Hochschule Neu-Ulm
University of Applied Sciences

Bachelorarbeit
im Bachelorstudiengang **Betriebswirtschaft**
an der Hochschule für angewandte Wissenschaften Neu-Ulm

Thema

Die Bedeutung der Integration von Governance, Risk und Compliance im Banksektor: Eine ganzheitliche Betrachtung von GRC

Erstkorrektor/-in: Professor Dr. Thomas Hänichen

Verfasser/-in: Steinhauer Emilia (Matrikel-Nr.: 266387)

Thema erhalten: 26.06.2023
Arbeit abgegeben: 29.08.2023

Abstract

Finanzinstitute leisten einen bedeutenden Beitrag zur Bereitstellung von Kapital an Standorten, die für wirtschaftliche Aktivitäten von essentieller Bedeutung sind. Als bedeutende Katalysatoren fördern Banken Investitionen, Innovationsprojekte und gesellschaftlichen Fortschritt. Diese Funktion ermöglicht es ihnen, einen fundamentalen Einfluss auf das Wirtschaftswachstum und die Beschäftigungslage auszuüben,[1] wodurch die Gewährleistung ihrer Kontinuität von hoher Relevanz ist. Die Finanzkrise hat sowohl in ökonomischer als auch gesellschaftlicher Hinsicht tiefgreifende Spuren hinterlassen.[2] In diesem Kontext wurde die mangelhafte Corporate Governance der Banken zunehmend als eine der Hauptursachen für die Finanzkrise diskutiert.[3] Die Zielsetzung der vorliegenden Arbeit besteht darin, basierend auf dem aktuellen Stand der Wissenschaft zusätzlichen Forschungsbedarf in den maßgeblich mit Finanzkrisen verknüpften Bereichen aufzuzeigen. Der Hauptfokus dieser empirischen Untersuchung liegt auf der Analyse der aktuellen Governance, Risk und Compliance (GRC)-Praktiken und -Herausforderungen. Gleichzeitig werden die Vorzüge eines ganzheitlichen, integrierten GRC-Ansatzes sowie die damit verbundenen Schwierigkeiten identifiziert. Um die Forschungsfrage zu beantworten, wurden strukturierte Experteninterviews unter Verwendung eines Leitfadens durchgeführt. Die aus diesen Ergebnissen abgeleiteten Daten wurden mithilfe einer qualitativen, zusammenfassenden Inhaltsanalyse nach der Methode von Mayring analysiert und abschließend interpretiert. Mittels der resultierenden Erkenntnisse wurden verschiedene Kategoriesysteme entwickelt, um die aktuell praktizierten GRC-Verfahren zu konturieren und somit die Vor- und Nachteile eines integrierten GRC-Ansatzes herauszuarbeiten. Die Ergebnisse zeigten, dass die Vorteile eines integrierten Ansatzes im Bereich GRC sich über mehrere Aspekte erstrecken. Diese beinhalten den gezielten Transfer von Fachwissen, die Neugestaltung von Machtstrukturen, die Realisierung von Kosteneinsparungen, die Minimierung von Redundanzen, die Vereinfachung komplexer Prozesse sowie die Steigerung der Gesamteffizienz. Damit einher gehen die Herausforderungen, die sich ergeben, wie erschwerte Austauschmöglichkeiten in Organisationen mit getrennten Compliance- und Risikomanagementstrukturen, mögliche Redundanzkonflikte zwischen Effizienz und umfassender Perspektive sowie die

[1] vgl.Bankenverband (Rolle der Banken in Deutschland auf einen Blick, 22.06.2023)
[2] vgl. Gill u.a. (Anreize, systemische Risiken und Intransparenz: Lehren aus der Finanz-und Staatsschuldenkrise, 2012), S. 1
[3] vgl.Kirkpatrick (The corporate governance lessons from the financial crisis, 2009), S. 61-87

Vereinheitlichung individueller Fachkenntnisse. Demnach ist das Thema von großer Relevanz für die Gesamtheit der Bankinstitute in Deutschland.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AktG	Aktiengesetz
AT	Allgemeine Teil der MaRisk
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
CARS	Creating a Research Space
CRD IV	Capital Requirements Directive IV
CRR-VO	Capital Requirements Regulation - Verordnung
DCGK	Deutscher Corporate Governance Kodex
GRC	Governance, Risk & Compliance
GwG	Geldwäschegesetz
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KWG	Kreditwesengesetz
MaRisk	Mindestanforderungen an das Risikomanagement
OWiG	Ordnungswidrigkeitengesetz
WpHG	Wertpapierhandelsgesetz

Abbildungsverzeichnis

Gender Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Bachelorarbeit auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Formulierungen gelten gleichermaßen für alle Geschlechter.

Einleitung

1.1 Hintergrund und Bedeutung des Themas

Das internationale Bankensystem ist in den letzten Jahren immer wieder in den Blickpunkt des öffentlichen Interesses gerückt. Insbesondere die Instabilität des Bankensystems während der Finanzkrise von 2007 bis 2009 und die hohen Kosten dieser Krise haben weltweit zu massiver Kritik geführt.[4] Im September 2009 meldete als Folge der Finanzkrise bereits die 90. US-Bank Insolvenz an.[5] Aus wirtschaftspolitischer und volkswirtschaftlicher Sicht stellt sich die Frage, wie es trotz der umfassenden Regulierung der Finanzsysteme weltweit zu wiederholtem Fehlverhalten kommen konnte. Zunehmend wird die mangelhafte Corporate Governance der Banken als eine der Hauptursachen der Krise diskutiert.[6] Eine Konsequenz aus diesem Entwicklungsverlauf manifestiert sich in einer gesteigerten Diskussion hinsichtlich der Bedeutung von Governance, Risikomanagement und Compliance (GRC). Um substantielle Verluste und Insolvenzen von Banken abzuwenden und die Branche insgesamt zu stabilisieren, wurden auf globaler Ebene zahlreiche neuartige Regelungen implementiert. Um diese Anforderungen wirksam zu begegnen, ist ein angemessenes und leistungsfähiges Governance, Risk & Compliance Management erforderlich. Neben der essentiellen Aufgabe der Gewährleistung regulatorischer Konformität besteht die Herausforderung darin, gleichzeitig Effizienzpotenziale zu nutzen und Unternehmensrisiken über Abteilungsgrenzen hinweg zu managen.[7]

1.2 Zielsetzung und Forschungsfrage

Das Ziel der vorliegenden Arbeit besteht darin die regulatorischen Anforderungen im Kontext von GRC im Banksektor mit dem Fokus auf Aktiengesellschaften zu erläutern. Der empirische Abschnitt dieser vorliegenden Studie widmet sich der Analyse der gegenwärtigen isolierten Praktiken im Bereich GRC, sowie den gegenwärtigen Herausforderungen innerhalb des Bankensektors. In diesem Zusammenhang erfolgt eine Identifikation der Mehrwerte, welche durch die Anwendung eines umfassenden GRC-Ansatzes erzielt werden können. Gleichzeitig werden die dazugehörigen Herausforderungen innerhalb der Banken aufgedeckt. Abschließend

[4] vgl.Adelson (The Deeper Causes of the Financial Crisis: Mortgages Alone Cannot Explain It, 2013)
[5] vgl.Lister (Wege aus der Finanzkrise – Anpassungsbedarf im Risikomanagement der Kreditinstitute, 2010), S. 295
[6] vgl.Kirkpatrick (The corporate governance lessons from the financial crisis, 2009), S. 61-87
[7] vgl. Bruehl und Hiendlmeier (Auf dem Weg zu einem ganzheitlichen GRC-Management? Empirische Befunde zur Integration von Internem Kontrollsystem, Risikomanagement und Compliance, 2013), S. 1 ff.

werden aus den gewonnenen Erkenntnissen bewährte Methodiken für eine erfolgreiche GRC-Integration im Finanzsektor abgeleitet.

1.3 Methodik und Aufbau der Arbeit

Die vorliegende Arbeit ist in sieben Kapitel aufgeteilt. Zu Beginn wird die Problemstellung, die Forschungsfrage und die Relevanz des Themas sowie die Zielsetzung der Arbeit erläutert. Das zweite Kapitel beschäftigt sich mit den inhaltlichen und gesetzlichen Grundlagen von Corporate Governance, Risk und Compliance. Der Fokus im dritten Kapitel richtet sich auf eine detaillierte Erläuterung des Modells der "Three-Lines-of-Defense". Im vierten Kapitel erfolgt die Vorstellung eines weiteren Organs der Governance, die interne Revision, sowie eines weiteren externen Governance Organs, der Wirtschaftsprüfer. In diesem Zusammenhang werden die Aufgaben dieser Organe jeweils detailliert erläutert. Der theoretische Schwerpunkt dieser Arbeit bildet sich im Kapitel fünf ab. In diesem Abschnitt erfolgt eine umfassende Betrachtung der Thematik der ganzheitlichen Integration von GRC. Dabei wird sowohl die Relevanz sowie die Vorteile einer derartigen ganzheitlichen GRC-Integration eingehend beleuchtet. Im Anschluss daran widmet sich die vorliegende Arbeit dem empirischen Untersuchungsdesign. Hierbei erfolgt eine ausführliche Darlegung der methodischen Herangehensweise, einschließlich der Verfahren zur Datenerhebung und Datenanalyse, sowie der Präsentation der erzielten Resultate. Insbesondere wird die qualitative Forschungsmethode mithilfe Experteninterviews im Detail erörtert. Die Beantwortung der Forschungsfrage erfolgt dabei durch die eigenständige Entwicklung eines Modells. Den Abschluss der Arbeit bilden eine kritische Reflexion der gewonnenen Erkenntnisse sowie ein abschließendes Fazit.

2 Inhaltliche und gesetzliche Grundlagen

In der einschlägigen Literatur werden die Konzepte GRC oft in Kombination betrachtet. Dabei geht es nicht nur um eine bloße Verbindung der Begriffe, sondern vielmehr um ihre systematische Einordnung und Verknüpfung, da sie sich gegenseitig beeinflussen und in ihrer Anwendung wechselseitig ineinander übergehen können. Somit lassen sich diese Konzepte als untereinander subsumierbar und sich gegenseitig prägend auffassen.[8] In der nachfolgenden Ausführung werden zunächst die Begrifflichkeiten GRC definiert und die zugrundeliegenden theoretischen und gesetzlichen Grundlagen erläutert, um ein einheitliches Verständnis zu gewährleisten. Angesichts der universellen Relevanz von Corporate Governance in jeglicher Unternehmensstruktur, erfolgt im ersten Schritt eine generelle Einführung in das Thema Corporate Governance gefolgt von einer spezifischen Betrachtung im Kontext der Bankbranche.

2.1 Corporate Governance Allgemein

Corporate Governance ist nach der weltweit bekanntesten und inzwischen von der Europäischen Kommission adaptierten Definition der britischen Cadbury Commission von 1992: „the system by which companies are directed and controlled".[9] Der Begriff der Corporate Governance hat seine Wurzeln im angelsächsischen Raum und bezieht sich primär auf ein ökonomisches Problem. Die Kernthematik der Corporate Governance betrifft den sogenannten Principal-Agent-Konflikt zwischen den Aktionären als Eigentümern des Unternehmens (Principal) und dem Management als Träger der Verfügungsmacht (Agent).[10] Die Aktionäre streben nach Gewinnmaximierung, während das Management der Theorie zufolge risikoavers und konformistisch,[11] jedoch nicht notwendigerweise im Interesse der Anteilseigner handeln. Darüber hinaus befindet sich das Management aufgrund seines Informationsvorsprungs in einer Machtposition, die es ihm ermöglicht, das Unternehmen in seinem eigenen Interesse zu führen und zu lenken, was wiederum zu Lasten der Eigentümer führen kann. [12] Daher ist es von großer Bedeutung, Diskrepanzen zwischen dem Management und den Eigentümern eines Unternehmens durch geeignete Vereinbarungen oder ein angemessenes Regelwerk zu mildern. Ein bewährter Ansatz zur Erreichung dieses Ziels ist die Überwachung des Managements durch

[8] vgl.Schoch u.a. (Governance, Risk und Compliance als Führungsaufgabe im Lichte der sich verändernden regulatorischen Anforderungen in der Finanzbranche am Beispiel der Schweiz, 2016), S. 1
[9] Cadbury (Report of the Committee on the Financial Aspects of Corporate Governance, 1992), Abschn. 2.5.
[10] vgl. Hopt und Wohlmannstetter (Corporate Governance von Banken 2011), S. 5 ff., 33
[11] vgl.Schug (Risikoeinschränkung und -transfer in der Vorstandshaftung, 2010), S. 44
[12] vgl.Schug (Risikoeinschränkung und -transfer in der Vorstandshaftung, 2010), S. 45

interne Unternehmensorgane, die im Rahmen des dualistischen Systems des deutschen Rechts vom Aufsichtsorgan ausgeführt wird,[13] sowie die Schaffung positiver Anreize für das Management, z.B. durch erfolgsabhängige Vergütungssysteme.[14] Die Thematik des Interessenausgleichs bringt eine weitere Frage bezüglich der Ausrichtung des Leitungshandelns mit sich. Die Interessen der Anteilseigner sollten insbesondere durch erfolgsabhängige Vergütungsmechanismen geschützt und die Unternehmensführung dementsprechend ausgerichtet werden. Das shareholder value-Modell, das dieses Problem aufwirft, hat seinen Ursprung in der Ökonomie und wurde bzw. wird hauptsächlich im Rahmen des Aktienrechts in Deutschland diskutiert.[15] Die zentrale Problematik dieser Diskursanalyse fokussiert sich auf die Fragestellung, welche Interessen das Leitungsgremium bei der Steuerung des Unternehmens zu berücksichtigen hat.[16] Der shareholder value-Ansatz fokussiert sich primär auf die Interessen der Anteilseigner, den sog. Agenten. Im Gegensatz dazu werden beim stakeholder value-Ansatz auch die Interessen anderer Gruppierungen berücksichtigt. Unter den Stakeholdern können neben den Anteilseignern auch Fremdkapitalgeber, Arbeitnehmer, Lieferanten, Gewerkschaften und staatliche Institutionen subsumiert werden.[17] Es wird argumentiert, dass die Interessen der Stakeholder ebenfalls Berücksichtigung finden müssen, da diese in ähnlicher Weise wie die Interessen der Anteilseigner mit Risiken für das Unternehmen verbunden sind.[18] Diese Ausrichtungsproblematik zählt zu den meist debattierten Fragestellungen im Bereich des Aktienrechts.[19] Die zentrale Fragestellung der Corporate Governance lässt sich jedoch dahingehend formulieren, dass sie stets die Zielsetzung einer effektiven und ausgewogenen Unternehmensführung und -organisation einschließlich der Überwachung im Fokus hat.[20] Die Terminologische Ausprägung ist in der Forschung vielseitig und reichen von Begriffen wie Unternehmensverfassung bis hin zu dem System der Unternehmensführung und -kontrolle. Obgleich eine direkte Übersetzung des Terminus Corporate Governance ins Deutsche nicht möglich ist, besteht weitgehender Konsens darüber, dass Corporate Governance die Etablierung einer nachhaltigen Organisationsstruktur anstrebt, die die divergierenden Interessen angemessen berücksichtigt.[21]

[13] vgl.Schug (Risikoeinschränkung und -transfer in der Vorstandshaftung, 2010), S. 48 f.
[14] vgl.Schug (Risikoeinschränkung und -transfer in der Vorstandshaftung, 2010), S. 46 f.
[15] vgl. Albrecht (Corporate Governance von Banken, 2016), S. 59
[16] vgl. Albrecht (Corporate Governance von Banken, 2016), S. 58 f.
[17] vgl.Albrecht (Corporate Governance von Banken, 2016), S. 60
[18] vgl. Werder (Führungsorganisationen - Grundlagen der Corporate Governance, Spitzen- und Leitungsorganisationen 2015), S. 9
[19] vgl.Hopt und Wohlmannstetter (Corporate Governance von Banken 2011), S. 10
[20] vgl.Hopt und Wohlmannstetter (Corporate Governance von Banken 2011), S. 4 ff.
[21] vgl.Albrecht (Corporate Governance von Banken, 2016), S. 58 ff.

2.1.1 Besondere Merkmale der Corporate Governance im Banksektor

Im Bereich des Finanzsektors zeigen sich verschiedene spezifische Eigenschaften in Bezug auf die Unternehmensführung und die Gestaltung der Corporate Governance. Ein deutlicher Unterschied offenbart sich bei der Betrachtung der Interessensgruppen einer Bank im Vergleich zu einem Unternehmen, das in einer anderen Branche tätig ist. Eine klassische Bank im Sinne eines Einlagenkreditinstituts hat - unabhängig von ihrer Rechtsform - verschiedene Interessensgruppen, darunter Eigenkapitalgeber, Arbeitnehmer, Gläubiger sowie Einleger,[22] die dem Institut durch Einzahlung auf ihr Konto (Fremd-) Kapital zur Verfügung stellen. Auf den ersten Blick scheint die Interessenlage der Einleger parallel zu der der Anteilseigner, die als Eigenkapitalgeber agieren, zu verlaufen. Beide Parteien geben der Bank Geld und beabsichtigen eine Rendite auf ihr eingesetztes Kapital zu erzielen. In Abhängigkeit von der jeweiligen Konstellation, streben beide Interessengruppen häufig danach, dass die Rendite höher ist als die anfängliche Investitionssumme. Bei näherer Betrachtung offenbart sich jedoch eine grundlegende Divergenz in der Ausgangslage der Investition.[23] Der Anteilseigner ist sich der inhärenten Risiken seiner Investition bewusst, einschließlich der Möglichkeit, sein investiertes Geld teilweise oder vollständig zu verlieren. Im Gegensatz dazu fühlt sich der Einleger in Sicherheit, was seine Einlage betrifft. Bis zur Finanzkrise 2007/2008 war es unwahrscheinlich, dass Bankkunden ernsthaft damit rechneten, ihr bei der Bank hinterlegtes Geld nicht zurückzuerhalten. Ferner verfügen Einleger im Vergleich zu Anteilseignern über weniger rechtlichen Schutz hinsichtlich der Informationen über das Unternehmen. Selbst wenn der Einleger die Möglichkeit der Bankinsolvenz berücksichtigt, hat er weniger effektive Informationsmechanismen zur Verfügung als der Anteilseigner. Dies ist partiell darauf zurückzuführen, dass der Einleger nicht integraler Bestandteil der internen Organisationsstruktur des Unternehmens ist, sondern vielmehr in der Rolle eines externen Akteurs agiert, der als Stakeholder betrachtet wird. Daher gibt es im Verhältnis zwischen Einleger und Institut eine noch ausgeprägtere Informationsasymmetrie als im Verhältnis zwischen Anteilseigner und Institut.[24] Dementsprechend erweitert sich der Kreis der Interessenträger, die bei der Corporate Governance von Banken zu berücksichtigen sind. Ein weiterer wichtiger Stakeholder, der zu einer Differenzierung der Corporate Governance von Banken führt, ist der Staat oder die Aufsichtsbehörde der Branche. Sofern die Aufsichtsinstanz

[22] vgl. Thaten (Die Ausstrahlung des Aufsichts- auf das Aktienrecht am Beispiel der Corporate Governance von Banken und Versicherungen 2016), S. 42 ff.
[23] vgl. Thaten (Die Ausstrahlung des Aufsichts- auf das Aktienrecht am Beispiel der Corporate Governance von Banken und Versicherungen 2016), S. 42 f.
[24] vgl.Bronnert-Härle (Aufsichtsratsausschüsse als neue Akteure der internen Corporate Governance von Banken, 2016), S. 56

in der Kapazität eines eigenständigen Stakeholders interpretiert wird, dessen Bedeutung für die Unternehmensführung von nicht regulierten Unternehmen marginal ist, lässt sich schlussfolgern, dass die Besonderheit des Finanzsektors in erster Linie durch diese Gegebenheit im Vergleich zu anderen Industriesektoren geprägt ist. Andererseits wird die Notwendigkeit der Aufsicht gerade damit begründet, dass von der wirtschaftlichen Bedeutung der Banken für das System eine Gefahr für die Allgemeinheit ausgeht, die durch das Gefahrenabwehrrecht eingedämmt werden soll.[25] Die Bedeutung des Bankensektors ergibt sich aus seiner Relevanz für die gesamte Volkswirtschaft. Banken fungieren als Vermittler von Kapital und ermöglichen den Wirtschaftsakteuren, Zugang zu Fremdkapital zu erhalten. Infolgedessen nehmen die Banken eine bedeutende Rolle bei der Corporate Governance der kreditnehmenden Unternehmen ein. Eine schlechte Corporate Governance bei den Banken kann sich auf andere Unternehmen auswirken, denn durch die Zurverfügungstellung von Finanzmitteln leisten die Banken einen wesentlichen Beitrag zum Wirtschaftswachstum.[26]

2.1.2 Corporate Governance Systeme

Im Vergleich der internationalen Corporate Governance-Systeme gibt es unterschiedliche Modelle zur Führung und Überwachung von Aktiengesellschaften. Ein grundlegendes Charakteristikum der Modelle besteht in der Zuweisung der Kontroll- und Leitungsbefugnisse auf die jeweiligen Organe. In dieser Betrachtung lassen sich zwei konträre Corporate Governance-Systeme identifizieren: das monistische sowie das dualistische System.[27] Im monistischen System, das vorwiegend im angelsächsischen Raum anzutreffen ist, werden die Leitungs- und Kontrollfunktionen in einem einzigen Organ vereint. Im Kontrast dazu findet in deutschen Aktiengesellschaften die Anwendung des dualistischen Systems statt, das eine klare Separation der Funktionen vorsieht.[28] Im nachfolgenden Abschnitt erfolgt eine theoretische Erläuterung des dualistischen Systems. Da sich diese wissenschaftliche Arbeit ausschließlich auf deutsche Aktiengesellschaften konzentriert, erfolgt eine Abgrenzung zum monistischen System.

[25] vgl.Boegl und Fischer (Aufsicht über Kredit- und Finanzdienstleistungsinstitute, 2017) § 125 Rn.19.
[26] vgl.Thaten (Die Ausstrahlung des Aufsichts- auf das Aktienrecht am Beispiel der Corporate Governance von Banken und Versicherungen 2016), S. 48 ff.
[27] vgl.Schewe (Unternehmensverfassung: Corporate Governance im Spannungsfeld von Leitung, Kontrolle und Interessenvertretung, 2018), S. 87
[28]vgl.Welge und Eulerich (Corporate- Governance- Management: Theorie und Praxis der guten Unternehmensführung, 2021), S. 37

2.1.2.1 *Dualistisches System*

Im Unterschied zum monistischen System, das ausschließlich ein Organ für Leitungs- und Kontrollfunktionen vorsieht, zeichnet sich das in deutschen Aktiengesellschaften praktizierte dualistische System durch eine dezidierte Separierung dieser beiden Aufgabenbereiche aus. Hierbei obliegt die Kontrollfunktion dem Aufsichtsrat und die Leitungsfunktion dem Vorstand der Aktiengesellschaft. Angesichts dieser klar differenzierten Aufgabenverteilung wird das dualistische System ebenfalls als "Two-Tier-System" bezeichnet.[29] Innerhalb des deutschen dualistischen Systems werden nicht alleinig die Belange der Aktionäre adressiert, sondern es werden darüber hinaus unternehmerische Mitbestimmungsmechanismen zur Besetzung des Aufsichtsrats implementiert, um die Anliegen der Arbeitnehmer einzubeziehen.[30]

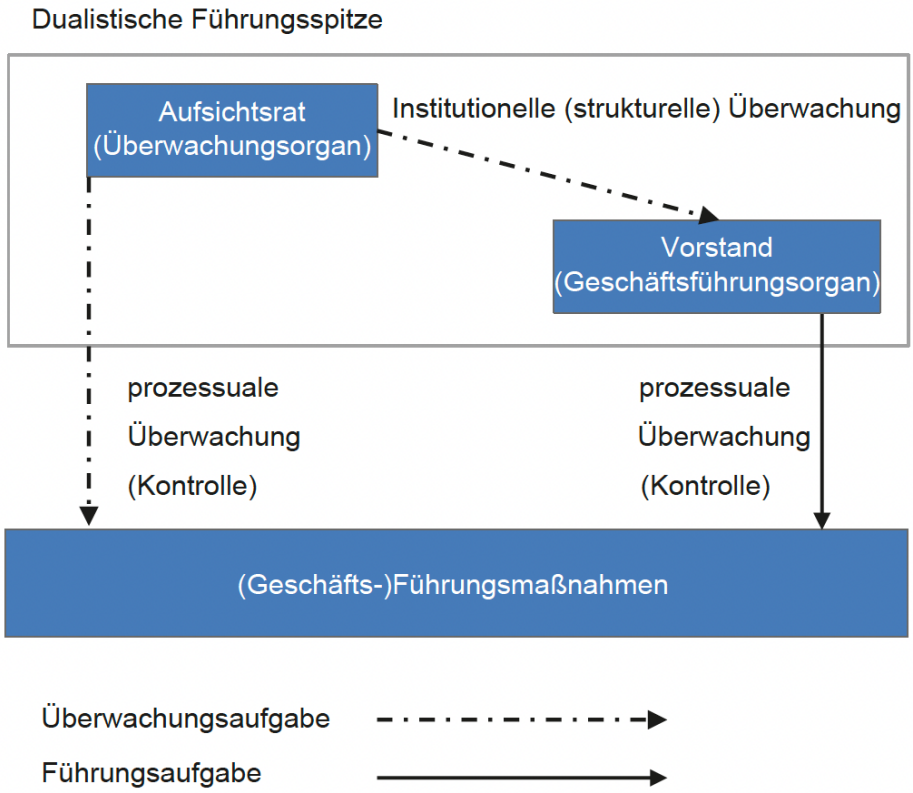


Abbildung 1: Führung und Überwachung im dualistischen System.[31]

Der Aufsichtsrat setzt sich aus Vertretern der Anteilseigner zusammen. In mitbestimmten Aufsichtsräten werden je nach Unternehmensgröße auch einzelne Mitglieder von Arbeitnehmern gewählt. Infolge der signifikanten Einflussnahme einer diversifizierten Anzahl von Interessengruppen, einschließlich Banken, Kunden und besonders Mitarbeitern, auf die

[29] vgl.Pönisch (Die Entwicklung des deutschen Systems der Coporate Governance Analyse und Entwicklungsdynamiken 2008), S. 20
[30] vgl. Pönisch (Die Entwicklung des deutschen Systems der Coporate Governance Analyse und Entwicklungsdynamiken 2008), S. 20
[31] Welge und Eulerich (Corporate- Governance- Management: Theorie und Praxis der guten Unternehmensführung, 2021), S. 40

Unternehmensführung, findet für dieses besagte Corporate Governance-System ebenfalls der Terminus "Managed Governance" Verwendung.[32] Die Diskrepanz zwischen Leitungs- und Kontrollinstanzen repräsentiert einen maßgeblichen Vorteil des dualistischen Systems und fungiert in gleichem Maße als Fördermittel für die Schaffung langanhaltender Beziehungen mit diversifizierten Stakeholdern, während auch ihre Anliegen berücksichtigt werden. Die strikte Scheidung von Führung und Kontrolle garantiert im Zuge seiner Überwachungsfunktionen die Autonomie des Aufsichtsrats.[33] Allerdings wird die Ausrichtung an den unterschiedlichen Interessen der Stakeholder kritisch betrachtet, da sie möglicherweise eine zielgerichtete Unternehmensführung erschweren kann. Zudem hängt die Effizienz der Aufsichtsratstätigkeiten in erheblichem Maße von der Beschaffenheit der Informationen ab, die vom Vorstand bereitgestellt werden.[34]

2.1.2.2 Organe im dualistischen System

Innerhalb des dualistischen Systems fallen die Zuständigkeiten für Führungs- und Überwachungsaufgaben verschiedenen Organen zu. Hierbei agiert der Vorstand als das exekutive Organ für die Unternehmensführung, während die Aufgabe der Kontrolle durch den Aufsichtsrat des Unternehmens wahrgenommen wird.[35]

2.1.2.2.1 Vorstand

Gemäß § 76 Abs. 1 AktG des dualistischen Systems obliegt es dem Vorstand als Geschäftsführungsorgan, die Gesellschaft eigenverantwortlich zu leiten, wodurch er nicht an Weisungen anderer Organe gebunden ist. Gemäß § 78 Abs. 1 S. 1 AktG ist der Vorstand sowohl für die gerichtliche als auch außergerichtliche Vertretung der Gesellschaft zuständig, wodurch er auch als Vertretungsorgan der Gesellschaft fungiert.[36] Die Handlungsfähigkeit der Aktiengesellschaft hängt maßgeblich vom Vorstand ab Gemäß den Bestimmungen des § 93 Abs. 1 und 2 des Aktiengesetzes ist der Vorstand rechtlich verpflichtet, bei der Ausführung seiner Geschäftsführung die Sorgfalt anzuwenden, die einem gewissenhaften und

[32] vgl. Paetzmann (Corporate Governance: Strategische Marktrisiken, Controlling, Überwachung, 2012), S. 36
[33] vgl.Mallin (Corporate Governance, 2019), S. 215
[34]vgl.Pönisch (Die Entwicklung des deutschen Systems der Coporate Governance Analyse und Entwicklungsdynamiken 2008), S. 26 und 44
[35]vgl.Welge und Eulerich (Corporate- Governance- Management: Theorie und Praxis der guten Unternehmensführung, 2021), S. 41
[36] vgl.Schindera (Die Kompetenzenverteilung der Organe einer Aktiengesellschaft im Übernahmeverfahren 2002), S. 50

verantwortungsbewussten Geschäftsleiter entspricht.[37] Die gesetzlich vorgeschriebenen Aufgaben des Vorstands betonen jedoch seine bedeutende Position innerhalb der Gesellschaft. Zu seinen Verantwortlichkeiten zählen unter anderem die Einberufung der Hauptversammlung gemäß § 121 Abs. 2 AktG, die Festlegung der Tagesordnung gemäß § 124 in Verbindung mit § 121 Abs. 2 AktG sowie die Vorbereitung und Durchführung von Hauptversammlungsbeschlüssen gemäß § 83 AktG. Darüber hinaus obliegen dem Vorstand beispielsweise die Organisation der Buchführung gemäß § 91 Abs. 1 AktG, die Einrichtung eines Überwachungssystems gemäß § 91 Abs. 2 AktG sowie die Berichterstattung gegenüber dem Aufsichtsrat gemäß § 90 AktG. Das Rechtssystem in Deutschland verankert grundsätzlich das Konzept des Gesamtführungsprinzips für den Vorstand, das gemäß § 77 Abs. 1 Satz 1 des Aktiengesetzes besagt, dass die Mitglieder des Vorstands nur gemeinschaftlich zur Geschäftsführung berechtigt sind.[38] Gleichwohl eröffnet Paragraph § 77 Abs. 1 S. 2 des Aktiengesetzes eine rechtliche Möglichkeit, die in der praktischen Umsetzung häufig genutzt wird, um mittels entsprechender Änderungen in der Satzung oder Geschäftsordnung von diesem grundlegenden Prinzip abzuweichen. Im Rahmen des Ressortprinzips haben die Vorstandsmitglieder die Befugnis, in den ihnen zugewiesenen Zuständigkeitsbereichen weitgehend eigenständige Entscheidungen zu treffen. Dennoch trägt jedes Mitglied des Vorstands trotz der Aufteilung der Ressorts eine Mitverantwortung für sämtliche Geschäftsführungsentscheidungen.[39] Die Befugnis des Vorstands zur Geschäftsführung kann gemäß § 82 Abs. 2 AktG durch die Satzung der Gesellschaft oder die Geschäftsordnung des Vorstands oder des Aufsichtsrats eingeschränkt werden. Zusätzlich können bestimmte geschäftliche Aktivitäten zustimmungspflichtig sein, dabei muss der Vorstand die Zustimmung des Aufsichtsrats einholen (§ 111 Abs. 4 AktG). Sofern die Satzung der Aktiengesellschaft keine abweichenden Regelungen enthält, liegt der vorrangige Zweck der Gesellschaft darin, Gewinne zu erzielen.[40] In Deutschland erfolgt die formelle Bestellung des Vorstands durch den gesamten Aufsichtsrat für einen Zeitraum von maximal fünf Jahren. Eine Wiederberufung ist erst ein Jahr vor Ablauf des Dienstvertrages des Vorstandsmitglieds zulässig (§ 84 Abs. 1 AktG). Die vorzeitige Abberufung des Vorstands erfordert die Existenz einer substantiellen Grundlage, wie etwa schwerwiegender Pflichtverletzungen, Unfähigkeit zur adäquaten

[37] vgl.Diederichs und Kißler (Aufsichtsratreporting: Corporate Governance, Compliance und Controlling 2008), S. 97
[38] vgl.Diederichs und Kißler (Aufsichtsratreporting: Corporate Governance, Compliance und Controlling 2008), S. 97
[39] vgl.Diederichs und Kißler (Aufsichtsratreporting: Corporate Governance, Compliance und Controlling 2008), S. 97
[40] vgl. Hirschmann (Aufgaben des Vorstandes als Leitungsorgan, 2005), S. 65

Geschäftsführung oder der Entzug des Vertrauens durch die Hauptversammlung gemäß § 84 Abs. 3 des Aktiengesetzes. Nach § 76 Abs. 2 Satz 2 AktG ist es gesetzlich vorgeschrieben, dass der Vorstand einer Aktiengesellschaft, die ein Grundkapital von mehr als drei Millionen Euro hat, aus mindestens zwei Mitgliedern bestehen muss. Diese Regelung kann jedoch durch die Satzung der Gesellschaft abweichend gestaltet werden. Die Festlegung der Anzahl der Vorstandsmitglieder wird üblicherweise in der Praxis gemäß den Vorgaben der Unternehmensgröße durch die Satzung verankert.[41] Der Deutsche Corporate Governance Kodex (DCGK) legt hinsichtlich der Zusammensetzung des Vorstands nahe, dass der Aufsichtsrat das Augenmerk auf Diversität legen und eine Altersbegrenzung für die Mitglieder des Vorstands etablieren soll.[42] Darüber hinaus wird empfohlen, dass die Erstbestellung von Vorstandsmitgliedern im Gegensatz zu den Bestimmungen des Aktiengesetzes für einen Zeitraum von höchstens drei Jahren erfolgt.[43] In Bezug auf Aktiengesellschaften, die unter das Mitbestimmungsgesetz oder das Montan-Mitbestimmungsgesetz fallen, ist es zwingend erforderlich, einen gleichberechtigten Arbeitsdirektor als Mitglied des Vorstands zu berufen. Der Arbeitsdirektor ist primär für soziale Themen und das Personalwesen verantwortlich.[44] Die Funktion des Vorstandsvorsitzenden nimmt in der ökonomischen Praxis eine herausragende Stellung ein, trotz der Tatsache, dass das Aktiengesetz keine konkret definierten Richtlinien für die Ernennung eines Vorstandsvorsitzenden vorsieht und keine Informationen über dessen rechtliche Positionierung bereitstellt. Bei einem Vorstand mit mehreren Mitgliedern kann der Aufsichtsrat gemäß § 84 Abs. 2 AktG frei darüber entscheiden, ob die Bestellung eines Vorstandsvorsitzenden erforderlich ist. Die herausgehobene Stellung des Vorstandsvorsitzenden in Bezug auf die Entwicklung der Aktiengesellschaft sowie deren öffentliche Wahrnehmung resultiert unter anderem aus den repräsentativen Aufgaben. Diese Aufgaben beinhalten die üblicherweise vom Vorstandsvorsitzenden übernommene Repräsentation der Gesellschaft bei Interaktionen mit Kunden, Geschäftspartnern und der allgemeinen Öffentlichkeit. Dies betont die Relevanz der Wahl einer geeigneten und überzeugenden Persönlichkeit für die Position des Vorstandsvorsitzenden.[45]

[41] vgl.Kuck (Aufsichtsräte und Beiräte in Deutschland: Rahmenbedingungen, Anforderungen, professionelle Auswahl, 2006), S. 22 f.
[42] vgl. Regierungskommission Deutscher Corporate Governance Kodex (Deutscher Corporate Governance Kodex 2022), B.1 und B.5
[43] vgl.Regierungskommission Deutscher Corporate Governance Kodex (Deutscher Corporate Governance Kodex 2022), B.3
[44] vgl.Gabler Wirtschaftslexikon (Montan-Mitbestimmungsgesetz (MontanMitbestG), o. J.)
[45]vgl.Welge und Eulerich (Corporate- Governance- Management: Theorie und Praxis der guten Unternehmensführung, 2021), S. 42

2.1.2.2.2 Aufsichtsrat

Innerhalb des dualistischen Systems fungiert der Aufsichtsrat in der Funktion des Kontroll- und Überwachungsorgans der Aktiengesellschaft. Neben seiner Kompetenz zur Berufung und Abberufung des Vorstands gemäß der Personalhoheit des Aufsichtsrats (§ 84 AktG, § 31 MitbestG) liegt sein vorrangiges Aufgabengebiet in der umfassenden Überwachung und Kontrolle der geschäftlichen Aktivitäten des Vorstands (§ 111 Abs. 1 AktG). In Übereinstimmung mit § 171 AktG obliegt es dem Aufsichtsrat auch, den Jahresabschluss und den Lagebericht zu prüfen. Durch seine Tätigkeit vertritt der Aufsichtsrat die Interessen der Anteilseigner und in Aufsichtsräten mit Mitbestimmung auch die Interessen der Mitarbeiter.[46] Im Einklang mit § 111 Abs. 4 Satz 2 des Aktiengesetzes besitzt der Aufsichtsrat das Privileg, ein Katalog von Geschäften zusammenzustellen, für die eine Zustimmung unabdingbar ist. Infolgedessen wird dem Kontrollgremium eine Form des Vetorechts oder eine unternehmerisch-politische Befugnis verliehen, die die Möglichkeit verschafft, aktiv auf die Geschäftsführung einzuwirken.[47] Der Aufsichtsrat erfüllt seine Kontroll- und Überwachungsaufgaben auf Grundlage von Berichten des Vorstands gemäß § 90 des Aktiengesetzes. Zusätzlich können sowohl der Prüfungsbericht des Abschlussprüfers als auch Erkenntnisse aus der internen Revision dem Aufsichtsrat zur Verfügung stehen, um eine Bewertung der Wirtschaftlichkeit, Rechtmäßigkeit, Ordnungsmäßigkeit und Zweckmäßigkeit der getroffenen Geschäftsführungsentscheidungen durchzuführen.[48]

2.2 Risikomanagement

Jede unternehmerische Entität ist einer Vielzahl von Risikofaktoren unterworfen, welche einer Identifikation, Bewertung, fortlaufenden Überwachung sowie Kontrolle bedürfen. Dieses Vorgehen ist essenziell, um potenzielle Bedrohungen für die Kontinuität der Geschäftsaktivitäten zu prävenieren. Gleichzeitig dient es der Generierung von Erträgen und der Steigerung des Unternehmenswerts.[49] Diese Aufgabe wird als Risikomanagement bezeichnet.[50] In der Betriebswirtschaftslehre wird der Implementierung eines umfassenden

[46] vgl. Schindera (Die Kompetenzenverteilung der Organe einer Aktiengesellschaft im Übernahmeverfahren 2002), S. 58
[47] vgl.Pönisch (Die Entwicklung des deutschen Systems der Coporate Governance Analyse und Entwicklungsdynamiken 2008), S. 41
[48] vgl. Diederichs und Kißler (Aufsichtsratreporting: Corporate Governance, Compliance und Controlling 2008), S. 100 f.
[49] vgl. Baums (Risiko und Risikosteuerung im Aktienrecht, 2011), S. 218, 225 ff.
[50] vgl.Romeike (Risikomanagement, 2018), S. 2 ff.

