

FINMA-Aufsichtsmitteilung 04/2026

Ergänzung zur Aufsichtsmitteilung 05/2023 hinsichtlich der
Geldwäschereirisikoanalyse nach Art. 25 Abs. 2 GwV-FINMA

4. Juni 2026

Inhaltsverzeichnis

Einleitung	3
1 Geldwäschereirisikotoleranz	4
2 Geldwäschereisikoanalyse	7
2.1 Zu berücksichtigende Geldwäschereirisiken.....	7
2.2 Umsetzung der Anforderungen nach Art. 13 Abs. 2 ^{bis} GwV-FINMA	10
2.3 Überwachung der Einhaltung der Geschäftsstrategie und der Risikopolitik	10
2.4 Weitere zu berücksichtigende Elemente.....	11
3 Verhältnis zur Rz 78 des FINMA-Rundschreibens 2017/1 «Corporate Governance – Banken»	12
4 Globale Überwachung der Geldwäschereirisiken	13
5 FINIG-Institute	13

Einleitung

Im Bereich der Geldwäschereibekämpfung stellt die Geldwäschereirisikoanalyse (nachfolgend «Risikoanalyse») das zentrale Steuerungsinstrument dar, welches Ausgangspunkt des Risikomanagements bildet. Die Risikoanalyse bestimmt die Risikotoleranz und legt die verbindlichen Leitplanken für Aufbau, Organisation und laufende Steuerung des Geldwäschereidispositivs fest. Dadurch stellt sie sicher, dass Ressourcen, Prozesse und Kontrollen risikoorientiert und angemessen ausgestaltet sind und somit die gesetzlichen und regulatorischen Anforderungen erfüllt werden. Inhaltlich dient die Risikoanalyse der systematischen Erfassung und Bewertung der mit dem Geschäftsmodell verbundenen inhärenten Geldwäschereirisiken. Sie bestimmt zunächst, welche Risiken als nicht akzeptabel gelten und daher vom Geschäftsmodell ausgeschlossen sind (Geldwäschereirisikotoleranz). Für die im Einklang mit der Geschäftsstrategie tolerierten Risiken legt sie transparent deren Umfang, Struktur und Ausprägung dar und definiert angemessene Begrenzungs- und Steuerungsmassnahmen. Sehr hohe Risiken sind entweder auszuschliessen oder durch ausreichende Massnahmen zur Risikominderung und entsprechende Ressourcen wirksam zu begrenzen. Auf dieser Grundlage werden die institutsrelevanten Risikokriterien festgelegt, insbesondere für die Geschäftsbeziehungen mit erhöhten Risiken.

Mit der Aufsichtsmitteilung 05/2023 «Geldwäschereirisikoanalyse nach Art. 25 Abs. 2 GwV-FINMA» (nachfolgend «Aufsichtsmitteilung 05/2023») hat die FINMA erstmals Transparenz zu ihren in der Aufsichtspraxis gemachten Beobachtungen und Erfahrungen zur Risikoanalyse geschaffen. Seither hat die FINMA einen Teil der Risikoanalysen von über 30 im Frühjahr 2023 geprüften Banken erneut untersucht und diejenigen zahlreicher weiterer Banken sowie FINIG-Instituten¹ (nachfolgend gemeinsam «Institute») analysiert. Die FINMA stellt im Ergebnis fest, dass die Banken Fortschritte in der Definition ihrer Risikotoleranz und in der Ausgestaltung ihrer Risikoanalyse erzielt haben. Auch FINIG-Institute wenden Aspekte der Aufsichtsmitteilung 05/2023 zum Teil bereits sinngemäss an. Trotzdem hat die FINMA sowohl bei den Banken wie auch den FINIG-Instituten weiteres Verbesserungspotential identifiziert, damit die Risikoanalyse von den Instituten noch effektiver als zentrales Kontroll- und Steuerungsinstrument in der Geldwäschereibekämpfung wirkt.

Die vorliegende Aufsichtsmitteilung ergänzt frühere Beobachtungen und Erfahrungen und präzisiert die Aufsichtsmitteilung 05/2023 betreffend Banken und FINIG-Institute. Für letztere können die gemachten Beobachtungen und Erfahrungen sinngemäss herangezogen werden.

