Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA-Aufsichtsmitteilung 05/2023

Geldwäschereirisikoanalyse nach Art. 25 Abs. 2 GwV-FINMA

24. August 2023

Laupenstrasse 27, 3003 Bern, Tel. +41 (0)31 327 91 00, www.finma.ch

Inhaltsverzeichnis

Einleitung

Gemäss Art. 25 Abs. 2 GwV-FINMA sind die Banken verpflichtet, unter Berücksichtigung des Tätigkeitsgebiets und der Art der geführten Geschäftsbeziehungen eine Geldwäschereirisikoanalyse (nachfolgend „Risikoanalyse“) zu erstellen. Basierend auf dieser Analyse müssen zudem die Banken für die Kriterien nach Art. 13 Abs. 2 GwV-FINMA je einzeln die Relevanz für die eigenen Geschäftsaktivitäten festhalten (vgl. Art. 13 Abs. 2bis GwV-FINMA) und gemäss Art. 6 Abs. 1 Bst. a GwV-FINMA ausdrücklich regelmässig auch eine entsprechende Risikoanalyse auf konsolidierter Basis vornehmen.[1]

Für Banken ergibt sich die Pflicht zur Erfassung, Begrenzung und Überwachung ihrer Risiken (inkl. Geldwäschereirisiken) auch aus den organisatorischen Anforderungen gemäss Art. 3 Abs. 2 Bst. a BankG i.V.m. Art. 12 Abs. 2 BankV sowie Art. 8 GwG. Die Anforderungen an das Risikomanagement sind zudem im FINMA-Rundschreiben 2017/1 „*Corporate Governance* – Banken“ festgehalten.

Die FINMA hat im Frühjahr 2023 Risikoanalysen von über 30 Banken geprüft. Dabei hat sie festgestellt, dass eine grosse Zahl der geprüften Risikoanalysen den grundsätzlichen Anforderungen an eine solche Analyse nicht entsprechen. Insbesondere fehlte teilweise eine adäquate Definition der Geldwäschereirisikotoleranz (nachfolgend "Risikotoleranz"), die durch festgelegte Limiten den begrenzenden Rahmen einer robusten Risikoanalyse bildet. Weiter mangelte es an verschiedenen strukturellen Elementen, die Voraussetzung bilden für eine Risikoanalyse. Im Anhang finden sich je ein vereinfachtes Beispiel einer nicht adäquaten und einer adäquaten Risikoanalyse aus unseren Praxisbeobachtungen.

Mit vorliegender Aufsichtsmitteilung schafft die FINMA Transparenz zu ihren in der Aufsichtspraxis gemachten Beobachtungen und Erfahrungen zur Risikoanalyse. Diese Beobachtungen und Erfahrungen können sinngemäss auch für FINIG-Institute herangezogen werden.[2]

1 Geldwäschereirisikotoleranz

Eine Bank erfasst, begrenzt und überwacht gemäss Art. 3 Abs. 2 Bst. a BankG i.V.m. Art. 12 Abs. 2 BankV sowie Art. 8 GwG unter anderem ihre Geldwäschereirisiken (inkl. Bekämpfung der Terrorismusfinanzierung). Hierfür hat die Bank gemäss Rz 10 FINMA-RS 17/1 die Grundzüge des Risikomanagements sowie gemäss Art. 19 GwV-FINMA die Zuständigkeit und das Verfahren für die Bewilligung von mit Risiken verbundenen Geschäften in einem Reglement oder in internen Richtlinien zu regeln. Eine Begrenzung

[1] Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 4. September 2017, S. 11

[2] Vgl. Art. 9 Abs. 2 FINIG, Art. 12 Abs. 4, Art. 26 Abs. 1, Art. 41 Abs. 2, Art. 57 Abs. 2 und Art. 68 Abs. 2 FINIV.

dieser Risiken setzt im Speziellen eine adäquate Definition einer Risikotoleranz durch das Institut voraus.[3]

Beobachtungen und Erfahrungen zu Ziff. 1:

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

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.

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 (siehe hierzu auch Ziff. 2.3 b)).

2 Geldwäschereirisikoanalyse

Gemäss Art. 8 GwG treffen Banken die Massnahmen, die zur Verhinderung der Geldwäscherei und der Terrorismusfinanzierung notwendig sind. Eine dieser organisatorischen Massnahmen ist die Erstellung einer Risikoanalyse nach Art. 25 Abs. 2 GwV-FINMA. Für die Risikoanalyse ist zudem Art. 13 Abs. 2bis GwV-FINMA zu berücksichtigen.

Gemäss Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 11. Februar 2015 (nachfolgend "Erläuterungsbericht 2015") handelt es sich bei der Risikoanalyse um «[…] eine Risikoanalyse, welche sämtliche Geldwäschereirisiken, denen der Finanzintermediär ausgesetzt ist, identifiziert, erfasst, analysiert und bemisst. Gestützt auf diese Erkenntnisse definiert er seine Massnahmen zur Bewirtschaftung, Steuerung, Kontrolle, Rapportierung und Überwachung dieser Risiken».[4]

[3] Siehe Rz 53 FINMA-Rundschreiben 2017/1 „*Corporate Governance* – Banken“

[4] Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 11. Februar 2015, S. 20 f.

