«Risk Governance» der Banken im Wandel: Neue Herausforderungen und neue Modelle

Christoph B. Bühler*

In a world characterized by increasing complexity, networking and volatility with disruptive innovations, new business models and rapidly developing technologies, effective risk governance represents a major challenge for banks. The decisive factor here is not only a functionally appropriate organizational structure for risk management staffed by qualified teams, but also a resilient process organization. If risks are also an opportunity, the levels of action of governance, risk management and compliance in the company must then be holistically integrated into the support and decision-making processes and designed as strategic management instruments. The governance structure and the underlying management systems as well as the need for consistent compliance with regulatory requirements and internal company rules must have the backing of the top management bodies and be exemplified by them. Last but not least, a healthy risk culture and the integrity of the management bodies are the cornerstones of sustainably successful entrepreneurial activity.

Inhaltsübersicht

I. Einleitung

Das Risikomanagement der Banken ist aktuell vor anspruchsvolle neue Herausforderungen gestellt: Die COVID-Pandemie hat unsere Arbeits- und Interaktionsweise verändert; die zunehmende Digitalisierung und KI beschleunigen die Transformation, und geopolitische Veränderungen sowie Umwelt-, Sozial- und Governance-Faktoren schaffen neue Risiken, die jedoch nur ungenau antizipiert werden können. Die Risikoverantwortlichen sind gefordert, innovative Ansätze zu entwickeln, um auf die neuen Risiken angemessen eingehen zu können.

Die grössten Gefahren für die Bankenindustrie werden in Cyberrisiken und in den Bereichen «Environment, Social, Governance» (ESG) sowie in der zunehmenden Regulierung und den damit einhergehenden neuen Rechtsrisiken gesehen. Hinzu kommen Betrug, Geldwäsche und die ständig wachsende Abhängigkeit von einem komplexen Netz von «Outsourcing»-Partnern und Drittparteien. Nicht nur eine angemessene Kapital- und Liquiditätsausstattung, sondern auch die operative Widerstandsfähigkeit und Resilienz gewinnen dabei zunehmend an Bedeutung. Es verändern sich dabei nicht nur die Rechtsrisiken, auch die «Risk Governance» der Bank selbst befindet sich in einem nachhaltigen Wandel.

Der vorliegende Beitrag befasst sich mit den Herausforderungen, welche die geschilderte Entwicklung an die «Risk Governance», also an die Organisation und Ausgestaltung des Risikomanagements der Banken, stellt. Beleuchtet wird dabei auch die Frage, inwieweit sich daraus auch ein Pflichtenentwicklungsrisiko für die Bankorgane ergibt. Aus den Erkenntnissen dieser rechtlichen Analyse werden schliesslich mögli-

* Prof. Dr. iur., LL.M., Rechtsanwalt und Partner in Basel; Titularprofessor für Handels- und Wirtschaftsrecht an der Universität Zürich.

che Handlungsfelder und neue Modelle für die Anpassung der «Risk Governance» der Banken abgeleitet.

II. Abgrenzung der «Risk Governance» vom Risikomanagement

Risiko bezieht sich auf die Ungewissheit über die Folgen einer Aktivität oder eines Ereignisses in Bezug auf etwas, das Menschen schätzen. Es geht um die Auswirkung der Ungewissheit auf Ziele bzw. um negative Abweichungen von Erwartungen. Unter einem Risiko ist ein Zufallsereignis zu verstehen, das in seiner Entstehung und Ausprägung schwer zu prognostizieren und zu beeinflussen ist. Risiken entstehen mit dem Wandel und werden oft von Chancen, Vorteilen und Kompromissen begleitet. Bessere Risikobeherrschung bedeutet, die Gesellschaft in die Lage zu versetzen, vom Wandel zu profitieren und gleichzeitig die negativen Folgen der damit verbundenen Risiken zu minimieren.

Unter Risikomanagement wird grundsätzlich der systematische Prozess des Umgangs mit externen und internen Unternehmensrisiken verstanden. Nach ihrem aktuellsten Risikomonitor[1] identifiziert die FINMA dabei für die Finanzbranche derzeit als bedeutendste Risiken: die Zinsrisiken, Kreditrisiken (Hypotheken und übrige Kredite), Marktrisiken (insbesondere das «Credit-Spread»-Risiko), Liquiditäts- und Refinanzierungsrisiken, Cyberrisiken, Geldwäscherei, der Marktzugang Europa und das «Outsourcing».

Das Risikomanagement umfasst nach dem Verständnis der FINMA die organisatorischen Strukturen sowie die Methoden und Prozesse, die der Festlegung von Risikostrategien und Risikosteuerungsmassnahmen sowie der Identifikation, Analyse, Bewertung, Bewirtschaftung, Überwachung und Berichterstattung von Risiken dienen.[2]

Die Herausforderung des Risikomanagements liegt einerseits im Auffinden von sog. «Black Swans», also Zufallsereignisse mit grossen negativen Auswirkungen, die mit herkömmlichen Risikomodellen nicht vorhersehbar sind, andererseits aber auch im Herbeiführen einer optimalen Balance zwischen notwendigem Risiko und erwünschtem Ertrag.[3]

Das Risikomanagement ist dem breiteren Themenfeld der «Corporate Governance» zuzuordnen.[4] Mit dem Begriff der «Risk Governance» werden die Anforderungen der «Corporate Governance» an das Risikomanagement von Finanzinstituten erfasst.[5] «Governance» bedeutet in diesem Zusammenhang, mögliche Risiken abzuschätzen, deren Eintritt vorzubeugen und Massnahmen zur Risikominderung zu treffen, und zwar einerseits durch organisatorische Vorkehrungen und eine angemessene Infrastruktur und andererseits durch das Aufstellen von Verhaltensregeln.

