Digitalisierung der Datenerhebung für die Geldwäschereirisikoanalyse mit Hilfe eines Kriterienkatalogs

Zertifikatsarbeit im
CAS Cyberrisiken, Compliance & Regtech

Zürcher Fachhochschule
HWZ Hochschule für Wirtschaft Zürich

Eingereicht am 12.11.2020 bei:

Gmünder, Eliane Co-Studiengangsleiterin
Hutter, Ralph Co-Studiengangsleiter

vorgelegt von:
Nadine Riera Mlaw
Oberrebenweg 4, 8304 Wallisellen

Voranmerkung: Im Rahmen meines CAS Cybersecurity, Compliance and RegTech an der HWZ in Zürich habe ich diese Zertifikatsarbeit verfasst. Die in dieser Arbeit wiedergegebenen Gedanken sind Erkenntnisse und Ansichten basierend auf eigenen Interpretationen der herangezogenen Quellen und liegen in der persönlichen Verantwortung der Autorin.

Management Summary

In den letzten vier Jahren sind die regulatorischen Anforderungen an die durch Banken durchzuführende Geldwäschereirisikoanalyse stetig gestiegen. Ziel dieser ist es je Bank ein auf seine Tätigkeit passende und möglichst effektive Geldwäschereiprävention aufzubauen. Eine Analyse, die ohne jegliche Finanztechnologieunterstützung (hier konkret RegTech) viel Aufwand bedeuten kann, da viele Daten zusammengesucht, ausgewertet und analysiert werden müssten. Ein Blick auf den Markt zeigt, dass grundsätzlich schon einige Regtech-Lösungen für Risikoanalysen angeboten werden (Deloitte, 2020). Trotzdem scheinen diese bei den Banken noch nicht flächendeckend Anwendung zu finden. Dabei ist wohl insbesondere der Weg zur Digitalisierung der Datenerhebung für die Geldwäschereirisikoanalyse mit Schwierigkeiten verbunden, da eine allfällige Regtech-Lösung noch mit den benötigten Daten abgefüllt werden und zudem eine solche auch noch alle regulatorischen Anforderungen aus der Geldwäschereiverordnung-FINMA («GwV-FINMA») erfüllen müsste. Dies umfasst einen Initialaufwand, der nicht ohne ist, da eine Bank nicht nur wissen muss, welche Daten sie überhaupt für die Risikoanalyse benötigt, sondern auch wo sie diese allenfalls in einer ihrer Datenerfassungssystemen überhaupt finden kann.

Die Arbeit zeigt auf, wie ein (Geldwäscherei-)Risikokriterienkatalog (nachfolgend «RKK») den Weg zur Digitalisierung der Datenerhebung für die Geldwäschereirisikoanalyse vereinfachen und zugleich einen positiven Effekt auf die Qualität der Analyse haben kann. Hierfür ist mit Hilfe bestehender Literatur zum allgemeinen Risikomanagementprozess und regulatorischer Vorgaben des GwV-FINMA erarbeitet worden, wie ein solcher RKK ausgestaltet sein muss. Auf Basis dieser Erkenntnisse wurde dann ein RKK erstellt und dessen Verwendung erläutert.

Entstanden ist ein im Anhang vorzufindender RKK, der nicht nur eine blosse Auflistung aller potentiellen (insbesondere der regulatorisch benötigten) Risikokriterien darstellt, sondern eine Bank (aber auch andere Finanzintermediäre, für die diese regulatorischen Vorgaben gelten) auch darin unterstützt zu verstehen, wie diese Kriterien durch Daten aus ihrem bestehenden Kundenstamm automatisiert dargestellt werden können und zur Überprüfung ihrer definierten Geschäfts- und Risikostrategie dienen. Denn erst dann kann ein Institut tatsächlich eine fundierte und effektive Geldwäschereirisikoanalyse ausführen.

Inhaltsverzeichnis

1 Einleitung

Seit 2016 sind die Banken gemäss Art. 25 Abs. 2 GwV-FINMA verpflichtet unter Berücksichtigung des Tätigkeitsgebiets und der Art der geführten Geschäftsbeziehungen eine Geldwäschereirisikoanalyse zu erstellen. Bei blosser Durchsicht dieses Artikels ist ein Leser geneigt, davon auszugehen, dass diese Verpflichtung «nur» den Teilaspekt «Risiken analysieren» des Risikomanagementprozesses nach ISO 31000 betrifft. Doch weitere Ausführungen im FINMA-Erläuterungsbericht 2015 machen deutlich, dass nicht nur ein einzelner Prozessschritt, sondern ein komplettes Geldwäschereirisikomanagement erwartet wird, das auch in der Geschäfts- und Risikostrategie einer Bank berücksichtigt werden muss (FINMA, 2015). Des Weiteren verlangt der Artikel, dass die Risikoanalyse als Ausgangspunkt für die Bestimmung der Geldwäschereirisikokategorien und -kriterien zu verwenden ist (FINMA, 2015).

Insbesondere die letzte Anforderung der Bestimmung scheint aber nicht bei allen Instituten angekommen zu sein, so fühlte sich der Regulator zwei Jahre später dazu gezwungen, Art. 13 Abs. 2bis GwV-FINMA einzuführen. Institute werden nun explizit aufgefordert «*bei der Festlegung der Kriterien, die sie für die Kategorisierung ihrer Geschäftsbeziehungen verwenden, die mit ihrer Geschäftstätigkeit verbundenen Geldwäschereirisiken besser zu berücksichtigen»* (FINMA, 2017, S. 28). Hiermit soll sichergestellt werden, dass Institute ihre Erkenntnisse aus ihren auf ihr jeweiliges Tätigkeitsgebiet angepassten Risikoanalysen zur Überprüfung ihrer bestehenden Risikostrategien und Risikokriterien nutzen. Es fällt aber auf, dass Institute zum Teil keine detaillierte Geldwäschereirisikostrategie festgelegt und/oder nicht alle notwendigen Geldwäschereirisiken identifiziert haben, um ein fundiertes Geldwäschereirisikomanagement sicherzustellen. Es erweckt den Eindruck als ob sich die verantwortlichen Personen nicht bewusst sind, welche nützliche Erkenntnisse sie aus einer angemessenen gestaltenden Geldwäschereirisikoanalyse ziehen können und den damit verbundenen Aufwand eher scheuen.

Meiner Meinung nach könnte genau hier eine Regtech-Lösung einen Beitrag zur Verbesserung der Qualität leisten. Auf dem Markt werden schon einige Regtech-Lösungen für Risikoanalysen angeboten (Deloitte, 2020)[1]. Zumeist bitten diese bereits ein ausgeklügeltes System zur Umsetzung einer Risikoanalyse an und nutzen hierfür eine automatisierte Datenerhebung. Trotzdem habe ich noch nicht viele solcher Regtech-Lösungen im Bereich der Geldwäschereirisikoanalyse konkret angewendet gesehen. Viele Banken scheinen insbesondere den Weg zur Digitalisierung der Datenerhebung für die Geldwäschereirisikoanalyse noch nicht eingeschlagen zu haben, da eine allfällige Regtech-Lösung erst noch mit den benötigten Daten abgefüllt werden müssten.

Dies setzt voraus, dass eine Bank genau weiss, welche Daten sie für eine regulatorisch konform ausgestaltete Geldwäschereirisikoanalyse benötigt, wo diese dann in ihren Datenerfassungssystemen vorzufinden sind und wie sie diese dann entsprechend zu aggregieren hat.

[1] Zum Beispiel: Artic Intelligence, Australien 2015: https://arctic-intelligence.com/products/risk-assessment (besucht am 17.09.2020); Ayasdi, USA 2008: https://www.ayasdi.com/solutions/financial-crime/ (besucht am 17.09.2020); Featurespace, Grossbritannien 2005: https://www.featurespace.com/products/aric-risk-hub/ (Besucht am 17.09.2020).

Während der zweite Teil dieser Voraussetzung *"Wo findet die Bank die benötigten Daten in einer ihrer Datenerfassungssystemen?"* von Bank zu Bank zumeist sehr individuell ausgestaltet ist, ist der erste Teil *"Welche Daten braucht die Bank für eine regulatorisch konforme Geldwäschereirisikoanalyse?"* für jede Bank gleich zu beantworten, auch wenn das Resultat der Analyse dann wieder sehr unterschiedlich sein kann. Genau hier möchte ich mit meiner Zertifikatsarbeit anknüpfen.