Risikomanagements eine bedeutende Rolle zugemessen,[51] da dieses sicherstellt, dass die Unternehmensleitung einen erforderlichen Überblick über die finanzielle Situation ihres Unternehmens hat und entsprechende Entscheidungen treffen kann.[52] Insbesondere im Bankensektor ist die Bedeutung eines umfassenden Risikomanagements aufgrund des risikoreichen Geschäftsmodells und der besonderen Merkmale dieses Sektors von großer Bedeutung.[53] Aus juristischer Sicht besteht sowohl im Aktienrecht als auch im Bankaufsichtsrecht die Forderung nach adäquaten organisatorischen und prozessualen Maßnahmen zur Risikobewältigung, wobei der Umfang dieser Forderungen variiert. Das Aktiengesetz gemäß § 91 Abs. 2 AktG schreibt für alle Aktiengesellschaften[54] die Implementierung eines Mechanismus zur frühzeitigen Identifikation von möglicherweise existenzgefährdenden Entwicklungen vor. Im Vergleich dazu fordert das Bankaufsichtsrecht gemäß §25a Abs. 1 Satz 3 KWG ein umfassendes Management von wesentlichen Risiken. Im Rahmen der vorliegenden Ausführung werden primär die rechtlichen Verpflichtungen im Bereich des Aktienrechts und anschließend im Bereich des Bankaufsichtsrechts erläutert.[55]

2.2.1 Aktienrechtliche Anforderungen

Gemäß § 91 Abs. 2 des Aktiengesetzes ist der (Gesamt-)Vorstand[56] verpflichtet, adäquate Schritte zu unternehmen und insbesondere ein Überwachungssystem zu etablieren, um potenzielle Entwicklungen zu erkennen, die eine Gefährdung der Beständigkeit des Unternehmens darstellen könnten. Mit der Implementierung des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)[57] wurde die betreffende Norm am 1. Mai 1998 in das Aktiengesetz aufgenommen. Diese Maßnahme seitens des Gesetzgebers erfolgte als Reaktion auf eine Reihe von Unternehmenskrisen und -skandalen, die sich in den 1990er-Jahren ereigneten.[58] Laut der Begründung der Regierung handelt es sich bei diesem Sachverhalt lediglich um eine Klarstellung einer bereits aus den §§ 76 Abs. 1 und 93 Abs. 1 des Aktiengesetzes hervorgehenden entsprechenden Organisationspflicht des Vorstands. Aus rechtstheoretischer Sicht kann § 91 Abs. 2 des Aktiengesetzes als eine normative Vorschrift

[51] vgl. Spindler (Vorstandspflichten zur Einrichtung eines Frühwarnsystems, 2006), § 19 Rn. 57
[52] vgl. Spindler (Vorstandspflichten zur Einrichtung eines Frühwarnsystems, 2006), § 19 Rn. 1
[53] vgl.International Monetary Fund (Global Financial Stability Report: Risk Taking, Liquidity, and Shadow Banking - Curbing Excess while Promoting Growth, 2014), S. 105, 107
[54] § 91 Abs. 3 AktG; vgl. infra § 6 B. II. 1. A. bb. (2)
[55] vgl.Ihrig und Schäfer (Rechte und Pflichten des Vorstands, 2014), §21 Rn. 570
[56] vgl.Ihrig und Schäfer (Rechte und Pflichten des Vorstands, 2014), §21 Rn. 570; Spindler (Vorstandspflichten zur Einrichtung eines Frühwarnsystems, 2006), §. 19 Rn. 5.
[57] vgl. Bundesgesetzblatt (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), 27. April 1998), S. 786
[58] vgl. Fleischer (Organisation; Buchführung, 2019), § 91 Rn. 29.

betrachtet werden, die zwei wesentliche Elemente enthält. Zum einen umfasst sie eine Zielvorgabe in Form der Früherkennung bestandsgefährdender Entwicklung. Zum anderen beinhaltet sie eine offene und allgemein formulierte Organisationsvorgabe, die darauf abzielt, dieses Ziel zu erreichen. Diese Organisationsvorgabe fordert das Ergreifen geeigneter Maßnahmen und insbesondere die Einrichtung eines Überwachungssystems.[59]

2.2.1.1 Zielvorgabe: Früherkennung bestandsgefährdender Entwicklungen

Die Maßnahmen, die der Vorstand zu ergreifen hat, müssen darauf ausgerichtet sein, bestandsgefährdende Entwicklungen zu identifizieren.[60] Der Begriff Entwicklungen bezieht sich in diesem Kontext auf Veränderungen und Prozesse, die konkrete, bereits im Zeitverlauf fortgeschrittene negative Entwicklungen darstellen. Es handelt sich dabei nicht um abstrakte Einzelrisiken oder statische Risikozustände.[61] Wie bereits aus dem Wortlaut hervorgeht, bezieht sich dieser Aspekt zudem nicht auf die frühzeitige Erkennung jeder nachteiligen Entwicklung, sondern ausschließlich auf jene Risiken, die eine potenzielle Gefährdung des Fortbestands des Unternehmens darstellen können.[62] Risiken, die als normale oder gewöhnliche Risiken einzustufen sind und unterhalb dieser Schwelle liegen, sind demnach nicht zu erfassen und müssen daher nicht zwangsläufig vom Vorstand frühzeitig erkannt werden.[63] Gemäß der rechtlichen Erläuterung des Gesetzes sind vor allem jene Aktivitäten gemeint, die mit Risiken behaftet sind, Fehler in der finanziellen Berichterstattung aufweisen und gegen rechtliche Bestimmungen verstoßen, welche potenziell erhebliche Auswirkungen auf die finanzielle Situation, die finanzielle Leistungsfähigkeit und die Ertragslage eines Unternehmens entfalten könnten.[64] Gemäß der vorherrschenden Auffassung lässt sich aus der Bezugnahme auf den Fortbestand der Gesellschaft ableiten, dass damit lediglich Risiken gemeint sind, die das Insolvenzrisiko des Unternehmens erheblich erhöhen oder hervorrufen.[65]

Demnach ist es nicht ausreichend, dass lediglich eine potenzielle Gefährdung der langfristigen Rentabilität der Gesellschaft vorliegt.[66] Solche Entwicklungen müssen in einem frühzeitigen Stadium erkannt werden. Das bedeutet, zu einem Zeitpunkt, an dem noch geeignete Schritte

[59] vgl. Bundesregierung (Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), BT-Drucks. 13/9712 1998), S. 15
[60] vgl. Spindler (Vorstandspflichten zur Einrichtung eines Frühwarnsystems, 2006), § 19 Rn. 8.
[61] vgl. Baums (Risiko und Risikosteuerung im Aktienrecht, 2011), S. 218, 251
[62] vgl.Fleischer (Organisation; Buchführung, 2019), § 91 Rn. 31
[63] vgl.Wundenberg (Compliance und die prinzipiengeleitete Aufsicht über Bankengruppen, 2012), S. 119
[64]vgl. Bundesregierung (Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), BT-Drucks. 13/9712 1998), S. 15
[65] vgl.Baums (Risiko und Risikosteuerung im Aktienrecht, 2011), S. 218, 251
[66] vgl. Zimmer und Sonneborn (§ 91 Abs. 2 - Anforderungen und gesetzgeberische Absichten 2001), § 1 Rn. 182.

unternommen werden können, um die Kontinuität des Unternehmens zu gewährleisten und die möglicherweise riskante Entwicklung abzuwenden.[67]

2.2.1.2 Zielvorgabe: Geeignete Maßnahmen und Einrichtung eines Überwachungssystems

Um eine rechtzeitige Erkennung von Entwicklungen, die den Fortbestand der Gesellschaft gefährden können, sicherzustellen, ist es gemäß § 91 Abs. 2 des Aktiengesetzes Aufgabe des Vorstands, "geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten"[68]. Somit fordert diese Bestimmung lediglich die Implementierung eines Risikofrüherkennungssystems und nicht eines umfassenden Risikomanagementsystems.[69]

Zur Umsetzung der Organisationsvorgabe des § 91 Abs. 2 des Aktiengesetzes ist ein zweistufiges Vorgehen erforderlich.[70] In der ersten Stufe muss durch die Umsetzung von geeigneten Maßnahmen sichergestellt werden, dass der Vorstand die erforderlichen Informationen über potenziell bestandsgefährdende Entwicklungen rechtzeitig erhält.[71] Zu diesem Zweck erfordert es zunächst die Durchführung einer Risikoinventur, bei der die Ergebnisse an den Vorstand weitergeleitet werden müssen. Organisatorisch wird dies als Verpflichtung zur Einrichtung eines unternehmensweiten Informationssystems interpretiert, das alle relevanten Daten zur Früherkennung potenziell bestandsgefährdender Entwicklungen sammelt, aufbereitet und zeitnah an den Vorstand weiterleitet.[72] Um die fortlaufende Wirksamkeit dieses Systems zur Früherkennung von Risiken zu gewährleisten, ist es in der zweiten Stufe erforderlich, das vom § 91 Abs. 2 des Aktiengesetzes erwähnte Überwachungssystem einzurichten.[73] Mit diesem Begriff sind die unternehmensinternen Kontrollen gemeint, die sicherstellen, dass die angeordneten Maßnahmen tatsächlich umgesetzt werden und ihre Ziele erreichen. Es besteht jedoch keine rechtliche Verpflichtung, ein ganz bestimmtes System auszuwählen.[74] Bei Unternehmen von einer bestimmten Größenordnung wird jedoch die Einrichtung einer internen Revision sowie einer Risikocontrolling-Funktion empfohlen.[75] Des Weiteren ist es bedeutend, klare Zuordnungen von Verantwortlichkeiten und Aufgaben unter Berücksichtigung des Prinzips der Funktionstrennung sicherzustellen. Es wird geraten, ein umfassendes Berichtswesen einzurichten und angemessene

[67] vgl. Ihrig und Schäfer (Rechte und Pflichten des Vorstands, 2014), § 21 Rn. 575
[68] § 91 Abs. 2 AktG
[69] vgl.Fleischer (Organisation; Buchführung, 2019), § 91 Rn. 33
[70] vgl. Ihrig und Schäfer (Rechte und Pflichten des Vorstands, 2014), § 21 Rn. 573 ff.
[71] vgl.Fleischer (Organisation; Buchführung, 2019), § 91 Rn. 33
[72] vgl.Ihrig und Schäfer (Rechte und Pflichten des Vorstands, 2014), § 21 Rn. 575 f.
[73] vgl.Zimmer und Sonneborn (§ 91 Abs. 2 - Anforderungen und gesetzgeberische Absichten 2001), § 1 Rn. 187
[74] vgl.Fleischer (Organisation; Buchführung, 2019), § 91 Rn. 31
[75] vgl.Ihrig und Schäfer (Rechte und Pflichten des Vorstands, 2014), §21 Rn. 576

Dokumentationspflichten festzulegen.[76] Hierbei ist es erforderlich, eine angemessene Ausstattung mit finanziellen und personellen Ressourcen sicherzustellen.[77] Die konkrete Umsetzung der genannten zwei Stufen durch den Vorstand ist jedoch von Fall zu Fall unterschiedlich. Dabei ist es entscheidend, dass die unternehmensspezifischen Markt- und Risikobedingungen berücksichtigt werden respektive der Größe und Struktur des Unternehmens, der Branche und ihrer spezifischen Merkmale sowie des Zugangs des Unternehmens zum Kapitalmarkt.[78] Bei der konkreten Umsetzung steht dem Vorstand jedoch ein erheblicher Spielraum des Ermessens zur Verfügung.[79] Aus rechtlicher Perspektive ergibt sich bereits hieraus, dass die Verpflichtung des Vorstands zur Gewährleistung einer angemessenen Unternehmensorganisation, wie bereits in der Begründung des Gesetzes hervorgehoben, nicht durch § 91 Absatz 2 des Aktiengesetzes begründet wird. Vielmehr ist sie eine Ableitung aus der allgemeinen Leitungsaufgabe gemäß §§ 76 Absatz 1, 93 Absatz 1 des Aktiengesetzes.[80]

2.2.2 Bankaufsichtsrechtliche Anforderungen

Die Integration der internen Corporate Governance steht eng in Verbindung mit den Eigenkapitalanforderungen der Säule 1 des Basler Rahmenwerks.[81] Während das Hauptziel von Säule 1 darin besteht, standardisierte Eigenkapitalanforderungen für eine Vielzahl von Banken zu formulieren, ergänzt Säule 2 diese durch einen unternehmensspezifischen und gleichzeitig umfassenderen Ansatz zur Betrachtung aller wesentlichen Risiken und der verfügbaren Mittel zu ihrer Absicherung.[82] Die Identifizierung dieser Risiken sowie die Berechnung der erforderlichen Eigenmittel zur Absicherung obliegen den Kreditinstituten selbst. Um sicherzustellen, dass sie dieser Verantwortung sachgerecht nachkommen, müssen Kreditinstitute gemäß § 25a Abs. 1 Satz 3 Hs. 1 KWG über eine adäquate Geschäftsstruktur aufweisen, die insbesondere ein angemessenes und effizientes Risikomanagement einschließt. Auf Grundlage dieser Anforderungen sind die Kreditinstitute verpflichtet, ihre Risikotragfähigkeit kontinuierlich sicherzustellen. Das Aufsichtsrecht definiert ebenfalls qualitative Mindestanforderungen, die ein adäquates und effektives Risikomanagement

[76] vgl.Fleischer (Organisation; Buchführung, 2019), § 91 Rn. 36
[77] vgl.Baums (Risiko und Risikosteuerung im Aktienrecht, 2011), S. 218, 274
[78]vgl.Bundesregierung (Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), BT-Drucks. 13/9712 1998), S. 15
[79] vgl.Ihrig und Schäfer (Rechte und Pflichten des Vorstands, 2014), § 21 Rn. 575.
[80] vgl.Bundesregierung (Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), BT-Drucks. 13/9712 1998), S. 15
[81] Zur „janusköpfigen Zielrichtung“ der Corporate Governance-Regierung vgl. supra § 5 A. III.
[82] vgl.Deutsche Bank (Monatsbericht März 2013, 2013), S. 31, 32

einschließen. Gemäß § 25a Abs. 1 Satz 3 Halbsatz 2 KWG umfasst dies auf strategischer Ebene die Formulierung einer Geschäfts- und Risikostrategie sowie auf organisatorischer Ebene die Etablierung von internen Kontrollverfahren mittels eines internen Kontrollsystems und einer internen Revision.[83] Das organisatorische Leitbild, das dabei Anwendung findet, ist das sogenannte Modell der drei Verteidigungslinien ("three lines of defense").[84] Die erste Verteidigungslinie besteht aus den einzelnen operativen Geschäftseinheiten, während die zweite Verteidigungslinie spezielle, prozessabhängige Kontrollfunktionen wie Risikocontrolling und Compliance umfasst. Die dritte Verteidigungslinie wird von der prozessunabhängigen internen Revision gebildet, die die Effektivität der ersten beiden Verteidigungslinien überprüft.[85] Diese Kernelemente existieren nicht isoliert nebeneinander, sondern stehen in einer wechselseitigen Abhängigkeit zueinander.[86] Die im Folgenden zu diskutierenden Anforderungen sollten entsprechend als interne Prozesskette verstanden werden.[87] Die eher allgemein formulierten Anforderungen gemäß § 25a KWG werden durch das Rundschreiben Mindestanforderungen an das Risikomanagement (MaRisk)[88] der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) konkretisiert. Dieses Rundschreiben wird von der BaFin selbst als zentraler Baustein für die qualitative Aufsicht[89] bezeichnet. Gemäß § 25a Abs. 1 Satz 4 KWG stehen sämtliche Anforderungen an das Risikomanagement von Banken zudem unter dem Vorbehalt der Proportionalität.[90]

2.3 Compliance

Der Terminus „Compliance“ hat seine Wurzel aus dem angelsächsischen Raum und kann von dem Verb "to comply (with)" abgeleitet werden.[91] Aus einer linguistischen Perspektive aus betrachtet, kann der Begriff Compliance als Befolgung, Einhaltung, Erfüllung oder Folgsamkeit interpretiert werden.[92] Dabei wird das Verhalten im Rahmen der Corporate Compliance bezeichnet, das in Übereinstimmung mit den für das Unternehmen geltenden

[83] § 25a Abs.1 S.3 KWG; § 25b KWG; § 25b Abs.2 KWG;
[84] vgl. EBA (Final Report - Guidelines on internal governance under Directive 2013/36/EU, 2017), S. 66
[85] §§ 25a Abs. 1 S. 3 Nr. 3 lit. b, 25c Abs. 4a Nr. 3 lit. c KWG
[86] vgl. Mülbert und Wilhelm (Risikomanagement und Compliance im Finanzmarktrecht: Entwicklung der aufsichtsrechtlichen Anforderungen, 2014), S. 502, 508
[87] vgl.Hannemann u.a. (Mindestanforderungen an das Risikomanagement (MaRisk), 2019), AT 4.3.2 Rn. 2
[88] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (Rundschreiben 10/2021 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk, 2021)
[89] Bundesanstalt für Finanzdienstleistungsaufsicht (Rundschreiben 18/2005 - Mindestanforderungen an das Risikomanagement, 20.12.2005)
[90] Zum Proportionalitätsgrundsatz vgl. bereits supra § 5 A. II. 2. a. bb.
[91] vgl.Goette (Organisationspflichten in Kapitalgesellschaften zwischen Rechtspflicht und Opportunität, 2011), S. 388, 390
[92] vgl.Gabler Wirtschaftslexikon (Compliance, o. J.)

Gesetzen erfolgt.[93] Die Compliance-Funktion hat zum Ziel, den Risiken entgegenzuwirken, die mit der Nichtbefolgung gesetzlicher Bestimmungen einhergehen könnten.[94] Wie von der BaFin deutlich betont wird, bedeutet die allgemeine Compliance-Verpflichtung, dass alle gesetzlichen Bestimmungen und Vorgaben zu beachten sind. Es impliziert jedoch nicht, dass alle Rechtsbereiche gleichermaßen von der spezifisch einzurichtenden Compliance-Funktion abgedeckt werden müssen.[95] Im Rahmen des Regulierungszwecks soll sich die Compliance-Funktion vielmehr auf spezifische rechtliche Bestimmungen konzentrieren, die mit wesentlichen Compliance-Risiken verbunden sind.[96] Diese Risiken zeichnen sich insbesondere dadurch aus, dass bei Nichteinhaltung der rechtlichen Regelungen und Vorgaben vor allem Geldstrafen, Bußgelder, Schadenersatzansprüche und/oder die Nichteinhaltung von Verträgen drohen. Diese potenziellen Risiken sind hauptsächlich dadurch gekennzeichnet, dass bei Nichtbefolgung der rechtlichen Vorschriften und Vorgaben vornehmlich Sanktionen wie Bußgelder, Geldstrafen, Schadenersatzansprüche und/oder Vertragsverletzungen drohen. Diese Konsequenzen können eine potenzielle Bedrohung für das Vermögen des Instituts darstellen. Bei diesen Anforderungen handelt es sich in jedem Fall um spezifische gesetzliche Vorgaben, wie beispielsweise das Kreditwesengesetz (KWG), das Wertpapierhandelsgesetz (WpHG), die Verordnung über die Aufsichtsanforderungen an Kreditinstitute (CRR-VO), Vorschriften zur Geldwäscheprävention sowie Bestimmungen zum Verbraucherschutz. Weitere rechtliche Vorschriften, die von der Compliance-Funktion abgedeckt werden müssen, sind von den Banken eigenverantwortlich im Hinblick auf ihre spezifischen geschäftlichen Aktivitäten zu identifizieren. Daher kommt der vorherigen Erfassung und Analyse potenzieller Compliance-Risiken eine entscheidende Bedeutung zu.[97] Im Hinblick auf die organisatorische Integration der Compliance-Funktion ist die Gestaltungsfreiheit der Banken teilweise begrenzt.[98] Die Compliance-Funktion soll grundsätzlich direkt dem Vorstand unterstellt werden und hat diesem gegenüber mindestens einmal jährlich sowie bei Bedarf Bericht zu erstatten.[99] gemäß AT 4.4.2 Tz. 4 der MaRisk sind systemrelevante Banken verpflichtet[100], eine dedizierte Organisationseinheit für diese Zwecke einzurichten. Nicht-systemrelevante Banken haben

[93] vgl. Goette (Organisationspflichten in Kapitalgesellschaften zwischen Rechtspflicht und Opportunität, 2011), S. 388, 390
[94] AT 4.4.2 Tz. 1 MaRisk.
[95] vgl.Bundesanstalt für Finanzdienstleistungsaufsicht (Protokoll zur Sitzung des Fachgremiums MaRisk am 24.4.2013 in Bonn, Thema: Compliance-Funktion, 2013), S. 1
[96] AT 4.4.2 Tz 2 MaRisk.
[97] vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Protokoll zur Sitzung des Fachgremiums MaRisk am 24.4.2013 in Bonn, Thema: Compliance-Funktion, 2013), S. 1 ff.
[98] vgl.Mülbert und Wilhelm (Risikomanagement und Compliance im Finanzmarktrecht: Entwicklung der aufsichtsrechtlichen Anforderungen, 2014), S. 502, 523
[99] At 4.4.2 Tz. 3, 7 MaRisk
[100] Zur rechtlichen Bindungswirkung der MaRisk vgl. infra § 7 B. II 2. a. aa. (1).

grundsätzlich die Möglichkeit, selbst zu entscheiden, ob sie eine separate Organisationseinheit schaffen möchten oder die Compliance-Funktion an eine bestehende Einheit anbinden. Es ist jedoch zu beachten, dass die BaFin von größeren Banken die Einrichtung einer eigenständigen Einheit erwartet.[101] Für die Anbindung der Compliance-Funktion kommen verschiedene Möglichkeiten in Betracht respektive das Risikocontrolling, die Rechtsabteilung oder die Integration in bereits bestehende Compliance-Strukturen, die aufgrund der wertpapierrechtlichen Compliance (WpHG / MaComp) einzurichten sind.[102] Im Kontext des Proportionalitätsgesetzes, wie es in § 25a Abs. 1 S. 4 KWG zum Ausdruck kommt, ist es für kleinere Banken nicht zwingend erforderlich, eine separate und eigenständige Stelle zu schaffen. Es ist jedoch wichtig zu beachten, dass eine Anbindung an die interne Revision oder an die Vertriebsstrukturen unzulässig ist.[103] Eine zulässige und effiziente Option besteht darin, ein kombiniertes Risiko- und Compliance-Management zu etablieren. Des Weiteren muss eine Person als Compliance-Beauftragten benannt werden, der für die Aufgaben der Compliance-Funktion verantwortlich ist.[104] Das Aufgabenspektrum der Compliance-Funktion im Umgang mit Compliance-Risiken ergibt sich grundsätzlich direkt aus den gesetzlichen Bestimmungen. Gemäß § 25a Abs. 1 S.3 Nr. 3 c KWG ist die Compliance-Funktion ein integraler Bestandteil des internen Kontrollsystems, so des Risikomanagements. Diese Regelung ist in Bezug auf die Rechtsrisiken konsequent, da sie eine Form des operationellen Risikos darstellen. Die Hauptaufgabe der Compliance-Funktion kann dementsprechend als rechtliches Risikomanagement beschrieben werden und folgt damit der gleichen Funktionslogik wie das Management anderer wesentlicher Risiken.[105] Rechtsrisiken müssen daher sowohl auf strategischer Ebene des Risikomanagements als auch im Rahmen der Risikoinventur und bei der Festlegung der Risikotragfähigkeit berücksichtigt werden.[106] Eine Konkretisierung des Aufgabenspektrums der Compliance-Funktion lässt sich anhand der AT 4.4.2 Tz. 1 der Mindestanforderungen an das Risikomanagement (MaRisk) vornehmen. Gemäß dieser Regelung liegt es in der Verantwortung der Compliance-Funktion, darauf hinzuwirken, dass wirksame Prozesse zur Einhaltung der für das Institut relevanten rechtlichen Vorschriften und

[101] vgl.Bundesanstalt für Finanzdienstleistungsaufsicht (Protokoll zur Sitzung des Fachgremiums MaRisk am 24.4.2013 in Bonn, Thema: Compliance-Funktion, 2013), S. 3
[102] vgl. Mülbert und Wilhelm (Risikomanagement und Compliance im Finanzmarktrecht: Entwicklung der aufsichtsrechtlichen Anforderungen, 2014), S. 502, 524 ff.
[103] vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Protokoll zur Sitzung des Fachgremiums MaRisk am 24.4.2013 in Bonn, Thema: Compliance-Funktion, 2013), S. 3 f.
[104] vgl.Mülbert und Wilhelm (Risikomanagement und Compliance im Finanzmarktrecht: Entwicklung der aufsichtsrechtlichen Anforderungen, 2014), S. 502, 523 f.
[105] vgl.Mülbert und Wilhelm (Risikomanagement und Compliance im Finanzmarktrecht: Entwicklung der aufsichtsrechtlichen Anforderungen, 2014), S. 502, 521
[106] vgl. Hannemann u.a. (Mindestanforderungen an das Risikomanagement (MaRisk), 2019), AT 4.4.2 Rn. 17 f.

Vorgaben etabliert werden, und die entsprechenden Überprüfungen durchgeführt werden. Aus dem Wortlaut dieser Regelung geht bereits hervor, dass die Einführung wirksamer Verfahren zur Einhaltung der gesetzlichen Vorschriften nach wie vor als Verantwortung der jeweiligen Fachbereiche vorgesehen ist und nicht automatisch der Compliance-Funktion übertragen wird. Die Compliance-Funktion übernimmt vielmehr eine koordinierende Rolle und ist dafür verantwortlich sicherzustellen, dass die Fachbereiche ihren Verpflichtungen nachkommen und es nicht zu einer Vernachlässigung bestimmter Rechtsbereiche aufgrund unklarer Zuständigkeiten kommt.[107] Zu diesem Zweck obliegt es der Compliance-Funktion, die internen Abläufe des Instituts zu bewerten, deren Qualität und Angemessenheit sicherzustellen sowie eine kontinuierliche Überwachung durchzuführen.[108] Dies beinhaltet ebenfalls die Ausarbeitung von Compliance-Grundsätzen innerhalb der Bank und deren Kommunikation auf Unternehmensebene.[109] Es besteht die Verpflichtung zur Berichterstattung gegenüber dem Vorstand, dem Aufsichtsrat und der internen Revision.[110] Die Compliance-Funktion unterstützt und berät den Vorstand bei der Einhaltung der relevanten rechtlichen Regelungen und Vorgaben.[111] Dabei liegt die Letztverantwortung für die Einhaltung der rechtlichen Vorgaben weiterhin beim Vorstand. Um ihre Kontrollfunktion gegenüber den einzelnen Fachbereichen angemessen ausüben zu können, bedarf es der Einräumung entsprechender Kontrollrechte an die Compliance-Funktion.[112] Zur umfassenden Compliance gehört auch die Verpflichtung gemäß § 25a Abs. 1 Satz 4 Nr. 3 KWG zur Implementierung eines sogenannten Whistleblowing-Systems. Dieses System ermöglicht es den Mitarbeitern, Verstöße gegen das KWG, die CRR-VO oder Strafgesetz an eine geeignete Stelle zu melden.[113]

[107] vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (Protokoll zur Sitzung des Fachgremiums MaRisk am 24.4.2013 in Bonn, Thema: Compliance-Funktion, 2013), S. 3
[108] vgl. Bundesregierung (Entwurf eines Gesetzes zur Umsetzung der Richtlinie 2012/.../EU über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen und zur Anpassung des Aufsichtsrechts an die Verordnung (EU) Nr. .../2012 über die Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen (CRD IV-Umsetzungsgesetz), BT-Drucks. 17/10974, 2012), S. 85
[109] vgl. Gebauer und Niermann (Compliance in der Banken- und Wertpapierdienstleistungsbranche, 2016), § 48 Rn. 52 ff.
[110] AT 4.4.2 Tz. 6 MaRisk
[111] AT 4.4.2 Tz. 1 Satz 3 MaRisk
[112] vgl.Bundesanstalt für Finanzdienstleistungsaufsicht (Protokoll zur Sitzung des Fachgremiums MaRisk am 24.4.2013 in Bonn, Thema: Compliance-Funktion, 2013), S. 3
[113] vgl.Mülbert und Wilhelm (Risikomanagement und Compliance im Finanzmarktrecht: Entwicklung der aufsichtsrechtlichen Anforderungen, 2014), S. 502, 524

2.3.1 Aktienrechtliche Anforderungen

Im Vergleich zum Bankaufsichtsrecht findet sich im Aktienrecht keine ausdrückliche Äußerung zur Verantwortung des Vorstands in Bezug auf Compliance.[114] Erste Ansätze zur Ableitung der Compliance-Verantwortung des Vorstands stützten sich auf eine Gesamtanalogie zu den einzelnen Compliance-Vorschriften in verschiedenen Rechtsgebieten.[115] Angeführt werden zum Beispiel §14 GwG, § 130 OWiG und § 91 Abs. 2 AktG, § 25a KWG und § 33 WpHG.[116] Jedoch gibt es Einwände gegen diese Gesamtanalogie, da die einzelnen bereichsspezifischen Compliance-Vorschriften äußerst unterschiedliche Schutzziele verfolgen und die einzelnen Verpflichtungen teilweise speziell auf bestimmte Branchen zugeschnitten sind.[117] Auch eine isolierte Anwendung der Analogie auf § 91 Abs. 2 des Aktiengesetzes kann nicht überzeugend begründet werden.[118] In der Begründung zur Norm heißt es, dass Verstöße gegen gesetzliche Vorschriften zu den Risikobereichen gehören, die die Existenz des Unternehmens gefährden können.[119] Jedoch erfüllen Compliance-Verstöße nur selten die Voraussetzung eines Tatbestandsmerkmals einer potenziell existenzbedrohenden Entwicklung, wodurch bereits das erforderliche vergleichbare Interessenverhältnis für eine Analogie fehlt.[120] Ein effektives Compliance-System muss in einem umfassenderen Rahmen gestaltet sein und sicherstellen, dass regelkonformes Verhalten unabhängig von einer potenziellen Gefährdung der Unternehmensbestände gewährleistet wird.[121] Daher ist es überzeugender, die Verantwortung des Vorstands für Compliance aus der allgemeinen Leitungs- und Sorgfaltspflicht gemäß den Bestimmungen von §§ 93 Abs. 1 und 76 Abs. 1 des Aktiengesetzes abzuleiten.[122] Wie bereits zuvor erörtert, beinhaltet die Sorgfaltspflicht des Vorstands aufgrund der zulässigen Delegation auch eine Verpflichtung zur Überwachung der nachgeordneten Mitarbeiter.[123] Es besteht Einigkeit darüber, dass der Vorstand im Falle der Delegation nicht von seinen entsprechenden Verpflichtungen entbunden wird, sondern dass sich diese Verpflichtungen in eine Pflicht zur

[114] vgl. Spindler (Compliance in der multinationalen Bankengruppe, 2008), S. 905
[115] vgl. Schneider (Compliance als Aufgabe der Unternehmensleitung, 2003), S. 645, 648 f.
[116] Schneider (Compliance als Aufgabe der Unternehmensleitung, 2003), S. 645, 649
[117] vgl. Bachmann (Compliance – Rechtsgrundlagen und offene Fragen, 2008), S. 65, 74 f.
[118] vgl. Spindler (Compliance in der multinationalen Bankengruppe, 2008), S. 905, 906
[119] vgl.Bundesregierung (Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), BT-Drucks. 13/9712 1998), S. 15
[120]vgl. Verse (Compliance im Konzern: Zur Legalitätskontrollpflicht der Geschäftsleiter einer Konzernobergesellschaft, 2011), S. 401, 403 f.
[121] vgl.Ihrig und Schäfer (Rechte und Pflichten des Vorstands, 2014), § 22 Rn. 590
[122] vgl. Goette (Organisationspflichten in Kapitalgesellschaften zwischen Rechtspflicht und Opportunität, 2011), S. 288, 392; vgl. Verse (Compliance im Konzern: Zur Legalitätskontrollpflicht der Geschäftsleiter einer Konzernobergesellschaft, 2011), S. 401, 404
[123] vgl. supra § 6 B. I. 2. c.

gewissenhaften Auswahl, Einarbeitung und Überwachung des Delegationsempfängers umwandeln.[124]

2.3.2 Bankaufsichtsrechtliche Anforderungen

Im Gegensatz zum Aktiengesetz gibt das Bankaufsichtsrecht explizite Anweisungen zum Thema Compliance. Gemäß § 25a Abs. 1 Satz 1 KWG muss die ordnungsgemäße Geschäftsorganisation sicherstellen, dass die gesetzlichen Bestimmungen, die das Institut befolgen muss, eingehalten werden. Darüber hinaus muss das interne Kontrollsystem gemäß § 25a Abs. 1 S. 3 lit. c KWG eine Compliance-Funktion umfassen.[125] Gemäß § 25a Abs. 1 S. 3 Nr. 3 lit. c KWG besteht eine Verpflichtung für den Bankvorstand, eine spezielle Compliance-Funktion einzurichten. Die Notwendigkeit einer solchen Funktion war vor der Einführung dieser Vorschrift durch das CRD IV-Umsetzungsgesetz umstritten, fand jedoch in der vorherrschenden Meinung auch ohne ausdrückliche gesetzliche Anordnung Zustimmung.[126] Die Anforderungen an die Compliance-Funktion werden nun auch durch die MaRisk konkretisiert (AT 4.4.2). Für die Interpretation dieser Anforderungen wird in der Praxis auf ein Protokoll einer speziellen Sondersitzung des Fachgremiums MaRisk zurückgegriffen. Dieses Protokoll enthält Informationen über die Compliance-Risiken, das spezifische Aufgabenspektrum der Funktion sowie deren organisatorische Integration.[127]

[124] vgl. Fleischer (Organisation; Buchführung, 2019), § 91 Rn. 100 ff.
[125] vgl.Mülbert und Wilhelm (Risikomanagement und Compliance im Finanzmarktrecht: Entwicklung der aufsichtsrechtlichen Anforderungen, 2014), S. 502, 520
[126] vgl. Wundenberg (Compliance und die prinzipiengeleitete Aufsicht über Bankengruppen, 2012), S. 106 f.
[127] vgl.Bundesanstalt für Finanzdienstleistungsaufsicht (Protokoll zur Sitzung des Fachgremiums MaRisk am 24.4.2013 in Bonn, Thema: Compliance-Funktion, 2013)

3 Das Three-Lines-of-Defense-Modell

Die Erkenntnisse aus der Finanzkrise haben verdeutlicht, dass ein effektives Kontroll- und Überwachungssystem von entscheidender Bedeutung für den Unternehmenserfolg ist. Infolgedessen konzentriert sich die aktuelle Diskussion zur Corporate Governance auf die Gestaltung des Kontroll- und Überwachungssystems innerhalb einzelner Unternehmen sowie auf die Ausgestaltung ihrer "Organizational Governance".[128] Die Zielsetzung einer effektiven ihrer "Organizational Governance" besteht daher darin, die verschiedenen Unternehmensorgane innerhalb des Unternehmens so miteinander zu verbinden, dass ein umfassendes und funktionsfähiges Kontroll- und Überwachungssystem entsteht. Dabei sollen die einzelnen Aufgabenstellungen und ihre Schnittstellen klar definiert werden. Die Ausgestaltung dieses Kontroll- und Überwachungssystems basiert auf den regulatorischen Rahmenbedingungen der jeweiligen nationalen oder internationalen Rechtsprechungen. Die EU-Kommission hat beispielsweise mehrere Grünbücher veröffentlicht, die sich mit dieser Thematik befassen. Durch diese Grünbücher wurde der Fokus von klassischen Governance-Organen wie dem Board und der Beziehung zum Abschlussprüfer auf weitere Governance-Organe und deren Beziehungen untereinander erweitert. Die interne Revision entwickelt sich mit ihren Verbindungen zum Audit Committee und dem Austausch mit dem Abschlussprüfer zunehmend zu einem integralen Bestandteil der Governance-Organe.[129] Die Integration der Zustimmung zur erarbeiteten Risikopositionierung des Unternehmens in die Aufgaben des Board stellt eine zusätzliche Ausweitung des Kontroll- und Überwachungssystems dar.[130] Damit erfährt das Regelwerk eine wesentliche Erweiterung, die zwar noch nicht rechtskräftig umgesetzt ist, aber bereits heute für die Unternehmen richtungsweisend ist. Angesichts dieser Herausforderung stellt sich die Frage nach einem adäquaten Handlungsrahmen für die Ausweitung der "Organizational Governance". Das Three-Lines-of-Defense-Modell, das im Banken- und Finanzsektor Anwendung findet, bietet die Möglichkeit, einen allgemeingültigen Handlungsrahmen zu schaffen. Dieser Rahmen zeigt auf, wie die einzelnen Governance-Organe innerhalb ihres Kontroll- und Überwachungssystems strukturiert werden können und wie die Schnittstellen koordiniert werden sollten.[131] Die nachfolgende Abbildung gibt einen Überblick über die Struktur dieses Handlungsrahmens.