In organisatorischer Hinsicht sind die Verantwortlichkeiten zur Risikobewältigung festzulegen, unabhängige Experten für die Risikoanalyse einzusetzen und ein internes Kontrollsystem einzurichten. In der Verantwortung des obersten Leitungs- und Aufsichtsorgans, dem Verwaltungs- oder Bankrat, liegt vor allem die Definition der Risikopolitik und des entsprechenden Risikoappetits der Bank. Wie viele und welche Risiken ist die Organisation bereit einzugehen? Die Frage ist jedoch nicht, ob Risiken überhaupt eingegangen werden sollen, denn das Eingehen von Risiken gehört zum Kern des Bankgeschäfts.[6]

Das Weisungswesen, das typischerweise auf der Geschäftsleitungsebene angesiedelt ist, sollte weitgehend auf die Risikostrategie der Bank abgestimmt sein. Die «Risk Governance» umfasst Vorgaben zu den Risikomessverfahren und -modellen sowie zum Risikomanagementprozess (Identifikation, Messung, Steuerung, Kontrolle und Rapportierung der Risiken).[7]

Schliesslich ist vor allem auch die von allen Führungsorganen vorgelebte und von allen Mitarbeiten-

1 FINMA-Risikomonitor 2024, vom 18. November 2024, abrufbar unter <*https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/risikomonitor/20241118-finma-risikomonitor-2024.pdf?sc_lang=de&hash=67AEA2032B838E5737A5D0816E2AC5D5*>.

2 FINMA-Rundschreiben 2017/1 Corporate Governance – Banken, Corporate Governance, Risikomanagement und interne Kontrollen bei Banken vom 22. September 2016, Rz. 3.

3 *Axel P. Lehmann/Katja Roth Pellanda,* Agenda für ein (besseres) Risikomanagement durch den Verwaltungsrat, GesKR 2009, 317 ff., 318.

4 Vgl. dazu *Rolf H. Weber,* Risikomanagement in Finanzinstitutionen, SZW 2016, 558 ff., 558 f.; *Thomas Bauer,* Governance im Fokus der Bankenaufsicht, EF 2021, 608 ff., 612.

5 *Marc Ryser,* Risk Governance: Anforderungen an das Risikomanagement, in: Susan Emmenegger (Hrsg.), Corporate Governance, Basel 2011, 165 ff., 166.

6 *Ryser* (Fn. 5), 167.

7 *Weber* (Fn. 4), 559; *Ryser* (Fn 5), 165 ff.

den umgesetzte Risikokultur eine zentrale Grundvoraussetzung einer wirksamen «Risk Governance».

III. Anforderungen an die «Risk Governance» gemäss geltendem FINMA-Rundschreiben 2017/1 «Corporate Governance – Banken»

1. Hintergrund des FINMA-Rundschreibens

Im Anschluss an die internationale Finanzkrise in den Jahren 2007 und 2008 war klar geworden, dass die Steuerungsmechanismen der Finanzsektoren überprüft und entsprechend angepasst werden mussten. Das führte zu neuen Regulierungen insbesondere in den Bereichen Kapital, Liquidität und Vergütung. Aber auch die Anforderungen an die Governance der Banken waren zu wenig griffig, um eine nachhaltige Geschäftstätigkeit zu gewährleisten.[8]

Handlungsbedarf wurde insbesondere im Bereich des Risikomanagements festgestellt: «Financial institutions must do a better job at managing risks.» Diese Forderung erhob Senator *Barack Obama,* der spätere 44. Präsident der Vereinigten Staaten von Amerika, am 27. März 2008 während einer Rede zur wirtschaftlichen Lage der amerikanischen Nation in New York City. *Obama* identifizierte in seiner Ansprache ein unzureichendes Risikomanagement der Banken als grundlegende Ursache für die Entstehung der Subprimekrise und deren Ausbreitung zur internationalen Finanzkrise.[9] Auch der Basler Ausschuss teilte diese Auffassung und sah die Ursache der Finanzkrise im Wesentlichen in Unvollkommenheiten bei den Risikomanagementsystemen und in der Risikosteuerung der Finanzinstitute begründet.[10]

Es wurde kritisiert, dass die Banken viele Vorgaben zur Risikopolitik und -kultur machen, vielfach aber keine geeigneten Mittel haben, um zu überwachen, ob diese Vorgaben auch eingehalten werden. Eine umfassende Sicht auf die Risiken, wie und ob diese risikomindernden Massnahmen durchgeführt und kontrolliert werden, fehlte an vielen Orten.

In der Folge haben sowohl die G20 und die OECD ihre «Principles of Corporate Governance»[11] als auch der Basler Ausschuss für Bankenaufsicht die «Corporate Governance Principles for Banks»[12] entsprechend überarbeitet.

Die FINMA folgte dieser internationalen Entwicklung und publizierte am 1. November 2016 das Rundschreiben 2017/1 «Corporate Governance – Banken»[13], welches am 1. Juli 2017 in Kraft trat und bis heute gilt.

Die Anforderungen gemäss Rundschreiben sind im Einzelfall nach dem Proportionalitätsprinzip unter Berücksichtigung der Grösse, Komplexität, Struktur und des Risikoprofils der Bank umzusetzen. Die Anforderungen an die konkrete Umsetzung werden hinsichtlich wesentlicher Elemente des Rundschreibens anhand der aufsichtsrechtlichen Kategorien 1–5 abgestuft. Die Möglichkeit, sich nicht an die Vorgaben des Rundschreibens zu halten und dies entsprechend im Geschäftsbericht offen zu legen und zu erläutern, wurde gestrichen. Das früher massgebliche «Comply or explain»-Prinzip gilt seither nicht mehr. Abweichungen von den Regelungen des Rundschreibens müssen vielmehr vorgängig von der FINMA genehmigt werden.[14]

Das FINMA-Rundschreiben bewirkte neue Anforderungen an die «Risk Governance» von Banken. Kernpunkte des Rundschreibens waren die Vorgabe zur Implementierung eines umfassenden Rahmenkonzepts für das institutsweite Risikomanagement und die Anforderung, dass die Banken über mindestens zwei Kontrollinstanzen verfügen müssen: die ertragsorientierten Geschäftseinheiten und die unabhängigen Kontrollinstanzen.

8 *Susan Emmenegger/Regula Kurzbein,* Finanzmarktkrise und neue Corporate Governance von Banken, GesKR 2010, 462 ff., 463 f.; *Ryser* (Fn. 5), 168.

9 Zitiert bei *Philipp Gann/Bernd Rudolph,* in: Klaus J. Hopt et al. (Hrsg.), Handbuch Corporate Governance von Banken, München 2011, 601 ff., 602.

