ungewöhnliche Vertragsbedingungen ausbedungen hat, aufgrund der Risikosituation Ziel verstärkter Maßnahmen hinsichtlich Identifizierung sein. Gleiches gilt für Kunden, die juristische Personen innerhalb einer verzweigten Konzernstruktur, möglicherweise sogar mit Auslandsbezug sind, so dass risikobasierte und angemessene Maßnahmen zur Überprüfung der Identität des wirtschaftlichen Eigentümers deutlich stärker ausfallen werden, als bei einer einfachen Konzernstruktur im Inland.

- 64 Beaufsichtigte Unternehmen sollten die Angemessenheit der für eine Risikokategorie festgelegten Sorgfaltspflichten einer laufenden Beobachtung und einer Anpassung im Anlassfall nach Natur, Art und Komplexität der Geschäfte unterziehen.
- 65 Im Bereich der Geldwäscherei und Terrorismusfinanzierung sind zur Erfüllung der Sorgfaltspflichten risikobasierte und angemessene Maßnahmen in folgenden Bereichen anzuwenden:

2.2.3.1 Die Identität des wirtschaftlichen Eigentümers (§ 40 Abs. 2a Z 1 BWG, § 98b Abs. 3 Z 1 VAG)

- 66 Über Aufforderung des beaufsichtigten Unternehmens haben Kunden Informationen über die Identität des wirtschaftlichen Eigentümers (der Begriff ist in § 2 Z 75 BWG bzw. § 98a Abs. 2 Z 3 VAG definiert) bekannt zu geben, sodass dessen Identität festgestellt wird. Die Überprüfung der Identität des wirtschaftlichen Eigentümers erfolgt mittels risikobasierter und angemessener Maßnahmen.
- 67 Die Maßnahmen zur Überprüfung der Identität des wirtschaftlichen Eigentümers müssen so ausgestaltet sein, dass das beaufsichtigte Unternehmen überzeugt ist, die wirtschaftlichen Eigentümer zu kennen. Bei juristischen Personen, inklusive der Rechtskonstruktionen Stiftungen und Trusts, umfasst dies die Kenntnis der Eigentums- und Kontrollverhältnisse betreffend den Kunden. Erkenntnisquellen dafür sind öffentlich zugängliche Registerauszüge und nicht öffentliche Urkunden, aber auch Jahresberichte, Datenbanken oder Internetrecherchen. Sollten die Informationen über die wirtschaftlichen Eigentümer nicht den Erfordernissen für eine Identifizierung im Sinne des § 40 Abs. 1 BWG bzw. § 98b Abs. 1 VAG genügen, können diese trotzdem akzeptiert werden, sofern sie aus zuverlässigen und objektiven Informationsquellen stammen.
- 68 Bei der Ermittlung der Identität des wirtschaftlichen Eigentümers stellt die Kenntnis über die Zwischenglieder der Kette zwischen dem Kunden und den wirtschaftlichen Eigentümern ein notwendiges Element dar. Nur so kann das beaufsichtigte Unternehmen wissen, wer der wirtschaftliche Eigentümer ist und ob verschiedene Beteiligungen aufgrund von Personenidentität zusammenzurechnen sind. Die Überprüfungsschritte in Bezug auf die zwischengelagerten juristischen Personen werden, sofern keine Anhaltspunkte für ein Risiko vorliegen, gewöhnlich nicht dieselbe Intensität haben, wie die der am Ende stehenden natürlichen Personen.

- 69 Siehe dazu auch das FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Kreditinstitute vom 01.12.2011 (Rz 87 ff) und das FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Versicherungsunternehmen vom 01.12.2011 (Rz 102 ff).

2.2.3.2 Zweck und Art der angestrebten Geschäftsbeziehung (§ 40 Abs. 2a Z 2 BWG, § 98b Abs. 3 Z 2 VAG)

- 70 Informationen über Zweck und Art der angestrebten Geschäftsbeziehung sind wesentlich, um ein wirtschaftliches Profil des Kunden anlegen zu können. Dies ist Teil des Prozesses des beaufsichtigten Unternehmens, seinen Kunden kennenzulernen („know your customer“). Das Profil eines Kunden soll das beaufsichtigte Unternehmen in die Lage versetzen zu beurteilen, ob Transaktionen innerhalb der typischen Geschäftstätigkeit liegen oder als ungewöhnlich zu beurteilen sind.
- 71 Informationen über Zweck und Art der Geschäftsbeziehung können folgende Punkte sein:
- Zweck der Kontoeröffnung oder der Kundenbeziehung;
 - Voraussichtliche Zahlungsein- und Ausgänge vom bzw. auf das Konto (Häufigkeit und Höhe);
 - Erwartete Auslandsüberweisungen;
 - Arten von Transaktionen, die vorgenommen werden können;
 - Bekanntgabe der Quelle für die Herkunft der Geld- oder Finanzmittel bei Einzahlungen auf das Konto;
 - Erwartete Destination ausgehender Zahlungen und Leistungen vom Konto;
 - Größe und Herkunftsquellen der Vermögenswerte des Kunden und der Einkünfte;
 - Beschreibung der Geschäftsfelder und der Geschäftstätigkeit des Kunden und Darstellung der Unternehmensstruktur.
- 72 Für Versicherungsunternehmen kann der Zweck der Geschäftsbeziehung beispielsweise Vermögensaufbau, Ablebensschutz oder Kreditabsicherung sein.

2.2.3.3 Kontinuierliche Überwachung der Geschäftsbeziehung (§ 40 Abs. 2a Z 3 BWG, § 98b Abs. 3 Z 3 VAG)

- 73 Die Durchführung einer kontinuierlichen Überwachung der Geschäftsbeziehung, einschließlich einer Überprüfung der im Verlauf der Geschäftsbeziehung abgewickelten Transaktionen, ist wesentlich, um sicherzustellen, dass diese mit den Kenntnissen des beaufsichtigten Unternehmens über den Kunden, seine Geschäftstätigkeit und sein Risikoprofil, einschließlich erforderlichenfalls der Herkunft der Geld- oder Finanzmittel, kohärent sind, und Gewähr zu leisten, dass die jeweiligen Dokumente, Daten oder Informationen stets aktualisiert werden. Mittels der kontinuierlichen Überwachung der Geschäftsbeziehung können auch zusätzliche Risikoindikatoren festgestellt werden.