2.1 Zu berücksichtigende Geldwäschereirisiken

Art. 25 Abs. 2 GwV-FINMA verlangt, dass die Bank für die Risikoanalyse ihr Tätigkeitsgebiet und die Art der von ihr geführten Geschäftsbeziehungen berücksichtigen muss. Dafür sind insbesondere folgende Geldwäschereirisikokategorien heranzuziehen: Sitz oder Wohnsitz der Kundin und des Kunden, das Kundensegment sowie die angebotenen Produkte und Dienstleistungen. Im Erläuterungsbericht 2015 werden die geografische Präsenz des Instituts als weitere Risikokategorie genannt und zusätzliche Ausführungen zu den genannten Kategorien gemacht.[5] Diese Ausführungen verdeutlichen, dass die einzelnen Risiken jeweils für jede Risikokategorie zu erfassen, zu analysieren und zu bemessen sind. Ferner ist festzuhalten, dass der Katalog der in Art. 25 Abs. 2 GwV-FINMA genannten Risikokategorien nicht abschliessend und abhängig vom Geschäftsmodell und der Dienstleistungspalette einer Bank individuell zu ergänzen ist.

Beobachtungen und Erfahrungen zu Ziff. 2.1:

a) Regelmässig war festzustellen, dass nicht für jedes erfasste Geldwäschereirisiko jeder Geldwäschereirisikokategorie die Einschätzungen hinsichtlich des inhärenten Risikos und des Kontrollrisikos, sowie des daraus resultierenden Nettorisikos einzeln und nachvollziehbar aufgezeigt wurden. Hierbei ist insbesondere aufgefallen, dass nicht immer alle für das Institut relevanten Geldwäschereirisiken abgedeckt wurden.

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.

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

Eine Bank hat für die in Art. 13 Abs. 2 GwV-FINMA genannten Kriterien einzeln festzuhalten, ob diese für ihre Geschäftsaktivität relevant sind oder nicht. Die relevanten Kriterien hat sie für die Ermittlung ihrer Geschäftsbeziehungen mit erhöhten Risiken zu berücksichtigen (Art. 13 Abs. 2bis GwV-FINMA). Der Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 4. September 2017 (nachfolgend "Erläuterungsbericht 2017) hält dazu fest, dass ein Kriterium als relevant zu erachten ist, wenn es «*eine bedeutende Anzahl von Geschäftsbeziehungen des Finanzintermediärs betrifft*.»[6]

[5] Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 11. Februar 2015, S. 20

[6] Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 4. September 2017, S. 28

Beobachtungen und Erfahrungen zu Ziff. 2.2:

Häufig war die Beurteilung der Relevanz jedes in Art. 13 Abs. 2 GwV-FINMA genannten Kriteriums in der Risikoanalyse nicht so dargestellt, dass sie für Dritte ersichtlich und nachvollziehbar ist. Dabei fehlte es insbesondere an definierten Kennzahlen, um die Relevanz der Kriterien zu überprüfen (siehe hierzu auch Ziff. 2.3 a).

2.3 Überwachung der Einhaltung der Geschäftsstrategie und der Risikopolitik

Der Erläuterungsbericht 2015 hält fest, dass die Risikoanalyse schriftlich festzuhalten, periodisch zu überprüfen, bei Bedarf anzupassen und jeweils vom Verwaltungsrat oder dem obersten Geschäftsführungsorgan zu verabschieden ist.[7] Damit wird sichergestellt, dass Erkenntnisse der Risikoanalyse auch in die Risikopolitik und in die Geschäftsstrategie (z.B. Festlegung der strategischen Zielmärkte und Kundensegmente) eines Instituts einfliessen.[8]

Konkret bedeutet dies, dass eine Bank bei der Festlegung ihrer Geschäftsstrategie auch das Geldwäschereirisiko mitberücksichtigt. Es besteht somit eine enge Wechselwirkung zur Geschäftsstrategie und Risikopolitik einer Bank. Eine Bank überprüft dafür regelmässig, inwieweit die Zusammensetzung ihres bestehenden Kundenstamms und der Dienstleistungspalette mit ihrer Geschäftsstrategie und ihrer Risikopolitik übereinstimmt.

Bei wesentlichen Änderungen des Dienstleistungsangebots oder der Zusammensetzung des Kundenstamms sind die Kriterien für die Risikoanalyse entsprechend anzupassen und die Risikoanalyse ist zu aktualisieren.

Beobachtungen und Erfahrungen zu Ziff. 2.3:

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.