[128] vgl.Eulerich (Das Three Lines of Defence-Modell 2012), S. 1
[129] vgl.Europäische Kommission (EU-Greenbook: Corporate Governance in Finanzinstituten und Vergütungspolitik, 2010), S. 9
[130] vgl.Europäische Kommission (EU-Greenbook: Europäischer Corporate Governance Rahmen, 2011), S. 9
[131] vgl.Eulerich (Das Three Lines of Defence-Modell 2012), S. 1

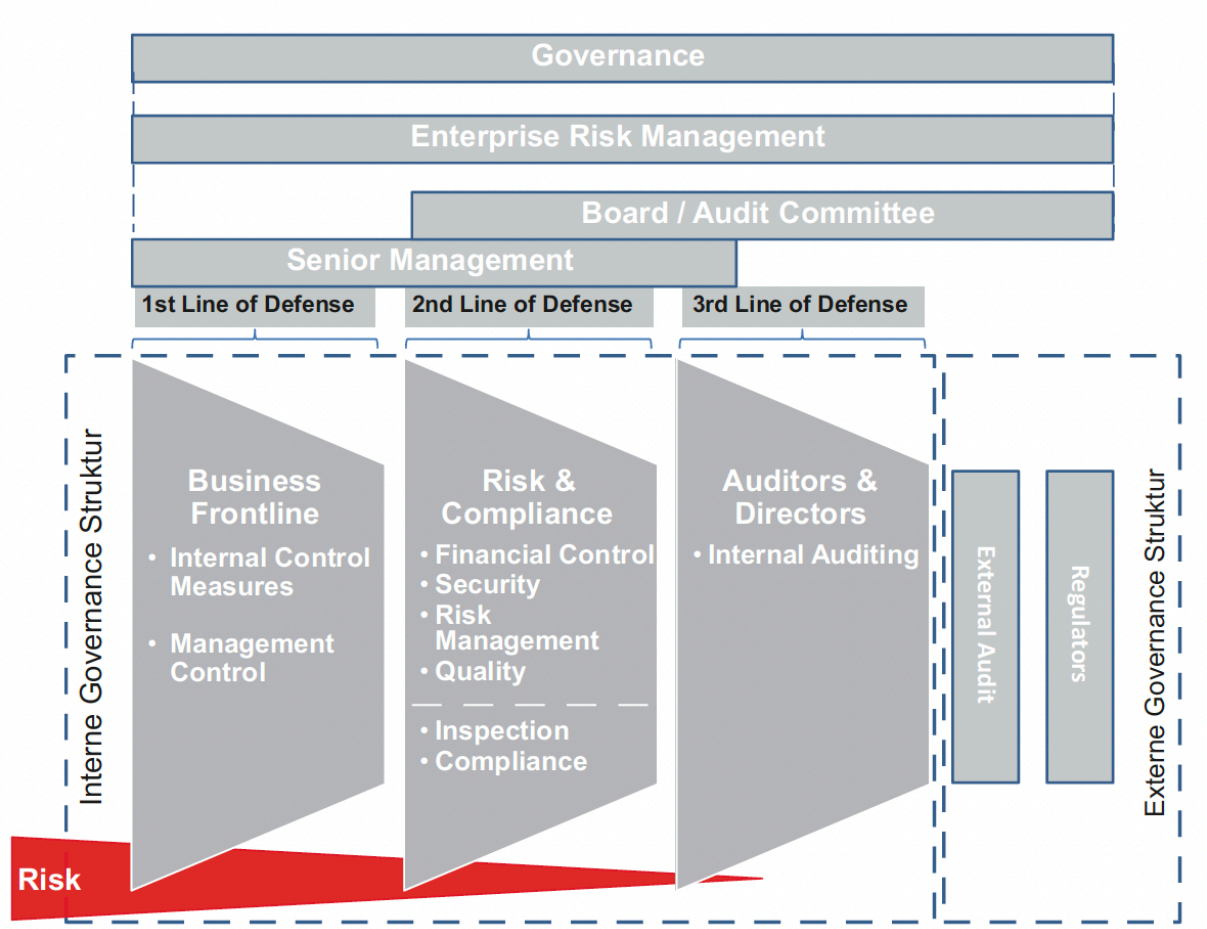


Abbildung 2: Das Three-Lines-of-Defense-Model zur Risikoabsicherung des Unternehmens.[132]

Die interne Revision spielt eine wesentliche Rolle innerhalb der Struktur der einzelnen Governance-Organe, indem sie sowohl beratende als auch prüfende Funktionen für alle Unternehmensbereiche wahrnimmt.[133] Die bedeutende Rolle der internen Revision spiegelt sich auch im Three-Lines-of-Defense-Modell wider. Gemäß Abbildung 2 besteht das Modell aus drei aufeinanderfolgenden Verteidigungslinien. Die zentrale Rolle der internen Revision im Three-Lines-of-Defense-Modell ergibt sich aus ihrer Funktion als Überwachungsinstanz im Unternehmen. Ihre Aufgabe besteht darin, dem Vorstand oder Aufsichtsrat einen zusammenfassenden Bericht über die Effektivität der internen Kontrollen vorzulegen. Dabei arbeitet sie eng mit dem Senior Management und den externen Prüfern zusammen.[134] Die interne Revision fungiert somit als die zentrale Schnittstelle zwischen den verschiedenen Kontrollorganen, die in den einzelnen Verteidigungslinien verankert sind, sowie den

[132] Welge und Eulerich (Corporate- Governance- Management: Theorie und Praxis der guten Unternehmensführung, 2021), S. 60
[133] vgl.Sarens und Abdolmohammadi (Monitoring effects of the internal audit function: agency theory versus other explanatory variables, 2011), S. 4
[134] vgl.EC–European Commission (Green Paper on the EU corporate governance framework, 2011)

verantwortlichen Einheiten in der Unternehmensführung und -kontrolle.[135] Die erste Verteidigungslinie des Three-Lines-of-Defense-Modells umfasst die traditionellen Kontrollen innerhalb der operativen Einheiten. Diese Kontrollen basieren auf der unternehmensinternen Motivation, die Effizienz und Effektivität der einzelnen operativen Bereiche und Prozesse durch Kontrollmaßnahmen auf kurz- und langfristiger Basis zu steigern. Die Durchführung dieser Kontrollen liegt in der Verantwortung von Managern auf mittlerer Hierarchieebene, die in den meisten Fällen direkten Einfluss auf die entsprechenden Bereiche haben, oder durch automatisierte Kontrollsysteme wie beispielsweise IT-gestützte Überwachungsmechanismen. Durch diese grundlegende Komponente des Three-Lines-of-Defense-Modells wird sichergestellt, dass jeder Unternehmensbereich in einer ersten Instanz zumindest von einer hierarchisch übergeordneten Einheit kontinuierlich überwacht wird. Die durchgeführten Kontrollen und implementierten Kontrollmechanismen werden an die spezifische Risikopolitik des Unternehmens angepasst und kontinuierlich aktualisiert. Im Rahmen der durchgeführten Kontrollen werden identifizierte Risiken oder bislang nicht erfasste Risiken, soweit möglich, entweder unmittelbar behoben oder innerhalb der Hierarchielinie weitergeleitet. Auf diese Weise wird das unternehmerische Risiko durch die Anwendung der genannten Kontrollen und Kontrollprozesse in der ersten Verteidigungslinie verringert.[136] Aufbauend auf dieser Grundlage erfolgt in der zweiten Verteidigungslinie eine Regulierung und Überwachung der operativen Kontrollen. Durch das Konzept des "Risk Oversight" respektive "Risk Guidance" werden die Rahmenbedingungen für die operativen Kontrollen und Kontrollmechanismen festgelegt und gesteuert. Diese Aufgabe wird nicht allein von einer einzigen Unternehmenseinheit wahrgenommen, sondern vielmehr sind zahlreiche verschiedene Unternehmenseinheiten an dieser Ausarbeitung und Steuerung involviert. Hierzu zählen das Risikomanagement, der Compliance-Bereich, das Controlling sowie die Unternehmenssicherheit und der Werkschutz. Darüber hinaus sind weitere Bereiche wie das Qualitätsmanagement, die IT-Sicherheit und der HR-Bereich darin beteiligt. Diese einzelnen Bereiche überwachen nicht nur die Berichte, die aus den operativen Kontrollen und Kontrollmechanismen hervorgehen, sondern sie beeinflussen auch aktiv die Risikopolitik und die damit verbundenen Kontrolltätigkeiten. Zusammenfassend lässt sich festhalten, dass die zweite Verteidigungslinie dazu dient, die Ergebnisse aus den operativen Einheiten zu aggregieren, gegebenenfalls erforderliche Maßnahmen zur Risikoreduktion einzuleiten und die gewonnenen Erkenntnisse durch ein geeignetes Reporting an die Unternehmensführung und -überwachung zu kommunizieren.[137]

[135] vgl.Eulerich (Das Three Lines of Defence-Modell 2012)
[136] vgl.Eulerich (Das Three Lines of Defence-Modell 2012), S. 208 f.
[137] vgl.Eulerich (Das Three Lines of Defence-Modell 2012), S. 208 f.

Dadurch wird letztendlich eine erneute Risikoreduzierung erreicht. Durch die dritte Verteidigungslinie wird das verbleibende Restrisiko, das von den ersten beiden Verteidigungslinien nicht erfasst wurde, weiter reduziert.[138] Diese Aufgabe wird von einer unabhängigen Instanz übernommen, die das Board of Directors sowie das Senior Management bzw. den Supervisory Board bei der abschließenden Kontrolle und Überwachung bestehender und potenzieller Restrisiken unterstützt. Zusätzlich liegt es in der Verantwortung dieser Instanz, die Wirksamkeit der vorangegangenen Verteidigungslinien zu überprüfen. Die interne Revision nimmt eine zentrale Position innerhalb des Handlungsrahmens ein, indem sie diese vielfältigen Aufgaben übernimmt. Neben ihrer prüfenden und beratenden Rolle für die verantwortlichen Gremien innerhalb der Organisation fungiert sie auch als überwachende Instanz der vorgelagerten Verteidigungslinien. Historisch betrachtet war es die Aufgabe der internen Revision, die Funktionsfähigkeit von Kontrollen im Finanzsektor und im operativen Tagesgeschäft (erste Verteidigungslinie) zu prüfen. Das Three-Lines-of-Defense-Modell erweitert und vertieft diesen Aufgabenbereich. Die Überprüfung und Überwachung der Governance-Organe, die in der zweiten Verteidigungslinie angesiedelt sind, gehören ebenfalls zu den Aufgaben im Three-Lines-of-Defense-Model. Aufgrund ihrer separaten Positionierung innerhalb der Unternehmensorganisation fungiert die interne Revision als letzte Verteidigungslinie. Ihre Schlüsselrolle besteht darin, die vorgelagerten Verteidigungslinien zu überwachen und diese gegebenenfalls auf der Grundlage von Prüfungsergebnissen anzupassen, bestehende Restrisiken weiter zu minimieren und die Unternehmensführung und -überwachung zu unterstützen.[139]

[138] vgl. Eulerich (Das Three Lines of Defence-Modell 2012), S. 208 f.
[139] vgl.Eulerich (Das Three Lines of Defence-Modell 2012), S. 208 f.

4 Weitere Interne und Externe Governance-Organe

Im kommenden Abschnitt werden die grundlegenden Prinzipien sowie die Funktionen der internen und externen Governance-Organe dargelegt. Die vorliegende Abhandlung legt besonderen Wert auf die Betrachtung der internen Governance-Organe, Compliance, Risikomanagement und interne Revision. Ebenso wird die externe Governance-Instanz, der Wirtschaftsprüfer, beleuchtet. Da eine umfassende Abhandlung des Risikomanagements bereits im Abschnitt 2.2 und der Compliance im Abschnitt 2.3 durchgeführt wurde, konzentriert sich dieses Kapitel auf die interne Revision und der Wirtschaftsprüfer.

4.1 Interne Revision

Das Aufgabenfeld der internen Revision unterliegt einem kontinuierlichen Wandel, der sich sowohl in einer Verschiebung der Schwerpunkte innerhalb der verschiedenen Prüfungsbereiche als auch in einer veränderten Rollenkonzeption der internen Revision manifestiert. Innerhalb der herkömmlichen Aufgabenteilung werden das Financial Auditing, das Operational Auditing, das Management Auditing sowie in neuerer Literatur auch das Internal Consulting differenziert.[140]

Das Konzept des Financial Audit umfasst die Durchführung formaler Prüfungen im Bereich des Finanz- und Rechnungswesens mit dem Ziel, die ordnungsgemäße Erfassung von Informationen zu gewährleisten. Die Hauptaufgabe dieser Prüftätigkeit besteht darin, die Angemessenheit, Genauigkeit und Zuverlässigkeit der bereitgestellten Informationen sicherzustellen. Des Weiteren erfolgt eine Überprüfung der Einhaltung von relevanten regulatorischen Vorgaben und internen Richtlinien. Diese Art von Prüfung zeichnet sich durch eine rein vergleichende Analyse von Soll- und Ist-Werten aus und bietet nur begrenzte Möglichkeiten konkrete Verbesserungsvorschläge zu entwickeln.[141]

Ein zentraler Bestandteil des Operational Auditing besteht in der Durchführung von Systemprüfungen. Diese Prüfungen dienen dazu, die organisatorischen und prozessualen Strukturen eines Unternehmens sowohl in der Gegenwart als auch im Hinblick auf die Zukunft zu überprüfen. Das Hauptziel dieser Prüfung besteht darin festzustellen, ob die Gestaltung von Unternehmensprozessen, -strukturen und -systemen zweckmäßig erfolgt. Dabei liegt der Fokus auf der Bewertung der Zweckmäßigkeit und Wirtschaftlichkeit nahezu aller Unternehmensprozesse im Hinblick auf die Sicherung der zukünftigen Entwicklung.[142]

---

[140] vgl.Füss (Die interne Revision: Bestandsaufnahme und Entwicklungsperspektiven, 2005), S. 62
[141] vgl. Amling und Bantleon (Handbuch der Internen Revision Grundlagen, Standards, Berufsstand 2007), S. 151
[142] vgl. Amling und Bantleon (Handbuch der Internen Revision Grundlagen, Standards, Berufsstand 2007), S. 151

Aufgrund fehlender standardisierter Normen als Vergleichskriterien obliegt es der internen Revision, mittels Prozessanalyse die Sollwerte festzulegen. Dies kann zur Entstehung unpräziser Beurteilungskriterien führen. An dieser Stelle nimmt die Prüfung durch die interne Revision zunehmend eine beratende Funktion ein. Die zuvor entwickelten Sollgrößen dienen als Grundlage für Empfehlungen zur Gestaltung.[143]

Im Management Auditing liegt der Fokus auf der Bewertung von Leistungen im Bereich der Führungsprozesse und -institutionen. Diese Art der Prüfung beinhaltet eine rückblickende Ursachenforschung in Verbindung mit der Identifikation zukünftiger Schwachstellen. Im Gegensatz zum Operational Auditing steht nicht mehr die Untersuchung des operativen Betriebsablaufs im Vordergrund, sondern die Beurteilung des Managements und seiner strategischen Entscheidungen. Die Prüfungskriterien - Zweckmäßigkeit und Wirtschaftlichkeit - bleiben wie beim Operational Auditing weiterhin von zentraler Bedeutung, um die Zukunftssicherung des Unternehmens zu gewährleisten. Dabei wird der Beratungsfunktion der internen Revision eine immer größere Bedeutung beigemessen. Dies führt zweifellos zu einer Veränderung des Berufsbildes des internen Revisors, da immer mehr Unternehmen auf Beratungsleistungen durch die interne Revision setzen. Die Aufgabe der internen Revision ist die Initiierung von Ansätzen zur Problemlösung, auf deren Grundlage die Betroffenen selbstständig eine Lösung erarbeiten sollen. Als prüfungsbegleitende Beratung kann daher die Bereitstellung von Verbesserungsvorschlägen bezeichnet werden, die während eines Prüfungsprozesses erarbeitet wurden. In den zuvor genannten Auditbereichen war die Beratung stets eng mit dem Prüfungsprozess verbunden. Jedoch ist eine solche Verbindung nicht zwingend erforderlich, da die interne Revision auch unabhängig vom Prüfungsprozess beratend tätig sein kann. Das Internal Consulting unterscheidet sich grundlegend von der Prüfung hinsichtlich der Gestaltung der Beurteilungskriterien. Im Rahmen einer Prüfung werden Beurteilungskriterien entwickelt und abgeleitet. Im Gegensatz dazu sind die Beurteilungskriterien bei der Beratung abhängig von der Qualifikation des Revisors, das heißt von seinem umfassenden oder spezialisierten Wissen sowie von seiner Erfahrung. Allerdings gibt es Kontroversen hinsichtlich der Beratungsfunktion der internen Revision, da diese die Unabhängigkeit der internen Revision und der Revisoren bei zukünftigen Prüfungstätigkeiten potenziell gefährden kann.[144]

[143] vgl. Amling und Bantleon (Handbuch der Internen Revision Grundlagen, Standards, Berufsstand 2007), S. 151
[144] vgl. Amling und Bantleon (Handbuch der Internen Revision Grundlagen, Standards, Berufsstand 2007), S. 151

4.2 Wirtschaftsprüfer

Die Aufgabe des Wirtschaftsprüfers besteht darin, die Abschlussprüfung im Unternehmen durchzuführen. Hierbei kann die Abschlussprüfung als eine Untersuchung aller wirtschaftlichen Aktivitäten eines Unternehmens durch ein unabhängiges und externes Prüfungsorgan definiert werden.[145] Die Hauptaufgabe dieser Prüfungstätigkeit besteht darin, die Jahresabschlüsse zu überprüfen, um auf dieser Grundlage eine zuverlässige Beurteilung über die Verlässlichkeit der Informationen im Jahresabschluss treffen zu können.[146] In diesem Zusammenhang übernimmt der Wirtschaftsprüfer eine externe Überwachungsfunktion, die dazu dient, die Ordnungsmäßigkeit der Rechnungslegung zu prüfen und somit auch die Interessen externer Anteilseigner hinsichtlich der Genauigkeit der veröffentlichten finanziellen Informationen zu wahren. Durch die Wahrnehmung dieser externen Interessen wird das Vertrauen der Anteilseigner in das betreffende Unternehmen im Kontext der Corporate Governance-Diskussion gestärkt.[147] Der Tätigkeitsbereich von Wirtschaftsprüfern umfasst je nach Größenordnung des geprüften Objekts auch die Prüfung der Angemessenheit und Wirksamkeit der internen Kontrollmechanismen sowie des Risikomanagements, die vom Unternehmen implementiert wurden.[148] Dadurch ergibt sich eine Überschneidung der Zuständigkeitsbereiche zwischen der internen Revision und der Wirtschaftsprüfung. Bei genauerer Betrachtung der jeweiligen Aufgabenbereiche wird deutlich, dass zahlreiche Möglichkeiten bestehen, die eine Zusammenarbeit zwischen beiden Prüfinstanzen nahelegen und als ökonomisch sinnvoll erscheinen lassen.[149] Das übergeordnete Ziel der Intensivierung dieser Kooperation besteht darin, Doppelarbeiten zu minimieren und Überwachungslücken zu schließen. Diese Möglichkeiten zur Verbesserung können jedoch nur dann umgesetzt werden, wenn bestimmte Voraussetzungen für eine effektive Zusammenarbeit erfüllt sind.[150] Die individuelle Ausgestaltung der Zusammenarbeit liegt in der Eigenverantwortung jedes Unternehmens. Im Allgemeinen werden jedoch folgende Formen vorgeschlagen, die einen unterschiedlichen Grad des Austauschs zwischen den beiden Akteuren ermöglichen.[151]

---

[145] vgl. Bungartz (Interne Revision und Abschlussprüfer, 2011), S. 538
[146] vgl.Krommes (Handbuch Jahresabschlussprüfung Ziele; Technik; Nachweise - Wegweiser zum sicheren Prüfungsurteil, 2015), S. 1
[147] vgl. Zitzelsberger (Wirtschaftsprüfer, vereidigte Buchprüfer und Wirtschaftsprüfgesellschaften, 2004), S. 48
[148] vgl. Bungartz (Interne Revision und Abschlussprüfer, 2011), S. 539
[149] vgl. Schmidt und Reimer (Zusammenwirken von Abschlussprüfung und Interner Revision, 2008), S. 645
[150] vgl.Bungartz (Interne Revision und Abschlussprüfer, 2011), S. 548
[151] vgl.Peemöller und Kregel (Grundlagen der Internen Revision: Standards, Aufbau und Führung, 2014), S. 367 f.

Interne Revision	Abschlussprüfer
Einhaltung der berufsethischen Grundsätze	Einhaltung der beruflichen und fachlichen Grundsätze
Einhaltung der Standards	Beachtung der Grenzen der Vereinbarkeit von Prüfung und Beratung
Ordnungsmäße Art der Tätigkeit	Besitz notwendiger fachspezifischer Kenntnisse
Angemessene Personal- und Sachausstattung	Angemessene interne und externe Qualitäts-kontrollen
Regelmäßige Abstimmung mit dem Abschluss-prüfer	Regelmäßige Abstimmung mit der Internen Revision
Information des Abschlussprüfers über alle relevanten Fragestellungen	Information der Internen Revision über alle relevanten Fragestellungen

Abbildung 3: Anforderungen an die Interne Revision und den Abschlussprüfer[152]

[152] Bungartz (Interne Revision und Abschlussprüfer, 2011), S. 549

5 Ganzheitlicher GRC-Ansatz

Die Vielzahl möglicher Ansätze und Instrumente von Governance, Risk und Compliance spiegeln sich in der Unternehmenspraxis häufig in isolierten Initiativen wider.[153] Insbesondere in stark regulierten Branchen wie der Pharmaindustrie und der Finanzdienstleistungsbranche gehen mit der Implementierung von GRC erhebliche Kosten einher. Peek und Rhode ermittelten in einer Untersuchung von bedeutenden Finanzdienstleistungsunternehmen in den USA, dass die durchschnittlichen Compliance-Kosten in den Jahren 2002 bis 2006 um 159 Prozent angestiegen sind.[154] Die geschätzten Kosten für das Compliance-Management in den befragten Unternehmen beliefen sich in absoluten Zahlen auf einen Bereich von 200 bis 400 Millionen US-Dollar pro Jahr.[155] Als Konsequenz dieser Entwicklungen wird die Integration von GRC derzeit als geschäftliche Belastung und als Kostenfaktor wahrgenommen. Es besteht daher die Vermutung eines Zielkonflikts zwischen regulatorischen Anforderungen und der Erreichung strategischer Ziele.[156] Zusätzlich zu den organisatorischen und prozessualen Optimierungen besteht ein Mangel an umfassenden GRC-Lösungen. Diese Lösungen könnten Unternehmen dabei unterstützen, die komplexe Interaktion zwischen Risiko und Compliance ganzheitlich zu erfassen, zu analysieren und zu steuern, während sie gleichzeitig nahtlos in die alltäglichen Geschäftsaktivitäten integriert werden. Im Hinblick auf angestrebte Zukunftsorientierung und breite Akzeptanz erweisen sich Standardapplikationen als prädestinierte Basistechnologie. Sie bieten Unternehmen eine kosteneffiziente und skalierbare Plattform, die regulatorische Anforderungen, Industriestandards, Kontrollen sowie interne Vorgaben für die Automatisierung notwendiger Prozesse abbildet und aktiv steuert.[157]

Eine integrierte GRC-Lösung erleichtert die Bewertung potenzieller Unternehmensrisiken, einschließlich der Risiken der Nicht-Compliance. Sie identifiziert Schwachstellen in der Einhaltung von Vorschriften und unterstützt durch zeitnahe Berichte, Analysen und kollaborative Funktionen. Auf diese Weise ermöglicht sie Unternehmen ein höheres Maß an Compliance, ein kosteneffizientes Risikomanagement sowie gesteigerte Effizienz und Präzision. Zudem ermöglicht sie die kontinuierliche Überwachung möglicher Auswirkungen potenzieller Bedrohungen.[158]

---

[153] vgl.Böhm (IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT, 2008), S. 22
[154] vgl.Marekfia (Strategisches GRC-Management: Anforderungen, Forschungsagenda und datenseitiges Modell, 2017), S. 26 f.
[155] vgl.Marekfia (Strategisches GRC-Management: Anforderungen, Forschungsagenda und datenseitiges Modell, 2017), S. 26 f.
[156] vgl.Böhm u.a. (Compliance und Alignment: Vorgabenkonformität und Strategieabgleich als Erfolgsfaktoren für eine wettbewerbsfähige IT, 2009), S. 7
[157] vgl.Standke (Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung, 2010), S. 269
[158] vgl. Standke (Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung, 2010), S. 269

Nachfolgend wird die Definition eines umfassenden GRC-Ansatzes sowie die Ausführung der Zielsetzungen, die mit einem solchen ganzheitlichen GRC-Ansatz verfolgt werden, dargelegt.

5.1 Definition

GRC als Abkürzung für Governance, Risk and Compliance hat sich seit dem Jahr 2004, als der Terminus in einer Publikation von PricewaterhouseCoopers[159] aufgeführt wurde, zu einem weit verbreiteten Schlagwort in der Forschung und Unternehmenspraxis entwickelt.[160] Somit kann ein ganzheitlicher GRC-Ansatz wie folgt definiert werden: „GRC ist ein integrierter, holistischer Ansatz einer unternehmensweiten Governance, Risk und Compliance, die dazu dient sicherzustellen, dass eine Organisation ethisch korrekt und in Übereinstimmung mit ihrer Risikoneigung, internen Richtlinien und externen Anforderungen agiert. Durch eine Abstimmung von Strategie, Prozessen, Technologie und Personal / Strukturen werden Effektivität und Effizienz verbessert."[161]

5.2 Vorteile eines ganzheitlichen GRC-Ansatzes

Der Einsatz einer GRC-Lösung strebt wie andere systemgestützte Lösungen danach, einen geschäftlichen Mehrwert zu generieren und einen Beitrag zur Gesamtkostenreduktion zu leisten, ohne die Gesamtkomplexität zu erhöhen oder diese im besten Fall sogar zu verringern. Die Hauptkategorien der Ziele einer GRC-Lösung lassen sich daher wie folgt zusammenfassen:

- Steigerung des Unternehmenswertes
- Reduktion von Komplexität
- Kostensenkung[162]

5.2.1 Steigerung des Unternehmenswertes

Für die Entwicklung und Implementierung von Risiko- und Compliance-Lösungen sind umfassende Kompetenzen erforderlich, um Unternehmen bei der Vermeidung von Verlusten und der Steigerung der Effizienz zu unterstützen. Es ist entscheidend, dass Risiko- und Compliance-Probleme schnell und proaktiv angegangen werden, und es ist erforderlich, eine langfristige Unternehmensstrategie zu entwickeln, um Compliance-Kosten zu senken und

[159] vgl.PricewaterhouseCoopers (Integrity-Driven Performance: A New Strategy for Success Through Integrated Governance, Risk and Compliance Management. A White Paper, 2004)
[160] vgl. Marekfia (Strategisches GRC-Management: Anforderungen, Forschungsagenda und datenseitiges Modell, 2017), S. 23
[161] Otremba (GRC-Management als interdisziplinäre Corporate Governance: Die Integration von Revision, Risiko- und Compliance-Management in Unternehmen, 2016), S. 149
[162] vgl.Standke (Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung, 2010), S. 269 ff.

gleichzeitig Risiken zu minimieren. Ein positiver Beitrag entsteht beispielsweise durch einen guten Ruf des Unternehmens und die Vermeidung nicht akzeptabler Probleme (realisierter Risiken) aufgrund einer definierten Compliance-Strategie. Im Zuge der Implementierung einer Lösung besteht weiterhin die Möglichkeit, Prozesse zu optimieren.[163] Dabei wird die Ausrichtung der Unternehmensstrategie im Einklang mit den spezifischen Compliance-Anforderungen angestrebt, indem:

- Die geschäftliche und operative Effektivität im Unternehmen sichergestellt wird.
- Integrierte Compliance-Ansätze im gesamten Unternehmen eingesetzt werden, um Synergien im Rahmen von Risiko- und Sicherheitsinitiativen zu erzeugen.
- Compliance-Schwachstellen frühzeitig identifiziert werden, um signifikante Risiken oder mögliche Verstöße gegen gesetzliche Anforderungen zu beheben.

Im Rahmen des Compliance-Managements erfolgt eine Generierung von Nutzen durch:

- Die Nutzung von Compliance-Daten, um eine bessere Informationsbereitstellung für Entscheidungsfindung und Prüfungsvorbereitung zu ermöglichen.
- Die gezielte Auseinandersetzung mit identifizierten Ineffizienzen und Risiken gemäß der Compliance-Gap-Analyse.
- Die Steigerung des Reifegrads von Prozessen, die für Compliance relevant sind.[164]

5.2.2 Reduktion von Komplexität

Die Nutzung einer integrierten Plattform zur Verwaltung von Unternehmensrisiken und Compliance ist ein möglicher Ansatz, um die Gesamtkomplexität zu reduzieren und besser beherrschbar zu machen. Diese Lösungsplattform wird auf verschiedene Bereiche wie Finanzen, Beschaffung, Betrieb, Vertrieb, Marketing und IT angewendet und berücksichtigt dabei unterschiedliche Anforderungen wie regulatorische Vorgaben, strategische Entscheidungen und externe Faktoren. Darüber hinaus fördert sie die organisatorische Zusammenarbeit beim Risiko- und Compliance-Management und vermeidet eine Konzentration von Verantwortlichkeiten und Fachwissen durch verbesserte Transparenz. Die Verringerung der Komplexität wird unter anderem durch folgende Maßnahmen erreicht:

- Entwicklung und Implementierung schlanker und technologieunterstützter Compliance-Ansätze für effiziente Prozesse.[165]

[163] vgl. Standke (Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung, 2010), S. 269 ff.
[164] vgl.Standke (Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung, 2010), S. 269 ff.
[165] vgl.Standke (Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung, 2010), S. 269 ff.

- Reduzierung der Komplexität von Kontrollprozessen im Geschäfts- und IT-Bereich durch die Nutzung bereits vorhandener Tools und deren Integration in die Gesamtlösung (wie z.B. Approva BizRights, SAP GRC).
- Schaffung von Transparenz zur Identifizierung und Behebung von Mängeln.[166]

5.2.3 Kostensenkung

Ziel ist die Bereitstellung einer kostengünstigen, flexiblen Lösung mit kurzer Implementierungszeit und hoher Benutzerakzeptanz durch die Verwendung einer Standardplattform mit vertrautem Look and Feel. Wenn bereits benötigte Basistechnologien im Unternehmen vorhanden sind, kann ihr Nutzen durch eine umfassendere Verwendung im Rahmen der GRC-Lösung weiter gesteigert werden. Kostenreduktionen werden unter anderem durch folgende Maßnahmen realisiert:

- Aufbau eines effizienten und nachhaltigen Compliance-Prozesses, der auf bewährten Ansätzen, erprobten Lösungen und technischen Werkzeugen basiert.
- Vermeidung von Forderungen aufgrund von Nicht-Compliance, wie zum Beispiel Konventionalstrafen, die zu Gewinnschmälerungen führen können.
- Minimierung der Kosten und Aufwände durch eine Evaluierung der unternehmensspezifischen Compliance-Anforderungen und die Implementierung einer GRC-Lösung, die genau auf diesen Umfang zugeschnitten ist. [167]

[166] vgl. Standke (Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung, 2010), S. 269 ff.
[167] vgl.Standke (Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung, 2010), S. 269 ff.

6 Empirischer Teil

Im Anschluss an die theoretische Abhandlung erfolgt nun die Darlegung des methodischen Ansatzes. Das vorangegangene Kapitel 5.2 beleuchtete die Vorteile einer ganzheitlichen Integration eines GRC-Ansatzes in deutschen Bankinstituten. Ein isolierter GRC-Ansatz kann zu Redundanzen und steigenden Kosten in Banken führen. Angesichts dessen ist es von großer Bedeutung, dass sowohl politische als auch wirtschaftliche Akteure weitere Forschungsaktivitäten nachhaltig unterstützen. Es sollten Lösungsansätze erarbeitetet werden, die sich damit beschäftigen, wie eine erfolgreiche GRC-Integration in Banken umgesetzt werden kann.