- 74 Die Art der Überwachung ist abhängig von der eingesetzten Überwachungsmethode (manuell, automatisch oder eine Kombination aus beidem). Der Umfang der Überwachung ergibt sich aus der Einstufung des Kunden in eine Risikokategorie. Bei Anwendung eines risikoorientierten Ansatzes werden nicht alle Transaktionen, Konten oder Kunden auf dieselbe Art und Weise überwacht werden. Je mehr Risiken wahrgenommen wurden, wie z.B. der Rechtsnatur des Kunden, die vom Kunden genutzten Produkte oder Dienstleistungen, Wohnsitz des Kunden, Transaktionen, desto höher ist die Risikokategorie und desto intensiver die Überwachung der Kundenbeziehung. Generell gilt, dass jede Geschäftsbeziehung oder Transaktion ein Risiko darstellt (es gibt keine Risikokategorie „kein Risiko“) und daher immer eine Überwachung der Geschäftsbeziehung oder Transaktion stattfinden muss. Dies gilt auch dann, wenn die Überweisung von einem Konto eines anderen inländischen oder ausländischen Kreditinstituts durchgeführt wurde.
- 75 Für die Risikokategorien mittleres Risiko und hohes Risiko (bzw. leicht erhöhtes Risiko, erhöhtes Risiko, hohes Risiko) sollten beaufsichtigte Unternehmen gemäß BWG jährlich Überprüfungsschritte für die in diesen Risikokategorien eingestufteten Geschäftsbeziehungen vornehmen. Die Transaktionsüberwachung hat laufend zu erfolgen. Bei Auffälligkeiten (z.B. Warnmeldungen eines computerunterstützten Überwachungsprogramms, ungewöhnliches Kundenverhalten) ist eine Überprüfung und eine etwaige daraus resultierende Umstufung in eine höhere Risikokategorie unverzüglich vorzunehmen.
- 76 Versicherungsunternehmen und betriebliche Vorsorgekassen können geschäftsbezogen auch längere als die in Rz 75 empfohlenen Intervalle festlegen, aber jedenfalls anlassbezogen (z.B. Vertragsänderung, Rückkauf und Auszahlung).
- 77 Maßnahmen zur Überwachung einer Geschäftsbeziehung, die risikobasiert und angemessen zu setzen sind, können sein:
- Aktualisierung der Informationen zur Identitätsfeststellung und Unterlagen zur Identitätsüberprüfung unter Berücksichtigung des Umstandes, ob es sich beim Kunden um eine natürliche oder juristische Person handelt;
 - Überprüfung und Aktualisierung der Angaben, ob auf eigene oder fremde Rechnung bzw. im fremden Auftrag gehandelt wird;
 - Überprüfung und Aktualisierung der Angaben zum wirtschaftlichen Eigentümer;
 - Überprüfung der Herkunft der Geld- oder Finanzmittel und Beschaffung zusätzlicher Daten;
 - Verfahren zur Bestimmung, ob eine politisch exponierte Person in die Geschäftsbeziehung, sei es z.B. als Kunde, Treugeber oder wirtschaftlicher Eigentümer eingebunden ist. Diese Verfahren sind nicht nur am Beginn der Geschäftsbeziehung, sondern auch während der Geschäftsbeziehung anzuwenden;
 - Kontrolle, ob das typische Kundenverhalten Änderungen erfahren hat, wie z.B. Höhe der Transaktionen, Frequenz der Transaktionen, Absender und Empfänger der Transaktionen, Zeichnungsberechtigungen;
 - Berücksichtigung des Umstandes, dass eine Verdachtsmeldung erstattet oder zumindest erwogen wurde;

- Berücksichtigung des Umstandes, ob bei Geldtransfers vollständige Auftraggeberdaten enthalten sind;
- Einbeziehung von Informationen aus institutsexternen Quellen wie z.B. Terror- und Sanktionslisten, Verdachtslisten, Konzerninformationen, andere Informationsquellen mit Breitenwirkung.

2.2.4. Gesetzlich vorgegebene Sorgfaltspflichten

- 78 Die gesetzlichen Bestimmungen zu den Sorgfaltspflichten nehmen auf sektorspezifische Unterschiede teilweise Bezug. Sie werden darum im „Besonderen Teil“ dieses Rundschreibens getrennt für beaufsichtigte Institute gemäß BWG und Versicherungsunternehmen behandelt (Abschnitt 3).

3. Besonderer Teil: Gesetzlich vorgegebene Sorgfaltspflichten

3.1. Vereinfachte Sorgfaltspflichten

- 79 Die Anwendung vereinfachter Sorgfaltspflichten gegenüber Kunden ist fakultativ und auf die im Gesetz aufgezählten Fälle beschränkt (§ 40a BWG bzw. § 98c VAG). Voraussetzung für ihre Anwendung ist die Bewertung als geringes Risiko. Sobald Hinweise darauf bestehen, dass mehr als nur ein geringes Risiko, etwa aufgrund zusätzlicher Risikofaktoren, besteht, wird die Anwendung vereinfachter Sorgfaltspflichten als unzulässig erachtet (§ 40a Abs. 1 bis 4 BWG bzw. § 98c Abs. 1 und 2 VAG).
- 80 Vereinfachte Sorgfaltspflichten bedeuten eine Verminderung der
- Identifizierungspflichten gemäß § 40 Abs. 1 BWG bzw. § 98b Abs. 1 VAG,
 - Ermittlungs- und Offenlegungspflichten gemäß § 40 Abs. 2 und 2a Z 1 und 2 BWG bzw. § 98b Abs. 2 und 3 Z 1 und 2 VAG, und
 - Überwachungspflichten (Monitoring) gemäß § 40 Abs. 2a Z 3 BWG bzw. § 98b Abs. 3 Z 3 VAG.
- 81 Bei Anwendung der vereinfachten Sorgfaltspflichten muss das beaufsichtigte Unternehmen über ausreichende Informationen verfügen, um der FMA nachweisen zu können, dass die Voraussetzungen für die Anwendung einer Ausnahme gemäß § 40a BWG bzw. § 98c VAG fortdauernd und nicht nur im Zeitpunkt der Vertragsbegründung erfüllt sind. Das bedeutet, dass in jedem Fall ein Mindestmaß an Identifizierungsmaßnahmen angewendet werden muss, um beurteilen zu können, ob ein geringes Risiko vorliegt. Je nach individuellem Risikoverlauf bzw. -situation müssen daher unter Umständen schon bei Beginn der Geschäftsbeziehung oder zu einem späteren Zeitpunkt „normale“ oder sogar verstärkte Sorgfaltspflichten angewendet werden (§ 40a Abs. 1 bis 4 BWG bzw. § 98c Abs. 1 und 2 VAG). Zur Überprüfung des fortdauernden Vorliegens der Voraussetzungen für die Anwendung vereinfachter Sorgfaltspflichten sind in angemessenen Abständen Überprüfungshandlungen zu setzen.
- 82 Dieser Nachweis ist von den beaufsichtigten Unternehmen durch eine ausreichende Dokumentation über die Geschäftsbeziehungen erbringen. Soweit Geschäftsbeziehungen eine komplexe oder unübliche Vertragsgestaltung zum Inhalt haben, oder Transaktionen keinen offensichtlichen wirtschaftlichen oder erkennbaren rechtmäßigen Zweck haben (§ 41 Abs. 1 BWG bzw. § 98f Abs. 1 VAG), wird bei Anwendung vereinfachter Sorgfaltspflichten vor allem darzulegen sein, warum diese Umstände nicht als Hinweis gewertet wurden, dass kein geringes Risiko besteht. Gemäß § 40a Abs. 5 BWG bzw. § 98c Abs. 3 VAG haben die beaufsichtigten Unternehmen ausreichende Informationen aufzubewahren, um nachweisen zu können, dass die Voraussetzungen für die Anwendung der vereinfachten Sorgfaltspflichten vorliegen. In diesem Sinne ist das Vorliegen eines geringen Risikos zur späteren Nachvollziehbarkeit ausdrücklich und ausreichend zu dokumentieren.

- 83 Vier Fälle der fakultativen Anwendung vereinfachter Sorgfaltspflichten gelten für beaufsichtigte Unternehmen gemäß BWG und Versicherungsunternehmen gleichermaßen und werden darum hier für beide Sektoren gemeinsam dargestellt. Sie gelten bei Kunden, die Kredit- oder Finanzinstitute bzw. Versicherungsunternehmen aus einem EWR-Mitgliedstaat oder gleichwertigen Drittstaat, börsennotierte Gesellschaften, inländische Behörden oder EU-Behörden oder öffentliche EU-Einrichtungen sind.
- 84 Für die im Gesetz und im Nachfolgenden angeführten Fälle wird auch auf die Ausführungen im FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Kreditinstitute vom 01.12.2011 und im FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Versicherungsunternehmen vom 01.12.2011 verwiesen.
- 85 Weitere Anwendungsfälle vereinfachter Sorgfaltspflichten werden im sektorspezifischen Teil dargestellt (siehe Abschnitt 3.1.2 bzw. 3.1.3).