10 Bank für Internationalen Zahlungsausgleich, Basler Ausschuss für Bankenaufsicht, Basel III: Ein globaler Regulierungsrahmen für widerstandsfähige Banken und Bankensysteme, Basel, Dezember 2010 (rev. Juni 2011), abrufbar unter <*https://www.bis.org/publ/bcbs189_de.pdf*>.

11 G20/OECD, Principles of Corporate Governance, Paris 2015, abrufbar unter <*https://www.complianceonline.com/downloads/OECD-Corporate-Governance-Principles.pdf*>.

12 Bank for International Settlements, Basel Committee on Banking Supervision, Guidelines Corporate Governance Principles for Banks, Basel 2015, abrufbar unter <*https://www.bis.org/bcbs/publ/d328.pdf*>.

13 FINMA-RS 2017/1 (Fn. 2), Rz. 1 ff.

14 Vgl. *Thomas Romer/Yousuf Kahn,* Die FINMA definiert Corporate-Governance-Richtlinien für Banken, EF 2017, 88 ff.

2. Rahmenkonzept für das institutsweite Risikomanagement

Das von der FINMA geforderte Rahmenkonzept für das institutsweite Risikomanagement ist ein übergreifendes Dokument, welches die Risikopolitik, Risikotoleranz und Risikolimiten einer Bank abdeckt. Ausserdem müssen die Banken die verwendeten Instrumente und organisatorischen Strukturen beschreiben, mit welchen die definierten Risiken innerhalb jeder Risikokategorie identifiziert, bewertet, überwacht und gemeldet werden.

Der Verwaltungsrat muss das Rahmenkonzept für das institutsweise Risikomanagement jährlich evaluieren und genehmigen. Das oberste Leitungs- und Aufsichtsorgan der Bank wird damit institutionalisiert und stärker in die Verantwortung der effektiven «Risk Governance» genommen; es muss sich unabhängig von der internen Organisationsfreiheit intensiver mit dem Thema Risiko auseinandersetzen.[15]

Auch der Risikoausschuss spielt hier eine wesentliche Rolle, da dieser die jährliche Erörterung des Rahmenkonzepts dem gesamten Oberleitungsorgan unterbreitet und eine entsprechende Empfehlung zur Abnahme abgibt. Damit ist auch verbunden, dass die Wirksamkeit der Risikomanagementprozesse, der entsprechenden Kontrollen sowie die jeweilige Risikolage des Finanzinstituts jährlich beurteilt und abgenommen werden müssen.[16]

Für Banken der Aufsichtskategorien 1–3 wird mindestens je ein Prüfungs- und Risikoausschuss erwartet, wobei Banken der Aufsichtskategorie 3 einen gemischten Ausschuss (Prüfungs- und Risikoausschuss) aufweisen dürfen. Für die Banken der Kategorien 4 und 5 bestehen keine spezifischen Vorgaben. Soweit keine Ausschüsse gebildet werden, obliegen die einschlägigen Aufgaben sinngemäss dem gesamten Verwaltungs- oder Bankrat.[17]

3. Implementierung von Kontrollinstanzen

3.1 «Three Lines of Defence»-Modell

Im Rahmen des internen Kontrollsystems benötigen die Banken gemäss FINMA-Rundschreiben sodann *mindestens zwei Kontrollinstanzen:* die ertragsorientierten Geschäftseinheiten und die unabhängigen Kontrollinstanzen.

Von den Banken wird damit implizit die Implementierung des sog. *«Three Lines of Defence»-Modells* nach internationalem Standard[18] erwartet, basierend auf Frontoffice-Kontrollen im operativen Management (1. Line of Defence), Support-Funktionen/Backoffice-Kontrollen im Risiko- und Compliance-Management (2. Line of Defence) und der internen Revision (3. Line of Defence).[19]

3.2 Kontrollen der ertragsorientierten Geschäftseinheiten («First Line of Defence»)

Das Ziel von Kontrollen in den ertragsorientierten Geschäftseinheiten im Sinne der «First Line of Defence» ist die Übernahme der Verantwortung von eingegangenen Risiken durch das Frontoffice. Dies erfordert Kontrollen, um die Einhaltung der internen Richtlinien und Vorschriften der Bank sicherzustellen, einschliesslich der Verantwortung für die Einhaltung der Risikostrategie der Bank. Die Anreizsysteme der Banken sollten die ertragsorientierten Geschäftseinheiten darin bestärken, die Risiken effektiv und innerhalb der festgelegten Regeln zu verwalten.[20]

3.3 Unabhängige Kontrollinstanzen («Second Line of Defence»)

Die unabhängigen Kontrollinstanzen überwachen Risiken, die Einhaltung interner Richtlinien sowie die regulatorischen Vorgaben. Typischerweise werden die unabhängigen Kontrollinstanzen als *«Risiko»- und «Compliance»-Funktionen* definiert.[21] Für Banken der Kategorien 1–3 wird erwartet, dass eine eigenständige Risikokontrolle und eine Compliance-Funktion vorhanden sind. Zudem wird die Bestimmung eines *Chief Risk Offier (CRO)* verlangt. Bei den grössten Banken

15 Vgl. zum damit einhergehenden Pflichtenentwicklungsrisiko des Verwaltungsrats unten Abschnitt IV.2.

16 *Romer/Kahn* (Fn. 14), 89.

17 FINMA-RS 2017/1 (Fn. 2), Rz. 31.

18 Insbesondere nach der EU-Richtlinie 2006/43/EG vom 17. Mai 2006, ABl. L 157 vom 9. Juni 2006, 87–107.

19 *Andrin Bernet/Yousuf Khan/Alena Nicolai/Alexandra Burns,* PWC (Hrsg.), Anforderungen an Risikomanagement und internes Kontrollsystem, Zürich 2017, abrufbar unter <*https://www.pwc.ch/de/publications/2017/pwc-anforderungen-an-risikomanagement-flyer-2017-de.pdf*>.

20 *Bernet/Khan/Nicolai/Burns* (Fn. 19), 3.

21 *Bernet/Khan/Nicolai/Burns* (Fn. 19), 3.