Ziel dieser Arbeit ist es aufzuzeigen, dass ein (Geldwäscherei-) RKK den Weg zur Digitalisierung der Datenerhebung für die Geldwäschereirisikoanalyse vereinfachen und zugleich einen positiven Effekt auf die Qualität der Analyse haben kann. In Ziff. 2 wird hierfür auf Basis bestehender Literatur und regulatorischer Vorgaben erarbeitet, ob und wenn ja, weshalb ein solcher RKK, die Digitalisierung der Datenerhebung vereinfachen und verbessern würde. In Ziff. 3 werden dann die Schlussfolgerungen diesbezüglich festgehalten. Bei Bestätigung der These würde dann in Ziff. 4 die Erstellung und die Verwendung eines solchen RKK anhand der erarbeiteten Vorgaben erläutert und dieser in den Anhang hinzugefügt werden.

2 Die Geldwäschereirisikoanalyse

Gemäss Art. 25 Abs. 2 GwV-FINMA sind Banken verpflichtet *« […] unter Berücksichtigung des Tätigkeitsgebiets und der Art der geführten Geschäftsbeziehungen des Finanzintermediärs eine Risikoanalyse unter den Aspekten der Bekämpfung der Geldwäscherei […] »* zu erstellen. Wie bereits oben erwähnt, ist ein Leser bei blosser Durchsicht dieses Artikels geneigt, davon auszugehen, dass diese Verpflichtung «nur» den Teilaspekt «Risiken analysieren» des Risikomanagementprozesses nach ISO 31000 betrifft.

Folgende Ausführungen im entsprechenden FINMA-Erläuterungsbericht weisen aber eher auf eine gegenteilige Schlussfolgerung hin: « *[…] 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»* (FINMA, 2015). Mit der im GwV-FINMA Artikel umschriebenen Risikoanalyse wird somit nicht nur ein Prozessschritt, sondern ein komplettes Geldwäschereirisikomanagement erwartet[2]. Es ist daher wichtig zu verstehen, wie ein solcher Risikomanagementprozess aufzubauen ist und welche regulatorischen Vorgaben in der GwV-FINMA einzuhalten sind.

2.1 Risikomanagement-Grundlagen

Es gibt zahlreiche Normen und Rahmenwerke, die den Risikomanagement-Prozess umschreiben. In dieser Arbeit orientieren wir uns an die Norm ISO/IEC 31000 Risk Management, die den Prozess wie folgt darstellt:

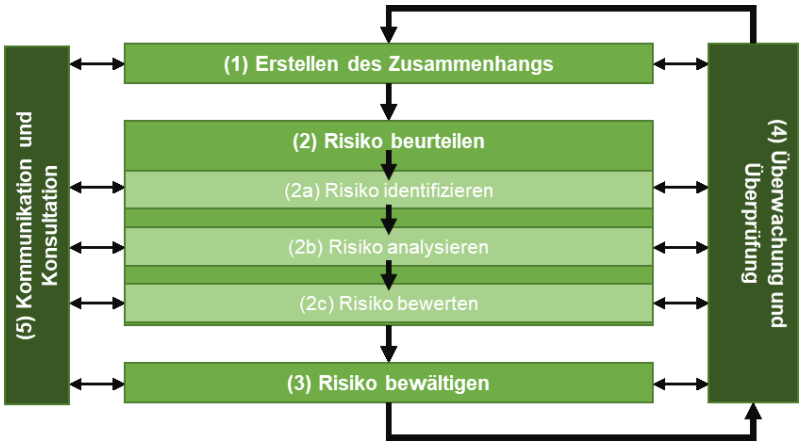


Abbildung 1: Risikomanagementprozess nach ISO 31000

[2] Fortan, wenn der Begriff Geldwäschereirisikoanalyse verwendet wird, ist grundsätzlich das komplette Geldwäschereirisikomanagement und nicht nur ein Teilaspekt zu verstehen.

2.1.1 Schritt 1: Erstellen des Zusammenhangs

Der erste Schritt eines Risikomanagement-Prozesses ist es die externen und internen Rahmenbedingen zu ermitteln (Brühwiller, 2012). Ein Unternehmen muss zu einem verstehen, in welchen Umfeld sie sich bewegt und zum anderen welche Ziele sie mit welchen Strategien und Prozessen umsetzen möchte (Brühwiller, 2012). Es geht darum, eine Risikostrategie aufsetzen zu können, die definiert wie ein Unternehmen grundsätzlich mit seinen Risiken umgehen möchte (Klein, 2016). Die Risikostrategie hat somit sowohl die Rahmenbedingungen der Geschäftstätigkeiten eines Unternehmens zu berücksichtigen, die Einbindung in die Aufbauorganisation sicherzustellen, sowie die akzeptierte Schwellenwerte für Risiken (sogenannter Risikoappetit) festzulegen (Romeike, 2018).

Eine Risikostrategie kann somit nicht innert kürzester Zeit aus den Boden gestampft werden, sondern muss unter Berücksichtigung vieler Aspekte sorgfältig erarbeitet werden (Klein, 2016). Auch darf sie nicht zu einen blossen Papiertiger verkommen, sondern muss von der obersten Stufe des Managements bis zum letzten einfachsten Mitarbeiter tatsächlich gelebt werden (Klein, 2016). Hierfür sind der «ton from the top», die Einbettung der Risikostrategie auf den unterschiedlichsten Unternehmensstufen und die fortwährende kritische Hinterfragung und Fortentwicklung der Strategie essentiell (Klein, 2016). Aspekte, die im Eifer der Geschäftstätigkeiten schnell vergessen gehen können.

2.1.2 Schritt 2: Risikobeurteilung

Beim nächsten Prozessschritt geht es darum, Risiken zu erkennen, diese zu analysieren und dann entsprechend für das Institut zu bewerten, damit darauf aufbauend im nächsten Prozessschritt Massnahmen zu deren Bewältigung definiert werden können.

2.1.2.1 Teilschritt 2a: Risiko identifizieren

Risikomanagement kann nur wirksam betrieben werden, wenn ein Unternehmen seine Risiken auch erkennt (Klein, 2016; Romeike, 2018). Dieser Teilschritt soll sicherstellen, dass ein Unternehmen seine Risiken aufspürt (Klein, 2016; Romeike, 2018). Eine Aufgabe, die sehr anspruchsvoll ist, denn es gibt unzählige interne und externe Faktoren, die ein Unternehmen in ihrer Suche zu berücksichtigen hat (Klein, 2016; Romeike, 2018). Für die Risikoidentifikation können unterschiedlichen Arbeitsmittel verwendet werden, wie Checklisten, Workshops, Arbeitsprozessanalysen, Benchmarks, Fragenbogen, Betriebsbesichtigungen usw. (Gleissner & Klein, 2017; Klein, 2016).

Bei der Sammlung der Risiken ist es besonders wichtig strukturiert mit einer Risikosystematisierung vorzugehen, so kann am ehesten gewährleistet werden, dass keine Risiken verloren gehen (Klein, 2016). Zur Gliederung dieser gibt es viele Möglichkeiten, um hier nur ein paar wenige zu nennen: nach Risikofelder, nach Organisationseinheiten, nach Schadenspotential, anhand der Wertschöpfungskette, nach Ursachen beziehungsweise Umfeldbereichen usw. (Klein, 2016).

Die in diesem Prozessschritt erkannten Risiken sollten nicht nur in einem Risikokatalog entsprechend der gewählten Systematisierung aufgelistet werden, sondern auch ausreichend in der Risikobeschreibung erläutert werden (Klein, 2016). Somit kann eher sichergestellt werden, dass das gesamte Unternehmen unter einem bestimmten Risiko tatsächlich das Gleiche versteht.

2.1.2.2 Teilschritt 2b: Risiko analysieren

Die Erkennung von Unternehmensrisiken bringt nichts, wenn das Unternehmen diese nicht richtig versteht. Denn nur mit einem klaren Verständnis des Risikos können im Folgeschritt die Risiken auf das Institut entsprechend bewertet und die richtigen Massnahmen zur Risikominimierung definiert werden (Romeike, 2018). In dieser Prozessphase sind daher die Risiken sowohl nach ihrer Ursachen und Quellen, ihrer Auswirkungen (positive und negative) sowie die Häufigkeit resp. Wahrscheinlichkeit ihres Eintretens zu analysieren (Romeike, 2018).