¹ Wertpapierhäuser (Art. 41 FINIG), Fondsleitungen (Art. 32 FINIG), Verwalter von Kollektivvermögen (Art. 24 FINIG), Vermögensverwalter und Trustees (Art. 17 FINIG).

1 Geldwäschereirisikotoleranz

Die rechtlichen Grundlagen zur Geldwäschereirisikotoleranz für Banken sind in der Aufsichtsmitteilung 05/2023 festgehalten.

Für FINIG-Institute sind im Zusammenhang mit der Festlegung der Risikotoleranz folgende rechtlichen Grundlagen von Bedeutung: Art. 9 Abs. 2 des Finanzinstituts Gesetzes vom 15. Juni 2018 (FINIG; SR 954.1), Art. 12 Abs. 4, Art. 26 Abs. 1, Art. 41 Abs. 2, Art. 57 Abs. 2 und Art. 68 Abs. 2 der Finanzinstitutsverordnung vom 6. November 2019 (FINIV; SR 954.11) sowie Art. 8 des Geldwäschereigesetzes vom 10. Oktober 1997 (GwG; SR 955.0) verlangen, dass FINIG-Institute ihre Geldwäschereirisiken (inkl. Bekämpfung der Terrorismusfinanzierung) identifizieren, steuern und überwachen sowie für wirksame interne Kontrollen sorgen.

In diesem und in den nachfolgenden Kapiteln werden ausgehend von den Beobachtungen gemäss Aufsichtsmitteilung 05/2023 die seither gewonnen Erkenntnisse dargestellt.

Definition der Risikotoleranz

Beobachtung gemäss Aufsichtsmitteilung 05/2023:

a) Oft fehlte es für eine adäquate Definition der Risikotoleranz am bewussten Ausschluss bestimmter Länder, Kundensegmente, Dienstleistungen und/oder Produkte (z.B. politisch exponierte Personen aus bestimmten Ländern).

- i. Häufig war zu beobachten, dass anstatt bewusste Ausschlüsse vorzunehmen lediglich risikomindernde Massnahmen beschrieben werden.
Beispiel: «Ausländische PEP werden nur angenommen, wenn diese über ein angemessenes KYC-Profil verfügen und die GL diese bewilligt hat.»
- ii. Der alleinige Ausschluss von zwingend auszuschliessenden inhärenten Risiken ist für eine adäquate Definition der Risikotoleranz ungenügend.
Beispiel: Ein Institut schliesst Nordkorea, Iran und einen geringen Kreis von Kunden (Drogen- und Menschenhandel, Proliferation) aus.
- iii. Beispiele für bewusste Ausschlüsse entsprechend dem jeweiligen Geschäftsmodell können sein:
 - Keine ausländischen PEPs
 - Keine komplexe Strukturen
 - Bestimmte Länder, die das Institut nicht bedienen möchte
 - Keine Kunden/innen aus den Industrien «XY»
 - Keine Krypto-Dienstleistungen

- Kein Trade Finance
- iv. Oft nehmen Institute keine ausreichend dokumentierte Einschätzung (tief/mittel/hoch) ihrer Risikotoleranz vor.

Exception to policy (nachfolgend «ETP») Prozess

Beobachtung gemäss Aufsichtsmittteilung 05/2023:

b) Auch fehlt zumeist ein geeigneter Prozess, um im Einzelfall Ausnahmen von der definierten Risikotoleranz zu ermöglichen (sog. *exception to policy* Prozess), wobei die Ausnahmen durch die Geschäftsleitung nach Festlegung von angemessenen risikomindernden Massnahmen zu erteilen und durch das Oberleitungsorgan zu überwachen sind.