3.1.1. Gleichermaßen für beaufsichtigte Unternehmen nach BWG und Versicherungsunternehmen anwendbare Fälle

3.1.1.1 Kredit- oder Finanzinstitut bzw. Versicherungsunternehmen aus einem EWR-Mitgliedstaat oder gleichwertigem Drittstaat (§ 40a Abs. 1 Z 1 BWG, § 98c Abs. 1 Z 1 lit. a und b VAG)

- 86 Handelt es sich bei dem Kunden um
- ein Kredit- oder Finanzinstitut gemäß § 1 Abs. 1 und 2 BWG bzw. gemäß Art. 3 der Richtlinie 2005/60/EG,
 - ein den §§ 98a ff VAG unterliegenden Versicherungsunternehmen bzw. ein Versicherungsunternehmen gemäß Art. 3 der Richtlinie 2005/60/EG oder
 - ein in einem Drittland ansässiges Kredit- bzw. Finanzinstitut oder Versicherungsunternehmen, das dort gleichwertigen Pflichten wie den in der Richtlinie 2005/60/EG vorgesehenen Pflichten unterworfen ist und einer Aufsicht in Bezug auf deren Einhaltung unterliegt,
- ist vorausgesetzt einer Beurteilung als geringes Risiko der Geldwäscherei und Terrorismusfinanzierung die Anwendung vereinfachter Sorgfaltspflichten zulässig.
- 87 Art. 3 Z 1 der Richtlinie 2005/60/EG definiert ein Kreditinstitut als „Kreditinstitut im Sinne von Art. 1 Nr. 1 Unterabsatz 1 der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates vom 20. März 2000 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute sowie — im Sinne von Art. 1 Nr. 3 jener Richtlinie — eine in der Gemeinschaft gelegene Zweigstelle eines Kreditinstituts mit Sitz innerhalb oder außerhalb der Gemeinschaft“.
- 88 Art. 3 Z 2 der Richtlinie 2005/60/EG (unter Berücksichtigung der Änderung durch Richtlinie 2009/110/EG) definiert ein Finanzinstitut als

- „a) ein anderes Unternehmen als ein Kreditinstitut, das eines oder mehrere der unter den Nummern 2 bis 12 sowie 14 der Liste in Anhang I der Richtlinie 2006/48/EG genannten Geschäfte tätig, einschließlich der Tätigkeiten einer Wechselstube („bureau de change“);
- b) ein Versicherungsunternehmen, das gemäß der Richtlinie 2002/83/EG des Europäischen Parlaments und des Rates vom 5. November 2002 über Lebensversicherungen ordnungsgemäß zugelassen ist, soweit es Tätigkeiten ausübt, die unter jene Richtlinie fallen;
- c) eine Wertpapierfirma im Sinne von Art. 4 Absatz 1 Nr. 1 der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates vom 21. April 2004 über Märkte für Finanzinstrumente;
- d) einen Organismus für die gemeinsame Anlage in Wertpapieren, der seine Anteilscheine oder Anteile vertreibt;
- e) einen Versicherungsvermittler im Sinne von Art. 2 Nr. 5 der Richtlinie 2002/92/EG des Europäischen Parlaments und des Rates vom 9. Dezember 2002 über Versicherungsvermittlung, mit Ausnahme der in Art. 2 Nr. 7 jener Richtlinie genannten Versicherungsvermittler, wenn er im Zusammenhang mit Lebensversicherungen und anderen Dienstleistungen mit Anlagezweck tätig wird;
- f) in der Gemeinschaft gelegene Zweigstellen von in den Buchstaben a bis e genannten Finanzinstituten, deren Sitz sich innerhalb oder außerhalb der Gemeinschaft befindet“.

89 Somit sind u.a. folgende Unternehmen umfasst:

- österreichische Kreditinstitute;
- österreichische Finanzinstitute gemäß § 1 Abs. 2 BWG;
- österreichische Lebensversicherungsunternehmen;
- österreichische Wertpapierfirmen;
- österreichische Zahlungsinstitute;
- österreichische E-Geld-Institute;
- EWR-Kredit- und Finanzinstitute, einschließlich EWR-Lebensversicherungsunternehmen, EWR-Zahlungsinstitute, EWR-E-Geld-Institute;
- Niederlassungen (Zweigstellen) von EWR-Kredit- und Finanzinstituten in Österreich.

90 Gleichwertige Drittländer sind jene Länder, die in der Mitteilung der FMA über Drittländer mit gleichwertigen Anforderungen in der Bekämpfung von Geldwäscherei und Terrorismusfinanzierung in der jeweils geltenden Fassung angeführt werden. Diese Liste ist auf der Homepage der FMA in der Rubrik „Sonderthemen“/„Geldwäscherei und Terrorismusfinanzierung“/„Mitteilungen“ veröffentlicht. Bei Kundenbeziehungen zu Kredit- und Finanzinstituten (mit Ausnahme von Korrespondenzbankbeziehungen) bzw. Versicherungsunternehmen aus diesen Ländern ist vorbehaltlich einer Beurteilung als geringes Risiko der Geldwäscherei und Terrorismusfinanzierung die Anwendung vereinfachter (im Sinne des § 40a BWG bzw. § 98c VAG) Sorgfaltspflichten zulässig.

3.1.1.2 Börsennotierte Gesellschaft (§ 40a Abs. 1 Z 2 BWG, § 98c Abs. 1 Z 1 lit. c VAG)

91 Bei börsennotierten Gesellschaften handelt es sich um

- solche Gesellschaften, deren Wertpapiere zum Handel auf einem geregelten Markt in einem oder mehreren Mitgliedstaaten zugelassen sind, oder
- börsennotierte Gesellschaften aus Drittländern, die gemäß einer auf Basis der Verordnungsermächtigung gemäß § 85 Abs. 10 BörseG durch die FMA zu erlassenden Verordnung Offenlegungsanforderungen unterliegen, die dem Unionsrecht entsprechen oder mit diesem vergleichbar sind.

92 Bei der erwähnten Verordnung handelt es sich um die Verordnung der Finanzmarktaufsichtsbehörde (FMA) über Inhalte von Zwischenberichten, Meldungen über Änderungen bedeutender Beteiligungen und die Gleichwertigkeit von vorgeschriebenen Informationen aus Drittländern (Transparenz-Verordnung - TransV), veröffentlicht in BGBl II 2007/175, in der jeweils geltenden Fassung.

3.1.1.3 Inländische Behörde (§ 40a Abs. 1 Z 3 BWG, § 98c Abs. 1 Z 1 lit. d VAG)

93 Behörden sind Staatsorgane, die aufgrund von Rechtsvorschriften einseitig verbindliche Normen erlassen oder Zwangsakte setzen können. Der Begriff der Behörde bezeichnet jedes Organ einer juristischen Person des öffentlichen Rechts. Dazu zählen alle Staatsbehörden, jedes Organ der staatlichen Legislative, Exekutive und Judikative (z.B. auch ein Gericht). Unter den Begriff „inländische Behörde“ werden auch inländische Gebietskörperschaften subsumiert.

3.1.1.4 Behörde oder öffentliche Einrichtung der EU (§ 40a Abs. 1 Z 4 BWG, § 98c Abs. 1 Z 1 lit. e VAG³)

94 Behörden oder öffentliche Einrichtungen der Europäischen Union sind solche Institutionen, die

- auf der Grundlage des Vertrags über die Arbeitsweise der Europäischen Union, der Verträge zur Gründung der Europäischen Gemeinschaften oder des Sekundärrechts der Union mit öffentlichen Aufgaben betraut wurden,
- deren Identität öffentlich nachprüfbar und transparent ist und zweifelsfrei feststeht,
- deren Tätigkeiten und Rechnungslegungspraktiken transparent sind, und
- die entweder gegenüber einem Organ der Union oder den Behörden eines Mitgliedstaats rechenschaftspflichtig sind oder bei ihnen anderweitige Kontroll- und Gegenkontrollmechanismen zur Überprüfung ihrer Tätigkeit bestehen.

