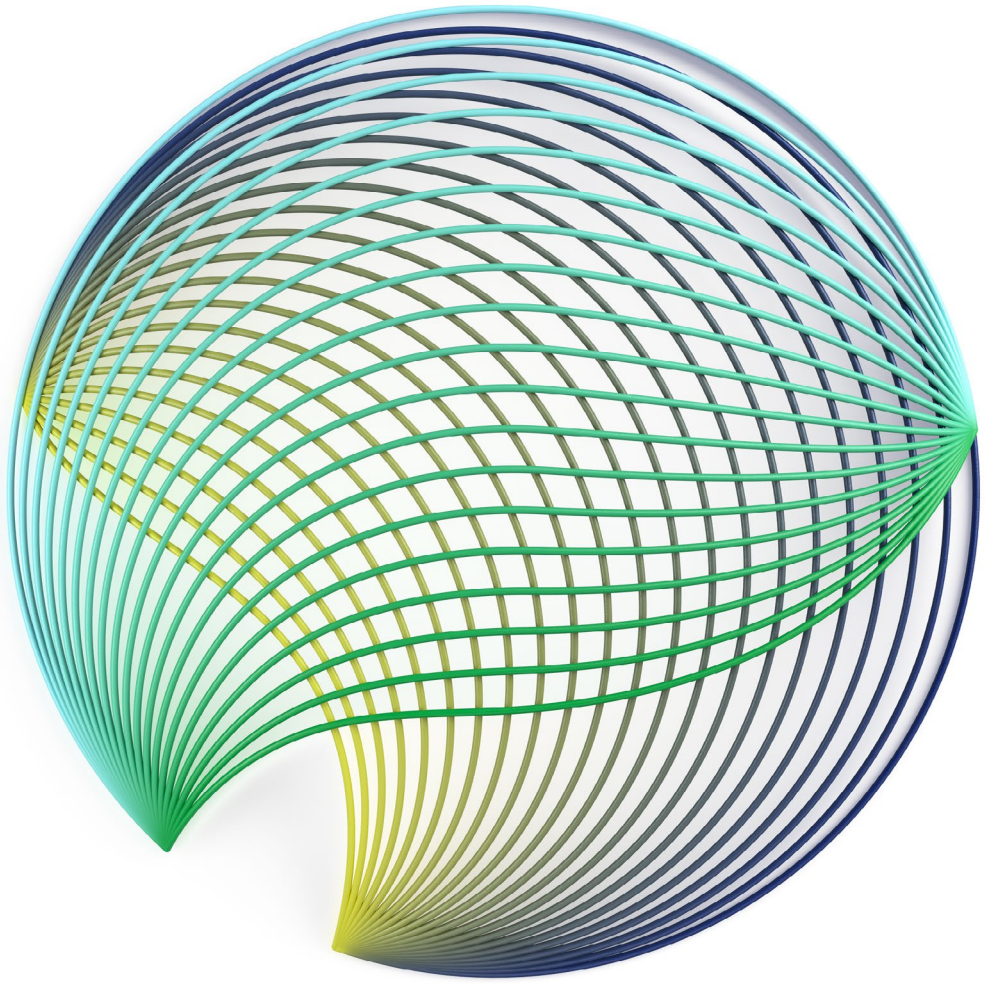
Deloitte.



Non-Financial Risk Management als Teil des Risikomanagementsystems in der Finanzbranche

Einleitung

Im Risikomanagement von Finanzinstituten wird üblicherweise der Fokus nahezu ausschließlich auf die Mitigation finanzieller Risiken wie Kredit-, Markt- und Liquiditätsrisiken gelegt. Diese sind direkt dem operativen Geschäftsablauf zuzuordnen und wurden zur Bildung von Rückstellungen für Verluste quantifiziert.[1] Insbesondere in den letzten Jahren wurde jedoch immer deutlicher, dass weitere Risiken existieren, die sich negativ auf die Wirtschafts- und Ertragslage sowie die Reputation und Integrität eines Instituts auswirken können.[2] Laut Schätzungen verbuchten allein die zwölf größten europäischen und acht größten amerikanischen Finanzinstitute nach der Finanzkrise einen jährlichen Verlust von über 44 Milliarden Dollar im Zeitraum von 2012 bis 2017 aufgrund der Realisierung nicht-finanzieller Risiken.[3]

[1] Vgl. Liermann et al. (2021), S. 161 f.
[2] Vgl. ACFE (2022), S. 5.
[3] Vgl. Franke (2020), S. 281.