Unter Berücksichtigung des Modells "Creating A Research Space" (CARS) von John Swales lässt sich die vorliegende Arbeit in den Forschungskontext der GRC-Integration einordnen.[168] Durch die Anwendung der verschiedenen Thesen von Swales können wissenschaftliche Arbeiten ihre spezifische Position in diesem Forschungsfeld definieren. Dies ermöglicht eine klare und überzeugende Darlegung von Argumenten und deren Beitrag zur bestehenden Wissensbasis. Die vorliegende Arbeit verfolgt das Hauptziel, eine Forschungslücke zu schließen und neue Erkenntnisse sowie praktische Impulse für die effektive Integration von GRC in Unternehmen zu liefern.[169] Das Ziel der vorliegenden empirischen Untersuchung besteht darin, mithilfe des Wissens von gezielt ausgewählten Experten die bestehenden Forschungslücken bezüglich der GRC-Integration im Bankensektor weiter zu schließen und ein umfassenderes Verständnis der Faktoren zu gewinnen, die für einen erfolgreichen GRC-Ansatz in Bankinstituten ausschlaggebend sind und welche Herausforderungen es zu bewältigen gibt. Die empirische Untersuchung wird in mehrere aufeinanderfolgenden Schritte unterteilt. Der erste Teil konzentriert sich auf die Methodik und die Vorgehensweise der Untersuchung. Hierzu wird das angewandte Forschungsdesign im Kapitel 5.4.1 detailliert erläutert, wobei insbesondere auf die Durchführung der Datenerhebung, die Art der Forschung und die Auswahl der Untersuchungsobjekte eingegangen wird. Anschließend erfolgt in Kapitel 5.4.1.4 eine umfassende Beschreibung der Datenanalyse. Im nachfolgenden Abschnitt, 6, werden die Ergebnisse der durchgeführten Untersuchung eingehend diskutiert. Im letzten Kapitel des empirischen Teils erfolgt eine ausführliche Auseinandersetzung mit den Ergebnissen sowie die Ableitung von Handlungsempfehlungen auf Grundlage der erlangten Erkenntnisse.

[168] vgl. Swales (Create a research space (CARS) model of research introductions, 2014), S. 12 f.
[169] vgl. Swales (Create a research space (CARS) model of research introductions, 2014), S. 12 f.

6.1 Methodisches Vorgehen

In den nachfolgenden Teilabschnitten wird das methodische Vorgehen eingehend erläutert. Im Rahmen dieser Arbeit werden Experteninterviews durchgeführt, die anschließend mittels der qualitativen Inhaltsanalyse nach Mayring (1994) ausgewertet und analysiert werden.[170]

6.1.1 Datenerhebung

6.1.1.1 Experteninterview

Im Zuge des methodischen Vorgehens zur Erhebung der erforderlichen empirischen Daten greift die vorliegende Arbeit auf qualitative Forschungsinstrumente zurück. Qualitative Forschung bezieht sich auf die Erhebung von überwiegend nicht standardisierten Daten, die mithilfe nicht statistischer Verfahren analysiert werden.[171] Dabei können auch standardisierte Daten in die Forschung einbezogen werden.[172] Die angewandte Datenerhebungsmethode in dieser Arbeit umfasst die Durchführung von Experteninterviews. Der Einsatz von Interviews bietet den Vorteil, dass während des Gesprächs eine Vielzahl von Nachfragen und Gegenfragen gestellt werden kann. Dies ermöglicht ein tiefgehendes Verständnis der Thematik und gewährleistet, dass das Gespräch auf einem hohen fachlichen Niveau stattfindet und relevante Informationen von hoher Bedeutung erfasst werden. Idealerweise ermöglicht das Experteninterview die Bereitstellung von Begründungen und Einsichten, die anderweitig nicht zugänglich wären. Demgegenüber besteht jedoch die Gefahr, dass die Befragten in umfangreiche Monologe abgleiten könnten und Details nennen, die für die eigentliche Befragung von geringer Relevanz sind und lediglich allgemeine Aussagen beinhalten. In diesem Kontext ist es entscheidend, dass der Interviewer die Fähigkeit zur objektiven Beurteilung im Verlauf des Gesprächs aufrechterhält und eine sorgfältige Steuerung des Interviews gewährleistet.[173] Es werden mehrere Formen von Experteninterviews unterschieden. Diese sind standardisiert, halb-standardisiert und nicht-standardisiert. In der vorliegenden Untersuchung wird das halb-standardisierte Interview angewandt. In diesem Kontext wurden zwar Gesprächsthemen durch einen Leitfaden vorgegeben, die Antwortmöglichkeiten wurden jedoch nicht vorstrukturiert. Diese Offenheit ermöglicht es den Befragten, ihre Antworten frei zu formulieren, und erlaubt einen flexiblen Gesprächsverlauf, bei dem die Fragen nicht zwangsläufig in der vorher festgelegten Reihenfolge behandelt werden müssen. Dadurch

[170] vgl.Mayring (Qualitative Inhaltsanalyse, 1994)
[171] vgl.Bacher und Horwath (Einführung in die qualitative Sozialforschung, 2011), S. 4
[172] vgl. Bacher und Horwath (Einführung in die qualitative Sozialforschung, 2011), S. 4
[173] vgl. Bogner u.a. (Interviews mit Experten: eine praxisorientierte Einführung, 2014), S. 52 ff.

entsteht ein natürlicher und dynamischer Dialog zwischen dem Interviewer und den Experten.[174] Vor der Durchführung der Interviews wurde ein Leitfaden entwickelt, der als strukturierter Orientierungsrahmen für die Gespräche diente.[175] Der Leitfaden ist als Anhang „A“ beigefügt. Aufgrund der Wünsche einiger Experten wurde ihnen der Leitfaden vorab zur Verfügung gestellt, um eine bessere Vorbereitung auf das Gespräch zu ermöglichen.

6.1.1.2 Experten

Die Informationen und Daten dieser Untersuchung wurden mit Unterstützung von Experten gewonnen, die über besonders praxisrelevantes Wissen verfügen. Aufgrund ihrer unterschiedlichen Hintergründe und ihrer Tätigkeit in verschiedenen Institutionen und Unternehmen fließen vielfältige Einflüsse in ihre Antworten ein. Ihre umfassende Expertise, ihre handlungsorientierten Ansätze und ihre fundierten Einschätzungen tragen dazu bei, dass andere Akteure ihr Handeln strukturierter gestalten können.[176] Die Kontaktaufnahme erfolgte durch Anfragen über LinkedIn. Die Interviews wurden per Telefoninterview durchgeführt und dauerten im Durchschnitt 35 min. Eine Abweichung von dieser allgemeinen Beobachtung stellte das telefonische Interview mit Klaus Abel dar, das eine Dauer von 54 Minuten aufwies. In diesem Gespräch griff er vermehrt auf praktische Beispiele zurück, um seine Aussagen zu untermauern.

Ein wesentlicher Vorteil von Telefoninterviews besteht in der zeitlichen Effizienz, da die Untersuchung schnell durchgeführt werden kann und eine geringere Wartezeit auf einen Termin besteht. Zudem weisen Telefoninterviews im Vergleich zu Online-Befragungen eine geringere Ausfallrate auf.[177]

Folgend werden nähere Informationen zu den Experten und deren Berufsfeldern zum Zeitpunkt der Interviews vorgestellt. Jerome Kögel ist Referatsleiter für MaRisk – Compliance bei der Kreditplus Bank AG. In seiner Funktion ist er als Experte für die Themen Compliance und Geldwäsche tätig. Seine Hauptaufgaben umfassen die Gewährleistung der angemessenen Implementierung und Umsetzung aller regulatorischen Vorgaben. Zudem obliegt ihm die Verantwortung für Analysen aus Sicht der Compliance. Darüber hinaus agiert er in beratender Funktion bei strategischen Entscheidungen. Ulrich Probst ist seit 25 Jahren als Bankangestellter bei der ING Diba AG tätig und hat in dieser Zeit verschiedene Rollen

[174] vgl.Gläser und Laudel (Experteninterviews und qualitative Inhaltsanalyse, 2010), S. 41 f.
[175] vgl. Lamnek (Qualitative Sozialforschung 2010), S. 23
[176] vgl. Bogner u.a. (Interviews mit Experten: eine praxisorientierte Einführung, 2014), S. 13
[177] vgl.Klandt und Heidenreich (Empirische Forschungsmethoden in der Betriebswirtschaftslehre: von der Forschungsfrage zum Untersuchungsdesign, eine Einführung, 2017), S. 149

innegehabt. Er ist seit über 20 Jahren Mitglied des Betriebsrats und nimmt die Position des Vorsitzenden der Haustarif Kommission für die GBV-Gewerkschaft ein, wobei er gleichzeitig im Bundesvorstand dieser Gewerkschaft aktiv ist. Zudem fungiert er intern als zentraler Whistleblowing-Officer. Darüber hinaus ist er im Aufsichtsrat der ING Diba AG vertreten und übt dieses Mandat im Zusammenhang mit seiner Funktion innerhalb der Gewerkschaft aus. Klaus Abel ist als Teamleiter im Workout-Management der Deutsche Bank AG tätig. Er übernimmt die Funktion des Teamleiters für die Zuständigkeitsbereiche Governance, Kreditentscheidung und Regulatorik. In seiner zugeordneten Rolle obliegt es ihm, Risiken in Bezug auf Kreditausfälle zu minimieren und potenziell Risiken zu lenken. Des Weiteren ist er zuständig für die Systematisierung der Regelgefüge, die im Kontext der Interaktion mit wirtschaftsprüferischen Instanzen sowie bei Kreditbewertungsprozessen Anwendung finden. Darüber hinaus widmet er sich der Vertiefung seiner Auseinandersetzung mit regulatorischen Aspekten im Bereich des Kreditwesens sowie den Belangen aufsichtsrechtlicher Natur.
In den darauffolgenden Abschnitten wird die Identifikationsnummer (ID) verwendet, um die Aussagen der Experten zu diskutieren.

ID	Institution	Befragter	Datum	Dauer	Expertise
I1	Kreditplus Bank AG	Jerome Kögel	13.06.2023	35 min	Referatsleiter für MaRisk – Compliance Compliance-Beauftragter
I2	ING Diba AG	Ulrich Probst	31.07.2023	34 min	Bankangestellter Whistleblowing-Officer Mitglied im Aufsichtsrat
I3	Deutsche Bank AG	Klaus Abel	07.08.2023	54 min	Teamleiter im Workout-Management (Risikomanagement)

Tabelle 1: Übersicht der Experten

6.1.1.3 Durchführung

Der vorliegende Leitfaden umfasst insgesamt neun Fragen, wobei Frage zwei, acht und neun jeweils durch spezifische thematische Unterpunkte in Form von a, b und c weiter untergliedert sind. Die anfängliche Fragestellung des Leitfadens soll eine aktuelle Einschätzung der Entwicklungen im Bereich GRC im Banksektor im Jahr 2023 geben. Die Experten sollen die gegenwärtigen Zustände, Herausforderungen und Trends im Hinblick auf GRC in Banken beschreiben. Die nächste Frage zielt auf einen Vergleichszeitraum ab, nämlich die Veränderungen im Banksektor zwischen 2007/09 und 2023. Hierbei sollen die Experten die Unterschiede, Fortschritte und Rückblicke auf die Entwicklung von GRC in Banken über diesen Zeitraum hinweg erläutern. Die dritte Frage zielt darauf ab, die Relevanz und den

Stellenwert der regulatorischen Anforderungen in Banken zu ermitteln. Das zentrale Anliegen der vierten Frage besteht darin, die Rolle von GRC in den Banken der Experten zu ermitteln. Hierbei werden die Experten gebeten, eine ausführliche Darlegung zur Bedeutung und Funktionsweise der individuellen GRC-Komponenten in ihren jeweiligen Bankinstituten zu geben. Ab Frage fünf wird eine konkrete Befragung zur Zusammenarbeit zwischen den internen und externen Governance-Organen in Bankinstituten durchgeführt. Frage sechs befasst sich mit den Herausforderungen und Risiken im Zusammenhang mit GRC. Die siebte Frage fokussiert sich auf die Identifizierung gezielter Optimierungsansätze für die Zusammenarbeit bzw. Kooperationsmechanismen der Schnittstellen, mit dem Ziel, redundante Prozesse und unnötige Kosten zu minimieren. Die Frage 8a) hat primär zum Ziel, die Definition eines integrierten GRC-Ansatzes aus der Perspektive der Experten zu erlangen, um ein klares Verständnis und eine klare Definition der GRC-Integration zu erlangen. Im Anschluss wurde die Definition des ganzheitlichen GRC-Ansatzes aus Kapitel 5 präsentiert, woraufhin die Experten gebeten wurden, ihre fachliche Stellungnahme dazu abzugeben. Durch die Frage 8b) soll festgestellt werden, ob die Institutionen, in denen die Experten tätig sind, bereits eine integrierte GRC-Strategie implementiert haben. Dabei liegt der Fokus auf der Identifikation vorhandener Maßnahmen und Strukturen, die auf eine umfassende Integration von GRC hindeuten. Die Frage 8c) soll potenzielle Vorteile einer Integration GRC in Banken identifizieren. Die Frage 8d) zielt darauf ab, spezifische Handlungsempfehlungen zu ermitteln, die von Banken ergriffen werden könnten, um einen integrierten GRC-Ansatz erfolgreich zu implementieren und effektiv umzusetzen. In Frage 8e) wird untersucht, welche technologischen Hilfsmittel von den Institutionen der Experten eingesetzt werden, um eine erfolgreiche Umsetzung eines integrierten GRC-Ansatzes zu unterstützen. Die Frage 9a) ermittelt, ob in den Banken regelmäßig Berichte GRC-Themen erstellt werden. In diesem Zusammenhang liegt das Interesse auf den vorhandenen Berichtsstrukturen und -inhalten, die in den regelmäßigen GRC-Reports verwendet werden. Die Frage 9b) soll die Organisationsstruktur des Reportings in den Banken aufdecken. Dabei wird untersucht, ob die Berichterstattung für GRC getrennt nach Funktionen erfolgt oder ob eine integrierte Berichterstattung stattfindet, bei der die drei Bereiche gemeinsam betrachtet werden. In der abschließenden Frage wird das Ziel verfolgt, mögliche Vor- und Nachteile eines einheitlichen Reporting-Ansatzes für alle GRC-Funktionen zu diskutieren. Es wird angestrebt, eine kritische Auseinandersetzung mit der Implementierung eines integrierten Reporting-Systems zu führen, um potenzielle Vorzüge und mögliche Herausforderungen im Hinblick auf die GRC-Funktionalität zu beleuchten.

6.1.2 Datenanalyse

Nach Abschluss der Gespräche wurden die Interviews transkribiert. Die Transkripte sind vollständig im Anhang zu finden. Die systematische Auswertung der Gespräche erfolgte unter Verwendung der Software Maxqda. Diese spezialisierte Software dient der Unterstützung bei der qualitativen Inhaltsanalyse von nicht strukturierten Daten wie Interviews. Sie bietet eine breite Auswahl an Visualisierungs-Tools und verschiedene Optionen zur Analyse von Interviewdaten. Die qualitative Inhaltsanalyse ist eine Technik aus dem Bereich der Kommunikationswissenschaft und dient als Instrument zur systematischen Bearbeitung von Kommunikationsmaterial.[178] Zur präziseren Erklärung des Instruments lassen sich drei unterschiedliche Definitionselemente identifizieren.[179] Die vorliegende Analyse befasst sich primär mit dem Kommunikationsmaterial, das in fester Form, wie beispielsweise in Textform, vorliegen sollte. Anhand des Inhalts dieses Materials werden weitere Aspekte der Kommunikation abgeleitet, darunter der subjektive Bedeutungshintergrund und die verborgenen Absichten des Kommunikators. Von zentraler Bedeutung ist hierbei der Einsatz eines systematischen, regelgeleiteten und analytischen Vorgehens, um eine gründliche Untersuchung zu gewährleisten.[180] Mayring unterscheidet in seinem Ansatz zwischen den drei grundlegenden Techniken der Zusammenfassung, Explikation und Strukturierung.[181] Für die gegenwärtige Untersuchung wurde die Methodik der Zusammenfassung als Ansatz gewählt. Dieser Ansatz konzentriert sich auf die Verdichtung des Materials mit dem Ziel, die relevantesten Inhalte zu bewahren und eine übersichtliche Darstellung zu ermöglichen. Die qualitative Inhaltsanalyse unterliegt einer Abfolge von aufeinanderfolgenden Phasen. In der anfänglichen Phase steht die Paraphrasierung im Mittelpunkt. Hierbei werden alle Formulierungen eliminiert, die keine inhaltliche Relevanz tragen, und die kodierten Einheiten werden präzise umformuliert. Dies trägt dazu bei, eine einheitliche Sprachebene zu etablieren. In der anschließenden Phase erfolgt die Festsetzung des Abstraktionsniveaus, auf das der paraphrasierte Text mittels der reduktiven Prozesse überführt wird.[182] Eine sukzessive Steigerung der Abstraktionsebene kann in diesem Kontext schrittweise realisiert werden. Im Anschluss daran erfolgt eine weitere Stufe der Reduktion, bei der Paraphrasierungen, die inhaltlich miteinander in Beziehung stehen, zusammengeführt werden. Diese Iteration des Prozesses kann fortlaufend wiederholt werden, bis die Materialreduktion das beabsichtigte

[178] vgl.Mayring (Qualitative Inhaltsanalyse 2010), S. 609
[179] vgl.Mayring (Qualitative Inhaltsanalyse, 1994), S. 159
[180] vgl. Mayring (Qualitative Inhaltsanalyse, 1994), S. 1
[181] vgl. Larcher (Zusammenfassende Inhaltsanalyse nach Mayring: Überlegungen zu einer QDA-Software unterstützten Anwendung, 2010), S. 4
[182] vgl. Mayring (Qualitative Inhaltsanalyse, 1994), S. 166

Resultat erreicht.[183] Im Rahmen der Inhaltsanalyse nimmt das Konzept der Kategorien eine herausragende Position ein. Es beinhaltet die Entwicklung eines Kategoriensystems, das dazu dient, die inhaltlichen Aspekte im Text in operationalisierbarer Weise zu repräsentieren und somit eine systematische Auswertung des Materials zu ermöglichen. Besonders förderlich ist es, wenn dieses System eine hohe Präzision bei der Zuordnung der Kategorien aufweist.[184] Der Vorgang, durch den den Bestandteilen des Materials Kategorien zugeordnet werden, wird als Kodierung bezeichnet. Die transkribierten Daten werden in einer tabellarischen Struktur analysiert. Die Tabelle beinhaltet Angaben zur ID, Haupt- und Subkategorie, Position und Paraphrase. Diese Anordnung zielt darauf ab, eine übersichtliche Darstellung zu gewährleisten. Ein Auszug aus der Inhaltsanalyse ist in der unteren Tabelle ersichtlich:

ID	Haupt- und Subkategorie	Position	Paraphrase
I1	Entwicklung im Banksektor > Stand des Banksektors im Jahr 2023	10	Ich würde es mal zusammenfassen, dass wir weiterhin in Entwicklungsstadium sind.
I2	Status quo: Governance, Risiken und Compliance > Organisatorische Verankerung	40	Zumal, weil die beiden unter Risk, also unter der Risiko Vorständin hängen.

Tabelle 2: Beispiel zusammenfassende Inhaltsanalyse

Gemäß der Methodologie von Mayring werden mittels einer qualitativen Inhaltsanalyse induktive Kategorien aus den Aussagen der Experten abgeleitet. Infolge dieser Vorgehensweise wurden die folgenden Kategoriensysteme entwickelt:

- Entwicklung im Banksektor
- Status quo: Governance, Risik und Compliance
- Herausforderungen und Risiken
- Ganzheitlicher GRC-Ansatz
- Herausforderungen eines ganzheitlichen GRC-Ansatzes

Das umfassende Kategoriensystem ist im Anhang „B“ abrufbar.

[183] vgl.Mayring (Qualitative Inhaltsanalyse 2010), S. 210 ff.
[184] vgl. Mayring (Qualitative Inhaltsanalyse, 1994), S. 170

6.2 Ergebnisse der empirischen Untersuchung

Nachfolgend werden die Ergebnisse der explorativen Erhebung anhand des Kategoriensystems dargelegt. Die ersten Kategorien: Entwicklung im Banksektor trägt nicht direkt zur Beantwortung der Forschungsfrage bei. Dennoch wurde im Gespräch mit den Experten gezielt darauf eingegangen, um einen Überblick über die grundsätzliche Wahrnehmung der Experten zu bekommen und wie diese mit der Literatur übereinstimmt.

Entwicklung im Banksektor:

Die erste Kategorie behandelt die Entwicklung im Banksektor. Diese Kategorie wurde in zwei Subkategorien unterteil:

Veränderungen seit 2007/2008 im Vergleich

Die weltweite Finanzkrise von 2007 bis 2009 hat einen fundamentalen Wandel im Bankensektor hervorgerufen.[185] Diese Krise erzwang eine klar erkennbare Neuausrichtung der Denk- und Handlungsweisen innerhalb der Banken. Hierbei spielte der regulatorische Druck, der sowohl von nationalen als auch internationalen Aufsichtsbehörden und Gesetzgebern ausging, eine entscheidende Rolle. Die internationale Dimension dieses regulatorischen Drucks manifestierte sich in der aktiven Intervention globaler Bankenaufsichtsinstanzen, die darauf abzielten, eine substantielle Transformation und Verbesserung im Bankensektor zu bewirken.[186] Obwohl die Aspekte von Governance, Risk und Compliance immer schon präsent waren, wurden sie historisch gesehen eher marginal behandelt und als potenzielle Hemmnisse für Wachstum und Profitabilität angesehen.[187]

Stand des Banksektors im Jahr 2023

Die Banken haben infolge der erforderlichen Anpassungen, aber auch aus eigenem Antrieb, eine deutliche Transformation durchlaufen. Diese Veränderung manifestiert sich in der Einführung vieler neuer Maßnahmen und Praktiken.[188] Im Bereich der Compliance wurde der derzeitige Zustand als Entwicklungsstadium charakterisiert, was darauf hindeutet, dass die Branche nach wie vor damit beschäftigt ist, den Umfang und die Tiefe der Compliance zu erfassen.[189] Die drei Konzepte – Governance, Risikomanagement und Compliance – haben

[185] vgl. I1, Pos. 10; l2, Pos. 14
[186] vgl. I3, Pos. 6
[187] vgl. I2, Pos. 14
[188] vgl. I3, Pos. 6
[189] vgl. I1, Pos. 10

insgesamt eine grundlegende Wertverschiebung erfahren, da sie heute im Bankensektor als fundamentale Grundlage für eine strukturierte, nachhaltige Geschäftstätigkeit mit Wachstum und stabilen Erträgen betrachtet werden. Früher wurden diese Aspekte eher als potenzielle Hemmnisse wahrgenommen, doch heutzutage bilden sie eine tendenziell bedeutsamere Grundlage für unternehmerische Aktivitäten.[190]

Status quo: Governance, Risk und Compliance

Organisatorische Verankerung

Insgesamt offenbarte die Untersuchung eine vielfältige strukturelle Ausgestaltung der organisatorischen Verankerung in den Banken. In einem Bankinstitut ist das Chief Administration Office als übergeordneter Vorstandsbereich federführend für Governance, Compliance und die Rechtsabteilung verantwortlich. In dieser konzeptuellen Ausrichtung sind die Bereiche Recht, Governance und Compliance miteinander verbunden. Parallel dazu ist der Risikobereich autonom unter der Führung eines eigenständigen Vorstands angesiedelt.[191]
Bei einem anderen Finanzinstitut zeigt sich eine ähnliche Struktur, bei der Governance und Compliance gemeinsam unter der Verantwortung eines Vorstandsressorts stehen, während die interne Revision und das Risikomanagement einem separaten Vorstand zugeordnet sind.[192] Hingegen ist in einem weiteren Bankinstitut die Verankerung von Governance und Compliance innerhalb einer agilen Aufbauorganisation als "Center of Expertise" realisiert. Sowohl das integrierte Risikomanagement als auch die Compliance fungieren als solche Fachzentren. Obwohl sie nicht direkt interagieren, bestehen enge Wechselbeziehungen zwischen diesen Bereichen. Beide sind dem Risikovorstand unterstellt und berichten direkt an diesen.[193]

Unternehmenskultur; - Politik

Die Unternehmenskultur und -politik in Banken stellen einen bedeutenden Einflussfaktor auf die hausinterne Kommunikation dar. Generell charakterisierten die Experten die Unternehmenskultur und -politik als "offen". Dies äußert sich insbesondere durch regelmäßige Gelegenheiten zum Austausch und die Förderung offener Diskussionen zur Findung konstruktiver Lösungen bei auftretenden Problemen und Herausforderungen.[194] Innerhalb eines

[190] vgl. I2, Pos. 14
[191] vgl. I3, Pos. 15
[192] vgl. I1, Pos. 22
[193] vgl. I2, Pos. 56
[194] vgl. I1, Pos. 20; I3, Pos. 10

Finanzinstituts wurde insbesondere die Anwendung einer "Duz-Kultur" hervorgehoben, die zusätzlich zu einem offenen Umgang unter den Mitarbeitern führt.[195]

Rolle von Governance, Risk und Compliance

Historisch gesehen wurden GRC in der Vergangenheit oft nicht angemessen gewürdigt und als potenzielle Hindernisse für die Ertragssteigerung betrachtet.[196] Es herrschte eine verbreitete Mentalität, die darauf abzielte, Maßnahmen zur Gewinnsteigerung ohne Berücksichtigung von GRC-Aspekten umzusetzen. In diesem Zusammenhang hat Compliance erst in den vergangenen zwei bis maximal fünfundzwanzig Jahren die Fähigkeit entwickelt, fundiert "Nein" zu sagen.[197]

Die zunehmende Bedeutung von GRC in Banken wird durch die direkte Berichterstattung von Compliance-Beauftragten, Risikomanagern und der internen Revision an den Vorstand unterstrichen. Vorstandsmitglieder sind zunehmend auf Meinungen und Einschätzungen aus diesen Bereichen angewiesen, nicht zuletzt als präventive Maßnahme für den Selbstschutz.[198] Ebenfalls wird die Arbeit der internen Revision und deren Feststellungen sowie Vorschläge zur Verbesserung in einem Bankinstitut als Chance betrachtet.[199]

Aufgabenabgrenzung

Es zeichnet sich eine kohärente Darstellung bezüglich der Abgrenzung der Aufgaben innerhalb der internen Governance-Elemente wie Risikomanagement, Compliance und interne Revision sowie der externen Governance-Instanzen wie den Wirtschaftsprüfer ab. Die Einschätzungen der Fachexperten legen nahe, dass die Aufgaben der internen und externen Governance-Organe nicht unbegründet voneinander getrennt sind. Dies erfolgt aufgrund der Notwendigkeit, verschiedene Interessen und Neutralitätsaspekte angemessen zu berücksichtigen.[200]

Demzufolge manifestieren sich eindeutig abgegrenzte Verantwortungsbereiche innerhalb der Bankinstitute, wie von sämtlichen Befragten betont wurde. Diese klare Aufgabenabgrenzung ist von besonderer Bedeutung, um eine klare Definition der Zuständigkeiten sicherzustellen. Dies minimiert die Möglichkeit, dass ein anderer Bereich für eine Aufgabe verantwortlich gemacht wird, die in der Verantwortung des eigenen Bereichs liegt, im Falle von Fehlern oder Problemen.[201]

---

[195] vgl. I1, Pos. 20
[196] vgl. I2, Pos. 14
[197] vgl. I1, Pos. 24
[198] vgl. I1, Pos. 12
[199] vgl. I3, Pos. 10
[200] vgl. I3, Pos. 10
[201] vgl. I1, Pos. 40

Kommunikation und Zusammenarbeit

Die empirischen Ergebnisse der Experteninterviews bieten aufschlussreiche Einblicke in die dynamische Interaktion zwischen den internen Governance-Organen, darunter Compliance, Risikomanagement und interne Revision, sowie den externen Governance-Organen wie Wirtschaftsprüfern, der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und anderen einschlägigen Behörden.[202] Eine übergreifende Erkenntnis aus diesen Befragungen besteht darin, dass der Austausch in sämtlichen Institutionen von einer tiefgehenden Verbundenheit, Intensität und Vertrauensbasis geprägt ist.[203] Diese Verflechtungen manifestieren sich als reziproker Prozess des Informations- und Wissensaustauschs.[204]

Hervorzuheben ist ein konkretes Beispiel eines Bankinstituts, das die signifikante Rolle der räumlichen Nähe unterstreicht. Hierbei wird betont, dass eine unmittelbare räumliche Nachbarschaft zwischen dem Risikomanagement und der Compliance-Abteilung einen kontinuierlichen, offenen Dialog fördert. In dieser Hinsicht wird die Wichtigkeit betont, Herausforderungen offen anzusprechen und eine ehrliche Kommunikation zu pflegen, selbst bei divergierenden Meinungen.[205]

Innerhalb eines anderen Bankinstituts wird auf der Managementebene ein regelmäßiger Austausch verzeichnet. Auf operativer Ebene variiert die Frequenz des Informationsaustauschs je nach spezifischen Belangen. Die Zusammenarbeit mit externen Partnern, beispielsweise Wirtschaftsprüfern, erfolgt auf Grundlage des aktuellen Bedarfs.[206] Zudem wird die Kooperation mit Regulierungsbehörden als intensiv beschrieben, insbesondere im Kontext von Aufsichtsratssitzungen, bei denen die Präsenz von Regulatoren regelmäßig gegeben ist.[207]

Die enge Kollaboration mit dem Vorstand und der Geschäftsführung wird als essenziell erachtet. In dieser Hinsicht betonen die Experten die fundamentale Bedeutung einer transparenten Kommunikation mit dem Vorstand und anderen Führungsebenen, um potenzielle Herausforderungen frühzeitig anzusprechen.[208] Es ergibt sich aus den Befragungen, dass ein regelmäßiger formaler Austauschmechanismus zwischen den internen Governance-Organen in Form eines Jour-Fix nicht etabliert ist.[209]

[202] vgl. I2, Pos. 18
[203] vgl. I1, Pos. 20; I2, Pos. 30; I3, Pos. 10
[204] vgl. I3, Pos. 15
[205] vgl. I1, Pos. 20
[206] vgl. I3, Pos. 21
[207] vgl. I2, Pos. 18
[208] vgl. I1, Pos. 12
[209] vgl. I1, Pos. 22

Technologische Lösungen

Der Einsatz technologischer Lösungen im Kontext von GRC in Banken veranschaulicht eine Vielzahl von Ansätzen zur Automatisierung und Systematisierung komplexer Prozesse. Es wurde über die Verwendung eines strukturierten technologischen Tools berichtet, das den Prozess zur Schließung von identifizierten Mängeln im Rahmen der jährlichen Abschlussprüfung übernimmt.[210] Eine Erwähnung des exakten Namens des verwendeten Instrumentes erfolgte hingegen nicht.

In einem weiteren Bankinstitut wird ein bedeutendes technologisches Instrument zur Erfassung und Weiterleitung neuer Vorschriften genutzt. Nach der Erfassung kommen die zuständigen Abteilungen ins Spiel, um die Vorschriften für die jeweiligen Risikoabteilungen zu übernehmen. Diese Vorgänge werden von einer systembasierten Herangehensweise begleitet, bei der Vorgesetzte die Initiation, Datierung und Entfernung aus dem System überwachen. Dieser Prozess folgt einer systematischen Erfassung und Weiterleitung.[211] Auch an dieser Stelle blieb die spezifische Bezeichnung des verwendeten Instruments unerwähnt.

In einer anderen Bank wurde ein konkretes Beispiel eines technologischen Tools mit dem Namen "Teamradar" gennant, das dazu dient, Regulierungen zu filtern und relevante Informationen für die Bearbeitung der Compliance bereitzustellen. Der Fokus liegt darauf, einschlägige Informationen zu erkennen und in einem kontrollierten Verfahren umzusetzen, um eine lückenlose und überprüfbare Dokumentation zu gewährleisten.[212] Ein weitere technologische Lösung namens "Q-SAC" ermöglicht die Erfassung und Verwaltung von Risiken in den verschiedenen Abteilungen, wobei das Risikomanagement auf die gemeldeten Risiken zugreifen kann.[213]

Reporting

Die Expertenäußerungen im Kontext einer integrierten GRC-Berichterstattung an den Schnittstellen von Governance, Risikomanagement und Compliance in Banken veranschaulichen unterschiedliche methodische Ansätze, die in Bankinstitutionen angewandt werden. In einem Fall erfolgt die Generierung von Berichten zunächst autonom innerhalb der individuellen Fachabteilungen. Diese spezifischen Berichte werden daraufhin konsolidiert und dem Finanzvorstand präsentiert, der eine umfassende Übersicht über die Gesamtsituation erhält. Dabei wurde speziell hervorgehoben, dass Vorstandsmitglieder verpflichtet sind, eine

[210] vgl. I3, Pos. 21
[211] vgl. I3, Pos. 19
[212] vgl. I1, Pos. 44
[213] vgl. I1, Pos. 30, Pos. 31

umfassende Lagebewertung durchzuführen, wobei ein quartäres Berichtswesen obligatorisch ist. Die Evaluierung der Berichte erfolgt wechselseitig durch die Vorstandsmitglieder, wobei die Betonung darauf liegt, dass keine isolierten Berichtsstrukturen entstehen sollten, um regulatorischen Anforderungen und Silo-Effekten entgegenzuwirken. Besondere Bedeutung wird dem Dialog zwischen den verschiedenen Vorstandsmitgliedern beigemessen, insbesondere im Kontext regulatorischer Herausforderungen.[214]

In einem anderen Bankumfeld wurde ein Schritt in Richtung eines ganzheitlichen, integrierten Ansatzes für das GRC-Reporting dokumentiert. Dies manifestiert sich in der praktischen Umsetzung durch regelmäßig quartalsweise abgehaltene gemeinsame Berichtssitzungen, die den gesamten Vorstand einbeziehen. Ergänzend dazu werden in halbjährlichen Intervallen spezialisierte Fachkollegen aus der übergeordneten Gruppenstruktur in den Prozess miteinbezogen. Diese koordinierte Abstimmung erfolgt in einer zeitlich definierten Abfolge. Die Inhalte der Präsentation umfassen verschiedene Dimensionen, in denen Compliance und Risikomanagement direkt aufeinanderfolgen. Folglich ist bereits eine ganzheitliche Berichterstattung an den Vorstand und den Aufsichtsrat implementiert. Diese Strukturen weisen Ähnlichkeiten auf.[215]

In Bezug auf eine der Banken wurde erörtert, dass derzeit kein vollständig integrierter GRC-Bericht vorliegt. Stattdessen erfolgt die separate Berichterstattung an den Vorstand bezüglich der Bereiche Compliance, Risikomanagement und interne Revision.[216]

Herausforderungen und Risiken

Zunehmende Gesetztes vorgaben

Eine zentrale Herausforderung innerhalb des Bankensektors ergibt sich aus den häufigen und raschen Änderungen der rechtlichen Anforderungen. Diese Umstände erfordern von den Banken die Fähigkeit, das laufende Geschäft zu bewältigen und gleichzeitig neue Produkte sowie regulatorische Änderungen zu überprüfen und umzusetzen. Es gestaltet sich oft als unpraktikabel, sämtliche bestehende Prozesse nach den neuen Vorgaben zu überprüfen.[217] Die kontinuierlich hinzukommenden rechtlichen Anforderungen zwingen zur Anpassung der organisatorischen Strukturen sowohl in der Aufbau- als auch in der Ablauforganisation. Dies betrifft auch die personelle Ebene.[218]

[214] vgl. I3, Pos. 35
[215] vgl. I1, Pos. 14
[216] vgl. I2, Pos. 26
[217] vgl. I1, Pos. 24
[218] vgl. I2, Pos. 44

Eine zusätzliche Herausforderung entsteht durch die verstärkte Aufmerksamkeit seitens Regulatoren, Stakeholdern und Kunden, insbesondere innerhalb der Bankenbranche. Dies führt zu einem erhöhten Druck, die Einhaltung von Compliance- und Risikomanagementrichtlinien sicherzustellen. Die sich verändernde Wettbewerbssituation in der Bankenbranche ist durch das Auftreten weniger regulierter neuer Marktteilnehmer gekennzeichnet.[219]

Integration neuer Gesetzte in bestehende Prozesse

Im Bankensektor ist eine deutliche Herausforderung in Bezug auf die Integration neuer Gesetze in bestehende Prozesse erkennbar. Diese Situation verdeutlicht die erheblichen Schwierigkeiten, die damit verbunden sind, bereits etablierte Prozesse gemäß den aktuellen Vorgaben zu überprüfen. Zugleich wird betont, dass aufgrund der umfangreichen Anzahl von Gesetzen und Vorschriften eine uneingeschränkte Behauptung, sämtliche Anforderungen zu 100 Prozent zu erfüllen, nicht realistisch ist. Stattdessen bleibt stets ein gewisses Risiko bestehen, dass bestimmte Vorgaben nicht in vollem Umfang eingehalten werden können. Diese inhärente Risikokomponente ist unvermeidlich vorhanden, und das übergeordnete Ziel besteht darin, dieses inhärente Risiko so minimal wie möglich zu halten. Dennoch ist es essenziell, trotz dieser Unsicherheiten sicherzustellen, dass die bereits etablierten Prozesse und Arbeitsabläufe zeitgerecht den neu auferlegten gesetzlichen Anforderungen entsprechend modifiziert werden.[220]

Künstliche Intelligenz

Die fortschreitende Bedeutung der Künstlichen Intelligenz (KI) in Bezug auf GRC im Bankensektor führt zu weiteren Herausforderungen. Die Einbindung von KI wird sowohl als Effizienzsteigerung als auch als Herausforderung betrachtet. Einerseits ermöglicht KI die Vereinfachung von Prozessen und die zügige, fehlerfreie Erledigung von Aufgaben. Dennoch bestehen Unsicherheiten hinsichtlich der Kontrolle und Überwachung von KI-Entscheidungen. Es wird betont, dass das Verständnis der KI-Funktionsweise und die Sicherstellung menschlicher Intervention essenziell sind, um regulatorische Standards zu erfüllen. Die Vorteile der KI liegen in der Prozessvereinfachung und Kosteneinsparungen, bedingen jedoch tiefgehendes Fachwissen in IT und Kreditwesen, um bspw. gegen logische Kreditvergabe-Strategien verstoßende Entscheidungen zu verhindern.