³

Eine Anpassung der Terminologie aufgrund des Vertrages über die Arbeitsweise der Europäischen Union ist im VAG noch nicht erfolgt.

3.1.2. Beaufsichtigte Unternehmen gemäß BWG

3.1.2.1 E-Geld (§ 40a Abs. 2 Z 1 BWG)

- 95 Der Begriff E-Geld ist in § 1 Abs. 1 E-Geldgesetz 2010 definiert.
- 96 Vorbehaltlich der Bewertung als geringes Risiko können Kunden in Bezug auf E-Geld, sofern
- der elektronisch auf dem Datenträger gespeicherte Betrag – falls der Datenträger nicht wieder aufgeladen werden kann – nicht mehr als 250 Euro oder bei Zahlungsvorgängen innerhalb Österreichs nicht mehr als 500 Euro beträgt, oder
 - bei wieder aufladbarem Datenträger sich der in einem Kalenderjahr insgesamt abgewickelte Betrag⁴ auf nicht mehr als 2 500 Euro beläuft,
- erleichterten Sorgfaltspflichten unterliegen.
- 97 Wird ein Betrag von 1 000 Euro oder mehr in demselben Kalenderjahr vom E-Geld-Inhaber gemäß §§ 18 und 19 E-Geldgesetz 2010 bzw. nach Art. 3 der Richtlinie 2000/46/EG erstattet, dürfen hinsichtlich dieses Kunden keine erleichterten Sorgfaltspflichten angewendet werden.
- 98 Faktoren, die die Bewertung als geringes Risiko beeinflussen können, sind etwa die Vertriebsform (z.B. ausschließlich über das Internet ohne physischen Kundenkontakt), der Auflademodus (ohne "paper trail", d.h. mittels Bargeld) oder die Verwendungsmöglichkeit (z.B. "offene Systeme", grenzüberschreitend, für Geldtransfers, Möglichkeit des Eintauschs gegen bzw. Auszahlung von Bargeld).

3.1.2.2 Schulsparen (§ 40a Abs. 2 Z 2 BWG)

- 99 Bei der Sparform des Schulsparens können erleichterte Sorgfaltspflichten angewendet werden, sofern es sich bei den Kunden um Minderjährige handelt, bei denen die Mitwirkung des gesetzlichen Vertreters bei der Identifizierung nicht erforderlich ist.
- 100 Siehe dazu auch die Rz 162 f. im FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Kreditinstitute vom 01.12.2011.

3.1.3. Versicherungsunternehmen

3.1.3.1 Bagatellverträge (§ 98c Abs. 1 Z 2 lit. a VAG)

- 101 Im Fall der Bagatellverträge wird besonders darauf hingewiesen, dass die Voraussetzungen für die Anwendung vereinfachter Sorgfaltspflichten andauernd bestehen müssen. Automati-

⁴ Siehe ErläutRV 982 BlgNR XXIV.GP zur Novellierung durch BGBl I 107/2010, in welcher eine Klarstellung des Begriffes „abgewickelt“ erfolgt: „Der abgewickelte Betrag ist im Sinne von aufgeladenen Betrag zu verstehen, es ist nicht auf die einzelne durchgeführte Transaktion [Bezahlungen, Überweisungen] abzustellen.“

sierte Überwachungsprogramme sollten so eingestellt sein, dass jede Abweichung vom Standardverhalten umgehend auffällt. Insbesondere sollte das beaufsichtigte Unternehmen in der Lage sein festzustellen, ob ein Versicherungsnehmer durch den Abschluss von mehreren Bagatellverträgen die Anwendung der normalen Sorgfaltspflichten umgehen will.

- 102 Siehe dazu auch die Rz 165 – 170 im FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Versicherungsunternehmen vom 01.12.2011.

3.1.3.2 Rentenversicherungsverträge (§ 98c Abs. 1 Z 2 lit. b VAG)

- 103 Siehe dazu die Rz 171 – 174 im FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Versicherungsunternehmen vom 01.12.2011.

3.2. Verstärkte Sorgfaltspflichten

- 104 Verstärkte Sorgfaltspflichten sind in den Fällen anzuwenden, bei denen ihrem Wesen nach ein erhöhtes Risiko der Geldwäscherei oder Terrorismusfinanzierung besteht (§ 40b BWG bzw. § 98d VAG). Das bedeutet, dass zusätzlich zu den im Gesetz angeführten Sorgfaltspflichten in weiteren Fällen Maßnahmen in Abhängigkeit von der Einstufung in eine Risikokategorie verpflichtend anzuwenden sind und die Geschäftsbeziehung einer verstärkten kontinuierlichen Überwachung zu unterziehen ist.⁵
- 105 Im Anwendungsbereich der verstärkten Sorgfaltspflichten ist es notwendig, den Umfang und die Art der im Rahmen der
- Identifizierungspflichten gemäß § 40 Abs. 1 BWG bzw. § 98b Abs. 1 VAG,
 - Ermittlungs- und Offenlegungspflichten gemäß § 40 Abs. 2 und 2a Z 1 und 2 BWG bzw. § 98b Abs. 2 und 3 Z 1 und 2 VAG,
 - Überwachungspflichten (Monitoring) gemäß § 40 Abs. 2a Z 3 BWG bzw. § 98b Abs. 3 Z 3 VAG, und
 - Aktualisierungspflichten gemäß § 40 Abs. 2e BWG bzw. § 98b Abs. 7 VAG
- gesetzten Maßnahmen anzupassen und zusätzliche Maßnahmen zu setzen.
- 106 Das Gesetz führt Anwendungsfälle für verstärkte Sorgfaltspflichten gegenüber dem Kunden an und schreibt fest, welche zusätzlichen Maßnahmen mindestens zu ergreifen sind. Die im Gesetz erwähnten Anwendungsfälle sind aber nicht die einzigen Anwendungsfälle verstärkter Sorgfaltspflichten, sondern es kann notwendig sein, auch in weiteren Fällen verstärkte Sorgfalt anzuwenden (zu den Maßnahmen der Überwachung der Geschäftsbeziehung siehe Rz 77).
- 107 Zwei Fälle der verpflichtenden Anwendung verstärkter Sorgfaltspflichten gelten für beaufsichtigte Institute gemäß BWG und Versicherungsunternehmen gleichermaßen und werden dar-

⁵ Zu weiteren Anwendungsfällen siehe auch die vom der FMA erlassene Geldwäscherei- und Terrorismusfinanzierungsrisiko-Verordnung – GTV, BGBl. II Nr. 377/2011.

um hier für beide Sektoren gemeinsam dargestellt. Es sind dies das Ferngeschäft und Transaktionen oder Geschäftsbeziehungen zu politisch exponierten Personen.

- 108 Weitere Anwendungsfälle verstärkter Sorgfaltspflichten werden im sektorspezifischen Teil dargestellt (siehe Abschnitt 3.2.2 bzw. 3.2.3).