Diese sog. nicht-finanziellen Risiken (NFR) werden nicht durch monetäre Risikokategorien erfasst oder quantifiziert, können allerdings indirekte negative Auswirkungen auf die Finanzlage eines Instituts haben. Beispiele für NFR sind regulatorische Risiken durch Nichteinhaltung von Vorschriften, strategische Risiken durch veränderte Marktbedingungen oder Wettbewerbsdruck und operative Risiken durch schlechte Reputation[4] aufgrund negativer Berichte in der Presse oder sozialen Medien. Nicht-finanzielles Risikomanagement bezieht sich dabei auf einen Prozess der Identifizierung, Bewertung und Minderung von Risiken, die durch regulatorische Strafen oder Vertrauensverlust der Kunden einen signifikant negativen Einfluss auf die wirtschaftliche Lage eines Instituts haben. Als Folge der Auswirkungen von NFR auf Instituts- sowie Marktebene rückten Identifikation und Mitigation nicht-finanzieller Risiken immer stärker in den Fokus von Instituten und Regulatoren.[5] Auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat sich dieser Risiken angenommen und führt regelmäßige Prüfungen durch, um einen ethischen und einwandfreien Geschäftsbetrieb sicherzustellen. In den letzten Monaten sind insbesondere Compliance-Abteilungen negativ aufgefallen, da Risiken zu spät erkannt oder nicht durch angemessene Präventionsmaßnahmen, z.B. zur Verhinderung von Geldwäsche und Terrorismusfinanzierung, minimiert wurden.[6]

Systematic-Integrity-Risk-Analysis-(SIRA-)Prozess

Nicht-finanzielle Risiken ändern sich fortlaufend, was eine systematische Überwachung erfordert. Für ein angemessenes Aufsetzen an Präventionsmaßnahmen ist die initiale Konzeption einer qualitativ hochwertigen Taxonomie zur Bewertung nicht-finanzieller Risiken von entscheidender Bedeutung. Aufgrund von Krisen und Skandalen in der Vergangenheit haben niederländische Banken ein Konzept entwickelt, das sich später auch im europäischen Raum und damit auch in Deutschland verbreitet hat. Das hierfür verwendete Instrument ist eine systematische Integritätsrisikoanalyse (Systematic Integrity Risk Analysis, SIRA) mit vier übergeordneten Prozessschritten, die insbesondere auch der Compliance dienlich sind:

Risikoidentifizierung

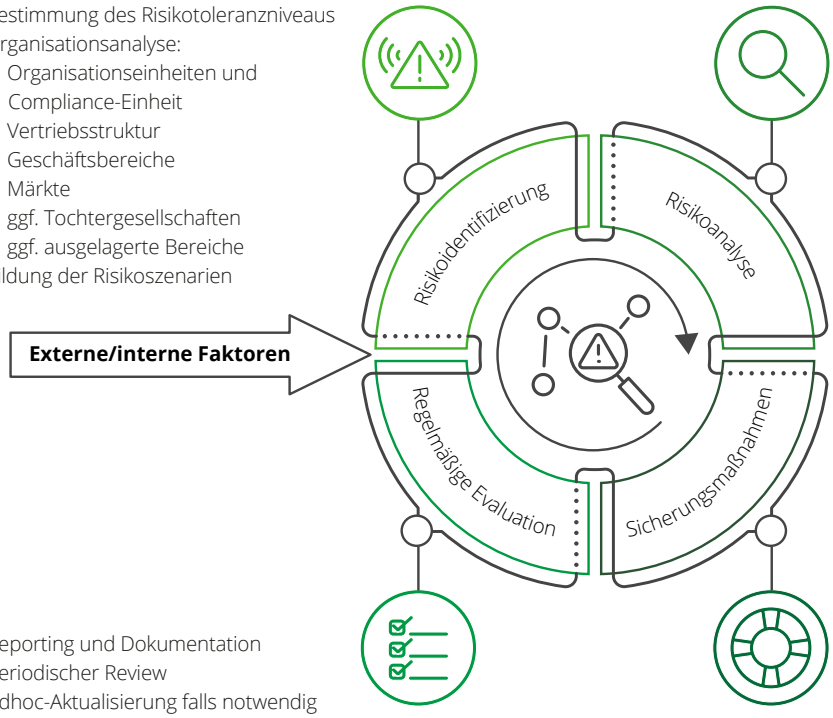
Risikoanalyse

Sicherungsmaßnahmen (Kontrollhandlungen zur Minimierung des Risikos)

Regelmäßige Evaluation

Abb. 1 – Schematischer Aufbau einer strukturierten Risikoanalyse zur Identifikation und Analyse neuer sowie bestehender Risikofelder

- Bestimmung des Anwendungsbereichs
- Bestimmung des Risikotoleranzniveaus
- Organisationsanalyse:
  - Organisationseinheiten und Compliance-Einheit
  - Vertriebsstruktur
  - Geschäftsbereiche
  - Märkte
  - ggf. Tochtergesellschaften
  - ggf. ausgelagerte Bereiche
- Bildung der Risikoszenarien



- Bestimmung der Bruttorisiken:
  - Kundenrisiko
  - Produktrisiko
  - Transaktionsrisiko
  - Geografisches Risiko
  - Vertriebskanalrisiko
  - ggf. Risiken der Tochtergesellschaften
  - ggf. Auslagerungsrisiko

- Reporting und Dokumentation
- Periodischer Review
- Adhoc-Aktualisierung falls notwendig

- Identifikation bestehender Maßnahmen
- Wirksamkeitsprüfung bestehender Maßnahmen
- Bestimmung des Nettorisikos
- Ableitung weiterer Handlungsmaßnahmen

[4] Vgl. Deloitte (2024), S. 1.
[5] Vgl. Deloitte (2020), S. 5 f.
[6] Vgl. BaFin: Maßnahmen der BaFin gegen Institute und Geschäftsleiter.