2.1.2.3 Teilschritt 2c: Risiko bewerten

Im letzten Teilschritt dieses Prozessschrittes werden dann die bisher erarbeiteten, qualitativen Ergebnisse in Zahlen ausgedrückt, indem die Risiken durch potenzielle Schäden oder Schadenszenarien und den damit verknüpften Häufigkeiten bzw. Eintrittswahrscheinlichkeiten bewertet werden (Romeike, 2018). Es stehen dann die inhärenten Risiken zur Verfügung, um die Risiken einschätzen zu können.

2.1.3 Schritt 3: Risiko bewältigen

Nachdem die Risiken beurteilt wurden, kann im dritten Prozessschritt die passende Strategie zur Bewältigung definiert werden (Romeike, 2018). Nicht tolerierbare Risiken müssen entweder vermieden, vermindert und überwacht werden (Brühwiller, 2012). Es gilt Massnahmen zu entwickeln, um die inhärenten Risiken zu vermindern. Das verbleibende Risiko ist dann das Restrisiko und müsste der definierten Risikotoleranz in der Risikostrategie einer Bank entsprechen (Brühwiller, 2012).

2.1.4 Überwachung und Überprüfung

Die bis jetzt beschriebenen drei Prozessschritte werden fortwährend überwacht und kritisch hinterfragt. Diese übergreifende Massnahme soll sicherstellen, dass die einzelnen Phasen des Risikomanagement korrekt ausgeführt werden, die definierten Massnahmen zur Risikobewältigung richtig umgesetzt werden und das Risikomanagement an sich die beabsichtigte Wirkung entfaltet (Romeike, 2018). Insbesondere sind die Wechselwirkungen zwischen der Überwachung und der einzelnen Phasen im Risikomanagement nicht zu unterschätzen. So kann eine Überprüfung dazu führen, dass Risiken neu definiert oder eingeschätzt werden oder ein Unternehmen sogar erkennt, dass ihr tatsächlich wahrgenommenes Risiko nicht mehr mit ihrer definierten Risikostrategie übereinstimmt und sie somit allenfalls sogar ihre Unternehmensstrategie nochmals zu hinterfragen hat (Klein, 2016).

2.1.5 Kommunikation und Konsultation[3]

Ein weiterer übergreifende Prozessschritt ist die «Kommunikation und Konsultation». Sie ist ein Schlüsselelement eines Unternehmens ihre Risikokultur aufzubauen, weiterzuentwickeln und zu etablieren (Romeike, 2018). Nur mit Unterstützung dieser kann sichergestellt werden, dass jeder im Unternehmen von der obersten Stufe des Managements bis zum letzten einfachsten Mitarbeiter tatsächlich die Risikostrategie so umsetzt, wie sie definiert worden ist (Klein, 2016).

2.2 Regulatorische Vorgaben der GwV-FINMA

Nachdem bereits die einzelnen Prozessschritten eines Risikomanagements beleuchtet wurden, werden nun die spezifischen Anforderungen des Art. 25 Abs. 2 GwV-FINMA beleuchtet, wobei auch noch Art. 13 Abs. 2bis GwV-FINMA mitberücksichtig wird[4].

2.2.1 Berücksichtigung der Geschäftstätigkeit

Art. 25 Abs. 2 GwV-FINMA stipuliert klar, dass die Geldwäschereifachstelle einer Bank für die Risikoanalyse «*ihr Tätigkeitsgebiet»* und die «*Art der von ihr geführten Geschäftsbeziehungen»* zu berücksichtigen hat. Hierfür sollen gemäss genannter Artikel bestimmte Hilfskriterien, nämlich «*Sitz und Wohnsitz der Kunde und des Kunden»*, «*das Kundensegment»*, sowie «*die angebotenen Produkte und Dienstleistungen»* herbeigezogen werden. Im relevanten FINMA Erläuterungsbericht wird die «*geografische Präsenz des Instituts»* als weiteres Kriterium genannt und weitere Ausführungen zu den genannten Hilfskriterien gemacht (FINMA, 2015). Grundsätzlich soll festgestellt werden, ob bestimmte Risiken für ein Institut allenfalls wegfallen, weil diese aufgrund der Geschäftstätigkeit des Instituts nicht vorgesehen sind. Je nach Art der Geschäftstätigkeit einer Bank ist nämlich das Geldwäscherei-Gesamtrisiko unterschiedlich gross[5].

Eine Bank hat sich zur Berücksichtigung der Geschäftstätigkeit gemäss Vorgaben folgende Fragen zu stellen:

a) Aus was für Kunden setzt sich die Kundschaft der Bank zusammen?
b) In welchem Land oder in welchen Ländern ist resp. möchte die Bank tätig (sein)?
c) Was für Produkte und Dienstleistungen bietet die Bank an?

Des Weiteren müsste gemäss Ausführungen der Wolfsberg Gruppe (The Wolfsberg Group, 2015) eine Bank auch noch folgendes abklären:

d) Über welchen oder welche Vertriebskanal / -kanäle akquiriert die Bank ihre Kunden?

Es ist wichtig zu betonen, dass es sich bei dieser Aufzählung von Hilfskriterien nicht um eine abschliessende handelt. Die Verwendung des Wortes «insbesondere» im Artikel weist darauf

[3] Im Rahmen dieser Zertifikatsarbeit wird aber auf diesen Teilaspekt nicht vertiefter eingegangen.
[4] Art. 6 GwV-FINMA hinsichtlich der konsolidierten Überwachung wird hier bewusst ausgeklammert.
[5] Eine entsprechende Aufstellung hat wiederum die Wolfsberg Group zusammengestellt (siehe The Wolfsberg Group, 2015, siehe Annex H). Zum Beispiel hat eine reine Kreditbank ein tieferes Geldwäschereirisiko als eine Private Banking Bank.

hin, dass die Bank noch weitere berücksichtigen sollte. Mögliche weitere Kriterien hat die Wolfsberg Gruppe in ihren FAQs zusammengestellt (The Wolfsberg Group, 2015, S.10 oder Annex H).

Bei näherer Betrachtung der im Erläuterungsbericht genannten Hilfskriterien zur Berücksichtigung der Geschäftstätigkeit fällt auf, dass diese Geldwäschereirisikokategorien darstellen, in denen die einzelnen Risiken noch zu identifizieren wären. Um es an einem Beispiel aufzuzeigen: Eine Retailbank müsste zur Beantwortung der Frage zur Zusammensetzung ihrer Kunden erst alle Geldwäschereirisiken, die mit einem Kunden auftreten können identifizieren (z.B. Höhe der Vermögenswerte, Partnertyp, Transaktionsverhalten usw.). Je identifiziertes Risiko hat sie sich dann die Frage zu stellen, ob das jeweilige Risiko für ihre konkrete Geschäftstätigkeit von Relevanz ist resp. sein sollte. Zum Beispiel kann für eine Retailbank gemäss ihrer Geschäftsstrategie die Betreuung von sehr vermögenden Kunden (sogenannte High-Networth-Kunden «HNW») wegfallen, womit für dieses Kriterium die Geschäftstätigkeit «kein Geschäft» vorzusehen wäre, wohingegen die Retailkunden ein Kerngeschäft darstellen würden.

2.2.2 Geldwäschereirisikostrategie

Art. 25 Abs. 2 GwV-FINMA sieht auch vor, dass der Verwaltungsrat oder das oberste Geschäftsführungsorgan die Risikoanalyse zu verabschieden hat. Gemäss Erläuterungsbericht stellt dies sicher, dass Erkenntnisse der Risikoanalyse auch in die Risikopolitik und in die Festlegung der strategischen Zielmärkte und Kundensegmente eines Institut einfliessen (FINMA, 2015). Konkret bedeutet dies, dass eine Bank eine Strategie unter Berücksichtigung des Geldwäschereirisikos zu definieren hat. Am besten macht sie das indem sie je identifiziertes Geldwäschereirisikokriterium feststellt, wie gross ihr Risikoappetit resp. ihre Risikotoleranz ist (z.B. Vermeidung, kleine, moderate oder grosse Risikotoleranz)[6]. Die festgelegte Risikotoleranz gilt es dann auch noch mit Schwellenwerten zu konkretisieren.