3.2.1. Gleichermaßen für beaufsichtigte Unternehmen nach BWG und Versicherungsunternehmen anwendbare Fälle

3.2.1.1 Ferngeschäft (§ 40b Abs. 1 Z 1 BWG, § 98d Abs. 1 Z 1 VAG)

- 109 In den Fällen, in denen der Kunde oder die für ihn im Sinne des § 40 Abs. 1 BWG bzw. § 98b Abs. 1 VAG vertretungsbefugte natürliche Person zur Feststellung der Identität nicht physisch anwesend ist, stellt die Durchführung der Identifizierung ein besonderes Risiko dar. Es ist darum ein Mindestmaß an zusätzlichen Maßnahmen für das Feststellen und die Überprüfung der Identität gesetzlich vorgeschrieben. Das „Ident. Brief Verfahren“, auch als „Post. Ident Verfahren“ bezeichnet, entspricht grundsätzlich den Anforderungen des § 40b Abs. 1 Z 1 lit. a BWG bzw. § 98d Abs. 1 Z 1 lit. a VAG. Risikobasierte und angemessene Maßnahmen sind entsprechend durchzuführen (siehe Abschnitt 2.2.3).
- 110 Zu den Identifizierungspflichten siehe das FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Kreditinstitute vom 01.12.2011 (Rz 159 ff) und das FMA-Rundschreiben zur Feststellung und Überprüfung der Identität für Versicherungsunternehmen vom 01.12.2011 (Rz 73 ff).

3.2.1.2 Transaktionen oder Geschäftsbeziehungen mit Bezug zu politisch exponierten Personen (§ 40b Abs. 1 Z 3 BWG, § 98d Abs. 1 Z 2 VAG).

- 111 Entscheidendes Kriterium für die Qualifikation als politisch exponierte Person (PEP) ist der geographische Bezug einer Funktion, wie in § 2 Z 72 BWG bzw. § 98a Abs. 2 Z 1 VAG aufgelistet.
- 112 Das Gesetz definiert den Begriff „politisch exponierte Person“ in § 2 Z 72 BWG bzw. § 98a Abs. 2 Z 1 VAG. Aus § 2 Z 72 in Verbindung mit § 40b Abs. 1 Z 3 BWG bzw. § 98a Abs. 2 Z 1 in Verbindung mit § 98d Abs. 1 Z 2 VAG ergibt sich, dass eine politisch exponierte Person eine natürliche Person ist, die für einen anderen Mitgliedstaat, ein Drittland oder für eine internationale Organisation ein wichtiges öffentliches Amt ausübt oder bis vor mindestens einem Jahr ausgeübt hat, und ihre unmittelbaren Familienmitglieder oder ihr bekanntermaßen nahe stehenden Personen. Diesen Personen sind auch solche gleichzuhalten, die erst im Laufe der Geschäftsbeziehung politisch exponierte Personen werden. Unabhängig davon ist die Anwendung erhöhter Sorgfaltspflichten bei Geschäftsbeziehungen mit einer ehemals politisch exponierten Person auch über die Jahresfrist hinaus geboten, sofern diese ein erhöhtes Risiko darstellen.

- 113 Bei der Beurteilung, ob verstärkte Sorgfaltspflichten auf politisch exponierte Personen anzuwenden sind, ist primär auf die Zuordnung der Funktion zu einem anderen Mitgliedstaat oder Drittland abzustellen. Bei Ausübung einer ausländischen Funktion sind zumindest die verstärkten Sorgfaltspflichten gemäß § 40b Abs. 1 Z 3 BWG bzw. § 98d Abs. 1 Z 2 VAG anzuwenden. Die Funktionsausübung wird gewöhnlich mit einer ausländischen Staatsbürgerschaft und Ansässigkeit im Ausland einher gehen, muss jedoch damit nicht notwendig verbunden sein.
- 114 Handelt es sich um eine Person, die eine österreichische Funktion im Sinne des § 2 Z 72 BWG bzw. § 98a Abs. 2 Z 1 VAG ausübt, so können normale Sorgfaltspflichten zur Anwendung gelangen, sofern nicht aufgrund von Ergebnissen der Risikoanalyse verstärkte Sorgfaltspflichten anzuwenden sind. Bei Ausübung einer ausländischen Funktion muss der Kunde in die höchste Risikoklasse eingestuft und die risikobasierten und angemessenen Maßnahmen entsprechend durchgeführt werden (siehe Abschnitt 2.2.3). Bei juristischen Personen ist der PEP-Status der wirtschaftlichen Eigentümer zu prüfen.
- 115 Beaufsichtigte Unternehmen müssen
- über angemessene, risikobasierte Verfahren verfügen, anhand derer bestimmt werden kann, ob es sich bei dem Kunden um eine politisch exponierte Person handelt oder nicht (lit. a): Die Verwendung automationsunterstützter Datenbanken ist ein wesentliches Hilfsmittel bei der Feststellung der PEP-Eigenschaft eines potentiellen Kunden, jedoch nicht Voraussetzung. Bei der Auswahl einer Datenbank ist zu überprüfen, ob sie den Ansprüchen der Angemessenheit genügt.
 - die Zustimmung der Führungsebene einholen, bevor sie Geschäftsbeziehungen mit diesen Kunden aufnehmen (lit. b): Dies bedeutet nicht die Verpflichtung zur Einholung der Zustimmung der Geschäftsleitung, sondern der Zustimmung jener Ebene, der die Person, die um eine derartige Zustimmung ersucht, unmittelbar untersteht.
 - angemessene Maßnahmen ergreifen, mit denen die Herkunft des Vermögens und die Herkunft der Gelder bestimmt werden kann, die im Rahmen der Geschäftsbeziehung oder der Transaktion eingesetzt werden (lit. c): Durch genaue Kenntnis über die Herkunft des Vermögens und der Gelder sollen die internationalen Anstrengungen auf dem Gebiet der Korruptionsbekämpfung unterstützt werden, indem ein Einschleusen in den Finanzkreislauf verhindert werden soll. In diesem Zusammenhang wird auf den Vortatenkatalog zur Geldwäscherei gemäß § 165 StGB hingewiesen, der auch die Bestechungsdelikte beinhaltet.
 - die Geschäftsbeziehung einer verstärkten kontinuierlichen Überwachung unterziehen (lit. d).
- 116 Bei PEP-Bezug der Geschäftsbeziehung ist der Kunde in die höchste Risikoklasse einzustufen. Dies gilt auch für den Fall, wenn der wirtschaftliche Eigentümer oder Treugeber eine politisch exponierte Person ist.
- 117 Die Verpflichtung der Anwendung verstärkter Sorgfaltspflichten gegenüber politisch exponierten Personen gilt nicht nur bei Begründung einer Geschäftsbeziehung, sondern auch für

den Fall, dass ein bestehender Kunde zu einem späteren Zeitpunkt die Voraussetzungen erfüllt. Die Verfahren zur Überwachung der Geschäftsbeziehung sollten das Hinzukommen der PEP-Eigenschaft während aufrechter Geschäftsbeziehung ersichtlich machen.

- 118 Die verstärkte Überwachung gilt jedenfalls bis mindestens ein Jahr nach Beendigung der Funktion. Die Beendigung der verstärkten Überwachung sollte individuell nach einer Analyse der nach einem Jahr nach Beendigung der PEP-Funktion aktuell bestehenden Risiken und nicht automatisch mit Stichtag erfolgen. Eine Beibehaltung der verstärkten Sorgfaltspflichten kann bei Anhaltspunkten für ein erhöhtes Risiko, wie etwa unverändert fortlaufender Geschäftstätigkeit, geboten sein.

3.2.2. Beaufsichtigte Unternehmen gemäß BWG

- 119 Verstärkte Sorgfaltspflichten sind nicht nur in den im Gesetz und der von der FMA erlassenen Geldwäscherei- und Terrorismusfinanzierungsrisiko-Verordnung – GTV (BGBl. II Nr. 377/2011) explizit angeführten Fällen anzuwenden, sondern generell in allen „Fällen, in denen ihrem Wesen nach ein erhöhtes Risiko der Geldwäscherei und Terrorismusfinanzierung besteht“ (§ 40b Abs. 1 BWG).