1. Risikoidentifizierung

Im ersten SIRA-Schritt wird der Anwendungsbereich der Risikoanalyse durch den Fachbereich Compliance definiert und kategorisiert; der Anwendungsbereich einer Geldwäsche- und Betrugs-Risikoanalyse beschränkt sich damit grundsätzlich auf die entsprechenden Risikobereiche Geldwäsche, Sanktionen/Embargos und Betrug. Neben der Spezifikation des Risikobereichs werden ebenfalls die für den Anwendungsbereich der Risikoanalyse entsprechenden internationalen, supranationalen (EU-rechtlichen) und nationalen (innerstaatlichen) regulatorischen Bestimmungen, aufsichtsbehördlichen Vorgaben, internationalen und nationalen Rechtsprechungen, Branchenstandards und weitere interne Kriterien bestimmt, um die für das Institut einschlägigen aufsichtsrechtlichen Vorgaben zu berücksichtigen und das Niveau der institutsinternen Risikotoleranz festzulegen. Unerlaubte Geschäfte und unerwünschte Produkte, Dienstleistungen, Transaktionen und Kundengruppen sind hierbei ebenso zu benennen und von der Geschäftstätigkeit des Instituts abzugrenzen.

Sind die vorgenannten internen und externen Faktoren bestimmt, hat das Unternehmen sich einen Überblick über gefährdete Bereiche (Szenarien der Finanz- und Wirtschaftskriminalität) zu verschaffen und das Ausmaß der damit verbundenen Risiken zu bestimmen. Es werden die möglichen Einzelrisiken unabhängig von ihrer Eintrittswahrscheinlichkeit identifiziert und dargestellt (bspw. Auslagerungsrisiko).[7] Dies geht ebenfalls mit den in Anlage 1 und 2 des GwG sowie den EBA-Leitlinien definierten Risikoklassifizierungen einher. In Verbindung mit dem deutschen Gesetz gibt die EU-Geldwäscherichtlinie vor, dass die identifizierten Risikofaktoren Art und Größe des jeweiligen Instituts entsprechen müssen.[8] Es empfiehlt sich hierbei grundsätzlich, nicht nur interne Faktoren (bspw. Produktänderungen) zu integrieren, sondern auch externe Faktoren aufzugreifen (bspw. Marktentwicklung, innovative Betrugsmuster etc.), um möglichst alle potenziell negativen Expositionen zu bewerten und in die Risikobetrachtung des Unternehmens[9] aufzunehmen. Um eine holistische und für einen sachverständigen Dritten nachvollziehbare Darstellung zu garantieren, sind hierbei neben den qualitativen Angaben ebenfalls quantitative Informationen in Form von Statistiken und Diagrammen einzubringen. Dies kann beispielsweise eine Abbildung der Kundenstruktur nach Länderzugehörigkeit und Risikoklassen sowie eine Darstellung der neuen sowie gekündigten Kundenbeziehungen beinhalten.

Im Rahmen einer Organisationsanalyse werden die Unternehmensbereiche inklusive (externen) Geschäftsbereichen, Partnerunternehmen, Märkten und Produkten sowie deren Vertriebskanäle identifiziert, in denen sich das zu untersuchende Risiko manifestieren könnte. Involvierte Unternehmensbereiche werden anschließend eingeladen, im Rahmen von Workshops Risikoszenarien zu entwickeln.[10] Die Einbindung der First Line of Defense ist von besonderer Bedeutung, da sie den operativen Input liefert, inwiefern sich ein Risiko im Tagesgeschäft zeigen könnte. Der Bereich Compliance wirkt hier unterstützend als Verbindung über die Geschäftsbereiche hinweg. Es empfiehlt sich ein zusätzlicher Einsatz externer Berater:innen, um industrieübergreifende Erfahrungswerte sowie innovative Modi Operandi von Straftäter:innen zu identifizieren und einfließen zu lassen. Handelt es sich bei dem Unternehmen um eine Gruppe, so sind ebenfalls die Risiken der Tochtergesellschaft zu ermitteln. Dies kann im Rahmen der jeweiligen Risikokategorie oder in einer separaten Darstellung erfolgen.

[7] Vgl. DeNederlandscheBank (2015), S. 11.
[8] Vgl. Richtlinie (EU) 2015/849 vom 20.05.2015, ABl. S. L 141/73, S. 90.
[9] BaFin (2021), S. 11–14.
[10] Vgl. DeNederlandscheBank (2015), S. 12.

2. Risikoanalyse

Die entwickelten Szenarien werden einem Bruttorisiko zugeordnet. Die niederländische Herangehensweise setzt für die Bewertung der Bruttorisiken eine Matrix ein, die aus Eintrittswahrscheinlichkeit und Schadenshöhe im Falle des Eintritts eines Schadens entsteht.[11] Die Wahrscheinlichkeit ist hierbei beispielsweise, inwieweit ein Kunde das Finanzprodukt für bestimmte Geldwäscheszenarien nutzen kann oder dieses zur Umgehung internationaler Sanktionen verwendet wird. Auch in Deutschland wird diese Methodik im Bereich der strafbaren Handlungen nach § 25h Abs. 1 KWG unter Zuhilfenahme der Schadensdatenfallbank angewendet.