Zum Beispiel würde die vorher erwähnte Retailbank in Anbetracht ihrer festgelegten Geschäftstätigkeit «kein Geschäft» mit HNW-Kunden, konsequenterweise die Risikostrategie «Vermeidung» wählen und einen Schwellenwert von 0% definieren. Eine Wealth Management Bank würde stattdessen für das gleiche Geldwäschereirisikokriterium sicherlich keine Risikostrategie «Vermeidung» wählen, sondern sich gut überlegen müssen, wie viel Risiko (klein, moderat oder gross) sie bereit ist mit dieser Kundenart auf sich zu nehmen, da diese mit hohen inhärenten Risiken verbunden ist.

2.2.3 Risikominimierende Massnahmen bestimmen

Auch wenn im Wortlaut des Art. 25 Abs. 2 GwV-FINMA nicht explizit die Pflicht zur Implementierung von risikominimierenden Massnahmen erwähnt wird, geht aus dem FINMA-Erläuterungsbericht klar hervor, dass « *[…] Massnahmen zur Bewirtschaftung, Steuerung, Kontrolle, Rapportierung und Überwachung dieser Risiken»* zu definieren sind (FINMA, 2015, S. 20).

[6] Eine Bank kann hier natürlich ihre eigenen und differenzierteren Metriken verwenden. Hier kommen lediglich vereinfachte Metriken zur Anwendung.

Eine Bank hat somit Massnahmen zu implementieren, die eine risikominimierende Wirkung auf die inhärenten Risiken haben. Eine Bank sollte hierfür je Geldwäschereirisikokriterien festzustellen, welches Risiko nach der Anwendung von Kontrollen auf das ursprünglich inhärente Risiko noch verbleibt (sogenanntes Restrisiko) (The Wolfsberg Group, 2015). Am Schluss verfügt die Bank über eine Auflistung aller im RKK aufgelisteten Restrisiken und kann diese mit der Risikostrategie abgleichen, um zu überprüfen, ob die definierte Risikostrategie mit den aufgestellten Massnahmen eingehalten werden kann.

Eine Auflistung in Betracht zu ziehende Massnahmen bietet wiederum die Wolfsberg Gruppe in ihren FAQs im Anhang I an (The Wolfsberg Group, 2015, Annex I).

2.2.4 Periodische Überprüfung

Des Weiteren ist die Risikoanalyse «*schriftlich festzuhalten, periodisch zu überprüfen und bei Bedarf anzupassen»* (FINMA, 2015, S. 21). Es besteht somit eine enge Wechselbeziehung zur Geschäftsstrategie und Risikopolitik einer Bank. Eine Bank muss hierfür fortwährend überprüfen, ob die Zusammensetzung ihres bestehenden Kundenstamms auch ihrer Geschäftsstrategie und Risikopolitik entspricht. Entspricht der Kundenstamm nämlich nicht (mehr) der Geschäftsstrategie und/oder der Risikopolitik muss eine Bank dies kritisch hinterfragen und allenfalls benötigte Anpassungen vornehmen.

Im Folgenden werden ich auf drei Überwachungsmassnahmen vertiefter eingehen. Zwei davon sind meiner Meinung aus den regulatorischen Vorgaben ableitbar und die dritte ergibt sich aus dem in den letzten Jahren immer stärker werdenden Paradigmenwechsel von der Überprüfung der rein technischen Konformität mit Geldwäschereivorschriften weg zur Überprüfung der tatsächlichen Wirksamkeit von Geldwäschereiabwehrsystemen (The Wolfsberg Group, 2020).

2.2.4.1 Überprüfung der Geldwäschereirisikokriterien nach Art. 13 Abs. 2bis GwV-FINMA

In ihrer Risikoanalyse hat die Bank noch eine weitere Besonderheit zu beachten, die in Art. 13 Abs. 2bis GwV-FINMA formuliert ist: Eine Bank muss aufgrund ihrer Risikoanalyse für die in Art. 13 Abs. 2 GwV-FINMA aufgelisteten Kriterien einzeln festhalten, ob sie für seine Geschäftsaktivität relevant sind oder nicht und berücksichtigt sie dann für die Ermittlung ihrer Geschäftsbeziehungen mit erhöhten Risiken. Im relevantem Erläuterungsbericht wird definiert, dass ein Kriterium als relevant zu erachten ist, wenn es *«eine bedeutende Anzahl von Geschäftsbeziehungen des Finanzintermediärs betrifft»* (FINMA, 2017). Wendet eine Bank ein Kriterium trotz Erfüllung dieser Bedingung nicht an, muss sie es entsprechend begründen (FINMA, 2017).

Konkret bedeutet dies, dass die Bank zwangsläufig für alle in Art. 13 Abs. 2 GwV-FINMA aufgelisteten Kriterien, jeweils feststellen muss, ob eine bedeutende Anzahl von Geschäftsbeziehungen betroffen ist. Die Kriterien nach Art. 13 Abs. 2 GwV-FINMA sind daher zwangsläufig als Geldwäschereirisiken in einem RKK zu identifizieren. Zudem muss eine Bank für sich definieren, wann «*eine bedeutende Anzahl von Geschäftsbeziehungen»* betroffen ist. Liegt

eine solche bedeutende Anzahl vor, ist grundsätzlich von einer Relevanz für die Geschäftstätigkeit der Bank auszugehen. In einem solchen Fall müsste das entsprechende Geldwäschereirisiko auch als Kriterium in der internen Weisung der Bank vorgesehen sein, ist das nicht der Fall muss die Bank schriftlich festhalten, warum dem nicht so ist. Meiner Meinung nach ist der Begriff *«Anzahl von Geschäftsbeziehungen»* zur Ermittlung der Relevanz nicht zu eng zu fassen, da auch der *«Anteil an Vermögenswerte»* zur Ermittlung der Relevanz verwendet werden kann.

Um das Beispiel von vorher wieder aufzugreifen: Eine Retailbank hat für das Kriterium vermögender Kunde (HNW-Kunde) die Geschäftstätigkeit «kein Geschäft» bestimmt und deswegen das Kriterium nicht berücksichtigt. Bei der Analyse stellt sich aber heraus, dass die Bank über zwei Geschäftsbeziehungen (0.00002% von der Gesamtanzahl Geschäftsbeziehungen) verfügt, die 10% der gesamten verwalteten Vermögen der Bank ausmachen. Die Bank hat für sich definiert, dass ein 10%-Anteil an der Gesamtanzahl Geschäftsbeziehungen respektive am verwalteten Gesamtvermögen für sie eine Relevanz darstellt. In diesem konkreten Fall müsste die Bank also dieses Risiko grundsätzlich in ihrer Weisung als Kriterium vorsehen, ansonsten wäre dies entsprechend schriftlich zu begründen.

2.2.4.2 Überprüfung der Geschäftstätigkeit und Risikostrategie

Auch zur Überprüfung der Geschäftstätigkeit und der Risikostrategie macht es Sinn wie in Ziff. 2.2.4.1 bereits umschrieben, je identifiziertes Geldwäschereirisiko festzustellen, wie viele Kunden tatsächlich betroffen sind. Nur so kann überprüft werden, ob eine Bank auch tatsächlich ihre gewählte Geschäftstätigkeit und Risikostrategie lebt und nicht nur über einen Papiertiger verfügt. Grundsätzlich sollten bei Risikokriterien, für die die Bank die Geschäftstätigkeit «kein Geschäft» festgelegt hat, keine bestehenden Kunden das Kriterium erfüllen. Falls das doch der Fall wäre, müsste mindestens eine Exception to Policy (EtP)-Bewilligung vorliegen.

Um das Beispiel der Retail Bank erneut zu verwenden: Auch wenn sie EtPs für die zwei Geschäftsbeziehungen mit HNW-Kunden eingeholt hat, muss sie kritisch hinterfragen, ob diese zwei Geschäftsbeziehungen tatsächlich nur Ausnahmen zur definierten Geschäftstätigkeit «kein Geschäft» und zur Risikostrategie «Vermeidung» darstellen oder nicht allenfalls die Geschäftstätigkeit und Risikostrategie angepasst werden muss resp. sie sich von den HNW-Kunden konsequenterweise trennen müsste.

2.2.4.3 Überprüfung der Wirksamkeit der Massnahmen (z.B. Backtesting)

International gesehen, entwickelt sich aktuell ein Trend dazu, den Fokus nicht auf einer blossen technischen Compliance in Form von Checklisten auszurichten, sondern vermehrt zu hinterfragen, ob die angewendeten Massnahmen, die im Rahmen der Risikoanalyse erarbeitet wurden, auch tatsächlich im Kampf gegen die Geldwäscherei wirksam sind (The Wolfsberg Group, 2020). Hierfür ist es wichtig, die gewählten risikominimierende Massnahmen regelmässig kritisch zu hinterfragen und aufgrund der daraus entstehenden Erkenntnisse, diese allenfalls anzupassen. Eine Unterfangen, das nicht einfach ist, da Wirksamkeit nicht einfach in Zahlen zu ermitteln ist (The Wolfsberg Group, 2020).