3.2.2.1 Grenzüberschreitende Korrespondenzbankbeziehungen (§ 40b Abs. 1 Z 2 BWG)

- 120 Unter einer Korrespondenzbankbeziehung („correspondent banking“) wird eine Vereinbarung verstanden, in deren Rahmen eine Bank Zahlungsverkehrs- und andere Dienstleistungen für eine andere Bank erbringt. Gegenstand der Vereinbarung über die Aufnahme oder Beibehaltung einer Korrespondenzbankbeziehung ist das Zurverfügungstellen eines Devisen- oder Passivkontos und damit verbundener Dienstleistungen an eine andere Bank, die von dieser Bank zur Geldverrechnung, Liquiditätssteuerung und kurzfristigen Zwecken oder Investitionszwecken verwendet werden. Praktisch erfolgt die Ausführung von Zahlungen durch Korrespondenzbanken oft über gegenseitige Konten (Loro- und Nostrokonten), die mit Kreditlinien verbunden sein können.
- 121 § 40b Abs. 1 Z 2 BWG schreibt zusätzlich zu den Pflichten des § 40 Abs. 1, 2, 2a und 2e BWG für grenzüberschreitende Korrespondenzbankbeziehungen zu Korrespondenzbanken aus Drittländern bzw. zu Korrespondenzbanken aus dem EWR, diese jedoch vorbehaltlich einer Beurteilung als erhöhtes Risiko, weitere Mindestpflichten vor:
- Sammeln ausreichender Informationen über eine Korrespondenzbank, um die Art ihrer Geschäftstätigkeit in vollem Umfang zu verstehen und sich auf der Grundlage öffentlich verfügbarer Informationen von ihrem Ruf und der Qualität der Beaufsichtigung überzeugen zu können (lit. a). Dazu können folgende Informationen zählen:
 - Informationen über den Sitzstaat der Korrespondenzbank und dessen Aufsichtsregime. Es gelten die Kriterien des geographischen Risikos, wie in Abschnitt 2.1.1.5 dargestellt;

- Informationen über Eigentümer und Organe inklusive Eigentümerstruktur und Leitungsstruktur. Hierbei sollte ermittelt werden, ob politisch exponierte Personen an der Korrespondenzbank beteiligt sind;
- Informationen über Geschäftstätigkeit und Kundenstruktur. Hierbei sollte sichergestellt sein, dass die Korrespondenzbank keine Beziehungen und Geschäfte mit Bankmantelgesellschaften („shell banks“) durchführt.

Viele dieser Informationen können mittels eines Fragebogens, den die angehende Korrespondenzbank ausfüllt, erlangt werden. Es ist jedoch notwendig, diese Informationen auf ihre Richtigkeit durch eine selbständige Recherche zu überprüfen. Dazu können beispielsweise Geschäftsberichte der Korrespondenzbank und der zuständigen Aufsichtsbehörde sowie selbständig erlangte Ergebnisse einer Internetrecherche herangezogen werden. Erweisen sich diese Ergebnisse als nicht ausreichend, kann ein Besuch in der potentiellen Korrespondenzbank erwogen werden.

- Sich von den Kontrollen zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung überzeugen, die die Korrespondenzbank vornimmt (lit. b):
 - im Bereich der Customer Due Dilligence sollte sichergestellt sein, dass die Korrespondenzbank ausreichende Maßnahmen zur Identifizierung seiner Kunden und Überwachung der Geschäftsbeziehungen zu seinen Kunden vornimmt.

Die Überzeugung von den Kontrollen hat soweit zu erfolgen, als sie möglich und zumutbar ist, wobei die Berufung auf Unmöglichkeit und Unzumutbarkeit nach objektiven Kriterien nachvollziehbar sein sollte. Die Anforderung einer Beschreibung der Maßnahmen der Korrespondenzbank zur Identifizierung ihrer Kunden und Überwachung der Geschäftsbeziehung wird in der Regel möglich und zumutbar sein.

- Einholen der Zustimmung der Führungsebene, bevor eine neue Korrespondenzbankbeziehung eingegangen wird (lit. c). Dies beinhaltet hier aus Risikogründen, im Gegensatz zu Abschnitt 3.2.1.2, die Verpflichtung zur Einholung der Zustimmung der Geschäftsleitung.
- Dokumentation der jeweiligen Verantwortlichkeiten einer jeden Korrespondenzbank (lit. d): Zu Nachweiszwecken wird eine schriftliche Dokumentation empfohlen. Die Dokumentation der jeweiligen Verantwortlichkeiten könnte folgendes enthalten:
 - welche Produkte und Dienstleistungen angeboten werden,
 - wie die Annahme von Überweisungen und Gegenverrechnung („clearing“) erfolgt, und
 - wann die Kontosalde abgerechnet werden.
- Vergewisserung im Falle von „Durchlaufkonten“ („payable through accounts“),
 - dass die Korrespondenzbank die Identität der Kunden überprüft hat, die direkten Zugang zu den Konten der Korrespondenzbank haben, und diese Kunden ferner einer kontinuierlichen Überwachung unterzogen hat und,
 - dass die Korrespondenzbank in der Lage ist, auf Ersuchen des ersten Instituts entsprechende Daten in Bezug auf diese Sorgfaltspflichten gegenüber Kunden vorzulegen (lit. e).

122 Korrespondenzbankbeziehungen sind in die höchste Risikoklasse einzustufen.

- 123 Hinsichtlich Korrespondenzbankbeziehungen zu Korrespondenzbanken aus EWR-Mitgliedstaaten sollte überprüft werden, ob die Voraussetzungen für die Anwendung erleichterter oder normaler Sorgfaltspflichten gegeben sind (siehe Abschnitt 3.1).

3.2.2.2 Sonstige Anwendungsfälle

- 124 Neben den in der von der FMA erlassenen Geldwäscherei- und Terrorismusfinanzierungsrisiko-Verordnung – GTV (BGBl. II Nr. 377/2011) normierten Fällen, bei denen verstärkte Sorgfaltspflichten verpflichtend anzuwenden sind, besteht bei den nachfolgenden Fällen die widerlegbare Vermutung, dass bei ihnen ihrem Wesen nach ein erhöhtes Risiko der Geldwäscherei und Terrorismusfinanzierung besteht, und sie sollten, sofern die Vermutung nicht widerlegt wurde, in eine hohe Risikokategorie eingestuft werden (§ 40b Abs. 1 BWG):
- Kunden mit Registrierungsland/ständigem Wohnsitz in einer Offshore-Destination, in einem Nicht-Kooperationsstaat, in einem nicht anerkannten Land oder in einem Drittland, mit der bzw. dem das beaufsichtigte Unternehmen noch keine Erfahrungen in der Zusammenarbeit sammeln konnte.
 - Unternehmen mit anonymen Inhaberpapieren bzw. Inhaberaktien, sofern sie nicht vereinfachten Sorgfaltspflichten unterliegen.
 - Unternehmensstrukturen mit Off-Shore-Beziehungen, Stiftungen, Treuhandschaften, Trusts oder andere Formen (z.B. nominee shareholder), die den wirtschaftlichen Eigentümer nicht klar erkennen lassen, es sei denn, dass die Struktur bis zum wirtschaftlichen Eigentümer offengelegt wird.
 - Nicht auf Gewinn ausgerichtete Vereinigungen unter Berücksichtigung des Organisationszwecks, des Herkunftslandes bzw. Registrierungslandes und der Tätigkeit mit häufigen Zahlungen ins Ausland.
 - Kunden mit Geschäftstätigkeit zu Ländern, die nicht FATF-konforme Maßnahmen im Bereich der Geldwäscherei und Terrorismusfinanzierung gesetzt haben.
 - Anträge auf Schließfachverträge von Personen, zu denen darüber hinaus keine Geschäftsbeziehung besteht.
 - Komplexe oder unüblich große Transaktionen und alle unüblichen Muster von Transaktionen ohne offensichtlichen wirtschaftlichen oder erkennbaren rechtmäßigen Zweck, insbesondere wenn diese im Zusammenhang mit Staaten stehen, in denen laut glaubwürdiger Quelle ein erhöhtes Risiko der Geldwäscherei und Terrorismusfinanzierung besteht (§ 41 Abs. 1 BWG). Beaufsichtigte Unternehmen gemäß BWG sollten so weit als möglich den Hintergrund und Zweck dieser Transaktionen überprüfen. Darüber sollten in geeigneter Weise schriftliche Aufzeichnungen erstellt werden und bis mindestens 5 Jahre nach Überprüfung aufbewahrt werden.
 - Vermögensverwaltung vermögender Privatkunden („private banking“): Obgleich vermögende Kunden nicht automatisch als verdächtig im Bereich der Geldwäscherei und Terrorismusfinanzierung angesehen werden sollen, besteht aufgrund der Größe der Vermögenswerte und der in manchen Fällen nur schwer nachvollziehbaren Mittelherkunft, die zur Veranlagung oder Verwaltung kommen, ein erhöhtes Risiko. Dabei ist insbesondere die Risikokumulierung in Zusammenhang mit der Destination der Kundenbeziehung zu beachten. Das besondere Vertrauensverhältnis, das zu vermögenden Privatkunden be-