Für den Bereich Geldwäsche lassen sich allerdings keine mathematische Taxonomie und Kalkulation bezüglich der Eintrittswahrscheinlichkeit und der Schadenshöhe errechnen, d.h., Eintrittswahrscheinlichkeit und Schadenshöhe sind ebenso wie die Beherrschbarkeit, mithin die Maßnahmen zur Reduzierung des Bruttorisikos, in diesem Deliktsbereich nicht oder nur in pauschalierter Form quantifizierbar. Die Eintrittswahrscheinlichkeit lässt sich jedoch näherungsweise skalieren, indem auf Basis von historischem Expertenwissen die Wahrscheinlichkeit ermittelt wird, mit der ein Produkt typischerweise zu Geldwäschezwecken genutzt wird; diese Methode ist auch der Bewertungslogik der nationalen Risikoanalyse immanent.

Keine geeignete Grundlage zur Ermittlung der Schadenshöhe als Bruttogröße bildet dabei die Bestimmung gemäß § 56 Abs. 3 GwG: Geldwäsche ist ein globales Phänomen, das nicht nur das Einzelinstitut betrifft, sondern den gesamten Finanzmarkt. Es ist in der Praxis äußerst schwierig, auf Institutsebene Geldwäsche nachzuweisen, da dies das Mitwirken und die grenzüberschreitende Informationsweitergabe anderer Institute und auch der Strafverfolgungsbehörden voraussetzt. Die vorgenannte Bestimmung sieht vor, dass gegen ein Institut, das seine geldwäscherechtlichen Pflichten nicht ordnungsgemäß durchführt, hohe Geldbußen (bis zu 5 Millionen Euro oder 10 Prozent des Gesamtumsatzes) festgesetzt werden können. Die Einbeziehung dieser potenziellen Schadenshöhe für jedes Szenario als Bruttorisiko würde dazu führen, dass das Nettorisiko trotz mitigierender Maßnahmen weiterhin hoch ist, da selbst das Eintreten einer Geldbuße ggf. zur Disruption des Unternehmens führen kann. Dem Institut wäre beispielsweise eine mangelhafte Informationsweitergabe eines anderen Institutes anzulasten, ohne für dessen Robustheit der Präventionsmaßnahmen verantwortlich zu sein. Eine mögliche oder festgesetzte Geldbuße eignet sich damit nicht zur Bestimmung der Schadenshöhe.

Bei der Bewertung der Bruttorisiken sind die Risikoeinschätzungen und Hinweise der nationalen Risikoanalyse des Bundesministeriums der Finanzen (BMF), der Typologiepapiere der FIU, der FATF und die Best Practices sowie Verlautbarungen und Hinweise anderer nationaler, EU-rechtlicher und internationaler Stellen zu beachten. Vor dem Hintergrund der quantitativen Angaben sind die entsprechenden Risikovariablen in angemessener Relation zum Markt und zum eigenen Portfolio zu gewichten. Beispielsweise hat ein Kredit mit einem großen Volumen in einem Spezialkreditinstitut ein höheres Risiko missbraucht zu werden als ein kleinerer Kredit, der im Gesamtportfolio nur einen geringen Prozentsatz ausmacht. Ebenfalls sollten hier wesentliche Feststellungen der Internen Revision und des Jahresabschlussprüfers einbezogen werden. Besonders wiederkehrende Mängel, die eine Art Muster darstellen, bieten einen Ansatzpunkt zur Steuerung der Risiken.[12] Diese Mängel deuten auf bestehende Prozessschwächen hin, die bei der Einschätzung des Bruttorisikos berücksichtigt werden müssen und gleichzeitig einen Hinweis darauf enthalten, dass die vorhandenen Sicherungsmaßnahmen unzureichend sind. Aus der Sicht des Risikomanagements ist zu entscheiden, ob das verbleibende Nettorisiko dem Risikoappetit entspricht. Sollte dies nicht der Fall sein, ist ferner zu prüfen, ob bestehende Maßnahmen für das spezifische Risiko zu erweitern (etwa durch erweiterte Kontrollhandlungen, häufigere Prüfungsintervalle, abgesenkte Schwellenwerte beim Monitoring/Screening von Transaktionen) oder weitere Maßnahmen zu implementieren sind. Zeigt sich, dass das Nettorisiko weiterhin größer als die Risikotoleranz ist, so ist über eine Beendigung der Kundenbeziehung oder Herausnahme des Produkts aus dem Produktportfolio zu entscheiden. Die finale Bewertung jedes Risikos beruht am Ende auf der Experteneinschätzung des Fachbereichs und ist für einen sachverständigen Dritten nachvollziehbar zu dokumentieren. Im Falle der Erstellung einer gruppenweiten Risikoanalyse nach § 5 Abs. 3 GwG sind die ermittelten Risiken der Tochtergesellschaft in die Gesamtbruttorisiken der Muttergesellschaft einzubeziehen.

[11] Vgl. Bank for International Settlements (2009), S. 156 f.
[12] Vgl. Kaiser (2023), S. 2.