[219] vgl. I2, Pos. 46
[220] vgl. I1, Pos 24; I3, Pos. 17

Die Governance spielt eine zentrale Rolle bei der Integration und Steuerung von KI. Menschliche Kontrolle und Governance sind unverzichtbar, um KI-Einsätze zu überwachen, anzupassen und zu kontrollieren. Die wachsende Bedeutung der Governance wird unterstrichen, da die Verantwortung für KI-Entscheidungen nicht auf die KI selbst übertragen werden kann. In Anbetracht bevorstehender Umwälzungen in der Finanzbranche und anderen Sektoren liegt der Fokus auf einer effektiven Kontrolle und Verantwortungsübernahme für KI-Entscheidungen, um regulatorische Standards zu erfüllen und unerwünschte Folgen zu vermeiden.[221]

Ganzheitlicher GRC-Ansatz

Definition

Ein integrierter GRC-Ansatz im Bankensektor bezieht sich auf eine umfassende und nahtlose Zusammenarbeit zwischen den Bereichen Governance, Risk Management und Compliance. Diese Zusammenarbeit wird als ähnlich dem Zusammenspiel eines perfekten Getriebes beschrieben, bei dem die einzelnen "Zahlenräder" der Bereiche ineinandergreifen müssen. Der Ansatz erfordert eine enge Abstimmung, wobei Compliance die gesetzlichen Rahmenbedingungen und Vorgaben liefert, während die anderen Bereiche die Ausarbeitung und Umsetzung übernehmen. Dieser Ansatz zielt darauf ab, sicherzustellen, dass die Unternehmensziele erreicht werden, während gleichzeitig die regulatorischen Anforderungen erfüllt und Risiken kontrolliert werden.

Die Definition eines integrierten GRC-Ansatzes betont, dass die Zusammenarbeit nicht bedeutet, Compliance in der Verantwortung für alle Aspekte zu lassen, sondern vielmehr eine gemeinsame und koordinierte Anstrengung darstellt. Jeder Bereich trägt gemäß seiner Expertise und Zuständigkeit zur Umsetzung bei, wobei das Endziel darin besteht, Erträge zu generieren und gleichzeitig die Vorschriften korrekt anzuwenden. Dies erfordert Verständnis für die spezifischen Bedürfnisse jedes Bereichs sowie die Anerkennung der regulatorischen Vorgaben. Ein integrierter Ansatz bezieht sich auch auf die Nutzung gemeinsamer Datenbanken, die Abstimmung von Prozessen und die gemeinsame Gestaltung von Lösungen. Insgesamt strebt der integrierte GRC-Ansatz an, eine Einheit zu schaffen, in der alle relevanten Themen abgedeckt werden und gleichzeitig die klare Abgrenzung der Zuständigkeiten erhalten bleibt. Der Fokus liegt auf der Erreichung von Unternehmenserträgen, ohne die regulatorischen Anforderungen zu vernachlässigen und dabei Risiken zu kontrollieren. Die Umsetzung dieses Ansatzes erfordert eine enge Koordination, eine kontinuierliche Zusammenarbeit und die

[221] vgl. I3, Pos. 23; I3, Pos. 24

Fähigkeit, Lösungen zu erarbeiten, die sowohl regulatorische Compliance als auch geschäftliche Rentabilität berücksichtigen. [222]

Strategie

In den Bankinstitutionen manifestiert sich eine differenzierte schichtweise in Bezug auf eine integrierte GRC-Strategie. Ein Fachexperte aus einem dieser Bankinstitute betont, dass eine vollständig integrierte Strategie noch nicht vollständig verwirklicht wurde. Deutliche Abgrenzungen bestehen hinsichtlich der Verantwortlichkeiten für verschiedene Bereiche wie Risikomanagement, Compliance und Geldwäsche. Dennoch unterstrich der Experte, dass eine gewisse Form der Kooperation und Abstimmung zwischen den Abteilungen vorhanden ist, um zukünftige Integrationen zu ermöglichen. Die klaren Abgrenzungen der Zuständigkeiten werden als notwendig erachtet, während gleichzeitig die Idee eines integrierten Ansatzes in Betracht gezogen wird.[223]

In einem anderen Bankinstitut äußerte ein Experte im Kontext einer integrierten GRC-Strategie, dass innerhalb ihrer Bank die verschiedenen organisatorischen Einheiten zwar kooperieren, jedoch nicht als eine homogene Einheit agieren. Es wurde auch auf die Aspekte "Integrated Compliance" und "Integrated Risk" hingewiesen, bei denen die Bereiche Compliance und Risikomanagement nebeneinander unter der Leitung desselben Vorstands agieren. Dies deutet auf eine Entwicklung in Richtung eines integrierten GRC-Ansatzes hin. Dennoch spiegelt sich diese Integration nicht in der organisatorischen Struktur wider.[224]

Im Hinblick auf die praktische Implementierung einer integrierten GRC-Strategie gewährt ein anderer Fachexperte Einblicke in interessante Entwicklungen im externen Kontext der Bank, die die Umsetzung der Strategie beleuchten soll. Besonders hervorgehoben wird die Rolle des Chief Administration Office, der die Bereiche Recht, Governance und Compliance verantwortet und im Vorstand eine Schlüsselposition einnimmt. Diese Position fungiert gleichzeitig als Landesleiter für Amerika, was auf eine strategische Anpassung von oberster Ebene hinweist. Die Umsetzung dieser Anpassungen zielt darauf ab, eine Person mit umfangreicher regulatorischer Expertise innerhalb der Organisation zu etablieren, um eine ganzheitliche Perspektive sicherzustellen und entsprechende Maßnahmen umzusetzen. Der Anstoß für diese Neuausrichtung war die Notwendigkeit, einen Governance-Experten in den USA einzusetzen, um potenzielle Schwachstellen zu identifizieren und zu beheben. Zudem besteht eine enge Kooperation mit dem Risikovorstand.

[222] vgl. I1, Pos. 36; I2, Pos. 54; I3, Pos. 26; I3, Pos. 28
[223] vgl. I1, Pos. 40
[224] vgl. I2, Pos. 56

Darüber hinaus wird ein intensiver Austausch mit dem Vorstand des Risikomanagement gepflegt. Trotz der engen Zusammenarbeit agieren die Fachbereiche natürlich unabhängig.[225]

Vorteile eines ganzheitlichen GRC-Ansatzes

Eine ganzheitliche Zusammenführung von Compliance, Risikomanagement und interner Revision ermöglicht einen Wissenstransfer sowie eine nahtlose Integration verschiedener Aspekte. Dies eröffnet die Chance, ein tieferes Verständnis für die Realitäten des Kreditgeschäfts zu gewinnen und gleichzeitig sicherzustellen, dass Compliance-Richtlinien bei Kreditentscheidungen beachtet werden. Eine kontinuierliche Fachwissens- und Informationsübertragung zwischen den beteiligten Sektoren sowie der unabhängigen internen Revision wird als unerlässlich betrachtet, um Verdachtsmomente zu minimieren und eine gemeinsame Basis zu schaffen. [226]

Ein weiterer Vorteil, der aus einem integrierten GRC-Ansatz resultiert, manifestiert sich in der Machtstruktur innerhalb des Unternehmens, insbesondere im Kontext von Compliance und Risikomanagement. Dieser Ansatz initiiert automatisch interdisziplinäre Diskussionen bei Problemerkennung durch Risikomanagement oder Compliance. Diese Kommunikation ermöglicht einen direkten Austausch zwischen diesen Bereichen und verleiht dem Vorstand eine ganzheitliche Perspektive. Die Allianz zwischen Compliance und Risikomanagement schafft zudem eine kohärente Grundlage für standhafte Positionen, um Herausforderungen effizient zu bewältigen.[227]

Der integrierte GRC-Ansatz reduziert Redundanzen in betrieblichen Abläufen durch strategische Kooperation. Eine frühzeitige Einbindung verschiedener Fachbereiche minimiert Doppelaufwände und schont personelle Ressourcen. Dies erhöht die Effizienz und ermöglicht eine gesteigerte Leistung mit weniger Aufwand.[228] Technologische Tools erleichtern die Zusammenarbeit und reduzieren die Komplexität, was zu einer effektiveren Nutzung von Informationen führt.[229]

Effizienzvorteile sind ein zentraler Aspekt des integrierten GRC-Ansatzes. Die intensive Zusammenarbeit zwischen Risikomanagement und Compliance ermöglicht effektive Problemidentifikation und -lösung. Die Integration moderner Tools steigert die Benutzerfreundlichkeit und fördert Effizienz und Effektivität. Redundanzen werden vermieden,

[225] vgl. I3, Pos. 31
[226] vgl. I3, Pos. 33
[227] vgl. I1, Pos. 16
[228] vgl. I1, Pos. 34; l2, Pos. 22
[229] vgl. I1, Pos. 34

indem Doppelaufwände durch frühe Koordination verhindert werden. Dies optimiert die Ressourcennutzung und maximiert die Produktivität.[230]

Die Einführung eines integrierten GRC-Ansatzes zeigt auch Kostenvorteile. Die gemeinsame Nutzung moderner Tools und die Vermeidung von Redundanzen führen zu gesteigerter Effizienz und Kosteneinsparungen. Durch die Nutzung digitaler Technologien werden Prozesse beschleunigt und die Verständlichkeit verbessert. Insgesamt strebt der integrierte GRC-Ansatz eine optimierte Arbeitsweise an, die Effektivität und Kosteneffizienz vereint.[231]

Herausforderungen eines ganzheitlichen GRC-Ansatzes

Die Einführung eines integrierten GRC-Ansatzes bringt einige Herausforderungen und potenzielle Risiken mit sich, die es zu berücksichtigen gilt. Eine zentrale Herausforderung besteht darin, dass bei einer Organisation, in der Compliance und Risikomanagement nicht unter einem Vorstand ressortieren und verschiedene Berichtswege existieren, der Austausch und die Möglichkeit für Diskussionen erschwert werden können. Dies kann die Zusammenarbeit und die Effektivität eines ganzheitlichen Ansatzes beeinträchtigen.[232]

Ein weiteres Risiko ergibt sich aus dem Bestreben nach Redundanzvermeidung im Rahmen eines integrierten GRC-Ansatzes. Während das Ziel darin besteht, Doppelarbeiten zu minimieren, um Effizienz zu steigern, kann es in manchen Fällen aus fachlichen Gründen sinnvoll sein, doppelte Arbeiten durchzuführen, um unterschiedliche Perspektiven zu erhalten.[233] Dies verdeutlicht, dass die Balance zwischen Redundanzvermeidung und der Notwendigkeit einer umfassenden Betrachtung komplexer Themen herausfordernd sein kann.

Die Einführung eines integrierten Ansatzes kann auch zur Vereinheitlichung von individuellen Expertisen führen, was in einer aufgeteilten Organisation möglicherweise anders wäre. Dies kann zu Komplexität, Abstimmungsschwierigkeiten und Reibungsverlusten führen. Zudem könnten mögliche Konkurrenzsituationen zwischen verschiedenen Abteilungen entstehen, die die Effektivität der Zusammenarbeit beeinträchtigen könnten.[234]

[230] vgl. I1, Pos. 34
[231] vgl. I1, Pos. 34; l2, Pos. 22; I3, Pos. 33
[232] vgl. I1, Pos. 22
[233] vgl. I2, Pos. 20
[234] vgl. I2, Pos. 60

6.3 Diskussion

Die Diskursanalyse umfasst eine kritische Evaluierung der angewandten Forschungsmethodik. Die Resultate der Experteninterviews werden einer eingehenden Analyse unterzogen und im Kontext der wissenschaftlichen Untersuchung erörtert.

6.3.1 Reflexion der Methodenauswahl

Für die vorliegende Arbeit wurde die qualitative Forschungsmethode des Experteninterviews als angemessen erachtet und angewendet. Die Interviews ermöglichten eine Vertiefung in Aspekte, die nicht unmittelbar im vorgegebenen Leitfaden enthalten waren. Der persönliche Kontakt wurde nicht als unabdingbar erachtet, weshalb die Experteninterviews telefonisch durchgeführt wurden. Diese Vorgehensweise ermöglichte eine flexiblere Terminvereinbarung. Die gewählte Herangehensweise beeinflusste nicht die Interviewsituation und hatte keinen negativen Einfluss auf die Ergebnisse. Jedoch erwies sich dies teilweise als Herausforderung bei der Transkription der Interviews, aufgrund von Hintergrundgeräuschen, schwacher Verbindung oder undeutlicher Aussprache. Es ist wichtig zu berücksichtigen, dass die Interviewteilnehmer oft eigene Erfahrungen, Beispiele und Perspektiven einbrachten. Hierdurch wurde die Möglichkeit geschaffen, die Aussagen mittels konkreter Beispiele aus der Praxis zu verstärken und zu erläutern. Die Aussagen der Experten trugen subjektiven Charakter, demensprechend war es teilweise herausfordernd möglichst objektive Schlussfolgerungen bezüglich einer GRC-Integration abzuleiten. Dies ermöglichte eine gewisse Verallgemeinerung der Aussagen.

Zudem ist anzumerken, dass, die Untersuchung durch die fehlende Möglichkeit des Vergleichs mit Unternehmen, die bereits einen integrierten GRC-Ansatz implementiert haben, beschränkt wurde. Der vorgegebene Leitfaden hat sich im Kontext der Interviewsituation als förderlich erwiesen. Durch die Anwendung dieses Leitfadens konnte eine Steigerung der persönlichen Interaktionsdynamik sowie eine Intensivierung des Informationsgehaltes durch die inhärente Offenheit der angewandten Methodik erreicht werden[235]. Infolgedessen wurde eine Struktur für die Orientierung etabliert.[236] Die Initiation des Interviews wurde erleichtert. Die Anwendung der Analysemethode nach Mayring (1994) aufgrund ihrer anpassungsfähigen Implementierung als adäquat erachtet wurde und zu einem optimalen Resultat führte.

[235] vgl. Röbken und Wetzel (Qualitative und quantitative Forschungsmethoden, 2017), S. 15
[236] vgl. Lamnek (Qualitative Sozialforschung 2010), S. 23

6.3.2 Ergebnisdiskussion

In diesem Kapitel erfolgt die Analyse der Forschungsfrage, die die empirische Untersuchung der aktuellen GRC-Praktiken von Banken umfasst. Des Weiteren werden die Vorteile eines integrierten Ansatzes für Governance, Risiko und Compliance in Banken sowie die damit verbundenen Herausforderungen und Risiken bei der Umsetzung eines umfassenden GRC-Ansatzes anhand der Analyseergebnisse der zentralen Hauptkategorien erörtert.

Zunächst werden die Ergebnisse zu den gegenwärtigen GRC-Praktiken in Banken genauer beschrieben. Hierbei haben die Experten eine Reihe von Faktoren hervorgehoben, die in der Praxis erhebliche Bedeutung besitzen. Als erster Erkenntnisgewinn lässt sich festhalten, dass gegenwärtige GRC-Praktiken von einer Vielzahl untereinander verknüpfter Faktoren beeinflusst werden. Dies führt zur Entstehung von diversen Subkategorien, die die relevanten Faktoren anschaulich gliedern. Diese Subkategorien umfassen die organisatorische Verankerung, die Unternehmenskultur und -politik, die Rollen von Governance, Risk und Compliance, die Aufgabenabgrenzung, die Kommunikation und Zusammenarbeit sowie Technologische Lösungen und das Reporting.

Im Hinblick auf die organisatorische Verankerung von GRC offenbaren die befragten Bankinstitute eine Vielzahl an Ansätzen. Diese reichen von integrierten Strukturen, in denen die verschiedenen Bereiche eng miteinander verknüpft sind, bis hin zu eigenständigen Ressorts. Diese Bandbreite betont die Anpassungsfähigkeit und Flexibilität der Banken bei der Ausgestaltung ihrer GRC-Funktionen. Hierbei wurde deutlich, dass die organisatorische Verankerung einen signifikanten Einfluss auf die Struktur der Berichtswege, den Informationsaustausch sowie die Machtstruktur ausübt. Insbesondere wurde ersichtlich, dass die Zuordnung von Compliance, Risikomanagement und interner Revision zum selben Vorstand dazu führt, dass die Schnittstellen eine gemeinsame Berichtsstruktur aufweisen. Dies impliziert wiederum eine erleichterte Kommunikation und Interaktion zwischen den betreffenden Bereichen im Vergleich zu Szenarien, in denen diese Abteilungen unter unterschiedlichen Vorständen operieren. Wenn die Abteilungen gemeinsam Bericht erstatten, beispielsweise in derselben Vorstandssitzung oder innerhalb eines integrierten GRC-Berichts, erfährt die Machtstruktur eine zusätzliche Stärkung. Diese Konstellation ermöglicht eine verstärkte Aufmerksamkeit für Probleme und Risiken sowie eine intensivere Kommunikation mit dem Vorstand, im Vergleich zu Szenarien, in denen jede Schnittstelle einem eigenständigen Vorstandsmitglied zugeordnet ist.

Ein weiterer wichtiger Aspekt ist die klare Abgrenzung der Zuständigkeiten zwischen internen und externen Governance-Organen. In diesem Zusammenhang wurde deutlich, wie wichtig eine klare Abgrenzung der Aufgaben und Verantwortlichkeiten innerhalb der verschiedenen Bereiche ist, um sicherzustellen, dass jede Funktion ihre spezifischen Verantwortungsbereiche erfüllt und potenzielle Fehlzuweisungen vermieden werden. Ungeachtet dieser Abgrenzung betonen sämtliche Befragten die Bedeutung eines tiefgreifenden Informationsaustauschs zur Förderung einer effektiven Zusammenarbeit. Dieser Austausch wird als essenziell erachtet, um Synergien zu nutzen und Herausforderungen gemeinsam anzugehen. Jedoch wird hervorgehoben, dass die Schnittstellenüberschneidungen nicht dazu genutzt werden sollten, die Grenzen der Verantwortlichkeiten zu übersteigen.

Ein weiteres Element, das in den GRC-Praktiken von besonderem Belang ist, betrifft die Rolle von GRC im Bankensektor. Die Bedeutung von GRC im Bankensektor hat im Laufe der Zeit eine grundlegende Veränderung erfahren. In der historischen Betrachtung wurden diese Bereiche häufig als mögliche Hemmnisse für die Maximierung der Gewinne angesehen. Die vorliegenden Ergebnisse deuten jedoch auf eine Verschiebung dieser Wahrnehmung hin. Die direkte Berichterstattung der GRC-Bereiche an den Vorstand unterstreicht zunehmend ihre wachsende Bedeutung sowie ihre Rolle im Kontext des Schutzes der Vorstandsinstanz. Dieser veränderte Blickwinkel verdeutlicht die neu gewonnene Anerkennung der Rolle von GRC bei der Gewährleistung der Stabilität und Integrität des Bankensektors.

Des Weiteren wurde eruiert, dass eine transparente innerbetriebliche Kommunikation einer hohen Bedeutung beigemessen wird. Die Förderung von regelmäßigem Austausch und offenen Diskussionen trägt dazu bei, konstruktive Lösungsansätze für auftretende Probleme zu entwickeln. In allen befragten Bankinstituten, in denen eine offene Unternehmenskultur vorherrscht, wird eine größere Bereitschaft zur offenen Ansprache von Problemen beobachtet. Im Gegensatz dazu könnte dieser offene Austausch in Organisationen mit einer weniger transparenten Kultur möglicherweise eingeschränkt sein. Darüber hinaus begünstigt eine offene unternehmensinterne Politik einen regelmäßigen und konstruktiven Austausch zwischen den internen und externen Governance-Organen. Die Einführung einer informellen Kommunikationskultur, wie beispielsweise die Verwendung des "Du"-Ansatzes, sowie ein offener Umgang unter den Mitarbeitern unterstützen zusätzlich die hausinterne Kommunikation. Dies fördert eine Atmosphäre, in der Informationen und Erkenntnisse frei fließen können, um die effektive Zusammenarbeit und Koordination zwischen den verschiedenen GRC-Bereichen zu erleichtern. Die räumliche Aufteilung innerhalb der Bankinstitutionen korreliert ebenfalls eng mit der Qualität der hausinternen Kommunikation.

Die räumliche Nähe der Schnittstellen zueinander, insbesondere wenn sie sich im selben Büro oder Raum befinden, fördert einen flexibleren und offeneren Austausch. Die unmittelbare räumliche Nachbarschaft der relevanten Bereiche, wie beispielsweise dem Risikomanagement und der Compliance-Abteilung, schafft die Grundlage für einen kontinuierlichen Dialog. Diese räumliche Anordnung unterstreicht die Wichtigkeit, Herausforderungen direkt anzusprechen und eine offene Kommunikation aufrechtzuerhalten, auch wenn unterschiedliche Meinungen vorhanden sind.

Der Einsatz technologischer Lösungen zur Automatisierung und Systematisierung komplexer GRC-Prozesse wird als bedeutende Investition betrachtet, um Transparenz, Effizienz und Dokumentation zu verbessern. Verschiedene Tools werden genutzt um die Erfassung, Weiterleitung und Implementierung von Vorschriften sowie die Verwaltung von Risiken.

Schließlich verdeutlicht die Untersuchung verschiedene methodische Ansätze bei der GRC-Berichterstattung. Die Bedeutung einer ganzheitlichen Berichterstattung wird hervorgehoben, um regulatorischen Anforderungen und Silo-Effekten entgegenzuwirken. Quartalsweise Berichtssitzungen und der regelmäßige Dialog zwischen verschiedenen Vorstandsmitgliedern tragen zur umfassenden Lagebewertung und zur Bewältigung regulatorischer Herausforderungen bei.

Die gewonnenen Ergebnisse aus den Experteninterviews veranschaulichen in hohem Maße die gegenwärtigen GRC-Herausforderungen im Bankensektor. In diesem Zusammenhang wurde die Problematik der rapiden rechtlichen Veränderungen erörtert, die von Finanzinstituten die gleichzeitige Bewältigung laufender geschäftlicher Aktivitäten erfordert, sowie die Prüfung regulatorischer Anforderungen bei der Einführung neuer Produkte. Die stetigen rechtlichen Neuerungen erzwingen Anpassungen sowohl in den organisatorischen Strukturen als auch im personellen Bereich. Die verstärkte Aufmerksamkeit seitens Regulatoren, Stakeholdern und Kunden auf Compliance- und Risikomanagementrichtlinien setzt Banken unter Druck, die notwendigen Standards einzuhalten. Die Integration neuer Gesetze in bestehende Prozesse stellt im Bankensektor eine erhebliche Herausforderung dar. Angesichts der umfangreichen rechtlichen Bestimmungen ist es unrealistisch anzunehmen, dass sämtliche Anforderungen zu 100 Prozent erfüllt werden können.

Die wachsende Bedeutung der Künstlichen Intelligenz (KI) im Bereich GRC führt zu Effizienzsteigerungen und gleichzeitig zu Herausforderungen. KI ermöglicht Prozessvereinfachungen und Kosteneinsparungen, erfordert jedoch eine angemessene Kontrolle und menschliche Intervention, um regulatorische Standards sicherzustellen. Hierbei

spielt Governance eine zentrale Rolle, um KI-Einsätze zu überwachen, zu kontrollieren und unerwünschte Auswirkungen zu verhindern.

Im Folgenden erfolgt eine Ausführung der Ergebnisse hinsichtlich der Vorteile eines ganzheitlichen GRC-Ansatzes. Insgesamt wurde eine Vielzahl positiver Effekte, die aus der Anwendung eines integrierten GRC-Ansatzes resultieren, ersichtlich. Die Fusion von Compliance, Risikomanagement und interner Revision eröffnet ein hohes Potenzial für Wissensaustausch und nahtlose Integration verschiedener unternehmensinterner Facetten. Diese ganzheitliche Herangehensweise ermöglicht nicht nur ein tieferes Verständnis der Realitäten des Kreditgeschäfts, sondern gewährleistet auch die Einhaltung von Compliance-Richtlinien während des Kreditentscheidungsprozesses. Dies wird durch eine kontinuierliche Übertragung von Fachwissen und Informationen zwischen den involvierten Sektoren sowie der unabhängigen internen Revision unterstützt. Dies ist eine wesentliche Grundlage zur Minimierung potenzielle Verdachtsmomente. Ein zusätzlicher Vorzug eines integrierten GRC-Ansatzes kristallisiert sich in der Veränderung der Machtstruktur innerhalb des Unternehmens, insbesondere im Kontext von Compliance und Risikomanagement. Dieser Ansatz initiiert von Natur aus interdisziplinäre Diskussionen im Falle der Problemerkennung durch das Risikomanagement oder die Compliance-Abteilung. Diese Kommunikation ermöglicht einen direkten Austausch zwischen diesen Funktionsbereichen und verschafft dem Vorstand eine ganzheitliche Perspektive. Die enge Kooperation von Compliance und Risikomanagement schafft zudem eine kohärente Grundlage für robuste Positionierungen zur effizienten Bewältigung von Herausforderungen.

Der integrierte GRC-Ansatz reduziert außerdem Betriebsredundanzen durch strategische Zusammenarbeit. Die frühzeitige Einbeziehung unterschiedlicher Fachabteilungen minimiert die Duplizierung von Arbeitsschritten und schont somit die personellen Ressourcen. Diese Vorgehensweise steigert die Effizienz und ermöglicht eine höhere Leistung bei gleichzeitig geringerem Aufwand. Die Integration technologischer Werkzeuge erleichtert die Zusammenarbeit und reduziert die Komplexität, was letztlich zu einer optimierten Nutzung von Informationen führt.

Die Generierung von Effizienzvorteilen stellt einen zentralen Aspekt des integrierten GRC-Ansatzes dar. Die intensive Kooperation zwischen Risikomanagement und Compliance ermöglicht eine effektive Identifikation und Lösung von Problemen. Durch die Implementierung moderner Tools wird die Nutzerfreundlichkeit gesteigert und somit Effizienz und Effektivität gefördert. Die Vermeidung von Redundanzen durch eine frühzeitige Koordination trägt zur Ressourcenoptimierung bei und maximiert die Produktivität.

Die Einführung eines integrierten GRC-Ansatzes birgt ebenso Kostenvorteile. Die gemeinsame Nutzung von modernen Werkzeugen und die Eliminierung von Redundanzen führen zu gesteigerter Effizienz und folglich zu Kosteneinsparungen. Die Integration digitaler Technologien beschleunigt die Prozesse und verbessert die Verständlichkeit. Insgesamt strebt der integrierte GRC-Ansatz eine optimierte Arbeitsweise an, die Effektivität und Kosteneffizienz harmonisch vereint.

Abschließend erfolgt eine Darlegung der Erkenntnisse im Hinblick auf die Herausforderungen und Risiken eines integrierten GRC-Ansatzes. Die Umsetzung eines integrierten GRC-Ansatzes bringt verschiedene Herausforderungen und potenzielle Risiken mit sich, die eine sorgfältige Berücksichtigung erfordern. Eine Herausforderung entsteht durch die Organisationstruktur, in der Compliance und Risikomanagement unter getrennten Vorstandsressorts angesiedelt sind, wodurch verschiedene Berichtswege existieren.

Diese Trennung kann die Kommunikation, den Austausch von Informationen und die Möglichkeit für konstruktive Diskussionen beeinträchtigen. Eine solche Hürde kann wiederum die Zusammenarbeit und die Effektivität eines ganzheitlichen Ansatzes erheblich behindern.

Ein weiteres signifikantes Risiko entsteht aus dem Bestreben, Redundanzen im Rahmen eines integrierten GRC-Ansatzes zu minimieren. Obschon das Hauptziel in der Effizienzsteigerung durch die Vermeidung von Doppelarbeiten besteht, kann es in einigen Fällen aus fachlicher Perspektive durchaus sinnvoll sein, wiederholte Tätigkeiten auszuführen, um diverse Blickwinkel und Aspekte zu erfassen. Dies hebt hervor, dass die Balance zwischen der Vermeidung von Redundanzen und der Notwendigkeit einer umfassenden Betrachtung komplexer Fragestellungen eine Herausforderung darstellen kann.

Die Einführung eines integrierten Ansatzes kann auch zur Vereinheitlichung individueller Expertisen führen, die in einer segmentierten Organisation möglicherweise diverser wären. Dies kann zu Komplexitätszunahmen führen, begleitet von Schwierigkeiten in der Abstimmung und potenziellen Reibungsverlusten. Darüber hinaus könnten wettbewerbliche Situationen zwischen verschiedenen Abteilungen entstehen, die die Effizienz und Zusammenarbeit beeinträchtigen könnten. Diese Punkte verdeutlichen, dass die Harmonisierung von Fachwissen und die gleichzeitige Aufrechterhaltung der notwendigen Diversität in einem integrierten GRC-Ansatz eine anspruchsvolle Aufgabe darstellen.

6.3.3 Ansatzpunkte für die Unternehmenspraxis in Banken

Die Vorteile eines ganzheitlichen GRC-Ansatzes eröffnen vielfältige Ansatzpunkte für die Anwendung in der Unternehmenspraxis von Banken. Durch die Integration von Compliance, Risikomanagement und interner Revision ergeben sich folgende Implikationen:

1. Ein periodisch etablierter Jour-Fix, bei dem die Schnittstellen der Bereiche Compliance, Risikomanagement und interne Revision einmal monatlich in einen Dialog treten. In diesem Rahmen erfolgt ein Austausch über gegenwärtige fachliche Schnittmengen sowie die Exploration von Möglichkeiten zur gegenseitigen Unterstützung und Synergienutzung.
2. Die Implementierung einer Softwareapplikation, die sämtlichen Schnittstellenpartnern zugänglich ist, und die durch ihre Nutzerfreundlichkeit geprägt ist. Diese sollte sowohl Fachexperten als auch Nicht-Spezialisten eine mühelose und zügige Handhabung des Tools ermöglichen.
3. Sofern die Schnittstellen einer einheitlichen Vorstandsstruktur untergeordnet sind, bietet ein umfassendes GRC-Berichtswesen den Einheiten die Chance, Problematiken effizienter gegenüber dem Vorstand zu kommunizieren, wobei sie ihre hierarchischen Strukturen zur Unterstützung nutzen können.

7 Reflexion und Ausblick

Zum Abschluss erfolgt in diesem Abschnitt eine detaillierte Betrachtung der Gütekriterienreflexion sowie die Zusammenfassung der Erkenntnisse dieser Arbeit.

7.1 Gütekriterien

Messfehler stellen inhärente Aspekte empirischer Untersuchungen dar. Infolgedessen manifestiert sich das primäre Bestreben darin, die Präzision der Messprozedur zu evaluieren und die Fehler zu reduzieren. Im Kontext der Beurteilung sowohl des Verfahrenscharakters als auch der interpretativen Kapazität der Resultate kristallisieren sich drei essenzielle Gütekriterien heraus: Validität, Reliabilität und Objektivität.[237] Die drei Gütekriterien wurden weitestgehend adhäriert. „Die Validität einer Skala bezeichnet den Grad der Genauigkeit, mit der ein Verfahren tatsächlich das misst oder vorhersagt, was es messen oder vorhersagen soll“[238] In Kapitel 5 wurde genau beschrieben, was unter GRC zu verstehen ist. Die Untersuchung sollte die gegenwärtigen GRC-Praktiken und Herausforderungen sowie die Vorteile und Nachteile eines integrierten Ansatzes beleuchten. Dies wurde erfüllt. Der Untersuchungsgegenstand, in diesem Fall die Experten, wurde basierend auf der Größe der Banken ausgewählt, da in der Arbeit der Schwerpunkt auf Aktiengesellschaften gelegt wurde. Zudem wurden die Experten aus verschiedenen Regionen in Deutschland rekrutiert, um eventuelle regionale Disparitäten angemessen zu berücksichtigen. Diese Experten weisen vielfältige berufliche Hintergründe auf. Im Hinblick auf den Verlauf der Datenerhebung wurden sämtliche Interviews in zeitlichen Abständen von mehreren Tagen durchgeführt, wobei allen Fachexperten anhand eines Leitfadens identische Fragen gestellt wurden. Die Interviews wurden nicht in Person durchgeführt. Daher waren die Rahmenbedingungen für alle Befragten homogen. Im Verlauf der Datenanalyse konnten sämtliche Antworten und Interviewergebnisse uneingeschränkt herangezogen werden, ohne Verluste zu verzeichnen. Das Gütekriterium der Reliabilität impliziert die Reproduzierbarkeit der Forschungsprozedur. Es konzentriert sich demnach auf die Methodik der Messung. Dies impliziert, dass die angewandte Methodik bei wiederholter Durchführung zu konsistenten Ergebnissen führen sollte.[239] Mittels des Leitfadens wurde der Rahmen für das Interview definiert, der Leitfaden gewährleitet die Möglichkeit zur Reproduktion der Messresultate eröffnet. Nichtsdestotrotz wurden einige Fragen teilweise in variierender Abfolge gestellt, und zusätzliche Nachfragen zu differenzierten Aspekten

[237] vgl.Himme (Gütekriterien der Messung: Reliabilität, Validität und Generalisierbarkeit, 2007), S. 375
[238] Rammstedt (Reliabilität, Validität, Objektivität, 2010), S. 250
[239] vgl. Himme (Gütekriterien der Messung: Reliabilität, Validität und Generalisierbarkeit, 2007), S. 375

formuliert, abhängig von der Interviewdynamik und -situation. Die Graduierung der Objektivität verweist darauf, in welchem Ausmaß das erzielte Resultat frei von externen Einflüssen ist, die außerhalb des Kontexts des untersuchten Objekts wirken.[240] Sämtliche Individuen wurden unter homogenen und gerechten Rahmenbedingungen einer Befragung unterzogen. Mittels eines strukturierten Kategoriensystems wurde der Ansatz verfolgt, den Verlauf des Vorgehens so transparent wie möglich zu gestalten. Es erfolgte eine detaillierte Darlegung des methodischen Vorgehens von der Datenerhebung bis hin zu den abgeleiteten Schlussfolgerungen, wodurch die Schritte der Interpretation rückverfolgbar sind. Im Verlauf der Interviewdurchführung wurde eine partielle Unklarheit in der Formulierung einiger Fragen bemerkt, was für zukünftige Untersuchungen ein Verbesserungspotenzial birgt. Durch die Analyse des Themenkomplexes "Vor- und Nachteile eines holistischen GRC-Ansatzes" wurde eine Evidenz erbracht, die Parallelen zu Erkenntnissen anderer Forscher aufweist, die eine vergleichbare Thematik untersuchten.