steht, darf zu keiner Verringerung der Sorgfaltspflichten führen. Vielmehr sollte das objektive Risiko in die Kundenbewertung und das Kundenmonitoring einfließen.

- Kombination von Risikokriterien wie in Abschnitt 2.1.1 dargestellt: Enthält eine Geschäftsbeziehung oder Transaktion mehr als einen Faktor, der in den Risikokriterien als Bewertungsmaßstab angeführt wurde (z.B. jenen, die in den Abschnitten 2.1.1.1, 2.1.1.2 und 2.1.1.5 angeführt sind), wie z.B. höheres Produktrisiko (Online-Banking) mit höherem geographischen Risiko (Wohnsitz außerhalb des EWR), ist zu überprüfen, ob nicht verstärkte Sorgfalt anzuwenden ist.

3.2.3. Versicherungsunternehmen

- 125 In manchen Fällen ist durch das Gesetz die Anwendung verstärkter Sorgfaltspflichten vorgeschrieben. § 98d Abs. 1 VAG führt zwei Fälle (Ferngeschäfte und PEP) ausdrücklich an, die verstärkte Sorgfaltspflichten erfordern und die an anderer Stelle dieses Rundschreibens bereits behandelt wurden.
- 126 Verstärkte Sorgfaltspflichten sind aber nicht nur in den im Gesetz und in der von der FMA erlassenen Geldwäscherei- und Terrorismusfinanzierungsrisiko-Verordnung – GTV (BGBl. II Nr. 377/2011) explizit angeführten Fällen anzuwenden, sondern generell in allen „Fällen, in denen ihrem Wesen nach ein erhöhtes Risiko der Geldwäscherei und Terrorismusfinanzierung besteht“ (§ 98d Abs. 1 VAG).

3.2.3.1 Sonstige Anwendungsfälle

- 127 Je nach Vertriebsstruktur kann die Nähe oder Distanz zum Kunden zu beachten sein. Den Daten über Kunden, zu denen der Kontakt ausschließlich über Dritte im Sinne des § 98e VAG, wie Versicherungsvermittler besteht, ist eine besondere Aufmerksamkeit hinsichtlich ihrer Richtigkeit und Vollständigkeit zu widmen, da die endgültige Verantwortung für die Erfüllung der Sorgfaltspflichten beim Versicherungsunternehmen verbleibt. Dies umfasst z.B. Identitätsdaten, aber auch Informationen zur Herkunft der Mittel.
- 128 Bei den nachfolgenden Fällen besteht die widerlegbare Vermutung, dass bei ihnen ihrem Wesen nach ein erhöhtes Risiko der Geldwäscherei und Terrorismusfinanzierung besteht, und sie sollten, sofern die Vermutung nicht widerlegt wurde, in eine hohe Risikokategorie eingestuft werden (§ 98d Abs. 1 VAG):
- Komplexe oder unübliche Vertragsgestaltung (§ 98f Abs. 1 VAG): Sobald ein Vertrag vom Standardvertrag des Massengeschäftes abweicht, sollten die Gründe für den Wunsch des Kunden nach Abweichung hinterfragt und glaubhaft gemacht werden. Versicherungsunternehmen sollten so weit wie möglich den Hintergrund und Zweck dieser Vertragsgestaltung überprüfen. Darüber sollten in geeigneter Weise schriftliche Aufzeichnungen erstellt werden und bis mindestens 5 Jahre nach Überprüfung aufbewahrt werden.

- Transaktionen, die keinen offensichtlichen wirtschaftlichen oder erkennbaren rechtmäßigen Zweck haben (§ 98f Abs. 1 VAG): Transaktionen sollten den Ansprüchen der Unbedenklichkeit genügen. Sobald Elemente vorliegen, die eine Abweichung vom „vernünftigen Verhalten“ indizieren, sollten die Beweggründe dafür hinterfragt und glaubhaft gemacht werden. Dies betrifft insbesondere Bareinzahlungen und Rückkäufe, die zu unwirtschaftlichen Bedingungen erfolgen.
- Kombination von Risikokriterien wie in Abschnitt 2.1.1 dargestellt. Enthält eine Geschäftsbeziehung oder Transaktion mehr als einen Faktor, der in den Risikokriterien als Bewertungsmaßstab angeführt wurde, wie z.B. höheres Produktrisiko (Einmalerlag) mit höherem geographischen Risiko (Wohnsitz außerhalb des EWR), ist zu überprüfen, ob nicht verstärkte Sorgfalt anzuwenden ist.
- Abschluss von mehreren Bagatellverträgen.

4. Anhang

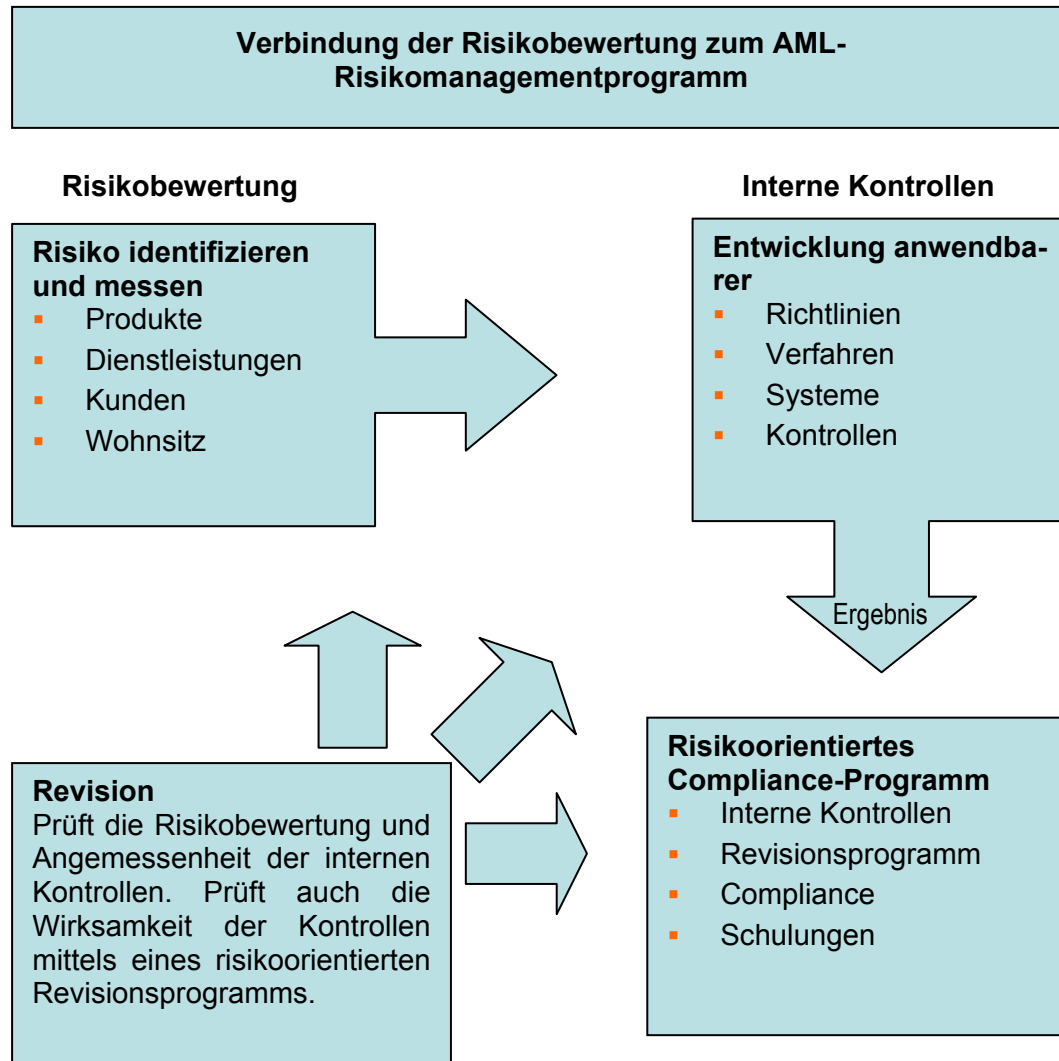
4.1. Basler Ausschuss für Bankenaufsicht - Risikomatrix