3. Sicherungsmaßnahmen

Um die eigene Integrität zu schützen, ergreifen die Compliance-Abteilungen von Finanzdienstleistungsunternehmen Maßnahmen nach § 6 GwG, wozu z.B. die Einführung von Richtlinien und Verfahren sowie die Implementierung von Kontroll- und Überwachungssystemen gehören. Es wird vorab überprüft, ob die Ausgestaltung der individuellen Maßnahme geeignet ist, das Risiko zu minimieren, und ob mögliche Schwachstellen bestehen. Die Compliance-Abteilung erstellt daraufhin einen Kontrollplan nach den Maßgaben des § 6 GwG. Innerhalb eines strukturierten Vorgehens sollen die Angemessenheit und Wirksamkeit der einzelnen Sicherungsmaßnahmen geprüft werden. Dies beinhaltet ebenfalls die Ziehung von Stichproben zur Bestimmung der operationellen Effektivität (bspw. Überprüfung von 10% der Fälle aus dem Kunden-Onboarding). Da die Auslegungs- und Anwendungshinweise der BaFin explizit von einem „strukturierten" Vorgehen sprechen, sind Turnus, Population, Datenquellen und auch die Kriterien der Stichprobenauswahl zu beschreiben. In einer abschließenden Bewertung wird der Einfluss der Sicherungsmaßnahmen auf das Bruttorisiko bewertet.

Das Nettorisiko wird durch Subtraktion des Kontrollniveaus vom Bruttorisiko ermittelt. Das Nettorisiko ist somit das um die Kontrollmaßnahmen reduzierte Bruttorisiko. Je wirksamer die Kontrollmaßnahmen sind, desto geringer ist das Nettorisiko. Beispielsweise kann es mit einem geringeren Wert eingeordnet werden, wenn das erhöhte Bruttorisiko im digitalen Kunden-Onboarding mit Video-Ident-Verfahren aufgrund eines größeren Stichprobenumfangs durch die Compliance abgedeckt werden kann. Kann die Sicherungsmaßnahme das Bruttorisiko minimieren und bewegt sich das Nettorisiko im Rahmen der Risikotoleranz des Instituts, sind keine weiteren Maßnahmen zu implementieren. Ist dies allerdings nicht der Fall, sind weitere Kontrollen festzulegen bzw. bestehende Kontrollen zu intensivieren, Kundenbeziehungen zu beenden oder Produkte aus dem Portfolio zu entfernen. Die abschließende Dokumentation der Risikoanalyse bietet dann die Arbeitsgrundlage des folgenden SIRA-Zyklus.

4. Regelmäßige Evaluation

In Deutschland verlangt der Gesetzgeber nach § 5 Abs. 1 GwG, dass die Risikobewertung in regelmäßigen Abständen durchgeführt wird. Es ist zu betonen, dass die Risikoanalyse im Unternehmen keine statische Rolle einnehmen sollte. Sie ist vielmehr als „lebendiges" Dokument zu nutzen, während des Geschäftsjahres durch eine fortlaufende Risikobewertung anzupassen und zur Evaluierung einzelner Sachverhalte zu verwenden. Eine Aktualisierung der Risikoanalyse auf jährlicher Basis ist insbesondere in den Fällen gemäß § 5 Abs. 2 GwG nicht ausreichend, sobald bspw. neue Produkte angeboten werden oder der Kundenstamm in kurzer Zeit besonders stark angestiegen ist. Wenn sich die Risikofaktoren aus anderen Gründen in kurzer Zeit erheblich verändert haben und dies Auswirkungen auf das finale Nettorisiko hat, ist eine Ad-hoc-Aktualisierung durchzuführen. Dies stellt den letzten Schritt der allumfassenden institutsspezifischen SIRA dar.

Bedeutung für die Aufsichtsbehörden

Sind Geschäfte aufgrund mangelnder Sicherungsmaßnahmen oder einer fehlerhaften Beurteilung des Risikos aufgefallen und stellen für das Institut, den Finanzmarkt sowie die Verbraucher:innen selbst ein Risiko dar, wird dies spätestens im Rahmen der Jahresabschlussprüfung festgestellt und mit dem Jahresabschluss an die Aufsichtsbehörde gemeldet. Im schlimmsten Fall kann dies dazu führen, dass die BaFin eine Anordnung nach § 51 GwG trifft, wozu ein Verbot der Tätigung expliziter Geschäfte gehören kann, vgl. § 51 Abs. 2 S. 2 GwG. Ziele einer solchen Anordnung sind die Ermöglichung der Behebung schwerwiegender Mängel in den Prozessen sowie die Sicherstellung angemessener Geschäfte in der Zukunft. Darüber hinaus können aufgrund unzureichenden Managements nicht-finanzieller Risiken Geldbußen nach § 56 GwG verhängt werden, die das Institut über die klassische Geldbuße hinaus im operationellen Tagesgeschäft treffen können (beispielsweise eine Wachstumsbeschränkung durch eine limitierte Anzahl an Neukunden).