7.2 Fazit

Das primäre Ziel dieser Bachelorarbeit bestand darin, die aktuell praktizierten GRC-Ansätze zu untersuchen und sowohl die positiven Aspekte als auch die potenziellen Herausforderungen eines ganzheitlichen integrierten GRC-Ansatzes zu identifizieren. Mittels einer Analyse auf Grundlage von Experteninterviews wurden die bestehenden GRC-Praktiken sowie die Vorzüge und Schwierigkeiten einer integrierten GRC-Vorgehensweise untersucht. Hierbei erfolgt die Erfassung eines Kategoriensystems, das daraufhin in einem eigenständigen Modell dargestellt und kohärent zusammengeführt wurde. An dieser Stelle können die Erläuterungen von Kirkpatrick, Bruehl und Hiendlmeier nochmals aufgegriffen werden: Zunehmend wird die mangelhafte Corporate Governance der Banken als eine der Hauptursachen der Krise diskutiert.[241] Eine Folge der Entwicklung ist ein erhöhter Diskurs bezüglich der Relevanz von GRC. Um hohe Verluste und Insolvenzen von Bankinstituten zu verhindern und die Branche insgesamt zu stabilisieren, wurden weltweit neue Vorschriften eingeführt. Um diesen Anforderungen wirksam zu begegnen, ist ein angemessenes und leistungsfähiges GRC-Management erforderlich. Neben der essentiellen Aufgabe der Gewährleistung regulatorischer

[240] vgl.Rost (Lehrbuch Testtheorie, 1996) zitiert nach Rammstedt (Reliabilität, Validität, Objektivität, 2010), S. 240
[241] vgl.Kirkpatrick (The corporate governance lessons from the financial crisis, 2009), S. 61-87

Konformität besteht die Herausforderung darin, gleichzeitig Effizienzpotenziale zu nutzen und Unternehmensrisiken über Abteilungsgrenzen hinweg zu managen.[242]

Die signifikante Relevanz dieser Thematik wurde bereits in der einleitenden Phase ausführlich erörtert. Diese Aussage kann jedoch durch die gewonnenen Erkenntnisse der vorliegenden Arbeit zusätzlich angereichert werden.

Zusammenfassend ergibt sich aus den Forschungsergebnissen, dass eine Vielzahl von determinierenden Elementen existiert, die in der gegenwärtigen Praxis des GRC eine signifikante Funktion einnehmen. Diese Faktoren umfassen die strukturelle Integration auf organisatorischer Ebene, die präzise Definition der Aufgabenabgrenzung, die Ausgestaltung der Unternehmenskultur sowie Unternehmenspolitische Gegebenheiten, die zu Grunde liegende Rolle des GRC-Konzepts selbst, die Qualität der Kommunikation und Kollaboration, das Berichtswesen sowie nicht zuletzt technologische Lösungsansätze zur effizienten Bewältigung der Anforderungen.

Durch die Implementierung eines umfassenden GRC-Ansatzes ergeben sich für Bankinstitute potenzielle Vorteile. Die holistische Vereinigung von Compliance, Risikomanagement und interner Revision vermag den Wissenstransfer zu begünstigen und die nahtlose Integration verschiedenster Facetten zu ermöglichen. In diesem Kontext wird ein verbessertes Verständnis der Kreditgeschäftsdynamik gefördert, dass wiederum die Einhaltung der Compliance-Richtlinien im Rahmen von Kreditentscheidungen begünstigt. Eine fortlaufende Übertragung von Fachwissen und Informationen trägt dazu bei, Verdachtsmomente zu minimieren und interdisziplinäre Diskurse zu stimulieren. Der holistische GRC-Ansatz stärkt die hierarchischen Strukturen, erleichtert die Kommunikation zwischen verschiedenen Fachrichtungen und legt ein kohärentes Fundament für die Lösungsfindung. Die Integration technologischer Werkzeuge steigert die Effizienz und vereinfacht den Informationszugang. Neben den Effizienzsteigerungen, die aus intensiver Kooperation, frühzeitiger Abstimmung und modernen Instrumenten erwachsen, generieren sich ebenfalls Effekte zur Kostenreduktion. Diese ergeben sich aus der gemeinsamen Nutzung von Werkzeugen, der Minimierung von Redundanzen sowie der Beschleunigung von Abläufen. Der ganzheitliche GRC-Ansatz strebt somit eine optimierte Betriebsweise an, die sowohl Effektivität als auch Kosteneffizienz in sich vereint. Im Gegenzug zur Vielzahl von Vorteilen sind jedoch auch bei der Implementierung eines integrierten GRC-Ansatzes diverse Herausforderungen und Risiken zu berücksichtigen. Die Einführung eines solchen Ansatzes ist nicht frei von kritischen Aspekten. Eine zentrale

[242] vgl. Bruehl und Hiendlmeier (Auf dem Weg zu einem ganzheitlichen GRC-Management? Empirische Befunde zur Integration von Internem Kontrollsystem, Risikomanagement und Compliance, 2013), S. 1 ff.

Herausforderung liegt in der strukturellen Organisation, bei der Compliance und Risikomanagement separate Berichtswege verfolgen, was potenziell den reibungslosen Informationsaustausch behindern kann. Die kohärente Zusammenführung dieser Abteilungen zur Erreichung eines integrierten Ansatzes kann sich als komplex erweisen. Ein weiteres Risiko ergibt sich aus dem Bestreben nach Redundanzvermeidung. Diese Absicht kann jedoch in bestimmten Szenarien dazu führen, dass vielfältige Perspektiven und Herangehensweisen beeinträchtigt werden. Die Notwendigkeit, Redundanzen zu minimieren, sollte also in Einklang mit dem Ziel stehen, unterschiedliche Blickwinkel angemessen zu berücksichtigen. Darüber hinaus könnten die Bemühungen um einheitliche Expertise zu einer Zunahme an Komplexität führen. Dies könnte zu Abstimmungsproblemen und potenziellen Konflikten zwischen verschiedenen Abteilungen führen, insbesondere wenn es um die Ausübung von Aufgaben und Verantwortlichkeiten geht. Ein solcher Versuch, Einheitlichkeit zu erreichen, sollte daher sensibel gestaltet werden, um nicht unvorhergesehene Konkurrenzsituationen und Beeinträchtigungen der Arbeitsabläufe hervorzurufen. Die Forschungsfrage konnte dementsprechend beantwortet werden und die Zielsetzung wurde erreicht. Es ist zu vermerken, dass ursprünglich lediglich die Prämisse vorlag, dass ein integrierter Ansatz ausschließlich Nutzen in Form von Redundanzvermeidung, gesteigerter Effizienz sowie ökonomischen Vorteilen erwirken würde. Jedoch ergaben die Experteninterviews zusätzliche potenzielle Vorteile, wie etwa die Beeinflussung der Machtstruktur und die erleichterte Übertragung von Fachwissen. Diese anfängliche Hypothese konnte durch die umfassende Untersuchung in ihrer Gänze zufriedenstellend erörtert werden.

Von essenzieller Bedeutung ist die Notwendigkeit für Finanzinstitute, angesichts der stetig wachsenden Flut regulatorischer Anforderungen und Herausforderungen in diesem Sektor ein leistungsstarkes Management für GRC zu etablieren.[243] Diese Entwicklung zwingt zu einem umfassenden Ansatz, der über die Gewährleistung regulatorischer Konformität hinausgeht und die komplexe Aufgabe beinhaltet, sowohl die Bewältigung dieser Herausforderungen zu gewährleisten als auch gleichzeitig Effizienzsteigerungspotenziale zu erkennen und zu nutzen, während Unternehmensrisiken über die Grenzen der einzelnen Abteilungen hinweg effektiv gesteuert werden müssen.

[243] Bruehl und Hiendlmeier (Auf dem Weg zu einem ganzheitlichen GRC-Management? Empirische Befunde zur Integration von Internem Kontrollsystem, Risikomanagement und Compliance, 2013)

Eidesstattliche Erklärung

Ich versichere, dass ich die vorliegende Abschlussarbeit selbständig angefertigt, nicht anderweitig für Prüfungszwecke vorgelegt, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt, sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe und die Überprüfung mittels Anti-Plagiatssoftware dulde.

Ulm, 25.08.2023 E. Steinhart

_____ _____

Ort, Datum Unterschrift

Literaturverzeichnis

Adelson, M. (The Deeper Causes of the Financial Crisis: Mortgages Alone Cannot Explain It, 2013): The Deeper Causes of the Financial Crisis: Mortgages Alone Cannot Explain It, in: The Journal of Portfolio Management 2013, S. 16-31.

Albrecht, S. (Corporate Governance von Banken, 2016): Corporate Governance von Banken, Frankfurt am Main 2016.

Amling, T., Bantleon, U. (Handbuch der Internen Revision Grundlagen, Standards, Berufsstand 2007): Handbuch der Internen Revision Grundlagen, Standards, Berufsstand Berlin 2007.

Bacher, J., Horwath, I. (Einführung in die qualitative Sozialforschung, 2011): Einführung in die qualitative Sozialforschung, in: Johannes Kepler Universität Linz 2011.

Bachmann, G. (Compliance – Rechtsgrundlagen und offene Fragen, 2008): Compliance – Rechtsgrundlagen und offene Fragen, in: Gesellschaftsrecht in der Diskussion 2007, hrsg. von G. Vereinigung 2008, S. 65-101.

Bankenverband (Rolle der Banken in Deutschland auf einen Blick, 22.06.2023): Rolle der Banken in Deutschland auf einen Blick, URL: https://bankenverband.de/unternehmensfinanzierung/rolle-der-banken-deutschland-auf-einen-blick/, abgerufen am: 23.08.2023.

Baums, T. (Risiko und Risikosteuerung im Aktienrecht, 2011): Risiko und Risikosteuerung im Aktienrecht, in: ZHR: Zeitschrift für das Gesamte Handels- und Wirtschaftsrecht 2011, S. 218 - 274.

Boegl, M., Fischer, R. (Aufsicht über Kredit- und Finanzdienstleistungsinstitute, 2017): Aufsicht über Kredit- und Finanzdienstleistungsinstitute, in: Bankrechts-Handbuch, hrsg. von H. Schimansky u.a., 5 Aufl., München 2017, S. §§ 125–133.

Bogner, A. u.a. (Interviews mit Experten: eine praxisorientierte Einführung, 2014): Interviews mit Experten: eine praxisorientierte Einführung 2014.

Böhm, M. (IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT, 2008): IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT, in: HMD - Praxis der Wirtschaftsinformatik 2008, S. 15-29.

Böhm, M. u.a. (Compliance und Alignment: Vorgabenkonformität und Strategieabgleich als Erfolgsfaktoren für eine wettbewerbsfähige IT, 2009): Compliance und Alignment: Vorgabenkonformität und Strategieabgleich als Erfolgsfaktoren für eine wettbewerbsfähige IT, in: HMD Praxis der Wirtschaftsinformatik 2009, S. 7-17.

Bronnert-Härle, C. (Aufsichtsratsausschüsse als neue Akteure der internen Corporate Governance von Banken, 2016): Aufsichtsratsausschüsse als neue Akteure der internen Corporate Governance von Banken, Baden-Baden 2016.

Bruehl, K., Hiendlmeier, A. (Auf dem Weg zu einem ganzheitlichen GRC-Management? Empirische Befunde zur Integration von Internem Kontrollsystem, Risikomanagement und Compliance, 2013): Auf dem Weg zu einem ganzheitlichen GRC-Management? Empirische Befunde zur Integration von Internem Kontrollsystem, Risikomanagement und Compliance, in: Zeitschrift für Interne Revision 2013.

Bundesanstalt für Finanzdienstleistungsaufsicht (Rundschreiben 18/2005 - Mindestanforderungen an das Risikomanagement, 20.12.2005): Rundschreiben 18/2005 - Mindestanforderungen an das Risikomanagement, URL: https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/risikomanagement/marisk/rundschreiben-18-2005-mindestanforderungen-an-das-risikomanagement-bafin--598652, abgerufen am: 30.05.2023.

Bundesanstalt für Finanzdienstleistungsaufsicht (Protokoll zur Sitzung des Fachgremiums MaRisk am 24.4.2013 in Bonn, Thema: Compliance-Funktion, 2013): Protokoll zur

Sitzung des Fachgremiums MaRisk am 24.4.2013 in Bonn, Thema: Compliance-Funktion, URL: https://www.bafin.de/SharedDocs/Downloads/DE/Protokoll/dl_protokoll_130424_FG_marisk.html, abgerufen am: 26.05.2023.

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (Rundschreiben 10/2021 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk, 2021): Rundschreiben 10/2021 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk, URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html?nn=9450904#doc16502162bodyText17.

Bundesgesetzblatt (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), 27. April 1998): Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl198s0786.pdf, abgerufen am: 28.05.2023.

Bundesregierung (Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), BT-Drucks. 13/9712 1998): Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), BT-Drucks. 13/9712 1998.

Bundesregierung (Entwurf eines Gesetzes zur Umsetzung der Richtlinie 2012/.../EU über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen und zur Anpassung des Aufsichtsrechts an die Verordnung (EU) Nr. .../2012 über die Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen (CRD IV-Umsetzungsgesetz), BT-Drucks. 17/10974, 2012): Entwurf eines Gesetzes zur Umsetzung der Richtlinie 2012/.../EU über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen und zur Anpassung des Aufsichtsrechts an die Verordnung (EU) Nr. .../2012 über die Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen (CRD IV-Umsetzungsgesetz), BT-Drucks. 17/10974, URL: https://dserver.bundestag.de/btd/17/109/1710974.pdf, abgerufen am: 26.05.2023.

Bungartz, O. (Interne Revision und Abschlussprüfer, 2011): Interne Revision und Abschlussprüfer, in: Kompendium der Internen Revision: Internal Auditing in Wissenschaft und Praxis, hrsg. von C.-C. Freidank und V. H. Peemöller, Berlin 2011, S. 527 - 556.

Cadbury, A. (Report of the Committee on the Financial Aspects of Corporate Governance, 1992): Report of the Committee on the Financial Aspects of Corporate Governance, URL: https://www.ecgi.global/sites/default/files/codes/documents/cadbury.pdf, abgerufen am: 12.04.2023.

Deutsche Bank (Monatsbericht März 2013, 2013): Monatsbericht März 2013, URL: https://www.bundesbank.de/resource/blob/669244/7e7ad9033c1a30bf39dd5c9dac221b10/mL/2013-03-monatsbericht-data.pdf, abgerufen am: 30.05.2023.

Diederichs, M., Kißler, M. (Aufsichtsratreporting: Corporate Governance, Compliance und Controlling 2008): Aufsichtsratreporting: Corporate Governance, Compliance und Controlling München 2008.

EBA (Final Report - Guidelines on internal governance under Directive 2013/36/EU, 2017): Final Report - Guidelines on internal governance under Directive 2013/36/EU, URL: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1972987/eb859955-614a-4afb-bdcd-aaa664994889/Final%20Guidelines%20on%20Internal%20Governance%20%28EBA-GL-2017-11%29.pdf?retry=1, abgerufen am: 30.05.2023.

EC–European Commission (Green Paper on the EU corporate governance framework, 2011): Green Paper on the EU corporate governance framework, in: European Commission Communication 2011.
Eulerich, M. (Das Three Lines of Defence-Modell 2012): Das Three Lines of Defence-Modell in: Zeitschrift Interne Revision 2012, S. 55-58.
Europäische Kommission (EU-Greenbook: Corporate Governance in Finanzinstituten und Vergütungspolitik, 2010): EU-Greenbook: Corporate Governance in Finanzinstituten und Vergütungspolitik 2010.
Europäische Kommission (EU-Greenbook: Europäischer Corporate Governance Rahmen, 2011): EU-Greenbook: Europäischer Corporate Governance Rahmen 2011.
Fleischer, H. (Organisation; Buchführung, 2019): Organisation; Buchführung, in: Kommentar zum Aktiengesetz, hrsg. von G. Spindler und E. Stilz, 4 Aufl., München 2019.
Füss, R. (Die interne Revision: Bestandsaufnahme und Entwicklungsperspektiven, 2005): Die interne Revision: Bestandsaufnahme und Entwicklungsperspektiven, Berlin 2005.
Gabler Wirtschaftslexikon (Montan-Mitbestimmungsgesetz (MontanMitbestG), o. J.): Montan-Mitbestimmungsgesetz (MontanMitbestG), URL: https://wirtschaftslexikon.gabler.de/definition/montan-mitbestimmungsgesetz montanmitbestg-38952, abgerufen am: 13.05.2023.
Gabler Wirtschaftslexikon (Compliance, o. J.): Compliance, URL: https://wirtschaftslexikon.gabler.de/definition/compliance-27721, abgerufen am: 23.04.2023.
Gebauer, S., Niermann, S. (Compliance in der Banken- und Wertpapierdienstleistungsbranche, 2016): Compliance in der Banken- und Wertpapierdienstleistungsbranche, in: Corporate Compliance: Handbuch der Haftungsvermeidung im Unternehmen hrsg. von C. E. Hauschka u.a., 3 Aufl., München 2016, S. 1 Online-Ressource.
Gill, A. u.a. (Anreize, systemische Risiken und Intransparenz: Lehren aus der Finanz-und Staatsschuldenkrise, 2012): Anreize, systemische Risiken und Intransparenz: Lehren aus der Finanz-und Staatsschuldenkrise.
Gläser, J., Laudel, G. (Experteninterviews und qualitative Inhaltsanalyse, 2010): Experteninterviews und qualitative Inhaltsanalyse 2010.
Goette, W. (Organisationspflichten in Kapitalgesellschaften zwischen Rechtspflicht und Opportunität, 2011): Organisationspflichten in Kapitalgesellschaften zwischen Rechtspflicht und Opportunität, in: ZHR: Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht 2011, S. 388-400.
Hannemann, R. u.a. (Mindestanforderungen an das Risikomanagement (MaRisk), 2019): Mindestanforderungen an das Risikomanagement (MaRisk), 5 Aufl., Stuttgart 2019.
Himme, A. (Gütekriterien der Messung: Reliabilität, Validität und Generalisierbarkeit, 2007): Gütekriterien der Messung: Reliabilität, Validität und Generalisierbarkeit, in: Methodik der empirischen Forschung, hrsg. von S. Albers u.a., Wiesbaden 2007, S. 375-390.
Hirschmann, J. (Aufgaben des Vorstandes als Leitungsorgan, 2005): Aufgaben des Vorstandes als Leitungsorgan, in: Vorstand der AG: Führungsaufgaben, Rechtspflichten und Corporate Governance, hrsg. von J. van Kann, Berlin 2005, S. 59-96.
Hopt, K. J., Wohlmannstetter, G. (Corporate Governance von Banken 2011): Corporate Governance von Banken München 2011.
Ihrig, H.-C., Schäfer, C. (Rechte und Pflichten des Vorstands, 2014): Rechte und Pflichten des Vorstands, Köln 2014.
International Monetary Fund (Global Financial Stability Report: Risk Taking, Liquidity, and Shadow Banking - Curbing Excess while Promoting Growth, 2014): Global Financial Stability Report: Risk Taking, Liquidity, and Shadow Banking - Curbing Excess while Promoting Growth, URL: https://www.imf.org/en/Publications/GFSR/Issues/2016/12/31/Global-Financial-

Stability-Report-October-2014-Risk-Taking-Liquidity-and-Shadow-Banking-41631, abgerufen am: 28.05.2023.
Kirkpatrick, G. (The corporate governance lessons from the financial crisis, 2009): The corporate governance lessons from the financial crisis, in: OECD Journal: Financial market trends 2009, S. 61-87.
Klandt, H., Heidenreich, S. (Empirische Forschungsmethoden in der Betriebswirtschaftslehre: von der Forschungsfrage zum Untersuchungsdesign, eine Einführung, 2017): Empirische Forschungsmethoden in der Betriebswirtschaftslehre: von der Forschungsfrage zum Untersuchungsdesign, eine Einführung 2017.
Krommes, W. (Handbuch Jahresabschlussprüfung Ziele; Technik; Nachweise - Wegweiser zum sicheren Prüfungsurteil, 2015): Handbuch Jahresabschlussprüfung Ziele; Technik; Nachweise - Wegweiser zum sicheren Prüfungsurteil, 4 Aufl., Wiesbaden 2015.
Kuck, D. (Aufsichtsräte und Beiräte in Deutschland: Rahmenbedingungen, Anforderungen, professionelle Auswahl, 2006): Aufsichtsräte und Beiräte in Deutschland: Rahmenbedingungen, Anforderungen, professionelle Auswahl, Wiesbaden 2006.
Lamnek, S. (Qualitative Sozialforschung 2010): Qualitative Sozialforschung 5Aufl., Weinheim Basel.
Larcher, M. (Zusammenfassende Inhaltsanalyse nach Mayring: Überlegungen zu einer QDA-Software unterstützten Anwendung, 2010): Zusammenfassende Inhaltsanalyse nach Mayring: Überlegungen zu einer QDA-Software unterstützten Anwendung, Wien 2010.
Lister, M. (Wege aus der Finanzkrise – Anpassungsbedarf im Risikomanagement der Kreditinstitute, 2010): Wege aus der Finanzkrise – Anpassungsbedarf im Risikomanagement der Kreditinstitute, in: Corporate Governance, Risk Management und Compliance: Innovative Konzepte und Strategien, hrsg. von F. Keuper und F. Neumann, Wiesbaden 2010, S. 295 - 309.
Mallin, C. A. (Corporate Governance, 2019): Corporate Governance, 6 Aufl., Oxford 2019.
Marekfia, W. (Strategisches GRC-Management: Anforderungen, Forschungsagenda und datenseitiges Modell, 2017): Strategisches GRC-Management: Anforderungen, Forschungsagenda und datenseitiges Modell, 3 Aufl., Ilmenau 2017.
Mayring, P. (Qualitative Inhaltsanalyse, 1994): Qualitative Inhaltsanalyse 1994.
Mayring, P. (Qualitative Inhaltsanalyse 2010): Qualitative Inhaltsanalyse in: Handbuch Qualitative Forschung in der Psychologie, hrsg. von G. Mey und K. Mruck 2010, S. 601-613.
Mülbert, P. O., Wilhelm, A. (Risikomanagement und Compliance im Finanzmarktrecht: Entwicklung der aufsichtsrechtlichen Anforderungen, 2014): Risikomanagement und Compliance im Finanzmarktrecht: Entwicklung der aufsichtsrechtlichen Anforderungen, in: ZHR: Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht 2014, S. 502-546.
Otremba, S. (GRC-Management als interdisziplinäre Corporate Governance: Die Integration von Revision, Risiko- und Compliance-Management in Unternehmen, 2016): GRC-Management als interdisziplinäre Corporate Governance: Die Integration von Revision, Risiko- und Compliance-Management in Unternehmen, Wiesbaden 2016.
Paetzmann, K. (Corporate Governance: Strategische Marktrisiken, Controlling, Überwachung, 2012): Corporate Governance: Strategische Marktrisiken, Controlling, Überwachung, 2 Aufl., Berlin, Heidelberg 2012.
Peemöller, V. H., Kregel, J. (Grundlagen der Internen Revision: Standards, Aufbau und Führung, 2014): Grundlagen der Internen Revision: Standards, Aufbau und Führung, Berlin 2014.
Pönisch, S. (Die Entwicklung des deutschen Systems der Coporate Governance Analyse und Entwicklungsdynamiken 2008): Die Entwicklung des deutschen Systems der Coporate Governance Analyse und Entwicklungsdynamiken Saarbrücken 2008.

PricewaterhouseCoopers (Integrity-Driven Performance: A New Strategy for Success Through Integrated Governance, Risk and Compliance Management. A White Paper, 2004): Integrity-Driven Performance: A New Strategy for Success Through Integrated Governance, Risk and Compliance Management. A White Paper, URL: https://docplayer.net/9573578-Integrity-driven-performance.html, abgerufen am: 30.05.2023.

Rammstedt, B. (Reliabilität, Validität, Objektivität, 2010): Reliabilität, Validität, Objektivität, in: Handbuch der sozialwissenschaftlichen Datenanalyse, hrsg. von C. Wolf und H. Best, Wiesbaden 2010, S. 239-258.

Regierungskommission Deutscher Corporate Governance Kodex (Deutscher Corporate Governance Kodex 2022): Deutscher Corporate Governance Kodex 2022.

Röbken, H., Wetzel, K. (Qualitative und quantitative Forschungsmethoden, 2017): Qualitative und quantitative Forschungsmethoden 2017.

Romeike, F. (Risikomanagement, 2018): Risikomanagement, Wiesbaden 2018.

Rost, J. (Lehrbuch Testtheorie, 1996): Lehrbuch Testtheorie, in: Testkonstruktion, Huber, Bern 1996.

Sarens, G., Abdolmohammadi, M. J. (Monitoring effects of the internal audit function: agency theory versus other explanatory variables, 2011): Monitoring effects of the internal audit function: agency theory versus other explanatory variables, in: International Journal of Auditing 2011, S. 1-20.

Schewe, G. (Unternehmensverfassung: Corporate Governance im Spannungsfeld von Leitung, Kontrolle und Interessenvertretung, 2018): Unternehmensverfassung: Corporate Governance im Spannungsfeld von Leitung, Kontrolle und Interessenvertretung, 4 Aufl., Berlin 2018

Schindera, H. (Die Kompetenzenverteilung der Organe einer Aktiengesellschaft im Übernahmeverfahren 2002): Die Kompetenzenverteilung der Organe einer Aktiengesellschaft im Übernahmeverfahren Tübingen 2002.

Schmidt, S., Reimer, B. (Zusammenwirken von Abschlussprüfung und Interner Revision, 2008): Zusammenwirken von Abschlussprüfung und Interner Revision, in: Corporate Governance und Interne Revision: Handbuch für die Neuausrichtung des Internal Auditings, hrsg. von C.-C. Freidank und V. H. Peemöller, Berlin 2008, S. 644 - 660.

Schneider, U. H. (Compliance als Aufgabe der Unternehmensleitung, 2003): Compliance als Aufgabe der Unternehmensleitung, in: ZIP: Zeitchrift für Wirtschaftsrecht 2003, S. 645 - 650.

Schoch, C. G. u.a. (Governance, Risk und Compliance als Führungsaufgabe im Lichte der sich verändernden regulatorischen Anforderungen in der Finanzbranche am Beispiel der Schweiz, 2016): Governance, Risk und Compliance als Führungsaufgabe im Lichte der sich verändernden regulatorischen Anforderungen in der Finanzbranche am Beispiel der Schweiz, in: Kölner Schrift zum Wirtschaftsrecht 2016, S. 282-293.

Schug, C. (Risikoeinschränkung und -transfer in der Vorstandshaftung, 2010): Risikoeinschränkung und -transfer in der Vorstandshaftung, 4 Aufl., Baden-Baden 2010.

Spindler, G. (Vorstandspflichten zur Einrichtung eines Frühwarnsystems, 2006): Vorstandspflichten zur Einrichtung eines Frühwarnsystems, in: Handbuch des Vorstandsrechts, München 2006, S. 1 Online-Ressource.

Spindler, G. (Compliance in der multinationalen Bankengruppe, 2008): Compliance in der multinationalen Bankengruppe, in: Wertpapier Mitteilungen 2008, S. 905 - 918.

Standke, F. (Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung, 2010): Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung, in: Corporate Governance, Risk Management und Compliance: Innovative Konzepte und Strategien, hrsg. von F. Keuper und F. Neumann, Wiesbaden 2010, S. 267 - 290.

Swales, J. (Create a research space (CARS) model of research introductions, 2014): Create a research space (CARS) model of research introductions, in: Writing about writing: A college reader 2014, S. 12-15.

Thaten, M. (Die Ausstrahlung des Aufsichts- auf das Aktienrecht am Beispiel der Corporate Governance von Banken und Versicherungen 2016): Die Ausstrahlung des Aufsichts- auf das Aktienrecht am Beispiel der Corporate Governance von Banken und Versicherungen Berlin 2016.

Verse, D. A. (Compliance im Konzern: Zur Legalitätskontrollpflicht der Geschäftsleiter einer Konzernobergesellschaft, 2011): Compliance im Konzern: Zur Legalitätskontrollpflicht der Geschäftsleiter einer Konzernobergesellschaft, in: ZHR: Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht 2011, S. 401-424.

Welge, M. K., Eulerich, M. (Corporate- Governance- Management: Theorie und Praxis der guten Unternehmensführung, 2021): Corporate- Governance- Management: Theorie und Praxis der guten Unternehmensführung, 3 Aufl., Wiesbaden 2021.

Werder, A. (Führungsorganisationen - Grundlagen der Corporate Governance, Spitzen- und Leitungsorganisationen 2015): Führungsorganisationen - Grundlagen der Corporate Governance, Spitzen- und Leitungsorganisationen 3Aufl., Wiesbaden 2015.

Wundenberg, M. (Compliance und die prinzipiengeleitete Aufsicht über Bankengruppen, 2012): Compliance und die prinzipiengeleitete Aufsicht über Bankengruppen 2012.

Zimmer, D., Sonneborn, M. (§ 91 Abs. 2 - Anforderungen und gesetzgeberische Absichten 2001): § 91 Abs. 2 - Anforderungen und gesetzgeberische Absichten in: Risikomanagement nach dem KonTraG, hrsg. von K. W. Lange, München 2001, S. 38 - 59.

Zitzelsberger, S. (Wirtschaftsprüfer, vereidigte Buchprüfer und Wirtschaftsprüfgesellschaften, 2004): Wirtschaftsprüfer, vereidigte Buchprüfer und Wirtschaftsprüfgesellschaften, in: Wirtschaftsprüfung und Interne Revision hrsg. von G. Förschle und V. Peemöller, Heidelberg 2004, S. 41 - 83.

Rechtsquellenverzeichnis

1. Aktiengesetz

§ 91 Abs. 2 AktG
§ 91 Abs. 3 AktG
§§ 93 Abs. 1 und 76 Abs. 1 AktG vgl. supra § 6 B. I. 2. c.

2. Kreditwesengesetz

§ 25a Abs. 1 S. 1 KWG
§ 25a Abs.1 S.3 KWG
§§ 25a Abs. 1 S. 3 Nr. 3 lit. b, 25c Abs. 4a Nr. 3 lit. c KWG
Zum Proportionalitätsgrundsatz vgl. bereits supra § 5 A. II. 2. a. bb. Siehe § 25a Abs. 1 Satz 4 KWG
§ 25b KWG
§ 25b Abs.2 KWG

3. Mindestanforderungen an das Risikomanagement

AT 4.4.2 Tz. 1 MaRisk
AT 4.4.2 Tz. 1 Satz 3 MaRisk
AT 4.4.2 Tz 2 MaRisk
At 4.4.2 Tz. 3 MaRisk
Zur rechtlichen Bindungswirkung der MaRisk vgl. infra § 7 B. II 2. a. aa. (1). Siehe AT 4.4.2 Tz. 4
AT 4.4.2 Tz. 6 MaRisk
At 4.4.2 Tz. 7 MaRisk

Anhang

A Leitfaden: Ganzheitliche Betrachtung von Governance, Risk, Compliance

Das Hauptziel besteht darin, mithilfe Ihres Expertenwissens die bestehenden Forschungslücken zu identifizieren und eine umfassende Analyse eines integrierten Ansatzes von Governance, Risk und Compliance (GRC) zu erstellen. Durch Ihre Expertise sollen bedeutende Erkenntnisse gewonnen werden, um das Verständnis in diesem Bereich zu erweitern.

1) Bitte stellen Sie sich kurz vor und erläutern Sie Ihre Aufgaben.

2) Entwicklung
   a) Wenn Sie jetzt in die Gegenwart schauen und die aktuellen Entwicklungen in Bezug auf Governance, Risk und Compliance im Banksektor betrachten: Wie würden Sie den derzeitigen Stand des Banksektors im Jahr 2023 beschreiben?
   b) Was hat sich im Banksektor im Jahr 2023 im Vergleich zu 2007/2008 verändert?

3) Welche Bedeutung haben regulatorische Anforderungen für die Bank, in der sie tätig sind, und wie wird die Einhaltung der gesetzlichen Anforderungen sichergestellt?

4) Wie würden Sie die Rolle von Governance, Risk und Compliance beschreiben?

5) Wie gestaltet sich die Zusammenarbeit zwischen den internen Governance-Organen Risikomanagements, Internen Revision und Compliance sowie den externen Governance-Organen, wie beispielsweise Wirtschaftsprüfern?

6) Welche spezifischen Herausforderungen und Risiken stellen sich für Banken in Bezug auf Governance, Risk und Compliance dar?

7) Auf welche Weise könnte die Zusammenarbeit sowie Kooperationsmechanismen zwischen den Schnittstellen des Risikomanagements, der Internen Revision und der Compliance optimiert werden, um Redundanzen und Mehrkosten zu vermeiden?

8) Ganzheitliche Betrachtung von GRC
   a) Wie würden Sie einen integrierten GRC-Ansatz definieren?
   b) Verfolgt die Bank, in der sie tätig sind, eine integrierte GRC-Strategie?
   c) Welche potenziellen Vorteile könnten sich durch einen integrierten GRC-Ansatz ergeben?
   d) Welche spezifischen Maßnahmen und Strategien könnten Banken implementieren, um einen integrierten GRC-Ansatz zu gewährleisten?
   e) Welche technologischen Lösungen und Tools könnten in Betracht gezogen werden, um einen integrierten GRC-Ansatz in Banken zu unterstützen?

9) Reporting
   a) Wird in der Bank, in der sie tätig sind, ein regelmäßiges Reporting zu Governance, Risk und Compliance Themen erstellt?
   b) Werden die Reportings von jeder Funktion separat erstellt?
   c) Welche potenziellen Vorteile könnten sich ergeben, wenn sich ein integrierter GRC-Ansatz durchsetzen würde, der ein einheitliches Reporting für alle Funktionen ermöglicht?

B Kategoriensystem

Entwicklung im Banksektor

- Veränderung seit 2007/2008 im Vergleich
- Stand des Banksektors im Jahr 2023

Status quo: Governance, Risk und Compliance

- Organisatorische Verankerung
- Unternehmenskultur; -politik
- Rolle von Governance, Risk und Compliance
- Aufgabenabgrenzung
- Kommunikation und Zusammenarbeit
- Technologische Lösungen
- Reporting

Herausforderungen und Risiken

- Zunehmende Gesetzesvorgaben
- Integration neuer Gesetze in bestehende Prozesse
- Künstliche Intelligenz

Ganzheitlicher GRC-Ansatz

- Definition
- Strategie
- Vorteile eines ganzheitlichen GRC-Ansatzes

Herausforderungen eines ganzheitlichen GRC-Ansatzes

C Inhaltsanalyse

ID	Haupt- und Subkategorie	Position	Paraphrase
I1	Entwicklung im Banksektor > Stand des Banksektors im Jahr 2023	10	Ich würde es mal zusammenfassen, dass wir weiterhin in Entwicklungsstadium sind.
I1	Herausforderungen und -Risiken > Zunehmende Gesetzesvorgaben	10	Ich meine klar, nach 2009 oder auch schon früher 2001, dann auch erst kürzlich, der Bankensektor hat sich stark verändert in den letzten, ja, im Prinzip... In den letzten 20 Jahren wahrscheinlich noch mehr.
I1	Entwicklung im Banksektor > Veränderungen seit 2007/2008 im Vergleich	10	Ich meine klar, nach 2009 oder auch schon früher 2001, dann auch erst kürzlich, der Bankensektor hat sich stark verändert in den letzten, ja, im Prinzip... In den letzten 20 Jahren wahrscheinlich noch mehr. Und gefühlt ist es auch, wenn man mal sieht, wie viele neue Anforderungen auf uns zukommen, wo sich Dinge ändern.
I1	Entwicklung im Banksektor > Stand des Banksektors im Jahr 2023	10	Und daran merkt man, denke ich, dass wir einige Themen, wo man vielleicht denken würde, na ja, wenn man Compliance sich mal als Schaubild malt, dass die Dinge schon drin wären. Und das ist für mich so ein klares Zeichen dafür, dass wir immer noch dabei sind zu umfassen, was muss Compliance eigentlich alles einfangen am Ende.