Eine Massnahme, die sicherlich in Betracht gezogen werden kann, ist das sogenannte Backtesting von neusten Geldwäschereifällen. Hierbei geht es darum, aktuelle Fälle zu analysieren und über den eigenen Kundenstamm laufen zu lassen, um zu prüfen, ob diese Geldwäschereifälle bei der Bank angeschlagen hätten und entsprechend abgeklärt worden wären. Je nach Resultat kann die Bank dann für ihre Risikoanalyse für den Schritt «risikominimierenden Massnahmen definieren» zu einem unterschiedlichen Ergebnis hinsichtlich des risikominimierenden Ausmasses einer Massnahme zum Vorjahr kommen und müsste allenfalls ihre definierten Massnahmen neu überdenken.

Auch kann die Bank versuchen, die Qualität der durch ihr eingesetztes Überwachungssystem ermittelten Treffer von Transaktionen mit erhöhten Risiken («TmeR») kritisch zu hinterfragen, indem sie sich die Frage stellt, wie viel Prozent dieser Treffer tatsächlich ein erhöhtes Risiko darstellen. Auch das Resultat dieser Wirksamkeitsprüfung könnte eine Auswirkung auf die Vorjahresbeurteilung der risikominimierende Wirkung einer Massnahme haben. Eine weitere Herangehensweise zur Wirksamkeitsprüfung wäre die Verdachtsmeldungen miteinander abzugleichen und zu analysieren, welche Fälle an die Staatsanwaltschaft weitergeleitet wurden und welche nicht.

Es gibt diverse Möglichkeiten, die ausprobiert und ausgetestet werden müssen. Strukturiert kann das die Bank angehen, indem sie einen allenfalls erstellten Massnahmenkatalog durchgeht und sich je Massnahme überlegt, wie diese durch quantitative Daten auf Wirksamkeit geprüft werden kann.

3 Schlussfolgerung / Empfehlung

Die Auseinandersetzung mit den Grundlagen des Risikomanagements und den regulatorischen Vorgaben der GwV-FINMA lassen mich hinsichtlich der Digitalisierung der Datenerhebung folgende Schlussfolgerungen ziehen:

(1) Art. 25 Abs. 2 GwV-FINMA kann mit der Wortwahl «Risikoanalyse» von vielen Anwender zu eng gefasst werden. Weitere Aspekte eines Risikomanagement-Prozesse (insbesondere die Berücksichtigung der Risikopolitik, die Überwachung und die Kommunikation) dürfen dadurch nicht vergessen oder zu wenig Beachtung geschenkt werden. und Es wird die Einrichtung eines kompletten Geldwäschereirisikomanagementprozesses erwartet. In einer Geldwäschereirisikoanalyse muss daher grundsätzlich sichergestellt werden, dass alle Prozessschritte eines Risikomanagement-Prozesses gemäss ISO 31000 abgedeckt sind. Für die Digitalisierung der Datenerhebung bedeutet dies, dass auch Aspekte anderer Prozessschritte und nicht nur die des zweiten Schrittes in einen RKK einzufliessen haben.

(2) Es ist grundsätzlich schwierig festzustellen, welcher Prozessschritt nach ISO 31000 in einer Geldwäschereirisikoanalyse zuerst auszuführen ist, insbesondere in einem Kreislauf und den starken Wechselwirkungen zwischen den unterschiedlichen Schritten[7]. Es hat sich aber herausgestellt, dass die Geldwäschereirisiken Dreh- und Angelpunkt einer Risikoanalyse sind. In jedem Prozessschritt wird wieder auf die Geldwäschereirisiken zurückgegriffen. Die Identifikation dieser ist daher als erstes auszuführen. Ein RKK, der bereits möglichst alle potentielle Geldwäschereirisiken aufgelistet hat, kann einer Bank am meisten dabei unterstützen, eine Digitalisierung der Datenerhebung sicherzustellen.

(3) Die regulatorischen Vorgaben in Art. 13 Abs. 2bis und Art. 25 Abs. 2 GwV-FINMA machen klare Vorschriften, welche Risikokriterien zwangsläufig in einer Risikoanalyse zu berücksichtigen sind. Ein RKK, der sicherstellt, dass alle zwangsläufig zu berücksichtigen Kriterien gemäss regulatorischen Vorgaben abgedeckt sind, gibt zudem einer Bank die Sicherheit, dass die Digitalisierung der Datenerhebung regulatorisch konform vonstatten gehen kann.

(4) In Art. 14 Abs. 2 und 3 GwV-FINMA sind auch noch Kriterien für Transaktionen vorgesehen. Im Gegensatz zu den Geschäftsbeziehungskriterien sind allerdings für diese grundsätzlich keine explizite Berücksichtigung in der Risikoanalyse analog Art. 13 Abs. 2bis GwV-FINMA vorgesehen. Da die Transaktionsüberwachung auch eine evidente Rolle in der Geldwäschereibekämpfung einnimmt, sollte meiner Meinung nach allerdings auch die Transaktionskriterien in die Risikoanalyse direkt[8] miteinbezogen werden[9]. Enthält ein RKK auch noch diese Kriterien, kann eine Risikoanalyse noch fundierter ausgestaltet werden.

(5) Es lassen sich auch regulatorische Anforderungen an die auszuführenden Überwachungsmassnahmen herleiten, die - gemäss Schlussfolgerung (1) oben - in den RKK einfliessen müssen: Die Zusammensetzung des bestehenden Kundenstamms je Geldwäschereirisiko muss in die Risikoanalyse miteinbezogen werden. Hierbei handelt es sich um Daten, die grundsätzlich automatisiert aus den Datenerfassungssystemen einer Bank hergeleitet werden können. Dies setzt allerdings voraus, dass eine Bank genau definiert, wie sie Risiken in ihrem Kundenstamm mit Daten quantitativ aufzeigen. Diese sollten dann für den Abgleich mit der Geschäftstätigkeit, der Risikopolitik und der von der Bank definierten Geschäftsbeziehungen mit erhöhten Risiken verwendet werden, wobei diese quantitativen Zahlen gleich darzustellen sind. Der RKK soll somit nicht nur eine Auflistung

---

[7] So muss ein Institut ja die Geldwäschereirisiken schon identifiziert haben (Prozessschritt 2a «Risiko identifizieren» nach ISO 31000), bevor sie feststellen kann, ob diese für ihre spezifische Tätigkeit jetzt überhaupt relevant sind (Prozessschritt 1 «Erstellen des Zusammenhangs» nach ISO 31000). Auch muss eine Bank bereits die Geldwäschereirisiken bewertet haben (Prozessschritte 2b und 2c «Risiko analysieren und beurteilen nach ISO 31000», um überhaupt festlegen zu können, wie ihre Risikostrategie (Prozessschritt 1 «Erstellen des Zusammenhangs» nach ISO 31000) dann auszugestalten ist.

[8] Indirekt werden sie durch Art. 13 Abs. 2 lit. e, f und i GwV-FINMA über die Geschäftsbeziehungskriterien berücksichtigt.

[9] Während die Wolfsberg Gruppe in ihren FAQs noch erklärte, dass es grundsätzlich akzeptiert ist, das Risikoassessment über die Geschäftsbeziehungsstruktur – und nicht auch noch oder stattdessen über die Transaktionsstruktur – vorzunehmen (The Wolfsberg Group, 2015), erklärte bereits die Nederlandsche Bank in ihrer Analyse zwei Jahre später, dass sowohl Geschäftsbeziehungs- wie auch Transaktionskriterien im Risk Assessment zu berücksichtigen sind (De Nederlandsche Bank, 2017).

möglichst aller Geldwäschereirisikokriterien sein, sondern die Bank in ihrer Definition der konkret zu erhebenden Daten unterstützen.

Es weist vieles darauf hin, dass ein RKK den Weg zur Digitalisierung der Datenerhebung für die Geldwäschereirisikoanalyse für eine Bank vereinfachen und zugleich einen positiven Effekt auf die Qualität der Analyse haben kann, wenn er die hier dargestellten Erkenntnisse berücksichtigt.