- i. Gelegentlich ist die FINMA auf Institute gestossen, welche die festgelegte Risikotoleranz systematisch überschritten haben, da sie ihren ETP-Prozess zu wenig restriktiv ausgestaltet haben. Dies zeigte sich beispielsweise an einer sehr hohen Anzahl bewilligter ETPs. Damit wurde im Ergebnis die definierte adäquate Risikotoleranz faktisch aufgehoben. Der ETP-Prozess regelt lediglich, wie im Einzelfall Ausnahmen für Geschäftsbeziehungen gewährt werden, die ausserhalb der definierten Geldwäschereirisikotoleranz liegen. In diesem Rahmen sollte nicht vorgesehen werden, dass eine definierte Risikolimiten generell oder dauerhaft überschritten wird. Wenn ein höheres Risikoneveau bewusst akzeptiert werden soll, wäre dies über eine entsprechende Anpassung der Risikotoleranz durch das Oberleitungsorgan abzubilden.
- ii. Einige Institute haben ihre ETP-Fälle nicht zentral erfasst und überwachen diese in quantitativer (insbesondere hinsichtlich Anzahl, Volumen und Entwicklung) und qualitativer (insbesondere hinsichtlich Gründe, Risikoprofile, Angemessenheit und Wirksamkeit der mitigierenden Massnahmen) Hinsicht nicht ausreichend. Des Weiteren fehlt es vereinzelt an der regelmässigen Rapportierung der ETP-Fälle an das Oberleitungsorgan.
- iii. Vereinzelte Institute sind demgegenüber positiv aufgefallen, da sie keine Ausnahmen (ETPs) vorsehen und ihre adäquat definierte Risikotoleranz strikt einhalten.

Schlüsselrisikoindikatoren

Beobachtung gemäss Aufsichtsmitteilung 05/2023:

c) Auch wurde regelmässig festgestellt, dass zur Überwachung der Einhaltung der Risikotoleranz keine Schlüsselrisikoindikatoren definiert wurden, die der Geschäftsleitung und dem Verwaltungsrat eine regelmässige Kontrolle ermöglichen. Bei der Definition der Schlüsselrisikoindikatoren kann auf die in der Risikoanalyse definierten Risikolimiten abgestellt werden.

- i. Vereinzelt war festzustellen, dass Institute die Schlüsselrisikoindikatoren mit den in der Risikoanalyse definierten Risikolimiten (vgl. Ziff. 2.3 b) gleichgesetzt haben. Schlüsselrisikoindikatoren dienen zur regelmässigen Kontrolle der Einhaltung der Risikotoleranz. Entsprechend sollte der Fokus auf Kennzahlen liegen, die für die wesentlichen Risiken aussagekräftig sind. Nicht jede bestehende Risikolimite ist dabei automatisch als Schlüsselrisikoindikator zu verstehen. Vielmehr sollten die Schlüsselrisikoindikatoren vom Institut so festgelegt werden, dass sie die relevanten Risiken angemessen berücksichtigen.
- ii. Folgende Definitionen von Schlüsselrisikoindikatoren sind nicht zielführend:
 - Relative Indikatorwerte, die auf die Veränderung eines Risikos zum Vorjahr abstellen, da diese faktisch eine schleichende Ausweitung der Risikotoleranz bewirken, ohne dass eine formelle Genehmigung durch die Geschäftsleitung erfolgt.
 - Indikatoren, die sich auf Risiken unterschiedlicher Kritikalität beziehen (tief, mittel und hoch), da dies zu einer Verzerrung der Aussage führt und keine klare Zuordnung zu einer definierten Kritikalitätsstufe erlaubt, z.B. Ein Indikator kombiniert Kunden aus Ländern mit tiefem, mittlerem und hohem Risiko in einer Gesamtquote, ohne offenzulegen, welche Kunden jeweils aus Ländern mit tiefem, mittlerem und hohem Risiko stammen.
- iii. Teilweise haben Institute lediglich Schlüsselrisikoindikatoren zur Einschätzung des Kontrollrisikos und keine Schlüsselrisikoindikatoren für inhärente Risiken definiert. Beispiele für Letztere können sein:
 - Anzahl und Asset under Management (AuM) von Geschäftsbeziehungen mit erhöhten Risiken und politisch exponierten Personen (PEP) sowie PEP-nahestehenden Personen;
 - Anzahl von bewilligten ETPs;
 - Exposition in Ländern mit erhöhten Risiken ausserhalb der Zielmärkte des Instituts.

- iv. Zur adäquaten Darstellung eines Schlüsselrisikoindikators sollten mehrere Kennzahlen herangezogen werden (in der Regel: Anzahl Geschäftsbeziehungen sowie Höhe der AuM), um das Portfolio umfassend abzubilden.
- v. Die Höhe der definierten Limiten der Indikatoren sollte im Hinblick auf die definierte Risikotoleranz und Geschäftsstrategie regelmässig kritisch überprüft und gegebenenfalls angepasst werden. *Beispiel: Ein Institut ohne Geschäftsfokus auf PEP und einer deklarierten Risikotoleranz von «mittel» setzt sich für PEP eine Risikolimite von bis zu 15%.*

2 Geldwäschereirisikoanalyse

Die rechtlichen Grundlagen zur Geldwäschereirisikoanalyse für Banken sind in der Aufsichtsmitteilung 05/2023 festgehalten.