Nicht-finanzielle Risiken werden zunehmend Teil der aufsichtsrechtlichen Praxis in Deutschland. Beispielsweise waren IT- und Cyberrisiken sowie der Verbraucherschutz in der Anlageberatung bereits im Jahr 2021 expliziter Aufsichtsschwerpunkt der BaFin.[13] Zudem wurden weitere besondere Risiken nicht-finanzieller Art Gegenstand von Prüfungen.[14] Auch im Jahr 2023 waren die NFR ein Fokusthema der BaFin. Äußere Umstände wie COVID-19 und die anhaltenden geopolitischen Krisen in der Welt stellen Risiken dar, die insbesondere in der IT die Anzahl an Cyberattacken erhöht haben.[15] Den Bereich Geldwäscheprävention hat die BaFin besonders hervorgehoben, da sich aufgrund neuer Geschäftsfelder in Bezug auf Kryptowerte hohe Geldwäscherisiken ergeben. Weiterhin hat sie bei ausgelagerten Sicherungsmaßnahmen diverse Risiken in der Qualität festgestellt. Die Überwachung des entsprechenden Unternehmens war oftmals nicht ausreichend.[16] Die gesteigerte Aktivität der BaFin bei der Untersuchung der Compliance-Abteilungen zeigt sich nicht zuletzt in der Anzahl der veröffentlichten Anordnungen und der Bestellung von Sonderbeauftragten.[17]

Herausforderungen in der Praxis

Obwohl das Gesetz und die Auslegungs- und Anwendungshinweise der BaFin einige Angaben zu den Risikofaktoren und zum Prozessablauf von SIRA geben, ist die tatsächliche institutsspezifische Ausgestaltung der jeweiligen Risikoanalyse in der Realität doch komplexer und zeitintensiver. Insbesondere in der Praxis nehmen wir folgende Schwierigkeiten bei der Umsetzung der theoretischen Anforderungen wahr.

Institutsgröße und Geschäftsmodell

Bei der Durchführung von SIRA gibt es keinen Ansatz, der für alle Institutsgrößen und Geschäftsmodelle passend ist. Insbesondere Institute mit einem komplexen Geschäftsmodell oder einem großen und diversen Kundenstamm sind erhöhten Risiken ausgesetzt[18], da sie für den gleichen Risikofaktor aufgrund internationaler Verflechtungen ein größeres Interesse für kriminelle Aktivitäten erregen. Die potenziellen Gefahren der globalen Ausrichtung sind nicht nur für Großbanken vorhanden, sondern auch bei deren Zweigniederlassungen, die beispielsweise Transaktionen der Muttergesellschaft durchleiten. Die BaFin hat diese Risiken im Rahmen der von ihr durchgeführten Prüfung von Auslandsbanken mit kleinen Zweigniederlassungen in Deutschland einer gesonderten Prüfung unterzogen.[19]

Die Schwierigkeit bei der Erstellung der gruppenweiten Risikoanalyse nach § 9 Abs.1 GwG sorgt dabei insbesondere vor dem Hinblick der Harmonisierung der Risikoszenarien und der teilweise unterschiedlichen Definition und Behandlung je nach Jurisdiktion der Tochtergesellschaft bei der Muttergesellschaft für einen großen Aufwand. Bei der Fachtagung der BaFin vom Dezember 2023 zur Prävention von Geldwäsche und Terrorismusfinanzierung hat die Behörde darauf hingewiesen, dass ein übergeordnetes Risikomanagement nicht nur für die Compliance-Abteilung, sondern auch die Geschäftsführung notwendig ist, um die Unternehmenssteuerung zu gewährleisten.

Nicht alle Risikofaktoren sind im gleichen Ausmaß für jedes Geschäftsmodell anwendbar. Sollte sich nach detaillierter Analyse herausstellen, dass beispielsweise die Transaktionsrisiken sehr gering sind – etwa, weil das Institut keine Kundengelder selbst transferiert –, ist dies entsprechend in der Risikoanalyse für einen sachverständigen Dritten nachvollziehbar darzustellen. Sind bei sehr geringen Bruttorisiken Überwachungshandlungen implementiert, so kann dies nicht zum vollständigen Reduzieren auf null führen.[20] Es wird stets aufgrund der Natur des Produkts oder der Änderung von Kundenverhalten ein geringes Risiko für kriminelle Handlungen übrigbleiben.

[13] Vgl. BaFin (2021), S.14–17.
[14] Vgl. BaFin Journal (2021), S. 20 f.
[15] Vgl BaFin (2023), S. 20.
[16] Vgl BaFin (2023), S. 24.
[17] Vgl. BaFin: Maßnahmen der BaFin gegen Institute und Geschäftsleiter.
[18] Vgl BaFin (2023), S. 24.
[19] Vgl. BaFin: Maßnahmen der BaFin gegen Institute und Geschäftsleiter.
[20] Vgl. DeNederlandscheBank (2015), S. 32.

Technische Lösung

Die Digitalisierung manueller Prozesse ist ein wachsender Trend in der Finanzbranche. Damit wird versucht, menschliche Fehler zu reduzieren und die Effizienz zu verbessern. Auch im Bereich der Risikoanalyse werden mittlerweile von größeren Instituten Softwarelösungen verwendet, die eine kontinuierliche Risikokategorisierung auf Tagesbasis sicherstellen sollen. Dies entspricht dem Leitfaden der Aufsichtsbehörde, die Risikoanalyse als „lebendes" Dokument in der SIRA zu verwenden. Insbesondere bei Muttergesellschaften ist dies vorteilhaft, da sie dadurch die Risiken der Zweigniederlassungen einheitlich überwachen und steuern können. Oftmals sind die Risikoanalysen in der Gruppe über die Jahre unterschiedlich gewachsen und damit auch die Risikotoleranz sowie die Identifikation und Bewertung der jeweiligen Risikofaktoren nach SIRA. Auch wenn die Muttergesellschaft eine Risikomethodik vorgibt und die lokale Risikoanalyse später gemäß § 5 Nr. 3 GwG zusammengefasst wird, ist damit ein weitaus höherer Aufwand verbunden, als wenn gruppenweite Risikoanalyse und Einzelrisikoanalysen von vornherein aufeinander abgestimmt durch eine toolbasierte Softwarelösung erstellt und gesteuert werden.