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

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

[7] Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 11. Februar 2015, S. 21

[8] Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 11. Februar 2015, S. 21

2.4 Weitere zu berücksichtigende Elemente

Der Erläuterungsbericht 2015 hält fest, dass gestützt auf die Erkenntnisse der Risikoanalyse eine Bank ihre Massnahmen zur Bewirtschaftung, Steuerung, Kontrolle, Rapportierung und Überwachung dieser Risiken definiert.[9] Dies umfasst unter anderem den Nachvollzug der Entwicklung der Risiken und die Einschätzung der Ressourcensituation.

Beobachtungen und Erfahrungen zu Ziff. 2.4:

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.

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.

3 Verhältnis zur Rz 78 des FINMA-Rundschreibens 2017/1 „*Corporate Governance* – Banken“

Gemäss Rz 78 FINMA-RS 17/1 nimmt die *Compliance*-Funktion einer Bank eine jährliche Einschätzung des *Compliance*-Risikos der Geschäftstätigkeit des Instituts und die Ausarbeitung eines risikoorientierten Tätigkeitsplans vor, die durch die Geschäftsleitung zu genehmigen sind.

Die Risikoanalyse oder Teile davon können in diese *Compliance*-Risikoanalyse integriert werden. Die Bank hat aber sicherzustellen, dass die Anforderungen des Art. 25 Abs. 2 GwV-FINMA erfüllt sind.

4 Globale Überwachung der Geldwäschereirisiken

Nach dem globalen Risikomanagementgrundsatz in Art. 6 Abs. 1 GwV-FINMA hat eine Bank, die Zweigniederlassungen im Ausland besitzt oder eine Finanzgruppe mit ausländischen Gesellschaften leitet, ihre Rechts- und Reputationsrisiken im Zusammenhang mit Geldwäscherei und Terrorismusfinanzierung auch global zu erfassen, zu begrenzen und zu kontrollieren.

[9] Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 11. Februar 2015, S. 20 f.

Gemäss Art. 6 Abs. 1 Bst. a GwV-FINMA hat dies periodisch in Form einer Risikoanalyse auf konsolidierter Basis zu erfolgen. Die Ausführungen im Erläuterungsbericht 2017 stellen klar, dass es sich hierbei um eine Risikoanalyse nach Art. 25 Abs. 2 GwV-FINMA unter Einbezug der mit den Geschäftsbeziehungen und Transaktionen in den Zweigniederlassungen und Gruppengesellschaften verbundenen Risiken handelt.[10] Die oben in Ziff. 1 und 2 gemachten Ausführungen sind somit ebenfalls für die Risikoanalyse auf konsolidierter Basis relevant.

[10] Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 4. September 2017, S. 11

Anhang

Zur Konkretisierung der Erkenntnisse aus der Prüfung der Risikoanalysen nachfolgend ein Vergleich zwischen einem nicht adäquaten und einem adäquaten Modell einer Risikoanalyse. Die strukturellen Elemente wurden zum Zweck der Übersichtlichkeit stark vereinfacht.

Risikokategorie	Inhärentes Risiko	Risikominimierende Massnahmen
Kundensegmente		*Kurze Umschreibung*
Kurze Umschreibung	*Einschätzung des Risikos*	
Domizil		
Kurze Umschreibung	*Einschätzung des Risikos*	
Produkte und Dienstleistungen		
Kurze Umschreibung	*Einschätzung des Risikos*	

Siehe Ziff. 2.1
Siehe Ziff. 2.3
Siehe Ziff. 2.4

Tabelle 1: Beispiel einer nicht adäquaten Risikoanalyse

Geldwäschereirisikotoleranz						*Einschätzung der Risikotoleranz (tief / mittel / (sehr) hoch)*				
Risikokategorie (RK)	**Inhärentes Risiko**	**Entwicklung zum Vorjahr**	**Risikominimierende Massnahmen**	**Kontrollrisiko**	**Entwicklung zum Vorjahr**	**Nettorisiko**	**Entwicklung zum Vorjahr**	**Kennzahl 1**	**Kennzahl 2**	**Einhaltung der Risikotoleranz**
	Einschätzung des inhärenten Risikos (tief / mittel / (sehr) hoch)	*gesunken, gestiegen oder unverändert*	*detaillierte Umschreibung der für das jeweilige Risikokriterium relevanten Massnahmen (inkl. Kennzahlen sowie Erkenntnisse)*	*Einschätzung des Kontrollrisikos*	*gesunken, gestiegen oder unverändert*	*Einschätzung des Nettorisikos*	*gesunken, gestiegen oder unverändert*	*(z.B. Anzahl Gbz. & deren %-Relation zum Gesamtbestand)*	*(z.B. Höhe der AuM & deren %-Relation zum Gesamtbestand)*	*> / < / = Schwellenwert*
RK1: Kundensegmente										
Kriterium 1 der RK1										
Usw.										
RK2: Domizil										
Kriterium 1 der RK2										
Usw.										
RK3: Produkte und Dienstleistungen DL										
Kriterium 1 der RK3										
Usw.										
RK4: Geografische Präsenz der Bank										
Kriterium 1 der RK3										
Usw.										
Gesamt										

Tabelle 2: Beispiel einer adäquaten Risikoanalyse