Für FINIG-Institute sind folgende rechtlichen Grundlagen relevant: FINIG-Institute sind verpflichtet, die organisatorischen Massnahmen gemäss Art. 8 GwG zu treffen. Diese werden in Art. 23 ff. der Geldwäschereiverordnung-FINMA vom 3. Juni 2015 (GwV-FINMA; SR 955.033.0) konkretisiert und umfassen insbesondere die Erstellung und regelmässige Aktualisierung einer institutsbezogenen Risikoanalyse. Eine Ausnahme von der Pflicht zur Erstellung einer Geldwäschereirisikoanalyse besteht einzig im Anwendungsfall von Art. 75 Abs. 1 GwV-FINMA², sofern Art. 75 Abs. 2 GwV-FINMA³ nicht zur Anwendung gelangt.

2.1 Zu berücksichtigende Geldwäschereirisiken

Vollständigkeit der zu berücksichtigenden Kriterien und Nachvollziehbarkeit der Einschätzung der einzelnen Risiken

Beobachtung gemäss Aufsichtsmitteilung 05/2023:

- a) Regelmässig war festzustellen, dass nicht für jedes erfasste Geldwäschereirisiko jeder Geldwäschereirisikokategorie die Einschätzungen hinsichtlich des inhärenten Risikos und des Kontrollrisikos, sowie des

² Voraussetzungen von Art. 75 Abs. 1 GwV-FINMA sind, dass: a. der Finanzintermediär eine Unternehmensgrösse von fünf oder weniger Vollzeitstellen oder einen jährlichen Bruttoertrag von weniger als 2 Millionen Franken aufweist; und b. ein Geschäftsmodell ohne erhöhte Risiken vorliegt.

³ Ist es zur Überwachung der Einhaltung der Pflichten zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung notwendig, so kann die FINMA aufgrund von Art. 75 Abs. 2 GwV-FINMA auch von einem Finanzintermediär, der die Voraussetzungen nach Art. 75 Abs. 1 GwV-FINMA erfüllt, verlangen, dass die Geldwäschereifachstelle auch die Aufgaben nach Art. 25 GwV-FINMA erfüllt.

daraus resultierenden Nettorisikos einzeln und nachvollziehbar aufgezeigt wurden. Hierbei ist insbesondere aufgefallen, dass nicht immer alle für das Institut relevanten Geldwäschereirisiken abgedeckt wurden.

- i. Nicht immer haben die Institute alle in Art. 25 Abs. 2 GwV-FINMA namentlich genannten und zwingend abzudeckenden Geldwäschereisikokategorien (Kundensegmente, Sitz/Wohnsitz, Produkte und Dienstleistungen) in ihrer Risikoanalyse berücksichtigt.
- ii. Kriterien mit einem mittleren oder tiefen inhärenten Risiko wurden oft nicht in der Risikoanalyse berücksichtigt. Entsprechend fehlte diesen Instituten der notwendige Überblick zur Risikoexposition des Gesamtportfolios.
- iii. Vereinzelt haben Institute unterschiedliche Kritikalitäten eines Risikokriteriums in einer Gruppe zusammengefasst. Eine solche Gruppierung ist jedoch ungeeignet, da sie keinen klaren Rückschluss auf das tatsächliche inhärente Risiko der einzelnen Kriterien zulässt.
Beispiele: Trotz unterschiedlicher inhärenter Risiken wurden Retail-, Affluent- und vermögende Kund/innen in der Gruppe «Höhe der Vermögenswerte» zusammengefasst. Ebenso wurden Länder mit tiefem, mittlerem und hohem inhärentem Risiko in der Gruppe «Länderrisiko (Sitz/Wohnsitz der Kundin)» gebündelt, anstatt sie entsprechend ihrer Kritikalität einzeln auszuweisen.
- iv. Vermögensverwaltungsbanken mit hoher oder sehr hoher Risikotoleranz verwenden teilweise zu wenig granulare Risikokriterien. Insbesondere werden Länderrisiken bezogen auf den Sitz bzw. Wohnsitz der Kund/innen nicht auf Ebene einzelner Länder ausgewiesen, sondern aggregiert. Je nach Geschäftsmodell kann bei geringerer Risikotoleranz eine Kategorisierung der Länder nach Kritikalität ausreichend sein.
- v. Zunehmend bieten Retailbanken auch vermögenden Privatkund/innen massgeschneiderte Dienstleistungen an. Dieses höhere inhärente Risiko wurde in der Risikoanalyse oft nicht mit einem entsprechend höheren Detaillierungsgrad berücksichtigt.
- vi. Institute schätzten das inhärente Risiko einzelner Geldwäschereisikokriterien hinsichtlich ihrer Kritikalität teilweise nicht angemessen ein:
 - Komplexe Strukturen mit einem inhärenten Risiko «mittel» statt «hoch»;
 - PEP mit einem inhärenten Risiko «mittel» statt «hoch»;
 - Krypto-Dienstleistungen mit einem inhärenten Risiko «mittel» statt «hoch».
- vii. Häufige Gründe für eine nicht angemessene Einschätzung der inhärenten Risiken sind:

- Risikomindernde Massnahmen werden bei den inhärenten Risiken berücksichtigt, obwohl sie ins Kontrollrisiko gehören;
- Die Risikotoleranz wird bereits bei den inhärenten Risiken mitberücksichtigt, obwohl sie über Risikolimiten und den Abgleich des Nettorisikos mit der Toleranz (siehe Ziff. 2.3 b) abzudecken ist.

- viii. Zum Teil werden Nettorisiken nicht korrekt bestimmt. Zur korrekten Bestimmung der Höhe des Nettorisikos wird auf Anhang 3 der Aufsichtsprüfverordnung FINMA vom 31. Oktober 2024 (SR 956.161.1) verwiesen. *Beispiel: Fälschlicherweise wurde ein Nettorisiko als «tief» statt «mittel» bei einem Geldwäschereirisikokriterium mit dem inhärenten Risiko «hoch» und dem Kontrollrisiko «tief» ausgewiesen.*
- ix. Vereinzelt ist den Instituten nicht bewusst, dass sehr hohe inhärente Risiken gemäss Anhang 3 der Aufsichtsprüfverordnung FINMA selbst durch effiziente risikomindernde Massnahmen nicht tiefer als «hoch» gesenkt werden können.

Beschreibung der risikomindernden Massnahmen (Kontrollrisiko)

Beobachtung gemäss Aufsichtsmitteilung 05/2023:

b) Zum Nachvollzug der risikomindernden Wirkung von Massnahmen (Kontrollrisiko) auf die inhärenten Risiken, fehlte es zumeist an einem ausreichenden Detaillierungsgrad der beschriebenen Massnahmen. Hierfür sollten insbesondere auch Kennzahlen sowie Erkenntnisse hinsichtlich der Effektivität der durchgeführten Kontrollen (controls of controls) herbeigezogen werden.

- i. Teilweise wurden die Massnahmen zur Risikominderung lediglich mit einem pauschalen Verweis auf interne Weisungen und Prozesse beschrieben. Dies ermöglicht keinen ausreichenden Nachvollzug der konkret vorgesehenen Massnahmen. Massnahmen zur Risikominderung sollten entweder konkret beschreiben oder mit einem Verweis auf bestimmte Kontrollen im Kontrollinventar des Instituts versehen werden.
- ii. Verschiedentlich wurden bloss Bestätigungen der Durchführung von Kontrollen festgehalten und keine Kennzahlen zur Effektivität der durchgeführten Kontrollen verwendet. Ein Beispiel für eine Kennzahl zur Effektivität der durchgeführten Kontrollen kann sein: *«Bei 5% der monatlichen Stichproben durch Compliance zu den Transaktionsabklärungen wurden Mängel bei der Dokumentation gefunden, aber in keinem der Fälle wurden Hinweise auf eine Meldepflichtverletzung festgestellt.»*

2.2 Umsetzung der Anforderungen nach Art. 13 Abs. 2^{bis} GwV-FINMA

Die gewonnenen Beobachtungen und Erfahrungen der FINMA entsprachen denjenigen, welche bereits in der Aufsichtsmitteilung 05/2023 abgebildet sind.