Eine Software bietet die Möglichkeit, eine einheitliche Methodik inkl. Risiko-Taxonomie auf die gesamte Gruppe zu übertragen und fortlaufend zu nutzen. Zielbild der Harmonisierung der Risikoanalyse unter Verwendung einer Software ist auch die Erstellung von tagesaktuellen Dashboards, die für die Analyse des Risikoprofils für die Geschäftsführung genutzt werden können. In Zukunft soll es dann möglich sein, eine 360-Grad-Sicht auf alle nicht-finanziellen Risiken zu erhalten und diese mit Finanzrisiken zu bündeln. Es besteht damit ebenfalls die Möglichkeit der Rückschau auf die historische Entwicklung des Risikos und einer Ableitung von Trends. Dies ist insbesondere hilfreich bei Absprachen bezüglich Marketingmaßnahmen und Geschäftsentwicklungen, wenn eine drohende Risikoentwicklung die Erweiterung des Kundenstamms für bestimmte Jurisdiktionen limitiert. Bevor der Schritt zur digitalen Risikoanalyse gewagt werden kann, sind Finanzinstitute allerdings angehalten, ihre Prozesse und Daten zu strukturieren und eine angemessene Qualität sicherzustellen, um das Potenzial einer Digitalisierung auszuschöpfen.

Ableitung der Sicherungsmaßnahmen

Institute haben oftmals Schwierigkeiten, jedem einzelnen Risikofaktor entsprechend dem SIRA-Prozess die richtige Sicherungsmaßnahme zuzuordnen. Grund hierfür ist, dass Kategorisierung und Gewichtung der Bruttorisiken einen großen zeitlichen Aufwand darstellen. Auch die Bewertung der angemessenen Konzeption der Sicherungsmaßnahmen und deren Wirksamkeit sind nicht trivial und werden stets von der Internen Revision und dem Jahresabschlussprüfer hinterfragt. Es ist nicht ungewöhnlich, dass Institute ihre SIRA-Präventionsmaßnahmen als wirksam einstufen, obwohl sie tatsächlich unwirksam sind. Die Ursache dafür liegt häufig in der mangelhaften Ausführung der Kontrollhandlungen, aber auch im mangelnden Verständnis für die Verwendung der Ergebnisse von Kontrollhandlungen in SIRA. Die BaFin hat nicht zuletzt durch ihre letztjährigen Prüfungsschwerpunkte gezeigt, dass eine korrekte Ableitung von Sicherungsmaßnahmen[21] notwendig ist, damit das Institut seine Risiken aktiv steuern kann.

[21] Vgl. BaFin: „Wäsche-Business" macht Geld sauber.

Auslagerungsrisiken

Auslagerungen sind bereits seit mehreren Jahren im Markt etabliert und einige Anbieter oder die eigenen Tochtergesellschaften haben sich als vertrauenswürdig bewährt, sodass diese als „Marktstandard" wahrgenommen werden. Die BaFin hat die häufige Nutzung von Auslagerungen, insbesondere im KYC-Bereich, ebenfalls erkannt und auch die teilweise mangelhafte Qualität identifiziert, mit der Institute im Prozessalltag zu kämpfen haben. Weiterhin wurde festgestellt, dass die Überwachung der ausgelagerten Präventionsmaßnahmen nicht immer angemessen war und die Wirksamkeit ggf. gemindert wurde.[22] Daher nutzt die BaFin ihre erweiterten Prüfungsmöglichkeiten auf Basis des Finanzmarktintegritätsstärkungsgesetzes (FISG)[23] und führt direkte Untersuchungen und Sonderprüfungen von Auslagerungsunternehmen durch. Ziel dieser Ausrichtung ist es, eine Vergleichbarkeit der Dienstleister zu ermöglichen und höhere Qualitätsstandards zu etablieren, von denen der gesamte Finanzmarkt profitieren kann.

Da insbesondere kleine Institute dazu tendieren, Sicherungsmaßnahmen aufgrund von Effizienzgründen und Kostenersparnis auszulagern, ergeben sich weitere Risiken, die innerhalb des SIRA-Prozesses zu betrachten sind. Die Bewertung von Auslagerungsrisiken ist keine direkt niedergeschriebene gesetzliche Anforderung nach Anlagen 1 und 2 des GwG, allerdings ist ein Institut angehalten, alle wichtigen Risikofaktoren zu berücksichtigen, die eine potenziell negative Exposition darstellen können.[24]

Ein proaktives und integriertes Risikomanagement ist wichtig, um Risiken rechtzeitig zu erkennen und die Integrität des Instituts zu schützen.

Fazit

Für Finanzinstitute empfiehlt es sich, den Prozess der systematischen Integritätsrisikoanalyse (SIRA) proaktiv als Teil des bestehenden Risikomanagementsystems zu etablieren und zur Sicherstellung der Effektivität kontinuierlich zu überwachen. Mit einem geeigneten Ansatz können Finanzinstitute nicht-finanzielle Risiken effektiv organisieren und dadurch den aufsichtsrechtlichen Druck mindern[25], Strafzahlungen vermeiden, nachhaltige Kundenbeziehungen aufbauen und ihre Wettbewerbs- und Marktposition stärken.