Gering	Mittel	Hoch
Stabiler bekannter Kundenbestand.	Zunehmender Kundenbestand durch Ausweitung des Filialnetzes, Fusionen oder Übernahmen.	Großer und wachsender Kundenbestand in einem weiten und vielfältigen regionalen Gebiet.
Keine elektronischen Bankgeschäfte (E-Banking) oder die Website ist nur informativ ohne Transaktionsmöglichkeit.	Die Bank hat E-Banking erst kürzlich eingeführt und offeriert begrenzte Produkte und Dienstleistungen.	Die Bank offeriert ein breites Spektrum an E-Banking-Produkten und -Dienstleistungen (d.h. Überweisungen, elektronische Rechnungsabgleichung, oder Kontoeröffnung per Internet).
Es gibt nur wenige Kunden und Unternehmen hohen Risikos.	Es gibt eine moderate Anzahl von Kunden und Unternehmen hohen Risikos. Darunter fallen u.a.: Check Cashers, Kioske, Finanztransferdienstleister, Wechselstuben, Import- und Exportunternehmen, Offshore-Betriebe, politisch exponierte Personen (PEPs) und ausländische natürliche Personen.	Es gibt eine große Zahl von Kunden und Unternehmen hohen Risikos. Darunter fallen u.a.: Check Cashers, Kioske, Finanztransferdienstleister, Wechselstuben, Import- und Exportunternehmen, Offshore-Betriebe, politisch exponierte Personen (PEPs) und ausländische natürliche Personen.
Keine ausländischen Korrespondenzbankkonten. Die Bank übt keine Werttransportdienste ("pouch activities") aus, offeriert keine Sondernutzungskonten ("special use accounts") oder Durchlaufkonten ("payable through accounts", PTAs).	Die Bank verfügt über ein paar ausländische Korrespondenzbankkonten, aber in der Regel bei Finanzinstituten mit angemessenen AML-Grundsätzen und -Verfahren aus Ländern geringen Risikos, minimale Werttransportdienste, Sondernutzungs- oder Durchlaufkonten.	Die Bank unterhält eine große Anzahl ausländischer Korrespondenzbankkonten bei Finanzinstituten mit unangemessenen AML-Grundsätzen und -Verfahren, vor allem in Ländern hohen Risikos, oder offeriert erhebliche Werttransportdienste, Sondernutzungs- oder Durchlaufkonten.
Die Bank bietet begrenzte oder keine Dienstleistungen für Privatkunden oder Treuhand- und Vermögensverwaltungsprodukte oder -dienstleistungen an.	Die Bank bietet begrenzte nationale Dienstleistungen für Privatkunden oder Treuhand- und Vermögensverwaltungsprodukte oder -dienstleistungen an, bei denen die Anlageentscheidungen im Ermessen der Bank stehen. Der strategische Plan kann eine Ausweitung des Treuhand-	Die Bank bietet in erheblichem Umfang nationale Dienstleistungen für Privatkunden oder Treuhand- und Vermögensverwaltungsprodukte oder -dienstleistungen an. Das Privatkunden oder Treuhand- und Vermögensverwaltungsgeschäft wächst. Die angebotenen Pro-

	geschäfts vorsehen.	dukte umfassen Vermögensverwaltungsdienste, und die Treuhandkonten sind vornehmlich ohne Dispositionsbefugnis statt voller Dispositionsbefugnis der Bank.
Wenig internationale Konten oder sehr geringes Volumen der Devisengeschäfte auf den Konten.	Moderate Zahl internationaler Konten mit Devisengeschäften, für die es keine Erklärung gibt.	Große Zahl internationaler Konten mit Devisengeschäften, für die es keine Erklärung gibt.
Begrenzte Zahl von Überweisungen für Kunden, Nicht-Kunden, begrenzte Zahl von Transaktionen dritter Parteien und keine ausländischen Überweisungen.	Moderate Zahl von Überweisungen. Nur wenig internationale Überweisungen von Privat- oder Geschäftskonten normalerweise in Ländern geringen Risikos.	Große Zahl von Überweisungen für Nicht-Kunden und bei ordnungsmäßiger Identifikation zahlbare Transaktionen (PUPID-Transaktionen). Häufig Mittelbewegung von Privat- oder Geschäftskonten an oder aus Ländern hohen Risikos oder Behörden oder Ländern mit Geheimhaltungspflichten.
Keine Transaktionen mit regionalen Gebieten hohen Risikos.	Minimale Transaktionen mit regionalen Gebieten hohen Risikos.	Erhebliches Volumen von Geschäften mit regionalen Gebieten hohen Risikos.
Geringe Fluktuation der Mitarbeiter in Schlüsselpositionen oder Positionen mit Kundenkontakt (z.B. Kundendienstvertreter, Kassierer oder andere Niederlassungsmitarbeiter).	Geringe Fluktuation der Mitarbeiter in Schlüsselpositionen. Positionen mit Kundenkontakt in Zweigniederlassungen wurden möglicherweise neu besetzt.	Hohe Fluktuation der Mitarbeiter insbesondere in Schlüsselpositionen.

4.2. Basler Ausschuss für Bankenaufsicht - Verbindung der Risikobewertung zum AML- Managementprogramm

(Arbeitsgruppe für das grenzüberschreitende Bankgeschäft)



4.3. Materialien

EU Terror-und Sanktionslisten:

http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm

FATF,

Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing, Juni 2007

<http://www.fatf-gafi.org>

Transparency International,
Corruption Perception Index

<http://www.transparency.org>

The Wolfsberg Group,

Statement on AML Screening, Monitoring and Searching, November 2009

Guidance on a Risk Based Approach for Managing Money Laundering Risks, März 2006

Anti-Money Laundering Principles for Correspondent Banking, November 2002

Wolfsberg AML Principles on Private Banking, Mai 2002, überarbeitet 2008

<http://www.wolfsberg-principles.com>

Anmerkung: Soweit Internetlinks in diesem Rundschreiben angegeben werden, ist dies ausschließlich zur Information. Die Richtigkeit der Links besteht zum Zeitpunkt der Beschlussfassung des Rundschreibens.