2.3 Überwachung der Einhaltung der Geschäftsstrategie und der Risikopolitik

Definition von Kennzahlen

Beobachtung gemäss Aufsichtsmitteilung 05/2023:

a) Regelmässig konnte festgestellt werden, dass keine Kennzahlen definiert wurden, um zu bestimmen, wie gross die jeweilige Risikoexposition im Gesamtbestand des Kundenstamms und der Dienstleistungspalette der Bank ist und inwieweit die Einhaltung der Geschäftsstrategie und Risikopolitik gewährleistet ist.

- i. Vereinzelt wurden im Rahmen der Risikoanalyse zur Darstellung der Risikoexposition einzelner Risikokriterien im Gesamtbestand lediglich einzelne Kennzahlen herangezogen, z.B. ausschliesslich das Verhältnis AuM zum Gesamtportfolio. Aussagekräftig ist hingegen eine Kombination mehrerer Kennzahlen. Dabei sollten mindestens die AuM und die Anzahl der Geschäftsbeziehungen berücksichtigt werden – jeweils in absoluten Zahlen sowie im Verhältnis zum Gesamtportfolio.
- ii. Gelegentlich wurden Risiken von unterschiedlicher Kritikalität gesamthaft in einer Kennzahl zusammengefasst. Damit sind aber keine Aussagen zur Risikoexposition einzelner Kritikalitäten möglich.

Definition von Risikolimiten

Beobachtung gemäss Aufsichtsmitteilung 05/2023:

b) Häufig fehlt eine Definition der Risikolimiten zur Überwachung der Risikotoleranz, um bei Nichteinhaltung der Schwellenwerte entsprechende Massnahmen zu ergreifen.

- i. Mitunter wurden Risiken mittels Limiten überwacht, die auf das Wachstum gegenüber dem Vorjahr abstellen. Eine solche Betrachtungsweise erlaubt jedoch keine sachgerechte Beurteilung der Risikoexposition im Verhältnis zum Gesamtbestand (siehe auch Ziff. 1 c.) ii.).

- ii. Vereinzelt wurde für Überschreitungen der Risikolimiten eine ETP-Bewilligung vorgesehen, was aus Risikomanagement-Sicht nicht tauglich erscheint. Vielmehr sollten bei Nichteinhaltung der Schwellenwerte entsprechende risikomindernde Massnahmen vorgesehen und implementiert werden, um die Einhaltung der Risikotoleranz sicherzustellen.

Abgleich Nettorisiken mit der Risikotoleranz

Beobachtung gemäss Aufsichtsmitteilung 05/2023:

c) Das Nettorisiko wurde oft nicht mit der Risikotoleranz abgeglichen. Ein solcher Abgleich ist notwendig, um bei Nichteinhaltung der Risikotoleranz Massnahmen zu ergreifen.

- i. Vermehrt haben Institute für jedes Geldwäschereirisiko ein Nettorisiko hergeleitet und dieses mit der Risikotoleranz abgeglichen. Die Aggregation zu einem Gesamtgeldwäschereinettorisiko fehlte hingegen. Entsprechend unterblieb ein aussagekräftiger Abgleich des Gesamtnettorisikos mit der festgelegten Geldwäschereirisikotoleranz.
- ii. Ferner wurde beobachtet, dass bei einer Überschreitung der Risikotoleranz keine Massnahmen ergriffen wurden. Übersteigt das Geldwäschereinettorisiko eines einzelnen Risikokriteriums oder das Gesamtnettorisiko die dafür definierte Toleranz sind risikomindernde Massnahmen zu ergreifen, mit dem Ziel, die Risiken wieder in den Toleranzbereich zu senken.

2.4 Weitere zu berücksichtigende Elemente

Änderungen der Risiken

Beobachtung gemäss Aufsichtsmitteilung 05/2023:

a) Oft waren die Änderungen der Risiken (inhärente Risiken, Kontrollrisiko und Nettorisiken) im Vergleich zum Vorjahr in der Risikoanalyse nicht ersichtlich und nachvollziehbar, obwohl diese dabei unterstützen, die benötigten Massnahmen zur Überwachung der Risiken zu bestimmen.

Vereinzelt wurde die Entwicklung nicht für alle Risiken (inhärente Risiken, Kontrollrisiken und Nettorisiken) nachvollziehbar dargelegt.