Bei der Umsetzung von SIRA in die Praxis ergeben sich einige Herausforderungen, die auf die Interpretation des Gesetzes und die Auslegungshinweise der Aufsichtsbehörde sowie das Rollenverständnis der Risikoanalyse zur aktiven und kontinuierlichen Risikosteuerung im Institut zurückzuführen sind. SIRA wird auch in den kommenden Jahren ein Kernthema der Bankenaufsicht bleiben, da geopolitische Umstände die potenziell negative Exposition schnell ändern können und Institute ihr Umfeld stets im Auge behalten sollten. Auch neue Themen wie Informations- und Kommunikationsrisiken[26] sowie der Umgang mit schwer identifizierbaren Risiken wie der Unternehmenskultur[27] zeigen, dass die Sensibilität für das Erkennen von potenziellen Herausforderungen unumstößlich ist. Eine strukturierte Prozessdurchführung in SIRA durch die Compliance-Abteilung ist daher unabdingbar, um sich vor Strafzahlungen und einer Limitation im Geschäftsmodell zu schützen.

[22] Vgl BaFin (2023), S. 24.
[23] Vgl. Bundesministerium der Finanzen und Bundesministerium der Justiz und für Verbraucherschutz (2021).
[24] Vgl. Richtlinie (EU) 2015/849 vom 20.05.2015, ABl. S. L 141/73, S. 90.
[25] Vgl. Deloitte (2024), S. 1.
[26] Vgl. Kaiser (2023), S. 1.
[27] Vgl. Deloitte (2024), S. 3.

Literaturverzeichnis

Bücher

- Franke, Günter: Management nicht-finanzieller Risiken: eine Forschungsagenda. Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung 72, 2020, 279–320.
- Kaiser, Thomas: Praxis des Non-Financial Risk Managements im Finanzsektor. Springer Gabler, 2023.
- Liermann, Volker; Viets, Nikolas; Radermacher, David: Breaking New Grounds in Non-Financial Risk Management. The Digital Journey of Banking and Insurance, Volume 1: Disruption and DNA, 2021, 161–182.

Rechtsquellen

- Gesetz zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz – FISG) des Bundesministeriums der Finanzen und des Bundesministeriums der Justiz und für Verbraucherschutz vom 10.06.2021.
- Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission vom 20.05.2015 (ABl. S. L 141/73).

Veröffentlichungen

- ACFE (2022): Occupational Fraud 2022: A Report to the Nations, https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf (abgerufen am 30.05.2024).
- Bank for International Settlements (2009): Issues in the Governance of Central Banks, https://www.bis.org/publ/othp04.htm (abgerufen am 30.05.2024).
- BaFin (2021): Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, https://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_ae_auas_gw.html?nn=19649860 (abgerufen am 30.05.2024).
- BaFin (2021): BaFin Journal – November 2021, https://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2021/bj_2111.html (abgerufen am 30.05.2024).
- BaFin (2023): Risiken im Fokus der BaFin, https://www.bafin.de/SharedDocs/Downloads/DE/Fokusrisiken/2023_Fokusrisiken.html (abgerufen am 30.05.2024).
- Deloitte (2020): Financial Crime Survey DACH-Region, https://www2.deloitte.com/de/de/pages/finance/articles/financial-crime-survey-dach-region.html (abgerufen am 30.05.2024).
- Deloitte (2024): Die Bedeutung von Kultur im Kampf gegen Finanzkriminalität, https://www2.deloitte.com/de/de/pages/finance/articles/unternehmenskultur-kampf-gegen-finanzkriminalitaet.html (abgerufen am 30.05.2024).
- DeNederlandscheBank (2015): Integrity risk analysis: More where necessary, less where possible, https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-themes/supervision-of-financial-crime-prevention-integrity-supervision/good-practices-integrity-risk-analysis-more-where-necessary-less-where-possible/ (abgerufen am 30.05.2024).

Internetquellen

- BaFin: Maßnahmen der BaFin gegen Institute und Geschäftsleiter, https://www.bafin.de/DE/Aufsicht/BankenFinanzdienstleister/Massnahmen/Mitteilungen/mitteilungen_node.html (abgerufen am 30.05.2024).
- BaFin: „Wäsche-Business“ macht Geld sauber, BaFin – Fachartikel – „Wäsche-Business“ macht Geld sauber (abgerufen am 30.05.2024).

Ansprechpartner

Matthias Rode
Partner | Anti-Financial Crime FSI
Tel: +49 151 58002270
mattrode@deloitte.de

Martin Hirtreiter
Partner | Anti-Financial Crime FSI
Tel: +49 69 75695 7059
mhirtreiter@deloitte.de

Christian Heinrich Paap
Senior Manager | Anti-Financial Crime FSI,
Rechtsanwalt (Syndikusrechtsanwalt)
Tel: +49 151 40678320
cpaap@deloitte.de

Matthias Heining
Senior Manager | Anti-Financial Crime FSI
Tel: +49 151 58073668
mheining@deloitte.de

Deloitte.

Stand 08/2024