I1 >	Status quo: Governance, Risiken und Compliance Rolle von Governance, Risk und Compliance	12	Ich glaube, das ist so dieses Chronische, was egal welchen Menschen aus egal welchem Bereich man frägt. Der Bereich, in dem man ist, ist immer unglaublich wichtig, denn sonst würde man da ja nicht arbeiten. Nichtsdestotrotz, Compliance für jemanden, der am Schluss in der Bank steht und irgendwelche Dinge verkauft, wird für ihn nicht so einen hohen Stellenwert haben wie jetzt für mich. Das ist klar. Aber man muss ganz klar sagen und da ist der Gesetzgeber eigentlich auch recht deutlich, ein Compliance Beauftragter - ich bin auch Compliance Beauftragter, hat direkt an den Vorstand zu berichten. Das ist etwas, wo im Prinzip verdeutlichen sollte, es gibt hier nicht noch irgendwelche Umwege, wo Dinge dann verschleiert werden, sondern es ist meine Aufgabe. Ich muss gemeldet werden und der Vorstand muss mich kennen und ich muss mit ihm sprechen. Ich denke, das zeigt eigentlich schon, in welchem Weg wir sind. Und wenn man mal, ich glaube, da kommt nachher auch noch die Frage zu den Reportings, wenn man mal sieht, wie oft ich mit Vorständen, mit Aufsichtsrat und mit unserer französischen Mutter, wie oft wir im Austausch sind. Und wenn ich mal eine rote Ampel melde, wo ich praktisch sage: „wir haben hier ein Problem“ - wenn man sieht, was das für Wellen schlägt. Das zeigt es schon deutlich, dass auch bei uns und ich glaube, das geht wahrscheinlich allen Banken so, vielleicht Wirecard nicht so ganz, aber bei allen, die gut geführt werden, ist es einfach so, dass für den Vorstand mit Sicherheit Compliance eine Stelle ist, die ich regelmäßig lieber mal

I1	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	12	Aber man muss ganz klar sagen und da ist der Gesetzgeber eigentlich auch recht deutlich, ein Compliance Beauftragter - ich bin auch Compliance Beauftragter, hat direkt an den Vorstand zu berichten. Das ist etwas, wo im Prinzip verdeutlichen sollte, es gibt hier nicht noch irgendwelche Umwege, wo Dinge dann verschleiert werden, sondern es ist meine Aufgabe. Ich muss gemeldet werden und der Vorstand muss mich kennen und ich muss mit ihm sprechen. Ich denke, das zeigt eigentlich schon, in welchem Weg wir sind.
I1	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	12	Und wenn man mal, ich glaube, da kommt nachher auch noch die Frage zu den Reportings, wenn man mal sieht, wie oft ich mit Vorständen, mit Aufsichtsrat und mit unserer französischen Mutter, wie oft wir im Austausch sind. Und wenn ich mal eine rote Ampel melde, wo ich praktisch sage: „wir haben hier ein Problem “- wenn man sieht, was das für Wellen schlägt. Das zeigt es schon deutlich, dass auch bei uns und ich glaube, das geht wahrscheinlich allen Banken so, vielleicht Wirecard nicht so ganz, aber bei allen, die gut geführt werden, ist es einfach so, dass für den Vorstand mit Sicherheit Compliance eine Stelle ist, die ich regelmäßig lieber mal frage, allein schon aus Selbstschutz.
I1	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	12	Und wenn man mal, ich glaube, da kommt nachher auch noch die Frage zu den Reportings, wenn man mal sieht, wie oft ich mit Vorständen, mit Aufsichtsrat und mit unserer französischen Mutter, wie oft wir im Austausch sind. Und wenn ich mal eine rote Ampel melde, wo ich praktisch sage: „wir haben hier ein Problem “- wenn man sieht, was das für Wellen schlägt. Das zeigt es schon deutlich, dass auch bei uns und ich glaube, das geht wahrscheinlich allen Banken so, vielleicht Wirecard nicht so ganz, aber bei allen, die gut geführt werden, ist es einfach so, dass für den Vorstand mit Sicherheit Compliance eine Stelle ist, die ich regelmäßig lieber mal frage, allein schon aus Selbstschutz.

I1	Status quo: Governance, Risiken und Compliance > Reporting	14	Ja, ich glaube, da sind wir wahrscheinlich schon, ohne es zu wissen, einen gewissen Schritt gegangen in Richtung GRC als gemeinsamen Ansatz. Denn wir berichten tatsächlich zusammen in einer Sitzung der ganzen Vorstandschaft, und zwar quartärlich. Und halbjährlich sind dann noch die Kollegen von der Gruppe dabei. Genau Wir kommen da direkt hintereinander. Es sind verschiedene Punkte in dieser Präsentation und da kommt eben Compliance, Risk gleich nacheinander. Das heißt vom Reporting her machen wir das schon gemeinsam an die Vorstände und auch an den Aufsichtsrat. Da läuft es ähnlich.
I1	Ganzheitlicher GRC-Ansatz > Vorteile eines ganzheitlichen GRC-Ansatzes	16	Also ein großer Vorteil ist natürlich, wenn wir oder wenn Risk eine Problemstellung identifiziert und sie in dieser Sitzung vorstellt, dann geht die zweite Frage automatisch immer an die jeweils andere Stelle. Das heißt: „was sagt denn ihr dazu?“. Dieser Austausch ist dann auch von Vorstandsseite her im Prinzip der logische Schritt. Und der Vorteil ist, dass eben auch genau für den Vorstand und schließlich müssen die das Unternehmen führen: wenn ein Thema kommt, können sie gleich im Prinzip alle mit verarzten. Sie haben alle direkt beisammen und müssen nicht noch eine extra Sitzung dazu machen. Und dann können sie eben sofort diese Antworten holen, die sie brauchen, um zu entscheiden.
I1	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	18	Ich würde natürlich sagen wir haben eine sehr sehr hohe Bedeutung im Unternehmen. Ich sehe das aber auch durchaus gespiegelt. Wir haben jetzt zum Beispiel ein bisschen Bewegung gehabt, wir haben neuen CEO, wir haben einen neuen CFO. In der ersten Terminrunde, die er hatte, war immer auch Compliance dabei, immer bilateral noch die Gespräche, das heißt man merkt das es ist eine hohe Relevanz hat

I1	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	18	Ich würde natürlich sagen wir haben eine sehr sehr hohe Bedeutung im Unternehmen. Ich sehe das aber auch durchaus gespiegelt. Wir haben jetzt zum Beispiel ein bisschen Bewegung gehabt, wir haben neuen CEO, wir haben einen neuen CFO. In der ersten Terminrunde, die er hatte, war immer auch Compliance dabei, immer bilateral noch die Gespräche, das heißt man merkt das es ist eine hohe Relevanz hat
I1	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	20	Also auch aus meinen vorherigen Stellen, kann ich sagen, es hängt natürlich immer viel mit den Menschen in den Teams ab. Wenn man mit denen gut kann, man, vielleicht sogar im gleichen Flur sitzt, dann ist der Austausch immer ein ganz anderer, als wenn es vielleicht jemand ist, der kurz vor der Rente steht und mit den jungen Leuten, die probieren was zu verändern, nicht so viel anfangen kann.
I1	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	20	Also auch aus meinen vorherigen Stellen, kann ich sagen, es hängt natürlich immer viel mit den Menschen in den Teams ab. Wenn man mit denen gut kann, man, vielleicht sogar im gleichen Flur sitzt, dann ist der Austausch immer ein ganz anderer, als wenn es vielleicht jemand ist, der kurz vor der Rente steht und mit den jungen Leuten, die probieren was zu verändern, nicht so viel anfangen kann.
I1	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	20	Bei uns jetzt in der Kreditplus habe ich den Vorteil, das Risikomanagement direkt gegenübersitzt, der Leiter ein ähnliches Alter wie ich hat und wir im Prinzip andauernd im Austausch sind. Das heißt, wenn ich irgendwo Probleme mit etwas habe, was er tut, oder andersrum, dann kommt man halt kurz rüber und klärt die Sache und kann auch einfach offen ehrlich miteinander sprechen. Auch wenn einem etwas gegen den Strich geht. Ich denke das ist wichtig.

I1	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	20	Bei uns jetzt in der Kreditplus habe ich den Vorteil, das Risikomanagement direkt gegenübersitzt, der Leiter ein ähnliches Alter wie ich hat und wir im Prinzip andauernd im Austausch sind. Das heißt, wenn ich irgendwo Probleme mit etwas habe, was er tut, oder andersrum, dann kommt man halt kurz rüber und klärt die Sache und kann auch einfach offen ehrlich miteinander sprechen. Auch wenn einem etwas gegen den Strich geht. Ich denke das ist wichtig.
I1	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	20	bei uns gibt es eine „Duz-Kultur“, ich glaube das ist ganz wichtig. Und wichtig ist, dass man dann einfach mal hinlaufen kann und das zeigt, glaube ich auch, dass die Zusammenarbeit eigentlich wirklich gut funktioniert, soweit.
I1	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	20	bei uns gibt es eine „Duz-Kultur“, ich glaube das ist ganz wichtig. Und wichtig ist, dass man dann einfach mal hinlaufen kann und das zeigt, glaube ich auch, dass die Zusammenarbeit eigentlich wirklich gut funktioniert, soweit.
I1	Herausforderungen eines ganzheitlichen GRC-Ansatzes	22	Das hängt bei uns, auch davon ab, dass im Prinzip, Governance, gut Governance und Risk, bin ich im Prinzip. Aber Risk und die Interne Revision zum Beispiel, wir haben jeweils einen anderen Head of, das heißt, darüber haben wir jetzt den Austausch nicht. Das heißt, wenn wir den gleichen Berichtsweg hätten, an den Head of, dann wäre das wahrscheinlich noch mal ein bisschen anders.
I1	Status quo: Governance, Risiken und Compliance > Organisatorische Verankerung	22	Das hängt bei uns, auch davon ab, dass im Prinzip, Governance, gut Governance und Risk, bin ich im Prinzip. Aber Risk und die Interne Revision zum Beispiel, wir haben jeweils einen anderen Head of, das heißt, darüber haben wir jetzt den Austausch nicht. Das heißt, wenn wir den gleichen Berichtsweg hätten, an den Head of, dann wäre das wahrscheinlich noch mal ein bisschen anders.

I1	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	22	Ich bin zum Beispiel mit Legal und Geldwäsche zusammen, an den gleichen Berichtsweg.

I1	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	22	Aber nein, wir haben keinen Jour-Fix, sondern eben diese quartärlichen Sitzungen, aber ansonst ist es eher ja, wenn wir es brauche, dann sprechen wir miteinander, wenn nicht, dann nicht.
I1	Status quo: Governance, Risiken und Compliance > Rolle von Governance, Risk und Compliance	24	B: Also, ich glaub ein großes Problem, dass wir jedenfalls für Governance und Compliance, kann ich sagen haben, dass die Maschinen die Laufen schon lange und Compliance ist erst seit naja 20 - 25 Jahre maximal überhaupt in der Lage, fundiert mal irgendwo nein zu sagen. Sonst hieß es glaub ich früher immer: was Geld bring wird gemacht, Ende.
I1	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	24	Also, ich glaub ein großes Problem, dass wir jedenfalls für Governance und Compliance, kann ich sagen haben, dass die Maschinen die Laufen schon lange und Compliance ist erst seit naja 20 - 25 Jahre maximal überhaupt in der Lage, fundiert mal irgendwo nein zu sagen. Sonst hieß es glaub ich früher immer: was Geld bring wird gemacht, Ende.

I1	Herausforderungen und -Risiken > Integration neuer Gesetze in bestehende Prozesse	24	Also, die große Herausforderung ist, zum einen muss man natürlich das laufende Geschäft im Auge behalten. Wenn wir neue Produkte haben, dann müssen wir die prüfen. Wir müssen gucken, wenn eine Regulatorik reinkommt, haben wir die nicht schon umgesetzt. Aber auch da, wenn man mal guckt, wie zum Beispiel die BASEL III Vorschriften oder irgendwann mal BASEL IV oder WpHG, man kann nicht sagen, okay es kommt eine neue MaRisk- Novelle oder WpHG-Novelle und wir prüfen jetzt mal das ganze Gesetz durch. Das geht nicht, da bräuchten wir glaub ich 50 Leute wahrscheinlich dafür, sondern das ist oft ebenso, dass wir nur die Änderungen antizipieren können. Und ich glaube eben, dass das eben ein großes Problem ist, das die Prozesse, die bereits stehen, nicht immer voll geprüft werden können nach den aktuellen Vorgaben und andererseits können wir auch nicht alle Vorgaben, also allein diese Riesenbase, die es gibt an Gesetzten und Vorschriften wir können niemals 100-prozentig sagen: Ja, wir erfüllen alle Vorgaben - sondern es gibt immer ein Risiko damit. Man muss sich eben bewusst sein, es gibt immer ein Risiko, das wir irgendwas nicht einhalten. Das ist inhärent, wir müssen nur versuchen es so klein wie möglich zu halten.

I1	Herausforderungen und -Risiken > Zunehmende Gesetzesvorgaben	24	Also, die große Herausforderung ist, zum einen muss man natürlich das laufende Geschäft im Auge behalten. Wenn wir neue Produkte haben, dann müssen wir die prüfen. Wir müssen gucken, wenn eine Regulatorik reinkommt, haben wir die nicht schon umgesetzt. Aber auch da, wenn man mal guckt, wie zum Beispiel die BASEL III Vorschriften oder irgendwann mal BASEL IV oder WpHG, man kann nicht sagen, okay es kommt eine neue MaRisk- Novelle oder WpHG-Novelle und wir prüfen jetzt mal das ganze Gesetz durch. Das geht einfach nicht, da bräuchten wir glaub ich 50 Leute wahrscheinlich dafür, sondern das ist oft ebenso, dass wir nur die Änderungen antizipieren können. Und ich glaube eben, dass das eben ein großes Problem ist, das die Prozesse, die bereits stehen, nicht immer voll geprüft werden können nach den aktuellen Vorgaben und andererseits können wir auch nicht alle Vorgaben, also allein diese Riesenbase, die es gibt an Gesetzten und Vorschriften wir können niemals 100-prozentig sagen: Ja, wir erfüllen alle Vorgaben - sondern es gibt immer ein Risiko damit. Man muss sich eben bewusst sein, es gibt immer ein Risiko, das wir irgendwas nicht einhalten. Das ist inhärent, wir müssen nur versuchen es so klein wie möglich zu halten.
I1	Status quo: Governance, Risiken und Compliance > Technologische Lösung	30	B: Genau, es wurde tatsächliche, haben wir jetzt erst seit letztem Jahr ein neues. Das heißt wir füttern das gerade noch, es läuft noch nicht 100-prozentig und, aber da hat der Konzern aber auch ordentlich Geld liegen lassen, damit wir praktisch jetzt ein neues Tool bekommen. Da merkt man glaube ich auch, immer wenn es ums Geld geht, dass es wahrscheinlich auch wichtig ist am Ende. Ich muss sagen, ich verstehe es noch nicht ganz das Tool, aber wenn ich das Zielbild ankucke, dann ist es genau das, wo wir jetzt praktisch daran arbeiten. Was aber auch natürlich, auch immer bedeutet, vielleicht hat man es bis dahin noch nicht so ganz 100-prozentig gut aufbereitet.

I1	Status quo: Governance, Risiken und Compliance > Technologische Lösung	32	Q-SAC, aber ich bin mir auch nicht sicher, dadurch dass wir die Gruppe haben. Die kaufen auch gerne mal irgendwas ein und nennen das dann anders
I1	Ganzheitlicher GRC-Ansatz > Vorteile eines ganzheitlichen GRC-Ansatzes	34	Ja, also ganz klar ist genau eben, dass wir zum Beispiel Tools nutzen, die wir am besten beide nutzen können. Diese moderneren Tools, die es natürlich auch gibt, sorgen auch dafür, dass das auch von der Bedienung her leichter ist. Also, ich kann ihnen die Risikotools reingucken und verstehe nicht nur Bahnhof, sondern verstehe auch tatsächlich, ich weiß, worauf, worauf ich ungefähr gucken muss, und dann kann man immer noch Fragen und andersrum natürlich auch. Das heißt, da muss man natürlich sagen, da gibt es extrem positive Effekte, die wir daraus haben, sobald wir halt, wenn wir digitaler werden, moderner werden, schneller werden.
I1	Ganzheitlicher GRC-Ansatz > Vorteile eines ganzheitlichen GRC-Ansatzes	34	Aber was, glaube ich, unersetzbar ist, ich glaube, der integrierte Ansatz ist auch genau das, worauf sie, glaube ich, rauswollen. Wenn wir von Grund auf miteinander arbeiten, dann haben wir natürlich genau die Probleme, nicht, dass wir irgendwann mal etwas fertig ist und wir zusammensitzen merken, wir haben viele Dinge doppelt gemacht. Das heißt, ich habe mir Sorgen gemacht um Op- Risk, aber Risiko auch, weil man muss ja sagen, eine Op- Kategorie gehört ja auch immer mir. Das heißt, ich habe sie bei mir drin, sie haben sie bei sich drin, Revision hat es wahrscheinlich auch noch irgendwo drin, und das ist genau das Problem. Jeder hat sich dreimal Gedanken gemacht, wir kommen vielleicht sogar zu etwas unterschiedlichen Ergebnissen, weil wir unterschiedliche Informationsbasis oder einfach das Gefühl, ein anderes ist. Und da ist natürlich wichtig, wenn wir von Anfang an bei allen möglichen Themen einfach uns mal zusammensetzen würden. Ich weiß nicht, ob es immer klappt, wahrscheinlich nicht. Dann hätten wir 100- prozentig Redundanzen würden vermieden werden, und wir bräuchten auch weniger Man-power für einzelne Dinge.

I1	Ganzheitlicher GRC-Ansatz > Definition	36	Wenn ich einen integrierten Ansatz mir überlegen müsste, dann wäre das auf jeden Fall, dass wir auf die gleichen Datenbanken zugreifen müssen. Das heißt, wenn wir mal überlegen, gibt es dann im Unternehmen eine Prozesslandkarte, und dann müssten wir eigentlich zu jedem Prozess die gleichen Einschätzungen am Schluss getroffen haben, beziehungsweise das Ergebnis muss das gleiche sein. Und integriert wäre für mich eben genau der Ansatz. Wenn wir einen Prozess verändern oder neu machen, dann müssen wir von Anfang an, an den Tisch sitzen und gemeinsam überlegen, okay, was sind die Auswirkungen von diesem Prozess? Was wollen wir aus unseren Abteilungen? Wollen wir zum Beispiel bestimmte Kontrollen drauf? Haben wir gewisse sorgen, was das angeht, und ich denke, dass der Austausch da halt zentral ist.

I1	Ganzheitlicher GRC-Ansatz > Definition	38	Ja, ich denke, von der, von der Definition finde ich sich gelungen. Dann ist es ungefähr das, was ich mir auch vorgestellt habe. Ich glaube, natürlich ist es immer schwierig, sich auszusuchen, welche Bereiche nenne ich jetzt. Mit GRC hat man halt dann Governance Risk und Compliance genommen. Man muss natürlich sehen, in jedem Unternehmen gibt es noch andere Themen, die wichtig sind. Manchmal gibt's Compliance noch aufgeteilt in WpHG und Ma-Risk. Wir haben noch Geldwäsche, das teilweise zu Compliance gehört, teilweise auch nicht. Wir haben die Datenschützer. Wir haben ja auch noch die Information Security, was gerade auch absoluter Trend ist. Und zum Beispiel auch ESG, das bei uns zum Beispiel jetzt eine eigene Position bekommen hat, weil guckt man die neue Novelle an, Ma-Risk die jetzt gerade kommt, die schreiben einfach überall ESG rein. Aber dadurch haben wir das Problem nicht gelöst, sondern müssen auch gucken, was macht man denn am Schluss damit? Deshalb ist wahrscheinlich wichtig, dass man eben schon auch klarstellt, dass GRC, das die drei praktisch das wiedergeben sollen, aber natürlich in einzelnen Unternehmen durchaus dann ist eben mal Risk mehr oder Risk weniger, genau wie Compliance auch.

I1	Ganzheitlicher GRC-Ansatz > Strategie	40	Ich glaube, von wirklich von einer integrierten Strategie zu sprechen, da fehlt noch einiges. Bei uns sind die Vorgaben schon relativ klar getrennt. Das heißt also, bei uns können sie gucken, wir haben die Regulatorien, dann haben wir aber auch die Gruppen, Vorgaben, die im Prinzip die Regulatorik teilweise schon enthalten, aber natürlich nicht die nationalen. Da muss man schon noch ganz klar sagen, es gibt Risk, und es gibt Compliance, und es gibt Geldwäsche, und die überschneiden sich natürlich teilweise. Aber es gibt klare Zuständigkeiten. Ich bin für die Bereiche eben Compliance zuständig und Risk für Risk. Und wenn die scheiß bauen, dann ist das ihr Problem, und wenn ich das tue, ist eben mein Problem und wirklich einen integrierten Ansatz, dass ich zum Beispiel auch, wenn die etwas umsetzen oder ich etwas umsetze, jeweils auch die anderen mit reinnehmen oder vielleicht es eben auch einfach eine Vorgabe ist zukünftig, dass man sagt: Hey, egal was ihr macht, ihr macht zumindest mal noch eine kurze Abstimmung. So ist auf jeden Fall noch nicht. Für mich sind es schon noch sehr klare Trennungen

I1	Status quo: Governance, Risiken und Compliance > Aufgabenabgrenzung	40	Ich glaube, von wirklich von einer integrierten Strategie zu sprechen, da fehlt noch einiges. Bei uns sind die Vorgaben schon relativ klar getrennt. Das heißt also, bei uns können sie gucken, wir haben die Regulatorien, dann haben wir aber auch die Gruppen, Vorgaben, die im Prinzip die Regulatorik teilweise schon enthalten, aber natürlich nicht die nationalen. Da muss man schon noch ganz klar sagen, es gibt Risk, und es gibt Compliance, und es gibt Geldwäsche, und die überschneiden sich natürlich teilweise. Aber es gibt klare Zuständigkeiten. Ich bin für die Bereiche eben Compliance zuständig und Risk für Risk. Und wenn die scheiß bauen, dann ist das ihr Problem, und wenn ich das tue, ist eben mein Problem und wirklich einen integrierten Ansatz, dass ich zum Beispiel auch, wenn die etwas umsetzen oder ich etwas umsetze, jeweils auch die anderen mit reinnehmen oder vielleicht es eben auch einfach eine Vorgabe ist zukünftig, dass man sagt: Hey, egal was ihr macht, ihr macht zumindest mal noch eine kurze Abstimmung. So ist auf jeden Fall noch nicht. Für mich sind es schon noch sehr klare Trennungen.

I1	Ganzheitlicher GRC-Ansatz > Vorteile eines ganzheitlichen GRC-Ansatzes	42	Also genau klar, die Redundanzen sind wichtig, auch die Manpower ist wichtig, die man vielleicht einsparen könnte, was aber auf jeden Fall auch wichtig ist, und dass man man natürlich sehen, größere Unternehmen, vor allem aber auch kleinere, es geht immer auch darum, um diese Machtspielchen. Also habe ich als der kleine Compliance Beauftragte, der mit seinen 30 Jahren herumspringt und meint, er könnte irgendwie den Alten erklären, dass es gerade so nicht geht. Es ist immer auch wichtig, dass man eine gemeinsame Machtbasis in Anführungszeichen hat, und eben auch, weil, wenn jetzt der Compliance Beauftragte, der Geldwäsche beauftragte, und der Risk, der Op-Risk Beauftragte, wenn die zusammenkommen und sagen: hey so geht's nicht. Dann habe ich eine ganz andere Argumentationsgrundlage, als wenn eben nur einer von denen ankommt, weil die anderen vielleicht überhaupt gar nicht Bescheid wissen. Wenn praktisch die alle zusammenkommen, gibt es meiner Meinung nach keinen Vorstand der Welt, der sagt: ja ja…komm passt schon. Was natürlich bei den Einzelnen auch nicht passieren sollte. Es ist auf jeden Fall wichtig, wenn da diese Allianz zusammenkommt und wenn man eine integrierte Strategie hat, dann hat man das immer schon, dann hat man komplett andere Möglichkeiten eben Sachen auch mal klarzustellen, mal zu Fordern und den Leuten nicht auch noch hinterher rennen muss, damit man seine Bedenken praktisch irgendwie gelöst bekommt

I1	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	42	was aber auf jeden Fall auch wichtig ist, und dass man man natürlich sehen, größere Unternehmen, vor allem aber auch kleinere, es geht immer auch darum, um diese Machtspielchen. Also habe ich als der kleine Compliance Beauftragte, der mit seinen 30 Jahren herumspringt und meint, er könnte irgendwie den Alten erklären, dass es gerade so nicht geht. Es ist immer auch wichtig, dass man eine gemeinsame Machtbasis in Anführungszeichen hat, und eben auch, weil, wenn jetzt der Compliance Beauftragte, der Geldwäsche beauftragte, und der Risk, der Op-Risk Beauftragte, wenn die zusammenkommen und sagen: hey so geht's nicht. Dann habe ich eine ganz andere Argumentationsgrundlage, als wenn eben nur einer von denen ankommt, weil die anderen vielleicht überhaupt gar nicht Bescheid wissen. Wenn praktisch die alle zusammenkommen, gibt es meiner Meinung nach keinen Vorstand der Welt, der sagt: ja ja…komm passt schon. Was natürlich bei den Einzelnen auch nicht passieren sollte. Es ist auf jeden Fall wichtig, wenn da diese Allianz zusammenkommt und wenn man eine integrierte Strategie hat, dann hat man das immer schon, dann hat man komplett andere Möglichkeiten eben Sachen auch mal klarzustellen, mal zu Fordern und den Leuten nicht auch noch hinterher rennen muss, damit man seine Bedenken praktisch irgendwie gelöst bekommt

I1	Status quo: Governance, Risiken und Compliance > Technologische Lösung	44	Wir haben so etwas, vor allem geht mein halbes Budget meine Abteilung im Prinzip immer für ein Tool drauf. Da sind wir aber auch Vorreiter. Ich war vor einem Monat in Frankreich und habt auch mit den anderen Ägypten, Irland, Spanien gesprochen und da sind wir wirklich absoluter Vorreiter und die einzigen die sowas haben. Wir haben ein Tool, das heißt Radar, Teamradar. Da kommen praktisch alle Regulationen, die wir haben, das heißt sei es von Europa, Deutschland, die kommen praktisch wie in so einen großen Filter rein in dieses Tool. Dann ist da eine Musterbank hinterlegt, das heißt wir geben an, haben wir mit Immobilien zu tun? Nein. Haben wir mit WphG zu tun? Nein. Haben wir mit MaRisk zu tun? Ja. Das wird dann praktisch vorgefiltert. Und alles, was am Schluss noch relevant für uns ist, kommt in dieses Tool und wird dann von Compliance bearbeitet. Das heißt da kommt jetzt neue Eva-Guidelines zum Beispiel, die kommen darüber rein. Erstmals, wir erfahren davon. Ich hoffe Eva- Guidelines hätten wir auch so erfahren. Aber zumindest bei kleineren Anpassungen, geht das durch aus, flutscht das mal durch. Wir haben die Information sichergestellt und wenn es da reinkommt, gucken wir es uns in Compliance an, verteilen es dann alle Interessengruppen, von denen wir denken, wahrscheinlich betrifft es euch. Dann müssen die alle in diesen Tools zurückmelden – „betrifft uns nicht“ oder „haben wir schon umgesetzt“ oder „wir setzen das bis zum 30.6. um“. Und dann fragen wir praktisch nochmal am 1.7. nach: „Hey wie sieht es aus, habt ihr es schon umgesetzt?“. Und wenn ja, dann haben

I1	Status quo: Governance, Risiken und Compliance > Technologische Lösung	46	Genau, also das ist natürlich immer verbunden, alles was technologisch ist und was taugt kostet meistens ordentlich Geld. Ich meine jetzt auch QSAC von den Kollegen im Risikomanagement, das kostet sicherlich auch einiges an Budget. Aber ja, ich kenne jetzt SAP nicht, aber wenn wir praktisch da mal einen kleinen Haushalt an Tools hat, die einem dabei helfen, dann kann man schon diese tägliche Arbeit, die man hat und die im Zweifel auch einfach nur Zeit kosten, kann das natürlich schon extrem dabei helfen. Wenn wir Abteilungsbudgets zusammenlegen würden, und es Tool gibt die uns beiden helfen, ist es sicherlich auch nochmal etwas was, wenn wir beide uns mit dem gleichen Tool auskennen, was hilft, wenn es eben richtig integrierte Tools gibt
I2	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	14	Da hat sich mit Sicherheit einiges geändert, also wenn ich den ganzen Sektor auf jeden Fall betrachte, Governance, Risk und Compliance waren logischerweise schon immer Themen, aber die wurden eher, also subjektiver Eindruck von mir natürlich, die wurden eher stiefmütterlich und wachstums- und ertragshemmend betrachtet und da empfinde ich auf jeden Fall jetzt einen erheblichen Wechsel von 2007/ 08 bis heute.
I2	Status quo: Governance, Risiken und Compliance > Rolle von Governance, Risk und Compliance	14	Da hat sich mit Sicherheit einiges geändert, also wenn ich den ganzen Sektor auf jeden Fall betrachte, Governance, Risk und Compliance waren logischerweise schon immer Themen, aber die wurden eher, also subjektiver Eindruck von mir natürlich, die wurden eher stiefmütterlich und wachstums- und ertragshemmend betrachtet und da empfinde ich auf jeden Fall jetzt einen erheblichen Wechsel von 2007/ 08 bis heute.

I2	Entwicklung im Banksektor > Veränderungen seit 2007/2008 im Vergleich	14	Da hat sich mit Sicherheit einiges geändert, also wenn ich den ganzen Sektor auf jeden Fall betrachte, Governance, Risk und Compliance waren logischerweise schon immer Themen, aber die wurden eher, also subjektiver Eindruck von mir natürlich, die wurden eher stiefmütterlich und wachstums- und ertragshemmend betrachtet und da empfinde ich auf jeden Fall jetzt einen erheblichen Wechsel von 2007/ 08 bis heute.
I2	Entwicklung im Banksektor > Stand des Banksektors im Jahr 2023	14	Also die GRC-Themen, die werden mittlerweile erstmal als insgesamt sogar sehr riskant betrachtet, wenn ich nicht compliant bin und die Risiken nur als Wachstumshemmer betrachte, also die Bedeutung der drei Begriffe ist erheblich gewachsen. Und die Gesamtheit der der drei Begriffe, die würde ich jetzt eher also für den ganzen Sektor als Grundlage für ordentliches, nachhaltiges Geschäft mit Wachstum und stabilen Erträgen betrachten. Früher eher Hemmnis, jetzt tendenziell deutlich stärker die Grundlage fürs Geschäft.
I2	Entwicklung im Banksektor > Veränderungen seit 2007/2008 im Vergleich	16	Viele haben gerne drüber weggesehen, haben Risiken in Kauf genommen, ausgesprochen starken Risikoappetit gezeigt und vielleicht auch noch drüber raus. Und die Geldbußen, Geldstrafen bei Compliance und Geldwäsche und ähnlichem, die haben natürlich auch einige auf den Boden der Tatsachen zurückgebracht. Fast alle.

I2	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	18	und, die Zusammenarbeit, ich gehe dann gleich mal ein Stück weiter, die Zusammenarbeit mit den Regulatoren, die ist auch ausgesprochen intensiv. Also das kriege ich jetzt bei uns, in der ING Diba, kriege ich es auf jeden Fall auch intensiv mit über die Aufsichtsratssitzungen, insbesondere wenn ich im Prüfungsausschuss teilnehme. Also da ist auf jeden Fall immer eingeladen die Bafin und Bundesbank, und das gleiche natürlich dann auch für die großen Aufsichtsratssitzungen insgesamt. Also, da herrscht reger Austausch und ist auch intensiver Dialog.
I2	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	20	Also die externen, die sind auf jeden Fall dauerhaft bei uns im Haus, ist auch mit Sicherheit erforderlich, weil wir ja auch als systemrelevant eingestuft sind, und ich denke, das ist Branchen Standard. Inwieweit allerdings die Wirtschaftsprüfer mit unserer internen Revision oder dann auch mit den Prüfern in Amsterdam und der Group Revision zusammenarbeiten, also sicherlich im Rahmen der Erfordernisse. Aber inwieweit die sich dann im täglichen Doing austauschen, da kann ich nichts dazu sagen, weil ich es schlicht nicht weiß
I2	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	22	Ja gut, guter Hinweis. Im Aufsichtsrat laufen da verschiedene Themen zusammen. Da berichtet eben auch die die interne Revision und legt auch ihren Prüfungsplan vor, und von Regulatoren her, bekommen wir ja auch Schwerpunkte zugewiesen, die dann der Wirtschaftsprüfer intensiver prüft. Also, da findet schon Austausch statt, also so, dass logischerweise vermieden ist oder vermieden wird, genau die gleiche Stelle doppelt zu prüfen, es sei denn, es macht aus fachlichen Gründen Sinn, aus zwei Perspektiven rauszugehen

I2	Ganzheitlicher GRC-Ansatz > Vorteile eines ganzheitlichen GRC-Ansatzes	22	Ja gut, guter Hinweis. Im Aufsichtsrat laufen da verschiedene Themen zusammen. Da berichtet eben auch die die interne Revision und legt auch ihren Prüfungsplan vor, und von Regulatoren her, bekommen wir ja auch Schwerpunkte zugewiesen, die dann der Wirtschaftsprüfer intensiver prüft. Also, da findet schon Austausch statt, also so, dass logischerweise vermieden ist oder vermieden wird, genau die gleiche Stelle doppelt zu prüfen, es sei denn, es macht aus fachlichen Gründen Sinn, aus zwei Perspektiven rauszugehen
I2	Herausforderungen eines ganzheitlichen GRC-Ansatzes	22	Ja gut, guter Hinweis. Im Aufsichtsrat laufen da verschiedene Themen zusammen. Da berichtet eben auch die die interne Revision und legt auch ihren Prüfungsplan vor, und von Regulatoren her, bekommen wir ja auch Schwerpunkte zugewiesen, die dann der Wirtschaftsprüfer intensiver prüft. Also, da findet schon Austausch statt, also so, dass logischerweise vermieden ist oder vermieden wird, genau die gleiche Stelle doppelt zu prüfen, es sei denn, es macht aus fachlichen Gründen Sinn, aus zwei Perspektiven rauszugehen
I2	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	24	Also, im Aufsichtsrat läuft auch an der Stelle viel zusammen, weil da quartalsweise auf jeden Fall ausführlich berichtet wird. Und zusätzlich dazu dann natürlich noch die, die Jahres berichtet
I2	Status quo: Governance, Risiken und Compliance > Reporting	26	Also, einen integrierten Bericht gibt's nicht.
I2	Herausforderungen eines ganzheitlichen GRC-Ansatzes	30	Austausch findet auf jeden Fall statt. Nur Doppelarbeiten bin ich mir also, ohne jetzt Details zu kennen und zu nennen. Aber ich bin mir sicher, dass Doppelarbeiten auch stattfinden, weil es, weil es durchaus auch Sinn machen kann, aus verschiedenen Perspektiven zu betrachten, weil es gibt ja dann auch noch interne Revision der Gruppe Amsterdam, die sich dann auch bei uns hier in Deutschland Vorgänge anschauen. Also, es kann durchaus sein, dass die Group, also die ING Group an der deutschen Kasse vorbei hier rein bei uns prüft.