4 Der (Geldwäscherei-)Risikokriterienkatalog

Aufgrund der im Kapitel 3 zusammengefassten Erkenntnisse habe ich einen RKK entwickelt, der im Anhang vorzufinden ist und auf den im Folgenden jeweils referenziert wird.

4.1 Zweck des RKK

Zweck des erstellten RKK ist es

(1) möglichst alle (insbesondere die durch die GwV-FINMA geforderten) Geldwäschereirisikokriterien aufzulisten und
(2) die Bank bei der Definition der zu erhebenden Daten je Geldwäschereirisiko konkret zu unterstützen.

Wenn eine Bank sich entscheidet, den angehängten Risikokatalog zu verwenden, muss sie sich bewusst sein, dass dieser als Hilfsmittel zur Datenerhebung einer automatisierten Lösung einer Risikoanalyse dient. Welche Lösung eine Bank zur konkreten Ausführung der Risikoanalyse verwendet, ist dabei nicht von Relevanz. Eine Bank hat aber sicherstellen, dass diese Lösung die in dieser Arbeit beschriebenen Prozesse abdeckt. Insbesondere sollten auch die in Ziff. 2.2.4 beschriebenen Überwachungsmassnahmen berücksichtigt sein.

Im Folgenden wird dargestellt, wie der im Anhang vorzufindende RKK erstellt wurde (Ziff. 4.2) und zu verwenden ist (Ziff. 4.3).

4.2 Erstellung des RKK

Zur Erstellung des RKKs wird in einem ersten Schritt dargestellt, wie die Auflistung möglichst aller (insbesondere die durch die GwV-FINMA geforderten) Geldwäschereikriterien vorgenommen wurde und in einem zweiten Schritt erläutert, was bei den zu erhebenden Daten je Geldwäschereirisiko zu beachten ist.

4.2.1 Geldwäschereirisikokriterien

4.2.1.1 Systematisierung

Zur Auflistung von Risiken ist es wichtig, eine Risikosystematisierung anzuwenden (Klein, 2016). Aufgrund der regulatorischen Vorgaben scheint hier eine Systematisierung nach Risikokategorie und -felder zweckmässig. Hierbei ist sicherzustellen, dass die regulatorisch vorgeschriebenen Risikokategorien (wie in Ziff. 2.2.1 bereits beschrieben) und mindestens alle Kriterien nach Art. 13 Abs. 2 GwV-FINMA (wie in Ziff. 2.2.4.1 bereits beschrieben) berücksichtigt werden. Zusätzlich sollten meiner Meinung nach (wie in Ziff. 3 in der Schlussfolgerung (4) beschrieben) die Transaktionskriterien nach Art. 14 Abs. 2 und 3 GwV-FINMA in die Risikoanalyse einfliessen.

Zur Erstellung der Risikokategorien des RKK im Anhang orientierte ich mich an die von der Wolfsberg Gruppe vorgeschlagen Grundkategorien (The Wolfsberg Group, 2015):

(1) Kunden;
(2) Geografie;
(3) Produkte und Dienstleistungen und
(4) Vertriebskanäle.

Aufgrund der erwähnten regulatorischen Vorgaben habe ich diese Grundkategorien der Wolfsberg Gruppe noch um folgende zwei ergänzt:

(5) Transaktionen und
(6) Komplexität der Geschäftsbeziehung

Jeder dieser Risikokategorie (Spalte B des RKK) ist wiederum in Risikofelder (Spalte D des RKK) eingeteilt. Je Risikofeld sind dann die einzelnen Kriterien (Spalte F des RKK) aufgelistet (The Wolfsberg Group, 2015).[10]

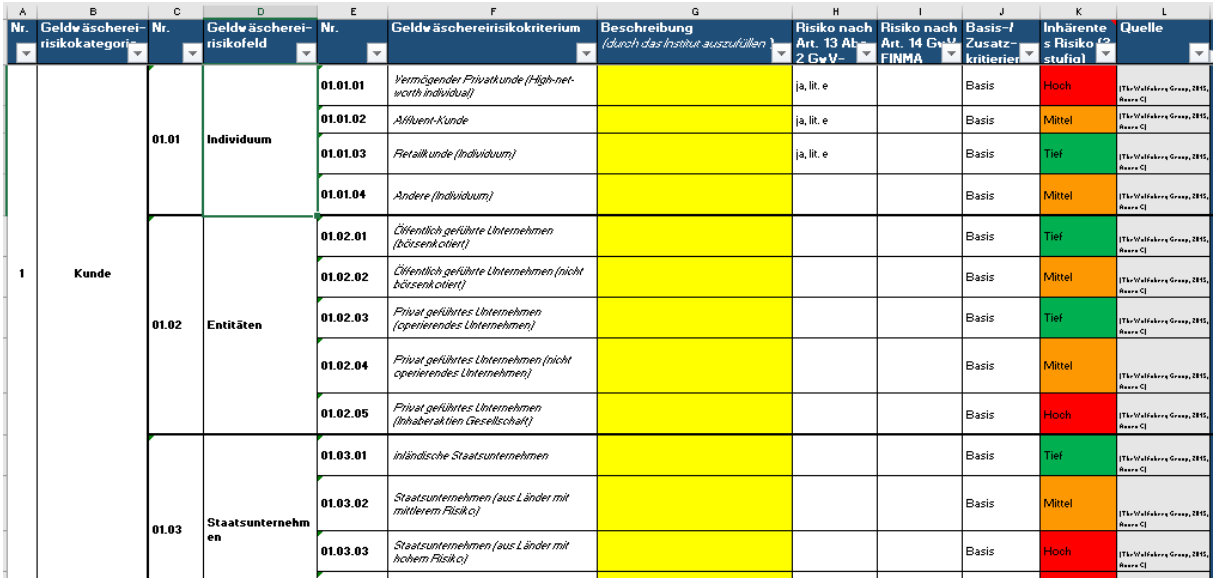
[10] Ein Beispiel: Für die Risikokategorie Kunde gibt es unter anderem die Risikofelder (siehe Kriterienkatalog Spalte D) Individuum, Entitäten, Staatsunternehmen usw. Für das Risikofeld Individuum sind dann die einzelnen Kriterien in der Spalte F aufgelistet.

A	B	C	D	E	F
Nr.	Geldwäscherei-risikokategorie	Nr.	Geldwäscherei-risikofeld	Nr.	Geldwäschereirisikokriterium
1	Kunde	01.01	Individuum	01.01.01	*Vermögender Privatkunde (High-net-worth individual)*
				01.01.02	*Affluent-Kunde*
				01.01.03	*Retailkunde (Individuum)*
				01.01.04	*Andere (Individuum)*
		01.02	Entitäten	01.02.01	*Öffentlich geführte Unternehmen (börsenkotiert)*
				01.02.02	*Öffentlich geführte Unternehmen (nicht börsenkotiert)*
				01.02.03	*Privat geführtes Unternehmen (operierendes Unternehmen)*
				01.02.04	*Privat geführtes Unternehmen (nicht operierendes Unternehmen)*
				01.02.05	*Privat geführtes Unternehmen (Inhaberaktien Gesellschaft)*
		01.03	Staatsunternehmen	01.03.01	*inländische Staatsunternehmen*
				01.03.02	*Staatsunternehmen (aus Länder mit mittlerem Risiko)*
				01.03.03	*Staatsunternehmen (aus Länder mit hohem Risiko)*

Abbildung 2: Ausschnitt aus dem RKK zur Darstellung der Risikosystematisierung

Im RKK kann in der Spalte H und I nachvollzogen werden, welche regulatorische Anforderungen durch welche Kriterien erfüllt werden[11]. Auch sind die Quellenangaben der einzelnen Risikokriterien aus der Spalte L des Katalogs ersichtlich.

[11] Ein Beispiel: Art. 13 Abs. 2 lit. e GwV-FINMA verlangt die Berücksichtigung der Höhe der Zu- und Abflüsse von Vermögenswerten. Dies wird durch die drei Kriterien im Risikofeld 01.05 «Transaktionsverhalten des Kunden» sichergestellt.