Ressourcenanalyse

Beobachtung gemäss Aufsichtsmitteilung 05/2023:

b) Häufig war festzustellen, dass für die Gewährleistung der Umsetzung des Geldwäschereidispositivs der Bank der benötigte qualitative und quantitative Ressourcenbestand nicht kritisch hinterfragt wurde, damit dieser bei Bedarf angepasst werden kann.

Die qualitativen und quantitativen Analysen zum Ressourcenbestand sollten mit entsprechenden Kennzahlen unterlegt werden, die eine Überwachung dieser Entwicklungen erleichtern.

3 Verhältnis zur Rz 78 des FINMA-Rundschreibens 2017/1 «Corporate Governance – Banken»

Die Geldwäschereirisikoanalyse nach Art. 25 Abs. 2 GwV-FINMA sollte einer anderen Methodologie als die Compliance-Risikoanalyse folgen. Die Compliance-Risikoanalyse fokussiert auf das Risiko der Nichteinhaltung gesetzlicher, regulatorischer und interner Vorgaben (Normverletzungsrisiko) sowie die daraus resultierenden aufsichtsrechtlichen, finanziellen und reputativen Auswirkungen. Demgegenüber beurteilt die Geldwäschereirisikoanalyse das Risiko, dass ein Institut aufgrund seiner Geschäftsaktivitäten, Kundenbeziehungen oder Transaktionen für Geldwäscherei oder Terrorismusfinanzierung missbraucht wird (Missbrauchsrisiko).

Diese unterschiedlichen Zielsetzungen bedingen unterschiedliche Ansätze sowohl bei der Identifikation der inhärenten Risiken als auch bei deren Bewertung. Die Identifikation und Bewertung des inhärenten Risikos im Rahmen der Geldwäschereirisikoanalyse hat unter Berücksichtigung von Art. 13 Abs. 2 GwV-FINMA bei allen Instituten grundsätzlich einheitlich zu erfolgen. Als Orientierungshilfe können hierbei auch die Einschätzungen entsprechender internationaler Fachorganisationen (z. B. Financial Action Task Force, Wolfsberg Group) herangezogen werden.

Auf dieser konsistenten Grundlage der Inhärenzbewertung baut die Ermittlung des Nettorisikos auf. Dieses ergibt sich aus der Kombination von inhärentem Risiko und Kontrollrisiko. Für die korrekte Herleitung des Nettorisikos wird auf Anhang 3 der Aufsichtsprüfverordnung FINMA verwiesen.

4 Globale Überwachung der Geldwäschereirisiken

Zu den diesbezüglichen Ausführungen in der Aufsichtsmitteilung 05/2023 werden keine Ergänzungen gemacht.

5 FINIG-Institute

Für FINIG-Institute können die in dieser Aufsichtsmitteilung dargestellten Beobachtungen und Erkenntnisse sinngemäss herangezogen werden. Deren Umsetzung hat unter Berücksichtigung der tatsächlichen Risikoexposition eines Instituts zu erfolgen. Der Detaillierungsgrad und die Ausgestaltung der Risikoanalyse sollte sich nach Art, Umfang, Komplexität und Risikogehalt der Geschäftstätigkeit des jeweiligen Instituts richten. Die Risikoanalyse ist umso detaillierter auszugestalten, je höher die inhärenten Risiken sind, denen sich ein Institut aussetzt. Dies ist insbesondere zu berücksichtigen

- bei der Bestimmung der Anzahl und der Ausgestaltung der verwendeten Schlüsselrisikoindikatoren (vgl. Ziff. 1 c) iv.) und
- bei der Granularität der zu berücksichtigenden Geldwäschereirisiken (vgl. Ziff. 2.1 a) iv.). Ein FINIG-Institut, das aufgrund seiner Tätigkeit keinen erhöhten Geldwäschereirisiken ausgesetzt ist, hat das Länder- (Domizil-) oder Branchenrisiko nicht zwingend auf einzelne Länder bzw. Branchen herunterzubrechen. Ebenso können Dienstleistungen entsprechend ihrer Kritikalität in gröbere Kategorien eingeteilt werden, ohne dass eine detaillierte Aufgliederung erforderlich ist (z. B. klassische Asset-Management-Dienstleistung: tief/mittel/hoch; weitere Nebengeschäfte: tief/mittel/hoch).