(Kategorien 1 und 2) muss der CRO zwingend Mitglied der Geschäftsleitung sein.[22]

3.4 Interne Revision («Third Line of Defence»)

Jedes Finanzinstitut hat sodann als «Third Line of Defence» eine interne Revision einzurichten. Soweit die Einrichtung einer betriebseigenen internen Revision nicht angemessen erscheint, können deren Aufgaben an die interne Revision im Konzern der Muttergesellschaft oder einer anderen Gesellschaft des Konzerns übertragen werden. Möglich ist auch die Übertragung dieser Funktion an eine zweite Prüfgesellschaft, welche von der externen Prüfgesellschaft der Bank unabhängig ist.

Die interne Revision ist dem Verwaltungsrat oder dessen Prüfungsausschuss unterstellt und nimmt die ihr übertragenen Prüf- und Überwachungsaufgaben in unabhängiger Art und Weise wahr. Sie erbringt unabhängige Prüfungen und Beurteilungen bezüglich der Angemessenheit und Wirksamkeit der Unternehmensorganisation und Geschäftsprozesse sowie insbesondere bezüglich des IKS und des Risikomanagements des Instituts.[23]

3.5 Rollen von Verwaltungsrat und Geschäftsleitung

Der Verwaltungsrat und die Geschäftsleitung sind in diesem Modell selber nicht als Verteidigungslinien vorgesehen, sondern in ihrer Funktion lediglich Anspruchsgruppen, welche von den drei Verteidigungslinien mit Informationen versorgt werden.[24]

Der Verwaltungsrat legt gemäss FINMA-Rundschreiben[25] die Geschäftsstrategie fest, verabschiedet die Risikopolitik und die Grundzüge des institutsweiten Risikomanagements; er trägt die Verantwortung für die Reglementierung, Einrichtung und Überwachung eines wirksamen Risikomanagements sowie die Steuerung der Gesamtrisiken.[26]

Die Oberleitungs- und Oberaufsichtsaufgabe des Verwaltungsrats beinhaltet damit auch die Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagements, verstanden als System und Prozess. Als *System* integriert das Risikomanagement die Komponenten des internen Kontrollsystems, des Notfall- und Krisenmanagements sowie des Business-Continuity-Managements. Der Prozess des integralen Risikomanagements hingegen besteht aus den beiden Teilschritten der Risikobeurteilung sowie der Risikobewältigung, sowohl präventiv als auch reaktiv.

Risikomanagement ist eine grundlegende Aufgabe der Geschäftsführung. Aus der in Art. 716*a* Abs. 1 OR verankerten Zuständigkeit des Verwaltungsrats zur Organisation des Unternehmens, zur strategischen Führung und zur Aufsicht über die Geschäftsführung sowie zur Ausgestaltung des Rechnungswesens und der Finanzkontrolle ergibt sich eine rechtliche Pflicht des Verwaltungsrats zur materiellen Auseinandersetzung mit den Unternehmensrisiken. Risikomanagement gehört zur Unternehmensführung, da sich das Eintreten von Risiken im künftigen Ertragspotential niederschlagen kann, welches den Wert des Unternehmens bestimmt. Umstritten ist dabei, inwiefern der Verwaltungsrat selbst tätig werden muss und ob er diese Aufgabe und die entsprechenden Verantwortlichkeiten delegieren kann.[27]

Der Verwaltungsrat ist zuständig für die Festlegung der allgemeinen Grundsätze im Bereich des Risikomanagements und deshalb für die Risikopolitik verantwortlich, welche die Entscheidungsgrundlagen für die Risikobewirtschaftung und -überwachung enthält. In der Praxis werden die Vorbereitungsarbeiten zumeist von der Geschäftsleitung gemeinsam mit dem Prüfungs- und Risikoausschuss vorgenommen und die Risikopolitik anschliessend vom Verwaltungsrat genehmigt sowie mindestens einmal jährlich auf deren Angemessenheit überprüft.[28] Aus rechtlicher Sicht ist jedoch zu beachten, dass der Verwaltungsrat durch diese Vorbereitungsarbeiten nicht von seiner diesbezüglichen Verantwortung entlastet wird.[29]

22 *Romer/Khan* (Fn. 14), 89.
23 FINMA-RS 2017/1 (Fn. 2), Rz. 82 ff.
24 *Mirjam Durrer/Marco Gruber,* Der Verwaltungsrat als erste Verteidigungslinie im integralen Risikomanagement, EF 2020, 124 ff., 124.
25 FINMA-RS 2017/1 (Fn. 2), Rz. 9 ff.
26 FINMA-RS 2017/1 (Fn. 2), Rz. 10.
27 *Peter Böckli,* Schweizer Aktienrecht, 5. Aufl., Zürich/Genf 2022, § 9 N 461; *Durrer/Gruber* (Fn. 24), 125; *Roland Müller/Lorenz Lipp/Adrian Plüss,* Der Verwaltungsrat, 5. Aufl., Zürich 2021, N 6.78 ff.; *Christoph B. Bühler,* Kommentar zu Art. 716*a*, in: Lukas Handschin (Hrsg.), Zürcher Kommentar, Die Aktiengesellschaft, Generalversammlung und Verwaltungsrat, Mängel in der Organisation, 3. Aufl., Zürich 2018, N 71.
28 *Durrer/Gruber* (Fn. 24), 125 f.
29 *Lehmann/Roth Pellanda* (Fn. 3), 322.

Die vom Verwaltungsrat festzulegende Risikopolitik bildet den Ordnungsrahmen für das integrale Risikomanagementsystem; sie umfasst namentlich die folgenden Bereiche:

- Ziele des Risikomanagements;
- Typologisierung der für die Bank relevanten Risikoarten und -faktoren;
- Entscheid über den Grad der Risikobereitschaft und die Risikotragfähigkeit («risk tolerance and risk appetite»);
- Grundsätze und Prinzipien bzgl. Identifikation, Messung, Bewirtschaftung und Überwachung der Risiken;
- Errichtung einer Risikokultur und die Verabschiedung von Integritätsstandards bzw. eines entsprechenden Verhaltenskodexes;
- Festlegung der Organisation sowie der Kompetenzen und Verantwortlichkeiten sowie die Bereitstellung der nötigen personellen und finanziellen Ressourcen;
- Errichtung eines Reportingsystems;
- Einrichtung eines Überwachungsprozesses zur periodischen Prüfung und allfälligen Anpassung der Risikopolitik an neue Gegebenheiten.[30]