A	B	C	D	E	F	G	H	I	J	K	L
Nr.	Geldwäscherei-risikokategorie	Nr.	Geldwäscherei-risikofeld	Nr.	Geldwäschereirisikokriterium	Beschreibung (durch das Institut auszufüllen)	Risiko nach Art. 13 Abs. 2 GwV-FINMA	Risiko nach Art. 14 GwV-FINMA	Basis-/Zusatzkriterien	Inhärentes Risiko (3-stufig)	Quelle
1	Kunde	01.01	Individuum	01.01.01	Vermögender Privatkunde (High-net-worth individual)		ja, lit. e		Basis	Hoch	[The Wolfsberg Group, 2015, Annex G]
				01.01.02	Affluent-Kunde		ja, lit. e		Basis	Mittel	[The Wolfsberg Group, 2015, Annex G]
				01.01.03	Retailkunde (Individuum)		ja, lit. e		Basis	Tief	[The Wolfsberg Group, 2015, Annex G]
				01.01.04	Andere (Individuum)				Basis	Mittel	[The Wolfsberg Group, 2015, Annex G]
		01.02	Entitäten	01.02.01	Öffentlich geführte Unternehmen (börsenkotiert)				Basis	Tief	[The Wolfsberg Group, 2015, Annex G]
				01.02.02	Öffentlich geführte Unternehmen (nicht börsenkotiert)				Basis	Mittel	[The Wolfsberg Group, 2015, Annex G]
				01.02.03	Privat geführtes Unternehmen (operierendes Unternehmen)				Basis	Tief	[The Wolfsberg Group, 2015, Annex G]
				01.02.04	Privat geführtes Unternehmen (nicht operierendes Unternehmen)				Basis	Mittel	[The Wolfsberg Group, 2015, Annex G]
				01.02.05	Privat geführtes Unternehmen (Inhaberaktien Gesellschaft)				Basis	Hoch	[The Wolfsberg Group, 2015, Annex G]
		01.03	Staatsunternehmen	01.03.01	Inländische Staatsunternehmen				Basis	Tief	[The Wolfsberg Group, 2015, Annex G]
				01.03.02	Staatsunternehmen (aus Länder mit mittlerem Risiko)				Basis	Mittel	[The Wolfsberg Group, 2015, Annex G]
				01.03.03	Staatsunternehmen (aus Länder mit hohem Risiko)				Basis	Hoch	[The Wolfsberg Group, 2015, Annex G]

Abbildung 3: Ausschnitt aus dem RKK zur Darstellung der Erfüllung regulatorischer Anforderungen und Quellenangaben

Diese hier dargestellten Risikokategorien sind die Basiskategorien, diese können durch weitere ergänzt werden. Auch hier hat die Wolfsberg Gruppe in ihren FAQs mögliche Kategorien aufgelistet:

(7) Stabilität der Kundenbasis;
(8) Integration von IT-Systemen;
(9) Erwartetes Konto-/Kundenwachstum;
(10) Erwartetes Ertragswachstum;
(11) Jüngste Anti-Geldwäscherei-Compliance-Mitarbeiterfluktuation;
(12) Abhängigkeit von Drittanbietern;
(13) Kürzliche/geplante Einführungen neuer Produkte und/oder Dienstleistungen und/oder kürzliche/geplante Akquisitionen; und
(14) Jüngste interne Revisionsprüfungen oder andere wesentliche Feststellungen (The Wolfsberg Group, 2015, Anhang G).

Diese Kategorien sind ebenfalls im RKK berücksichtigt worden[12]. Des Weiteren besteht im RKK in Spalte E die Möglichkeit, die Risiken zu beschreiben. Es wurde bewusst darauf verzichtet, Standardbeschreibungen hinzuzufügen, da die Institute individuell für sich definieren sollten, was sie unter den einzelnen Risiken verstehen. Durch diesen Prozess wird ein einheitliches Verständnis des Risikos innerhalb des Instituts sichergestellt und Missverständnisse vermieden.

Bei genauerer Betrachtung der bisher abgeleiteten Kriterien macht es den Anschein, dass nur interne Risikokategorien, also solche die sich konkret auf eine Bank beziehen, berücksichtigt wurden. Als externe Risikokategorien müssten auch aktuelle Entwicklungen von Bedrohungsszenarien / Geldwäschereirisiken, technologische Entwicklungen, Entwicklung von

[12] Im Kriterienkatalog ist in Spalte G «Basis-/Zusatzkriterium» festgehalten, ob es sich um ein Basis-/Zusatzkriterium handelt. Basiskriterien sind zwingend in der Risikoanalyse zu berücksichtigen.

neuen Produkten usw. bedacht werden. Diese Aspekte sind allerdings im RKK miteingeflossen: so wurden unter anderem neuste technologische Entwicklungen (z.B. virtual assets)[13] und die Konsultation von Schweizerischen National Risikoassessment oder anderen relevanten Berichten (Die interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), 2015, 2017, 2018a, 2018b, 2019) berücksichtigt. Da sich aber externe Risikokategorien fortwährend ändern, sollte eine Bank auch periodisch den RKK überarbeiten[14].

4.2.1.2 Bestimmung des inhärenten Risikos

Hat eine Bank alle potentiellen Geldwäschereirisiken erkannt, geht es an die Bestimmung des inhärenten Risikos. Das inhärente Risiko stellt die Gefährdung durch Geldwäschereirisiken dar, in der Annahme, dass kein Kontrollumfeld besteht (The Wolfsberg Group, 2015). Dies bedeutet, dass in dieser Risikobeurteilung noch keine institutsspezifische Beurteilung einer Bank hineinfliesst. Zur Bestimmung des inhärenten Risikos sind die Risiken, wie in Ziff. 2.1.2.2 und Ziff. 2.1.2.3 beschrieben, zu analysieren und zu beurteilen.

Im RKK sind aber bereits erfolgte grobe Einschätzungen zum inhärenten Risiko[15], wie zum Beispiel die der Wolfsberg Gruppe (The Wolfsberg Group, 2015) oder Hinweise diesbezüglich aus dem FINMA-Erläuterungsbericht (FINMA, 2015), eingebaut worden[16]. Als grobe Orientierung schadet eine solche erste Einschätzung nicht, ein Institut hat aber ihr inhärentes Risiko je Kriterium selber einzuschätzen und sollte ihre Methodologie hierzu schriftlich für Dritte nachvollziehbar festhalten (The Wolfsberg Group, 2015).

4.2.2 Konkret zu erhebenden Daten

Je identifiziertes Geldwäschereirisikokriterium hat eine Bank zu definieren, wie sie sich diese durch quantitative Daten aus ihrem bestehenden Kundenstamm aufzeigen lässt. In Frage kommen unter anderem folgende quantitative Kennzahlen (Liste nicht abschliessend):

a) Anzahl der vom Kriterium betroffenen Kundenbeziehungen in Relation zur Gesamtanzahl Kundenbeziehungen;
b) Höhe der Vermögenswerte der vom Kriterium betroffenen Kundenbeziehungen in Relation zu den Gesamtvermögenswerten;
c) Anzahl der vom Kriterium betroffenen Transaktionen in Relation zur Gesamtanzahl Transaktionen;
d) Höhe der vom Kriterium betroffenen Transaktion in Relation zur Gesamthöhe der Transaktionen;
e) Höhe der gesperrten Geschäftsbeziehungen in Relation zur Gesamtanzahl;
f) Anzahl offener Positionen in der Geldwäschereifachstelle in Relation zur Gesamtanzahl Positionen in der Geldwäschereifachstelle; und

[13] Siehe RK Nr. 1.08.11 im RKK.
[14] Siehe nachfolgend Schritt 1.) in Ziff. 4.3.
[15] siehe Spalte K in Abbildung 3 oben.
[16] Im Kriterienkatalog Lasche G «inhärente Risiken» wird auf bereit erfolgte Einschätzungen zurückgegriffen, jeweilige Quelle wird erwähnt. Wo keine gefunden wurden, erfolgte eine eigene Einschätzung ebenfalls gekennzeichnet.

g) Anzahl der weitergeleiteten Geldwäschereimeldungen an die STA / zur Gesamtanzahl Geldwäschereimeldungen.

Bei der Auswahl der anzuwendenden Kennzahlen je Kriterium hat die Bank sicherzustellen, dass sie die gleichen auch zur Darstellung für Schwellenwerte der Risikostrategie und zum Abgleich mit der Geschäftsstrategie und der definierten Kriterien für Geschäftsbeziehungen mit erhöhten Risiken verwendet. Im RKK werden je Risikokriterium ein bis zwei Kennzahlen zur Verwendung in der Spalte N und O vorgeschlagen. In den danach folgenden Spalten hat die Bank die Möglichkeit sich festzuhalten, wo die Quelle der jeweils benötigten Daten liegt. Für viele der Kriterien (konkret die der Kategorien 01-04 und 06) können die oben genannten Kennzahlen a.) und b.) verwendet werden. Für die Risikokategorie 05: Transaktionen kommen zwangsläufig die oben genannten Kennzahlen c.) und d.) zur Anwendung. Für die Risikokategorie 07: andere qualitative Kriterien muss die Bank im RKK individuell passende Kennzahlen definieren.

F	M	N	O	P	Q	R	S
Geldwäschereirisikokriterium		**Kennzahl 1 in % (Datenquelle 1a / Datenquelle 1b)**	**Kennzahl 2 in % (Datenquelle 2a / Datenquelle 2bb)**	***Datenquelle 1a*** *(durch das Institut auszufüllen)*	***Datenquelle 1b*** *(durch das Institut auszufüllen)*	***Datenquelle 2a*** *(durch das Institut auszufüllen)*	***Datenquelle 2b*** *(durch das Institut auszufüllen)*
Vermögender Privatkunde (High-net-worth individual)		Anzahl Gbz. mit Kriterium: Vermögender Privatkunde (High-net-worth individual) / Gesamtanzahl Gbz.	Höhe der AuM mit Kriterium: Vermögender Privatkunde (High-net-worth individual) / Höhe der Gesamt-AuM aller Gbz.				
Affluent-Kunde		Anzahl Gbz. mit Kriterium: Affluent-Kunde / Gesamtanzahl Gbz.	Höhe der AuM mit Kriterium: Affluent-Kunde / Höhe der Gesamt-AuM aller Gbz.				
Retailkunde (Individuum)		Anzahl Gbz. mit Kriterium: Retailkunde (Individuum) / Gesamtanzahl Gbz.	Höhe der AuM mit Kriterium: Retailkunde (Individuum) / Höhe der Gesamt-AuM aller Gbz.				
Andere (Individuum)		Anzahl Gbz. mit Kriterium: Andere (Individuum) / Gesamtanzahl Gbz.	Höhe der AuM mit Kriterium: Andere (Individuum) / Höhe der Gesamt-AuM aller Gbz.				
Öffentlich geführte Unternehmen		Anzahl Gbz. mit Kriterium: Öffentlich geführte	Höhe der AuM mit Kriterium: Öffentlich geführte				

Abbildung 4: Ausschnitt aus RKK zur Darstellung der Kennzahlen und ihrer Datenquelle

4.3 Anwendung des RKK

Entscheidet sich eine Bank den angehängten RKK zu verwenden, muss sie

1.) in einem ersten Schritt die Kriterien des RKK auf Vollständigkeit überprüfen. Allenfalls sind Kriterien anzupassen und/oder neue zu ergänzen, sei es zum Beispiel durch neue politische und/oder regulatorische Entwicklungen.

2.) in einem zweiten Schritt jedes Kriterium durchgehen, um jeweils eine detaillierte Risikobeschreibung in der Spalte G des RKK zu formulieren. Es gilt sicherzustellen, dass jeder in der Bank das gleiche Verständnis vom Risiko hat und dann auch die daraus resultierenden Kennzahlen richtig zusammengestellt werden können.

3.) in einem dritten Schritt für die Risikokategorie 2: Geografie für jedes Land der Welt definieren, ob nun ein tiefes, mittleres oder hohes Risiko gegeben ist. Hierfür kann eine Bank zum Beispiel den *Basel AML-Index Expert* verwenden (Basel Institute on Governance, 2020). Das Basel Institut on Governance bietet eine Liste an, die dabei hilft, das Risiko von Korruption, Geldwäsche und Terrorismusfinanzierung in jedem Land der Welt zu bewerten (Basel Institute on Governance, 2020).

4.) in einem vierten Schritt je Risikokriterium das vorgeschlagene inhärente Risiko überprüfen und allenfalls anpassen und

5.) im letzten Schritt je Risikokriterium Kennzahlen definieren und die entsprechenden Datenquelle ermitteln.

Nach diesen fünf Schritten verfügt die Bank über ein Hilfsmittel, das die Digitalisierung der Datenerhebung zur Umsetzung einer automatisierten Risikoanalysen vereinfachen sollte.

5 Quellenverzeichnis

Artic Intelligence. (2020). *Riskassessment*. Abgerufen am 17. September 2020 von https://arctic-intelligence.com/products/risk-assessment

Ayasdi. (2020). Financial Crime. Abgerufen am 17. September 2020 von https://www.ayasdi.com/solutions/financial-crime/

Basel Institute on Governance. (2020). *Basel AML Index Expert Edition*. Abgerufen am 7. Oktober 2020, von https://baselgovernance.org/basel-aml-index/expert-edition

Brühwiller, B. (2012). *Risikomanagement nach ISO 31000 und ONR 49000 mit 13 Praxisbeispielen* (2. Aufl.). Wien, Österreich: Austrian Standard Plus Publishing.

Deloitte. (2020). *Regtech Universe 2020*. Abgerufen am 17. September 2020 von https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html

De Nederlandsche Bank. (2017). *Post-event transaction monitoring process for banks*. Abgerufen am 25. September 2020, von https://www.toezicht.dnb.nl/en/binaries/51-236846.pdf

Die interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT). (2015). *Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz.* Abgerufen am 25. September 2020 von https://www.newsd.admin.ch/newsd/message/attachments/42572.pdf

Die interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT). (2017). *National Risk Assessment (NRA): Geldwäschereirisiken bei juristischen Personen*. Abgerufen am 25. September 2020, von https://www.sif.admin.ch/dam/sif/de/dokumente/Integrität des Finanzplatzes/national-risk-assessment.pdf.download.pdf/National Risk Assessment (NRA) - D.pdf

Die interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT). (2018a). *National Risk Assessment (NRA): Bericht über die Bargeldverwendung und deren Missbrauchsrisiken für die Geldwäscherei und Terrorismusfinanzierung in der Schweiz*. Abgerufen am 25. September 2020, von https://www.newsd.admin.ch/newsd/message/attachments/55177.pdf

Die interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT). (2018b). *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung.* Abgerufen am 25. September 2020 von https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf

Die interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT). (2019). *National Risk Assessment (NRA): Korruption als Geldwäschereivortat: Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung*. Abgerufen am 25.Septem-

ber 2020 von https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaesche-rei/nra-berichte/nra-bericht-april-2019-d.pdf

Eidgenössische Finanzmarktaufsicht (FINMA). (2015). *Geldwäschereiverordnung-FINMA (GwV-FINMA) Erläuterungsbericht zur Totalrevision der GwV-FINMA*. Abgerufen am 17. September 2020 von https://www.finma.ch/de/~/media/finma/dokumente/dokumenten-center/8news/eb-gwv-finma.pdf?la=de

Eidgenössische Finanzmarktaufsicht (FINMA). (2017). *Geldwäschereiverordnung-FINMA (GwV-FINMA) Erläuterungsbericht zur Teilrevision der GwV-FINMA*. Abgerufen am 17. September 2020 von https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/anhoerungen/laufende-anhoerungen/rs-gwv/20170904-eb-gwv-finma.pdf?la=de

Featurespace. (2020) ARIC™ Risk Hub. Abgerufen am 17. September 2020 von https://www.featurespace.com/products/aric-risk-hub/

Gleissner, W., & Klein, A. (2017). *Risikomanagement und Controlling: Chancen und Risiken erfassen, bewerten und in die Entscheidugnsfindung integrieren* (2. Auflage). Freiburg, München, Stuttgart, Deutschland: Haufe Gruppe.

Klein, A. (2016). *Risikomanagement und Risiko-Controlling*. Freiburg, München, Stuttgart, Deutschland: Haufe Gruppe.

Romeike, F. (2018). *Risikomanagement*. Wiesbaden, Deutschland: Springer Gabler

The Wolfsberg Group. (2015). *The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption*. Abgerufen am 10. September 2020 von https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf

The Wolfsberg Group. (2020). *Developing an Effective AML / CTF Programme*. *Abgerufen am 25. September 2020 von https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20Effective%20Financial%20Crimes%20Programme%20-%20August2020%20%28FFP%29.pdf*

6 Anhang: (Geldwäscherei-)Risikokriterien-katalog (RKK)

(siehe Excel-Datei)