Die Risikopolitik bildet den Ordnungsrahmen für die Umsetzung des Risikomanagements. Diese kann und soll durch den Verwaltungsrat an die Geschäftsleitung delegiert werden.[31] Zur Umsetzung und Durchführung gehört auch die Entwicklung geeigneter Strukturen und Prozesse für die Identifikation, Beurteilung und Überwachung der eingegangenen Risiken. Die Verantwortung für die zweckmässige Durchführung des Risikomanagements verbleibt hingegen beim Verwaltungsrat, weshalb dieser sowohl ein Reportingsystem als auch Risikolimiten zu errichten hat, die es ihm ermöglichen, einschreiten zu können, wenn ein Risiko eingegangen wird, das sich auf die Strategie, Risikotoleranz oder Risikotragfähigkeit des Unternehmens auswirken könnte. Es gilt der Grundsatz: «Boards have to keep their noses in and their hands out.»[32]

4. Gelebte Risikokultur

Prozesse, Modelle und Systeme müssen ergänzt werden durch eine Risikokultur, die nicht nur die Risikoorganisation, sondern vor allem auch das Frontoffice und die Marktbereiche teilen und leben. Der Verwaltungsrat erlässt die Leitsätze zur Unternehmenskultur,[33] einschliesslich der Risikokultur. Der gesamte Verwaltungsrat und die Geschäftsleitung müssen diese aber vor allem durch ihr Vorbild in die Organisation hineintransportieren. Zu einer in der Unternehmenskultur verankerten Risikokultur gehört zum einen eine strenge Disziplin im Umgang mit Limiten und Policies, die nicht nur als Leitlinien oder Planken gelten, sondern absolute Limiten ohne Diskussionsspielraum darstellen. Es sollte die Bereitschaft vorhanden sein, bisher unentdeckte Risiken offen zu legen und transparent zu machen. Um Risiken aktiv zu managen, ist auch eine fruchtbare Dissenskultur notwendig, bei der unterschiedliche Auffassungen über Risikofragen offen diskutiert werden können. Mit der offenen Kommunikation besteht für den Einzelnen wie auch für die Gesamtorganisation die Möglichkeit und auch die Bereitschaft, aus eigenen Fehlern der Vergangenheit zu lernen.[34]

IV. Nachhaltiger Wandel in der «Risk Governance» der Banken

Vor dem Hintergrund der eingangs geschilderten Entwicklung stellt sich die Frage, ob die dargelegten herkömmlichen Strukturen und Prozesse den neuen Herausforderungen der Zeit noch genügen oder ob diesbezüglich allenfalls ein Anpassungsbedarf besteht.

1. Neue Herausforderungen für die «Risk Governance» der Banken

Wie bereits erwähnt, befindet sich die Risikosteuerung in den Banken derzeit mitten in einem nachhaltigen Wandel. Insbesondere die COVID-Pandemie und die aktuellen geopolitischen Instabilitäten, neue Technologien sowie die Digitalisierung zeigen auf, dass die Herausforderungen komplexer werden und dass

30 *Lehmann/Roth Pellanda* (Fn. 3), 322.
31 *Durrer/Gruber* (Fn. 24), 125 f.
32 *Lehmann/Roth Pellanda* (Fn. 3), 323; vgl. auch *Roland Müller/Vinay Kalia,* Risk Management at Board Level – A Practical Guide for Board Members, Bern 2007, 20.
33 FINMA-RS 2017/1 (Fn. 2), Rz. 10.
34 *Stefan Schmittmann,* Die Rolle des Chief Risk Officer unter Corporate-Governance-Gesichtspunkten, in: Klaus Hopt et al. (Hrsg.), Handbuch Corporate Governance von Banken, München 2011, 481 ff., 489 f.

insbesondere die nichtfinanziellen Risiken nur unpräzise antizipiert werden können.

Da sich die Entwicklung von «Risk Governance»-Mechanismen viel langsamer vollzieht als die Prozesse, die den technologischen und sozialen Wandel vorantreiben, gibt es Grund zur Sorge, ob die bestehenden «Risk-Governance»-Mechanismen geeignet sind, um mit nichtfinanziellen Risiken wie denen des Klimawandels, des Verlusts der biologischen Vielfalt und der künstlichen Intelligenz effizient umzugehen oder Kompromisse zwischen verschiedenen, manchmal widersprüchlichen Bedürfnissen und Interessen zu schliessen.

Die grössten Gefahren für die Bankenindustrie werden nach der von PWC durchgeführten globalen Studie «Risk Management 2025»[35] insbesondere in den Cyberrisiken (77%) und ESG (77%) und der zunehmenden Regulierung (62%) gesehen. Hinzu kommen Betrug, Geldwäsche oder die ständig wachsende Abhängigkeit von einem komplexen Netz aus Geschäftspartnern und Drittanbietern. Diese Einschätzung der Banken wird auch durch andere jüngere Umfragen und Studien bestätigt.[36]

Diese Entwicklung führt zu einer umfassenden Transformation der «Risk Governance» von Banken selbst, namentlich in Bezug auf die Organisation und Integration des Risikomanagements im Geschäftsmodell der Bank. Die wesentlichen Herausforderungen werden in einem stärkeren Augenmerk auf der operativen Resilienz und der Integration der neuen Risiken in die Risikomanagementsysteme der Banken gesehen. Etwa zwei Drittel der Banken sehen den grössten Veränderungsbedarf der nächsten Jahre bei den nichtfinanziellen Risiken.

Herausforderungen bestehen hier vor allem in Zusammenhang mit den vorhandenen Daten und der Infrastruktur, welche auf die neuen Risiken noch nicht eingestellt sind, aber auch in der noch fehlenden, auf diese Risiken ausgerichteten Expertise bei den Risikoverantwortlichen.

2. Pflichtenentwicklungsrisiko der Bankorgane

Durch diese Entwicklung wird auch die Unternehmensführung für die Bankorgane zunehmend anspruchsvoller, die in Bezug auf die Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagements und die Compliance in der obersten Verantwortung stehen. Diese befinden sich in einem ständigen Wechselspiel zwischen den neuen gesetzlichen Vorgaben, ausserrechtlichen Kodexregeln und Transparenzrichtlinien, durch welche die entstehenden neuen Risiken erfasst und mitigiert werden sollen. Besonders dynamisch wird die Situation durch die kurzfristigen, manchmal überzogenen Reaktionen des Gesetzgebers auf Skandale bei einzelnen Unternehmen sowie durch die veränderten Erwartungen und rechtlichen Anforderungen in Zeiten politischer, wirtschaftlicher und sozialer Krisen wie Klimawandel und ESG. Diese Veränderungen können erhebliche Risiken für das Geschäftsmodell einzelner Finanzdienstleistungsunternehmen, die Finanzbranche und die Wirtschaft insgesamt darstellen. Die Bankorgane müssen dann oft feststellen, dass sie den vollen Umfang ihrer Pflichten nicht vollständig erfasst haben.

Die rechtlichen Herausforderungen spiegeln sich dabei vor allem im Aktien-, Finanzmarkt- und Rechnungslegungsrecht wider, ergänzt durch erweiterte internationale Anforderungen und «Best Practice»-Standards. Innerhalb des Unternehmens sind Massnahmen in den Bereichen Compliance, Risikomanagement und eine auf das Unternehmen zugeschnittene Corporate Governance notwendig. Die Handlungsspielräume der Bankorgane werden dabei zunehmend eingeschränkt. Dieses Phänomen der sich schleichend fortbildenden Risiken und verdichtenden Pflichten der Unternehmensorgane wird auch als «Pflichtenentwicklungsrisiko» bezeichnet.[37]

35 PWC, Risk Management 2025 and beyond – priorities and transformation agenda for the banking industry, Zürich 2021, abrufbar unter <*https://www.pwc.de/de/finanzdienstleistungen/banken/pwc-risk-management-2025-and-beyond.pdf*>.

36 Vgl. etwa PWC, Global Risk Survey 2023 – Risiken in Chancen wandeln, vom Dezember 2023, abrufbar unter <*https://www.pwc.de/globalrisksurvey*>.

37 *Klaus J. Hopt/Patrick C. Leyens*, Grundsatzfragen der Unternehmensführung und -überwachung, in: Peter Hommelhoff/Klaus J. Hopt/Patrick C. Leyens (Hrsg.), Unternehmensführung durch Vorstand und Aufsichtsrat, München 2024, 1 ff.; vgl. dazu die Rezension durch *Christoph B. Bühler*, Neues Praxishandbuch zum dynamischen Pflichtenentwicklungsrisiko in der Unternehmensführung, SZW 2024, 636 ff.

3. Handlungsfelder für die «Risk Governance» der Zukunft

Welche Handlungsfelder ergeben sich für die Banken und deren Leitungsorgane nun angesichts dieser Entwicklung und neuen Herausforderungen in Bezug auf die Ausgestaltung der «Risk Governance» der Zukunft?

3.1 Stärkung der operativen Widerstandsfähigkeit und Resilienz

Da sich die wachsende Zahl an Risiken als schwer oder gar nicht vorhersagbar erweist, dürfte vor allem die operative Resilienz zu einem zentralen Instrument der Geschäftsführung werden. Die FINMA definiert diese als Fähigkeit des Instituts, seine kritischen Funktionen bei Unterbrechungen innerhalb der Unterbrechungstoleranz wiederherstellen zu können.[38] Es geht konkret um die Fähigkeit, Bedrohungen und mögliche Ausfälle zu identifizieren, sich davor zu schützen und darauf zu reagieren. Es geht auch darum, bei Unterbrechungen den ordentlichen Geschäftsbetrieb wiederherzustellen und daraus zu lernen, um die Auswirkungen von Unterbrechungen auf die Erbringung der kritischen Funktionen zu minimieren.

Zur Stärkung der Resilienz ist das «Stress Testing» zu überprüfen und eventuell neu zu kalibrieren, um schneller und dynamischer zu sein und die Fähigkeit zur Erfassung risikoübergreifender Auswirkungen zu verbessern. Dazu müssen Strukturen und dynamische Instrumente entwickelt werden, welche auch sich anbahnende neue Risiken ermitteln und bewerten können. Auch das bewährte «Business Continuity Management»[39] ist einer Review zu unterziehen, was gemäss Art. 3 BankG bereits zu den Organisationserfordernissen einer Bank gehört.

Die Resilienz wird aber letztlich auch präventiv gestärkt, indem der Risikoappetit und die Risikotoleranz grundsätzlich überdacht und deren Stellenwert bei strategischen Entscheidungen konsequenter berücksichtigt werden.[40]

3.2 Weiterentwicklung und Befähigung der Risikomanagementteams insbesondere im Bereich der nichtfinanziellen Risiken

Eine weitere Priorität dürfte für die Banken darin liegen, dass Risikoverantwortliche und ihre Teams innovative Ansätze entwickeln, um auf nichtfinanzielle Risiken einzugehen. Das Bestreben, Risiken zu einem strategischen Faktor zu machen, um aus ihnen vor allem auch unternehmerische Chancen zu erschliessen, muss mit der Entwicklung von Kompetenzen und Fähigkeiten im Unternehmen einhergehen. Dies dürfte zu einem gesteigerten Weiterbildungs- oder zusätzlichen Personalbedarf für den Bereich dieser Risiken führen. So wird die Frage nach den richtigen Mitarbeitenden existenziell für die Banken. Der Risikoexperte der Zukunft wird ein wesentlicher Wettbewerbsvorteil sein, um die Opportunitäten der Digitalisierung nutzen und die Einführung neuer Technologien vorantreiben zu können, aber auch, um die Risikokultur zu verbessern und die Kosten zu senken.

Einen besonderen Stellenwert erhält in diesem Zusammenhang der «Chief Risk Officer» (CRO). In seiner Funktion spiegelt sich, wie in einem Brennglas, der für das Geschäftsmodell der Banken typische «Risk-return-trade-off» wider, also die permanente Abwägung zwischen Ertrag und Risiko. Es ist also wichtig, welchen Einfluss der CRO auf die Gesamtführung einer Bank hat und mit welchen Befugnissen er ausgestattet ist. CROs müssen mit Macht ausgestattet sein, «to spot promising opportunities and stop reckless trading operations».[41] Dabei dürfte letztlich nicht ausschlaggebend sein, ob der CRO in der Bank auf der Ebene der Geschäftsleitung oder eine Führungsstufe darunter positioniert ist. Entscheidend ist vielmehr, dass eine enge und vertrauensvolle Zusammenarbeit zwischen dem CRO und dem CEO sowie der gesamten Geschäftsleitung besteht.[42] Es versteht sich, dass der CRO über die nötigen Kompetenzen verfügen muss, wie insbesondere eine breite und tiefe Markt- und Produktkenntnis, hohe analytische Fähigkeiten zum Verständnis der sich ergebenden und ständig verändernden

38 FINMA-Rundschreiben 2023/1 Operationelle Risiken und Resilienz – Banken, Management der operationellen Risiken und Sicherstellung der operationellen Resilienz vom 7. Dezember 2022, Rz. 18.

39 FINMA-RS 2023/1 (Fn. 38), Rz. 83 ff.

40 Vgl. dazu *Martin Eckert*, Management der operationellen Risiken und Sicherstellung der operationellen Resilienz von Banken, SZW 2025, 71 ff.

41 Egon Zehnder International, Five answers from Lisa D. Zonino, New York 2011, zitiert bei *Stefan Reckhenrich*, Neue Anforderungen an den Bankvorstand, in: Klaus J. Hopt/Gottfried Wohlmannstetter (Hrsg.), Handbuch Corporate Governance von Banken, München 2011, 469 ff., 474.

42 *Susan Emmenegger*, Prudentielle Corporate Governance, in: Susan Emmenegger (Hrsg.), Corporate Governance, Basel 2011, 1 ff., 33 f.

Risikosituationen sowie einen gesunden Menschenverstand, gepaart mit hoher Überzeugungs- und Durchsetzungsfähigkeit. Er muss stark genug sein, um im Zusammenwirken mit der Geschäftsleitung im gesamten Haus eine gesunde und wirkungsvolle Risikokultur zu etablieren. Dabei muss er sich auf den uneingeschränkten Rückhalt der gesamten Geschäftsleitung und des Verwaltungsrats verlassen können, welche die Gesamtverantwortung der Bank tragen.[43]

Zu prüfen ist auch die Einrichtung von Kompetenzzentren in der ersten und zweiten Verteidigungslinie, um auf die sich ändernde Geschäfts-, Risiko- und Technologielandschaft angemessen reagieren zu können. Die Banken müssen ihre Risikofunktionen vor allem agiler ausgestalten, Silos auflösen und die Prozesse über alle Risikoverteidigungslinien hinweg ganzheitlicher ausrichten. Zu denken ist hier beispielsweise an fliessende Organisationsstrukturen oder integrierte Einheiten, die sich auf Teams der ersten und zweiten Verteidigungslinie erstrecken.

3.3 Automatisierung und Digitalisierung der Risiko- und Compliance-Funktionen

Technologisch setzen die Banken zur Steuerung der Risiken bereits heute verstärkt auf «Big Data», künstliche Intelligenz (KI) und «Machine Learning». In den vergangenen Jahren wurden in den Risiko- und Compliance-Funktionen über alle Linien des «Three-Lines-of-Defense»-Modells zunehmend Lösungen aus dem Bereich «Advanced Analytics» eingeführt. Mit KI lassen sich dynamische und zukunftsorientierte Szenarioanalysefunktionen aufbauen.[44]

Insbesondere die Ermittlung und Bewertung der nichtfinanziellen Risiken sollten digitalisiert werden, um dadurch die einschlägigen Anforderungen im Bereich der Sorgfaltspflichten und Berichterstattung zu vereinfachen. Die bestehenden Plattformen sind entsprechend neu zu gestalten und Datenmodelle für nichtfinanzielle Risiken zu definieren, um auch in diesem Bereich angereicherte Datensätze sammeln zu können. Es geht darum, die Fähigkeiten der Risikomanagementteams mit modernsten Technologielösungen und Datenanalysemethoden zu kombinieren, und nicht etwa darum, diese zu ersetzen: *«human led, but tech-powered».*

3.4 Anpassung des bestehenden «Risk-Governance»-Modells

Es stellt sich schliesslich auch die Frage, ob die geltenden Anforderungen an die Organisation der «Risk Governance» einer Bank, welche auf dem herkömmlichen «Three Lines of Defense»-Modell basieren, in Bezug auf die neu entstehenden und dynamisch sich weiterentwickelnden Risiken nicht grundsätzlich zu überdenken oder doch zumindest zu aktualisieren sind.[45] Es werden in der Praxis denn auch angepasste «Risk Governance»-Ansätze zur Debatte gestellt.

3.4.1 «Three Lines Model»: Aktualisierung des «Three Lines of Defense Model»

So hat das *Institute of Internal Auditors* (IIA) das «Three Lines of Defence»-Modell jüngst überarbeitet bzw. aktualisiert und neu als «Three Lines Model» bezeichnet.[46] Das neue Modell soll dem Umstand Rechnung tragen, dass es bei der risikobasierten Entscheidungsfindung nicht nur um den Schutz oder das Verteidigen von Unternehmenswerten, sondern auch um das Ergreifen von Chancen geht. Das aktualisierte Konzept betont entsprechend stärker die Abgrenzungen von Rollen und Verantwortlichkeiten des Verwaltungsrats, des Managements und der internen Revision mit einem Fokus auf die Governance.

Das oberste Leitungsorgan gibt die Richtung der Organisation vor, indem es die Vision, den Auftrag, die Werte und die Risikobereitschaft der Organisation definiert. Die erste Linie stellt die Produkte und Dienstleistungen für den Kunden bereit und verwaltet die diesbezüglichen Risiken. Die zweite Linie bringt die spezifische Expertise und Unterstützung zur Überwachung der Risiken ein, und die dritte Linie verschafft eine unabhängige Prüfsicherheit.[47]

43 *Reckhenrich* (Fn. 41), 474.

44 Vgl. *Florian Häller,* Künstliche Intelligenz in Finanzberichterstattung und Wirtschaftsprüfung, EF 2024, 516 ff.; *Madan Sathe/Teodor Pistalu,* Die Rolle der künstlichen Intelligenz im Audit, Chancen und Risiken für die Audit-Transformation, EF 2024, 500 ff.

45 Vgl. *Eric S. Soong/Tobias Ochs*, GRC: Ein koordiniertes und ganzheitliches Compliance- und Riskmanagement-Modell, CB 2021, 61 ff., 62.

46 The Institute of Internal Auditors, The IIA's Three Lines Model, Lake Mary 2024, abrufbar unter <*https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf*>.

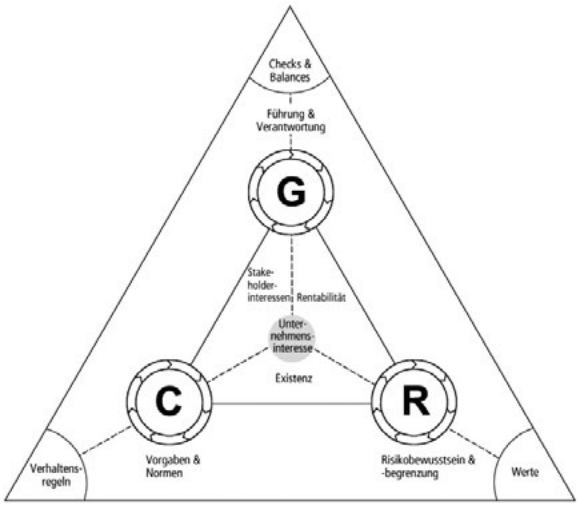
47 *Soong/Ochs* (Fn. 45), 62.

Diese Aktualisierung des «Three Lines of Defence»-Modells bekräftige, so der IIA Global Chairman *Jenitha John,* «dass Organisationen geeignete, pragmatische Strukturen für sich selbst bestimmen müssen, wobei ihre Ziele und Umstände vor dem Hintergrund einer sich ständig weiterentwickelnden Risikolandschaft zu berücksichtigen sind».[48]

3.4.2 Ganzheitliches GRC-Modell: Erweiterung des «Three Lines of Defense Model»

In der Praxis insbesondere der Prüfgesellschaften wird sodann zunehmend die Erweiterung des etablierten «Three Lines of Defense»-Modells auf ein umfassenderes und integrales Governance-, Risikomanagement- und Compliance-Modell, kurz GRC-Modell, diskutiert.[49]

Die Themen Governance, Risikomanagement und Compliance werden heute meist separat bearbeitet. Sie sind unterschiedlichen Funktionen oder Bereichen zugeordnet, verwenden eigenständige Prozesse und Instrumente und berichten in unterschiedlichen Formaten an die obersten Leitungsorgane. Die Anforderungen in den Bereichen der Governance, des Risikomanagements und der Compliance haben sich in den letzten Jahren laufend ausgeweitet, was dazu geführt hat, dass zunehmend Berührungspunkte und Überlappungen zwischen den Systemen festzustellen sind. Um den neuen Herausforderungen effizienter zu begegnen, sollen die drei Handlungsebenen Governance, Risk und Compliance strukturell verknüpft und unter einem Dach vereint werden.[50]



Das GRC-Managementmodell besteht dabei aus einem inneren und einem äusseren Dreieck: Im inneren Dreieck werden die GRC-Funktionen, ihre Beziehung untereinander und ihre Ausrichtung auf das Unternehmensinteresse dargestellt (Führung und Verantwortung, Risikobewusstsein und -begrenzung sowie Vorgaben und Normen).

Im äusseren Dreieck werden die GRC-Funktionen im Kontext der Kultur und des Führungs- und Wertesystems des Unternehmens eingebettet («Checks & Balances», Werte und Verhaltensregeln). Das Dreieck bringt die gegenseitigen Beziehungen zwischen den GRC-Funktionen zum Ausdruck. Im Mittelpunkt des Dreiecks steht das nachhaltige Unternehmensinteresse, auf welches die unternehmerische Tätigkeit letztlich ausgerichtet ist.

Mit diesem Ansatz sollen vor allem die obersten Leitungsorgane aufgrund von abgestimmten und einheitlich aufbereiteten Informationen bei der Unternehmensführung und -kontrolle besser unterstützt und Synergien zwischen den GRC-Funktionen erschlossen werden.

V. Fazit

In einer von zunehmender Komplexität, Vernetzung und Volatilität geprägten Welt mit disruptiven Innovationen, neuen Geschäftsmodellen und sich schnell entwickelnden Technologien stellt eine wirksame «Risk-Governance» für die Banken eine grosse Herausforderung dar. Entscheidend ist dabei nicht nur eine funktional zweckmässige, mit qualifizierten Teams be-

48 Zitiert bei *Soong/Ochs* (Fn. 45), 62.

49 *Soong/Ochs* (Fn. 45), 61 ff.; *Christen Marquard/Dirk Spacek/Hadi Mirzai/Marzia Schilleci,* Aktuelle rechtliche Neuerungen per «Governance, Risk and Compliance» (GRC)-Ansatz angehen, RR-COMP 2022, 2 ff.; *Markus Schumacher,* Integriertes GRC-Management, Wie die Integration von Governance, Risikomanagement und Compliance zum Erfolg des Unternehmens beitragen kann, RiU/LfE Bd. 44, Zürich 2021, 1 ff.

50 Darstellung bei *Schumacher* (Fn. 49), 1 ff.

setzte Aufbauorganisation für das Risikomanagement, sondern auch eine resiliente Ablauforganisation. Begreift man Risiken auch als Chance, müssen die Handlungsebenen der Governance, des Risikomanagements und der Compliance im Unternehmen sodann ganzheitlich in die Unterstützungs- und Entscheidungsprozesse integriert und als strategische Führungsinstrumente ausgestaltet sein. Die Governance-Struktur und die zugrundeliegenden Managementsysteme sowie die Notwendigkeit einer durchgängigen Einhaltung von regulatorischen Anforderungen und unternehmensinternen Regeln müssen bei den obersten Leitungsorganen einen Rückhalt haben und von diesen vorgelebt werden. «Last but not least» bilden eine gesunde Risikokultur und die Integrität der Leitungsorgane die tragenden Säulen für ein nachhaltig erfolgreiches unternehmerisches Handeln.