I2	Ganzheitlicher GRC-Ansatz > Vorteile eines ganzheitlichen GRC-Ansatzes	30	Nur Doppelarbeiten bin ich mir also, ohne jetzt Details zu kennen und zu nennen. Aber ich bin mir sicher, dass Doppelarbeiten auch stattfinden, weil es, weil es durchaus auch Sinn machen kann, aus verschiedenen Perspektiven zu betrachten
I2	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	36	Also, ich bin mir sicher, da heißt Center Of Expertise, also nach der agilen Struktur Aufbauorganisation sind, also integrated risk und Compliance sind beides Center Of Expertise, und die laufen relativ. Also die laufen nicht Hand in Hand, aber relativ eng nebeneinander.
I2	Status quo: Governance, Risiken und Compliance > Organisatorische Verankerung	36	Also, ich bin mir sicher, da heißt Center Of Expertise, also nach der agilen Struktur Aufbauorganisation sind, also integrated risk und Compliance sind beides Center Of Expertise, und die laufen relativ. Also die laufen nicht Hand in Hand, aber relativ eng nebeneinander.
I2	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	38	Also, Austausch findet da auf jeden Fall statt.
I2	Status quo: Governance, Risiken und Compliance > Organisatorische Verankerung	40	Zumal, weil die beiden unter Risk, also unter dem Risiko Vorständin hängen.
I2	Status quo: Governance, Risiken und Compliance > Organisatorische Verankerung	42	Ja, ja, also, die können gar nicht unabhängig voneinander arbeiten, weil sie regelmäßig, und zwar direkt an dem gleichen Risiko Vorstand berichten.
I2	Herausforderungen und -Risiken > Zunehmende Gesetzesvorgaben	44	Iso, es sind die sich regelmäßig und relativ schnell hintereinander ändernden rechtlichen Anforderungen, und da müssen auf jeden Fall die Aufbau- und die Ablauforganisation darauf zugeschnitten sein, auch personell. Und die die Aufmerksamkeit seitens Regulatoren und andere Stakeholder, also auch Kunden. Ich denke, das ist gerade bei Banken, die sich früher relativ wenig Gedanken drum gemacht haben, in der Masse zumindest das ist eine spezifische Herausforderung in der Bankenbranche. Und der sich verändernde Wettbewerb in Banken.

I2	Herausforderungen und -Risiken > Zunehmende Gesetzesvorgaben	46	Ja, also bei uns, bei den nenne ich mal alteingesessenen Mitspielern in der in der Bankenbranche. Wir sind gewohnt, eng getrackt und reguliert zu werden, und die Wettbewerber, die neu am Markt aufpoppen, die sind deutlich weniger reguliert, und das halte ich für eine spezielle Herausforderung in der Bankenbranche. Die anderen werden sich dran gewöhnen müssen, dass Risk und Compliance im Finanzdienstleistungsbereich extrem wichtig sind. Wir, wir sind an der Stelle eigentlich mehr mit uns beschäftigt, keine, keine Fehler zu machen und compliant zu sein, und wenn wir es irgendwann oder irgendjemand in der in der Branche nicht sein kann oder will, dann muss es auf jeden Fall in jeder Richtung sehr gut erklären können, wobei, das ist jetzt gar nicht so spezifisch für Banken. Aber bei uns ist es eben ein Thema, weil die die Bankenbranche insgesamt, die lebt natürlich auch stark von der Reputation. Ansonsten sind die, die Banken, relativ einfach austauschbar untereinander. Wir sind kein Rohstofflieferant, auf denen eine nicht verzichten kann. Also, wir sind erheblich leichter zu substituieren als Lieferanten für seltene Erden.
I2	Status quo: Governance, Risiken und Compliance > Technologische Lösung	48	Also da mit absoluter Sicherheit also dieses IKS, also interne Kontrollsystem, das gibt es, und zwar sowohl auf der nationalen, also deutschen Ebene als auch im Konzern, also das ist also das alles, was da gemacht werden muss und gemacht wird, das ist so weit als möglich Software unterstützt. Und das geht weit über Excel hinaus.
I2	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	50	Also so wie bei den Prüfungsplänen empfiehlt sich auf jeden Fall, sich auszutauschen, um auch vom anderen zu wissen, was er eigentlich gerade tut.

I2	Status quo: Governance, Risiken und Compliance > Aufgabenabgrenzung	50	Ansonsten würde ich aber nicht mit, also nicht immer mit mit der vollen Begeisterung Redundanzen und Mehrkosten vermeiden wollen, weil das kann durchaus gut investiert sein, wenn ich, eben weil die Bereiche sind ja nicht ohne Grund voneinander getrennt, also die, die Cas und Compliance und Risk, die haben ja alle alleinstehend ihre Berechtigung, und dieses auch gegenseitig oder redundant unter Inkaufnahme von Mehrkosten zu prüfen - das kann durchaus sinnvoll sein und sollte auch gewollt sein, aus unterschiedlichen Winkeln die gleiche Sache zu betrachten
I2	Ganzheitlicher GRC-Ansatz > Definition	52	Also mit dem Ziel, aus einer letztendlich Organisationseinheit alle, alle Themen vollumfänglich abzudecken. Das, das wäre für mich der der integrierte Ansatz
I2	Ganzheitlicher GRC-Ansatz > Definition	54	Das ist perfekt ausformuliert, das, was ich gemeint habe. Alle, alle drei oder alle drei sitzen in einem Raum. Jeder schreibt auf Sideboard, was er haben muss, und dann wird abgeglichen, was die anderen dazu liefern können und wo es vielleicht Limitierungen gibt, und im Endergebnis werden alle Anforderungen erfüllt.
I2	Ganzheitlicher GRC-Ansatz > Strategie	56	Also, genau das an sich ist, ist eigentlich und natürlich auch in Klammern ist, ist wichtig, weil bei uns arbeiten die Org-Einheiten schon zusammen, aber eben nicht als eine Org-Einheit. Aber vorhin bin ich am Rand ja drauf zu sprechen gekommen, so wie Compliance und Risk, also integrated compliance, integrated risk und was dann da alles drunter fällt. Die sitzen nebeneinander unterm gleichen Vorstand. Also faktisch geht's schon in Richtung eines integrierten GRC-Ansatzes, aber in der Organisation ist es so nicht abgebildet

I2	Status quo: Governance, Risiken und Compliance > Aufgabenabgrenzung	56	Also, genau das an sich ist, ist eigentlich und natürlich auch in Klammern ist, ist wichtig, weil bei uns arbeiten die Org-Einheiten schon zusammen, aber eben nicht als eine Org-Einheit. Aber vorhin bin ich am Rand ja drauf zu sprechen gekommen, so wie Compliance und Risk, also integrated compliance, integrated risk und was dann da alles drunter fällt. Die sitzen nebeneinander unterm gleichen Vorstand. Also faktisch geht's schon in Richtung eines integrierten GRC-Ansatzes, aber in der Organisation ist es so nicht abgebildet.
I2	Status quo: Governance, Risiken und Compliance > Organisatorische Verankerung	56	Also, genau das an sich ist, ist eigentlich und natürlich auch in Klammern ist, ist wichtig, weil bei uns arbeiten die Org-Einheiten schon zusammen, aber eben nicht als eine Org-Einheit. Aber vorhin bin ich am Rand ja drauf zu sprechen gekommen, so wie Compliance und Risk, also integrated compliance, integrated risk und was dann da alles drunter fällt. Die sitzen nebeneinander unterm gleichen Vorstand. Also faktisch geht's schon in Richtung eines integrierten GRC-Ansatzes, aber in der Organisation ist es so nicht abgebildet.
I2	Ganzheitlicher GRC-Ansatz > Vorteile eines ganzheitlichen GRC-Ansatzes	58	Das wäre die die Steigerung oder Maximierung der Effektivität und der Effizienz. Also das auf jeden Fall mit weniger Leuten am Ende des Tages sogar noch mehr erreichen. Durch Vermeidung von Redundanzen. Das wäre der Idealtypus.

I2	Herausforderungen eines ganzheitlichen GRC-Ansatzes	60	Ja, nämlich dass bei einer Gruppe, wie hast du es gesagt, holistischer Ansatz integriert, also alle, alle zusammen die individuelle Expertise nicht mehr so zum Tragen kommen wie in einer aufgeteilten Organisation. Die Formel getrennt, aber letztendlich natürlich auf Zusammenarbeit angewiesen, auch zusammenarbeitet. Und die, die Komplexität, die Abstimmungen sind, oder die Komplexität, ist natürlich auch um einiges größer. Wenn ich, wenn ich eine Org-Einheit aufsetze, die sehr unterschiedliche Themen bearbeiten soll, kann, kann gut funktionieren, wie eben in deiner Definition, mit Effizienz und Effektivität, aber dass das Risiko in Kurzform ist, möglicherweise untergehende individuelle Kompetenzen und Reibungsverluste. Und dass Konkurrenzen entstehen, die ich an der Stelle definitiv nicht brauche.
I2	Status quo: Governance, Risiken und Compliance > Technologische Lösung	62	Ja, also, egal welcher technologische Ansatz, er muss auf jeden Fall transparent für alle sein. Und wie es immer so ist bei technologischen Lösungen und Tools, er muss von der ersten Sekunde an Rund um die Uhr gepflegt sein. Ansonsten ist mir der technologische Ansatz oder die technologische Lösung ist mir schon fast egal. Weil, wenn eine Woche keine reinschaut, also Transparenz, auch aktiv reinschauen und natürlich auch Informationen wirklich transparent zur Verfügung stellen. Und das andere ist ohne akribische Datenpflege, egal in welchem Bereich, ohne die funktioniert keine technologische Lösung.

I3	Entwicklung im Banksektor > Veränderungen seit 2007/2008 im Vergleich	6	Bedingt durch die Bankenkrise hat sich natürlich dramatisch bei den Banken auch die Auffassung verändert es sind natürlich sehr viele Sachen festgestellt worden. Da gab es erheblichen regulatorischen Druck seitens des Gesetzgebers und seitens der Aufsichten. Das ist ja nicht nur hier die europäische Bank und die deutschen Aufsichten. Sondern das sind die internationalen Bankaufsichtsbehörden, die darauf gedrängt haben, dass sich bei den Banken dramatisch was verändert und verbessert.
I3	Entwicklung im Banksektor > Stand des Banksektors im Jahr 2023	6	Und diese dramatische Veränderung die zeigt sich heute sehr deutlich. Das heißt, die Banken haben auch, weil sie es mussten, aber auch, weil sie es wollten, natürlich sehr viel gemacht, sehr viel neues eingeführt.
I3	Entwicklung im Banksektor > Veränderungen seit 2007/2008 im Vergleich	6	Und wenn man das vergleicht mit der Situation vor der Bankenkrise 2007 ist das wirklich ein Verhaltenswechsel
I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	8	Sie achten darauf, dass die Einhaltung gewährleistet wird. – dies betrifft primär den Kreditbereich, aber auch andere Geschäftsbereiche und natürlich auch das Management. Das heißt, es werden hier intern auch immer wieder Schulungen, Pflichtschulungen durchgeführt, die man auch absolviert haben muss, und es wird natürlich auch drauf geguckt, dass man möglichst wenig Findings kriegt hinsichtlich regulatorischer Lücken, Governance Lücken, Kontrolllücken.
I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	10	Sehr eng und intensiv, natürlich auch vertrauensvoll, wobei man sagen muss, natürlich sind hier unterschiedliche Interessen und natürlich auch Neutralitätsaspekt zu betrachten.

I3	Status quo: Governance, Risiken und Compliance > Aufgabenabgrenzung	10	Sehr eng und intensiv, natürlich auch vertrauensvoll, wobei man sagen muss, natürlich sind hier unterschiedliche Interessen und natürlich auch Neutralitätsaspekt zu betrachten. Wir können nicht erwarten, dass ein Wirtschaftsprüfer sich mit uns hier zusammensetzt und uns im Zweifel Rechtsrat erteilt. Das ist klar, dass muss man selber hinbekommen.
I3	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	10	Andererseits ist es natürlich ein enger Austausch, das heißt, wir kommunizieren, unsere Politik hier im Haus war schon immer „offen“.
I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	10	Andererseits ist es natürlich ein enger Austausch, das heißt, wir kommunizieren, unsere Politik hier im Haus war schon immer „offen“.
I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	10	Und wenn die Auffassung des Wirtschaftsprüfers zumindest hinterfragbar ist, treten wir natürlich auch an und gehen in die Diskussion. Da findet dann ein offener Dialog statt. Und zum Schluss akzeptieren wir natürlich, wenn uns ein Wirtschaftsprüfer mit guten Argumenten sagt, dass er das anders sieht.
I3	Status quo: Governance, Risiken und Compliance > Unternehmenskultur; -politik	10	Jedoch freuen wir uns über klare Anweisungen und einen offenen Dialog. Wir sehen Revisionsprüfungen und auch externe Prüfungen als Chance.
I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	10	Jedoch freuen wir uns über klare Anweisungen und einen offenen Dialog. Wir sehen Revisionsprüfungen und auch externe Prüfungen als Chance.
I3	Status quo: Governance, Risiken und Compliance > Rolle von Governance, Risk und Compliance	10	Wir sehen Revisionsprüfungen und auch externe Prüfungen als Chance.

I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	11	Natürlich wehren wir uns im Zweifel, wenn wir merken es ist juristisch nicht haltbar, was der sagt. Dann führen wir konstruktive Gespräche, und bisher haben wir immer Lösungen gefunden. Die Wirtschaftsprüfer zeigen sich auch offen für Argumente. Wenn sie sagen, es ist vertretbar, dann schreiben sie das auch so rein. Wir wollen aber auf der anderen Seite natürlich auch Dinge annehmen, weil die klare Auffassung unseres Hauses ist: Wirtschaftsprüfer sollen nicht mit dem goldenen Ring durch die Arena geführt werden, sondern die sollen uns auch ein Stück weit sagen, wo wir besser werden können. Das ist etwas, was wir sehr ernst nehmen. Gleichzeitig treten wir natürlich auch an, um unseren Ansatz Argumentativ zu begründen und auch zu verteidigen. Bisher hat sich in solchen Fällen, auch während unserer langjährigen Zusammenarbeit mit KPMG, stets ein äußerst konstruktiver Dialog entwickelt.
I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	11	Es war sehr erfreulich zu sehen, wie wir voneinander lernen konnten. Ich habe auch persönlich eine Lernkurve bei Prüfern beobachtet, die teilweise als Junior begonnen haben. Es gab Momente, wo man ihnen die Basics erklären musste. Beeindruckend war jedoch zu beobachten, wie sie mit der Zeit das Wirtschaftsprüfungs- Examen bestanden haben und wie sich dadurch auch die Qualität der gestellten Fragen verändert hat. Diese Entwicklung hat uns besonders Freude bereitet.
I3	Herausforderungen eines ganzheitlichen GRC-Ansatzes	11	Weil da kriegen sie von außen, von Menschen, die nicht in dieser Mühle sind. Kriegen sie manchmal wertvolle Hinweise, neue Blickwinkel und auch manchmal Kritik, aber Kritik muss man dann konstruktiv nehmen

I3	Herausforderungen und -Risiken	13	Es ist jedoch oft die Herausforderung, mit den vorhandenen Ressourcen und Systemen zurechtzukommen. Es wäre leicht zu sagen: "Kauft ein neues System, das wird alles verbessern." Aber das ist nicht immer möglich und man kann auch nicht einfach dem Vorstand sagen: „investiere eine Milliarde in das Privatkundengeschäft, dann wird auch alles gut“. Dann wird der Vorstand sagen: „vielen Dank für den wichtigen Hinweis.“ Man muss also häufig abwägen, welche Möglichkeiten die internen Systeme der Bank hergeben und wie man dennoch den Vorgaben entsprechen kann. Es erfordert auch ein gewisses Maß an Pragmatismus, denn besonders im Retail Geschäft müssen viele Dinge standardisiert werden. Wenn man im Retail Geschäft ankommt und sagt: "Ich werde hier individuelle Bearbeitung und Analysen für jeden Fall durchführen", dann macht das Geschäft keinen Sinn mehr. Hier ist es notwendig, eine Vielzahl von Fällen zu standardisieren und kluge standardisierte Entscheidungen zu treffen.
I3	Status quo: Governance, Risiken und Compliance > Aufgabenabgrenzung	15	Ja, es sind unterschiedliche Bereiche.

I3 >	Status quo: Governance, Risiken und Compliance Rolle von Governance, Risk und Compliance	15	Ja, es sind unterschiedliche Bereiche. Wir haben ja einen großen Chief Administration Office, das unter der Leitung von Herrn Professor Dr. Simon ist. Er verantwortet federführend als versierter Jurist diese Bereiche unter einem Dach. Da ist Legal mit Governance und Compliance zusammen wohingegen der Risikobereich einen eigenen Vorstand hat, weil es dort nämlich auch um konkrete Risiken geht und deren Management. Und es ist aber so, dass es ein miteinander ist, nämlich auch ein wechselseitiger Austausch von Kow-How und ein Zuliefern. Wir sind natürlich für die konkreten Risiken zuständig im Risikomanagement. Ich kann mich nicht hinstellen und behaupten, dass Governance schuld ist, wenn es zu Problemen bei zahlreichen Krediten kommt, weil ich die Vorgaben nachlässig oder zu tolerant definiert und interpretiert habe. Aber der Anstoß für zum Beispiel neue Vorschrift kommt natürlich aus dem Compliance Bereich, da wir stets darüber informiert sein müssen, welche Veränderungen sich ergeben haben. Es gibt Konsultationen zum Beispiel für neue Vorgaben. Auch bezüglich der Umsetzungen und bis zu welchem Zeitpunkt die Umsetzung erfolgen muss. Beispiel dafür ist die Definition of Default, die neue Ausfall Definition. Der Anstoß zu neuer Regel kommt von Compliance. Compliance informiert uns mittels eines stark institutionalisierten und systematischen Verfahrens über neu erlassene Vorschriften. Anschließend greifen wir den Ball auf, der uns zugeworfen wird, und sind verpflichtet, die Umsetzung aus Risiko Sicht anzugeben. Wir sind

I3	Status quo: Governance, Risiken und Compliance > Aufgabenabgrenzung	15	Wir haben ja einen großen Chief Administration Office, das unter der Leitung von Herrn Professor Dr. Simon ist. Er verantwortet federführend als versierter Jurist diese Bereiche unter einem Dach. Da ist Legal mit Governance und Compliance zusammen wohingegen der Risikobereich einen eigenen Vorstand hat, weil es dort nämlich auch um konkrete Risiken geht und deren Management.
I3	Status quo: Governance, Risiken und Compliance > Organisatorische Verankerung	15	Wir haben ja einen großen Chief Administration Office, das unter der Leitung von Herrn Professor Dr. Simon ist. Er verantwortet federführend als versierter Jurist diese Bereiche unter einem Dach. Da ist Legal mit Governance und Compliance zusammen wohingegen der Risikobereich einen eigenen Vorstand hat, weil es dort nämlich auch um konkrete Risiken geht und deren Management.
I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	15	Und es ist aber so, dass es ein miteinander ist, nämlich auch ein wechselseitiger Austausch von Kow-How und ein Zuliefern.
I3	Status quo: Governance, Risiken und Compliance > Aufgabenabgrenzung	15	Wir sind natürlich für die konkreten Risiken zuständig im Risikomanagement. Ich kann mich nicht hinstellen und behaupten, dass Governance schuld ist, wenn es zu Problemen bei zahlreichen Krediten kommt, weil ich die Vorgaben nachlässig oder zu tolerant definiert und interpretiert habe.

I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	15	Aber der Anstoß für zum Beispiel neue Vorschrift kommt natürlich aus dem Compliance Bereich, da wir stets darüber informiert sein müssen, welche Veränderungen sich ergeben haben. Es gibt Konsultationen zum Beispiel für neue Vorgaben. Auch bezüglich der Umsetzungen und bis zu welchem Zeitpunkt die Umsetzung erfolgen muss. Beispiel dafür ist die Definition of Default, die neue Ausfall Definition. Der Anstoß zu neuer Regel kommt von Compliance. Compliance informiert uns mittels eines stark institutionalisierten und systematischen Verfahrens über neu erlassene Vorschriften. Anschließend greifen wir den Ball auf, der uns zugeworfen wird, und sind verpflichtet, die Umsetzung aus Risiko Sicht anzugeben. Wir sind sozusagen auch die Praktiker und die Risikomanager an sich. Aber die Vorgaben, die wir erfüllen müssen, die kriegen wir, wenn sich da was tut, dann über die Compliance schiene mitgeteilt und wir müssen dann sozusagen den Ball aufnehmen und in unsere Prozesse umsetzen.
I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	17	Mir ist lieber, ich kriege eine Regel zu viel als eine zu wenig, und da hat sich aber jetzt auch der Dialog entwickelt. Das heißt, die kriegen jetzt auch ein bisschen mehr Know-How in Compliance, dass wir wissen, was interessiert uns eigentlich, und dass wir uns dann auch speziell darauf hinweisen. Wir greifen die Aufgabe auf und analysieren die neuen Regelwerke oder nehmen an Konsultationen teil. In solchen Fällen können wir auch immer in Kontakt mit Bankenverbänden treten.
I3	Herausforderungen und -Risiken > Integration neuer Gesetze in bestehende Prozesse	17	Dennoch müssen wir sicherstellen, dass wir rechtzeitig unsere Prozesse und Arbeitsabläufe an das neue Recht anpassen.

I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	17	Dennoch müssen wir sicherstellen, dass wir rechtzeitig unsere Prozesse und Arbeitsabläufe an das neue Recht anpassen. Hierbei stehen wir im Austausch mit der Compliance, aber natürlich auch mit Legal und den Praktikern aus dem Marktseite. Wir müssen es letztendlich in die Praxis umsetzen. Das ist dann sozusagen eine ganzheitliche Betrachtungsweise. Der Impuls dazu kommt jedoch von der Compliance.
I3	Status quo: Governance, Risiken und Compliance > Technologische Lösung	19	Es ist schon automatisiert. Jedoch kann ich Ihnen nicht mit Sicherheit sagen, ob es sich dabei um ein normales Excel-Dokument handelt oder ob es ein eigenes Tool ist. Aber da bitte ich um Verständnis. Da bin ich leider nicht nah genug dran. Ich erhalte von unserer Fachabteilung eine umfassende Präsentation in Form einer ansprechenden PowerPoint, in der jede Regel zusammen mit einer kurzen Analyse aufgeführt wird. Dabei werden dann die verantwortlichen Personen zu benannt, die sich um die Umsetzung kümmern müssen. Diese Personen füllen dann entsprechende PowerPoint Templates aus, um darzulegen was wir getan haben oder noch tun wollen. Es gibt ein Tool, mit der die neuen Vorschriften erfasst werden und an uns weitergeleitet werden, und dann kommen die Bereiche ins Spiel, die das sozusagen dann für die einzelnen Risikoabteilungen aufnehmen. Das hilft mir auch nichts, wenn ich jetzt über Operation Risk 15 Vorschriften kriege. Da sag ich: „schön; toll! Ich habe mich weitergebildet aber betrifft mich nicht!“. Mein Vorgesetzter leitet das bereits ein, datiert es und entfernt es aus dem System – es ist also auch systembasiert. Das ist hier nicht nach dem Motto: ich schicke einmal allen eine Mail wo drinsteht: „hey passt mal auf - ich habe da gestern was gelesen.“ Es wird systematisch erfasst und systematisch weitergeleitet.

I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	21	Also, auf Managementebene ist das sicherlich ein regelmäßiger Austausch in Exkurs in diesen Gremien, wo natürlich auch der Head of Compliance mit drinsitzt. Auf Arbeitsebene, zu der ich mich jetzt mal erzählen möchte, ist es jetzt nicht so, dass wir alle vier Wochen mit denen reden, sondern wir sind dann im Gespräch, wenn die eine Prüfungsplanungen mit uns machen
I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	21	Genauso ist es auch mit den Wirtschaftsprüfern. Da hat man natürlich auch regelmäßige Meetings, aber da bin nicht ich dabei. Wenn ich kein Thema habe, setze ich mich nicht mit EY zusammen und reden über Gott und die Welt. Das machen dann die Bereiche, die halt die Prüfungskoordination machen. So ist es auch mit Group Audit. Die haben dort mit denen regelmäßig ein Austausch auch über die Planung. Wir kommen dann, ich nehme jetzt mal das Problem Kredit Betreuungssegment. Wir kommen dann ins Spiel, wenn wir auch wirklich Themen haben, das heißt Prüfungsplanung, Prüfungsdurchführung und dann natürlich, falls vorhanden, Finding und auch Finding Schließung.

I3	Status quo: Governance, Risiken und Compliance > Technologische Lösung	21	Und der Finding Schließungsprozess folgt dann auch wieder einem toolbasierten, sehr, sehr strukturierten Prozess. Das bedeutet, dass wir verschiedene Aspekte berücksichtigen müssen. Zuerst müssen wir eine Lösung finden, das hat erstmal Priorität. Anschließend ist es notwendig, diese Lösung dem entsprechenden Management vorzustellen, sie dort zur Genehmigung vorzulegen und bei einer bestimmten Schwere des Problems auch die Zustimmung von Group Audit einzuholen. Wenn wir ein schwerwiegendes Finding hätten mit einer hohen Variety, dann haben wir natürlich auch die Pflicht, vor der Schließung auch noch einmal Rücksprache mit Group Audit zu halten, um sicherzustellen, ob die die Schließung auch mittragen. Dies gilt sowohl intern als auch extern. Wir informieren die Wirtschaftsführung über unsere Vorgehensweise. Falls diese nicht richtig wäre, würden sie uns darauf hinweisen, dass es nicht ihren Vorstellungen entspricht. Sie greifen jedoch nicht so detailliert in die Angelegenheit ein. Die mischen sich natürlich nicht so im Detail ein.

I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	21	Daher ist es meine Aufgabe, die Mitarbeiter zu informieren und sie gegebenenfalls zu schulen, sobald es neue Entwicklungen gibt – sei es, um Fehler zu korrigieren oder um neue Vorschriften einzuführen. Die Angestellten müssen wissen, was sie tun müssen. Besonders im Retail ist es von großer Bedeutung, klare Anweisungen zu geben, wie standardisierte Verfahren durchgeführt werden sollten. Es geht darum zu erklären, wo und wie sie auf die Systeme zugreifen müssen, um sicherzustellen, dass die gleichen Abläufe befolgt werden. Wir müssen äußerst präzise Prozesse entwerfen, die auch von Personen umgesetzt werden können, die nicht unbedingt BWL studiert haben, sondern vielleicht eher einen kaufmännischen oder anlernenden Hintergrund haben. Dies ist notwendig, um sicherzustellen, dass sie die Vorgaben wirklich umsetzen können.

I3	Herausforderungen und -Risiken > Künstlicher Intelligenz (KI)	Das ist die künstliche Intelligenz, weil das wird kommen. Ich bin zwar kein Experte auf diesem Gebiet, sondern spreche hier allgemein, aber Künstliche Intelligenz ist ein Thema, über das sich auch Banken Gedanken machen müssen, wie sie es effektiv einsetzen können. Seit Freitag gibt es eine neue Veröffentlichung der EBA, die äußerst aufschlussreich ist. In dieser Veröffentlichung wurde eine Umfrage durchgeführt, um herauszufinden, wie Künstliche Intelligenz verwendet wird. Künstliche Intelligenz stellt eine Herausforderung dar, da sie dazu dient, Prozesse zu vereinfachen. Sie ist oft schneller und fehlerfrei, und sie kann viele Aufgaben übernehmen, die bisher von Menschen erledigt wurden – das ist uns allen bekannt. Das ist jedoch nur ein Aspekt. Man kann ja viel programmieren, aber das andere ist dann, und das spielt genau in die Governance rein. Wie können sie das dann so überwachen, und wie können sie die menschliche Intervention sicherstellen? Vor allem müssen Sie verstehen, was Künstliche Intelligenz bewirkt. Wenn Sie sich darauf verlassen, dass die KI-Entscheidungen allein treffen, basierend auf Black-Box denken, verlieren Sie die Kontrolle. Wenn Sie nicht verstehen, wie die KI ständig dazulernt und welche Prozesse sie genau ausführt, werden die Aufsichtsbehörden wahrscheinlich sofort einschreiten. Ihr könnt hier nicht loslegen und nicht den Algorithmus von irgendeiner ähnlichen Firma machen lassen, die bei euch gar nicht wegen des Copyrights sagt, was sie da programmiert hat. KI bietet enorme Chancen, da sie schnell und effizient einfache Abläufe bewältigen

I3	Herausforderungen und -Risiken > Künstlicher Intelligenz (KI)	23	Governance kommt dann ins Spiel, das ist nachher das, was die Menschen machen müssen. Ich kann die Governance nicht auch noch von der KI erledigen lassen, da wäre ich außen vor. Das wäre, als würde ein autonom fahrendes Auto gegen die Wand fahren, während ich darinsitze – in diesem Fall sicherlich nicht fröhlich, sondern eher gestikulierend. Die Governance wird vor diesem Hintergrund noch bedeutend wichtiger werden, als sie es ohnehin schon ist. Sie ist der Schlüssel dazu. Denn wenn man Algorithmen einsetzt, muss man in der Lage sein, immer noch zu wissen, was sie tun. Man muss sie stoppen, anpassen und stets den Überblick darüber behalten können, was gerade geschieht. Das wird dann zur Herausforderung für die Governance. In den kommenden Jahren, bis zum Ende des Jahrzehnts, werden wir wahrscheinlich eine Revolution erleben, nicht nur in Banken, sondern auch in anderen Bereichen. Wir müssen dann schlussendlich der Aufsicht erklären können, warum wir so viele Kreditausfällen haben. Wenn wir einfach sagen, dass hat die geniale elektronische KI entschieden und wir haben es aber auch nicht verstanden, aber wir haben die KI es dennoch machen lassen. Wenn wir so antreten, dann wird der Laden geschlossen. Dann wird die andere KI in der EZB sagen, ihr habt sie doch nicht mehr alle.

I3	Ganzheitlicher GRC-Ansatz > Definition	26	Es muss so ablaufen wie eigentlich ein perfektes Getriebe. Die Zahlenräder müssen ineinandergreifen greifen. Die Tätigkeiten, die einfach Compliance nicht leisten kann, müssen von uns übernommen werden. Wir müssen hier Hand in Hand arbeiten. Von Compliance müssen die Anstöße kommen hinsichtlich des gesamten Rahmenwerks, gesetzliche Vorgaben und von uns muss dann die Ausarbeitung kommen. Wir können das nicht Compliance überlassen, weil da sind die auch nicht dafür ausgebildet. Ich kann einen Compliance-Experten haben, der mir eine Menge Vorschriften detailliert und umfassend erklären kann. Aber am Ende kann ich ihn nicht das Kreditgeschäft für mich erledigen lassen. Hier komme ich ins Spiel. Ich muss die Vorschriften so interpretieren können, dass sie zu meinem Handlungsfeld passen und ich sie einhalten kann. Gleichzeitig muss ich sicherstellen, dass ich sie so umsetze, dass es letztendlich profitabel ist – schließlich wollen wir mit Krediten Geld verdienen. Manchmal wird vergessen, dass wir das Kreditgeschäft nicht nur betreiben, dass sich Compliance- und Governance-Personal freuen oder den Wirtschaftsprüfern Arbeit zu verschaffen. Unser Endziel ist natürlich auch die Erwirtschaftung von Erträgen. Das kann jedoch nur funktionieren, wenn wir die Vorschriften korrekt anwenden und sie so nutzen, dass wir am Ende auch einen Mehrwert erzielen. Ein einheitlicher Ansatz im Bereich Compliance erfordert natürlich Verständnis für unsere spezifischen Bedürfnisse. Gleichzeitig müssen wir für Compliance ebenfalls Verständnis aufbringen. Wir können

I3	Ganzheitlicher GRC-Ansatz > Definition	28	Genau, wir dürfen auch nicht versuchen, die Revision zu kopieren. Dies mag in einigen Fällen sinnvoll sein, vor allem wenn es hohe Ausfälle gibt. Jedoch sollte das nur punktuell geschehen, wenn es einen konkreten Bedarf gibt. Insbesondere dann, wenn man merkt, dass die im Vertrieb zu viel alleine machen, wenn man sie alleine lässt, was die große Sorge der Aufsicht ist. Obwohl unsere Vertriebsmitarbeiter erfahren und kompetent sind – schließlich sind sie qualifizierte Bankfachleute und keine unseriösen Drückerkolonnen – erhalten sie ihre Entlohnung auf Grundlage ihrer Abschlüsse, die sie machen. Natürlich besteht die Gefahr, dass bei dieser Art der Vergütung die Tendenz entsteht, Kredite anzubieten, auch wenn dies nicht immer angemessen ist. Daher müssen wir möglicherweise durch Stichprobenkontrollen überwachen, was sie produzieren. Dennoch können wir nicht einfach den Ansatz von Group Audit auf den Vertrieb übertragen, da die Aufgaben von Group Audit eine andere Schwerpunktsetzung haben. Stattdessen müssen wir eine engere Zusammenarbeit zwischen den Bereichen ermöglichen. Dies erfordert einen kontinuierlichen Austausch, gelegentliche Prüfungen und möglicherweise auch Schulungen für unsere Vertriebsmitarbeiter, um sicherzustellen, dass die Qualität der Kreditvergaben gewährleistet ist. Es ist stets von Vorteil, wenn jemand in der Revision tätig ist, der zuvor bereits praktische Erfahrung im Geschäftsbereich gesammelt hat und nicht nur rein theoretisch ausgebildet ist. Auf diese Weise könnt die auch ein besseres Gespür
I3	Status quo: Governance, Risiken und Compliance > Kommunikation und Zusammenarbeit	28	Dies erfordert einen kontinuierlichen Austausch, gelegentliche Prüfungen und möglicherweise auch Schulungen für unsere Vertriebsmitarbeiter, um sicherzustellen, dass die Qualität der Kreditvergaben gewährleistet ist.

I3	Ganzheitlicher GRC-Ansatz > Strategie	30	Also, intuitiv auf keinen Fall! Wir sind verpflichtet, unsere Strategie regelmäßig zu entwickeln und der Aufsicht vorzulegen. Wenn wir einfach intuitiv vorgehen würden, das würde die Aufsicht sagen: „intuitiv hier, euch helfen wir ja – wir sind das größte deutsche Institut.“ Das würde schiefgehen.
I3	Ganzheitlicher GRC-Ansatz > Strategie	31	Ich kann Ihnen jedoch mitteilen, dass es im Außenverhältnis interessante Entwicklungen in Bezug auf die Strategie gegeben hat. Insbesondere der erwähnte Professor Simon, dessen Schwerpunkt im Bereich Chief Administration liegt, ist nicht nur für formale Angelegenheiten zuständig, sondern er verantwortet auch die Bereiche Legal, Governance und Compliance unter sich. Zusätzlich hat er nun auch die Rolle des Länderchefs für Amerika übernommen. Ich zitiere hier lediglich Informationen, die öffentlich zugänglich sind, und bitte Sie, nicht anzunehmen, dass ich über besonderes Insiderwissen verfüge – das ist ohnehin nicht der Fall, da ich mich auf Deutschland beschränke. Es scheint, dass diese Änderungen in der Strategie von oben nach unten umgesetzt werden, wobei Herr Simon nun auch für die USA verantwortlich ist. In diesem Bereich müssen nicht nur Vorschriften eingehalten werden, sondern es ist auch erforderlich, mit Kunden zu interagieren. Man, strebt an, eine Person mit starkem regulatorischem Hintergrund in der Organisation zu haben, um eine ganzheitliche Betrachtung sicherzustellen und entsprechend umzusetzen. Aktuell gibt es noch Verbesserungsbedarf in diesem Bereich, wie aus den Medienberichten hervorgeht. Es gab unterschiedliche Meinungen und Reaktionen, aber der Auslöser für diese Veränderung war, einen Experten für Governance in den USA einzusetzen, um eventuelle Schwachstellen zu schließen. Dies dient dazu, sicherzustellen, wie diese Strategie im Vorstand tatsächlich umgesetzt wird. Hierbei möchte ich betonen,

I3	Ganzheitlicher GRC-Ansatz > Vorteile eines ganzheitlichen GRC-Ansatzes	33	Im besten Fall, wenn ein reibungsloser Austausch stattfindet und alles nahtlos zusammenpasst, entsteht eine Art ideale Welt. Hierbei entwickeln die Compliance- Manager ein besseres Verständnis für die Realitäten im Kreditgeschäft. Genauso wichtig ist es jedoch, dass die Personen, die über Kreditentscheidungen verantwortlich sind, ein umfassendes Verständnis für die Einhaltung von Compliance-Richtlinien haben. Es darf nicht mehr vorkommen, dass wir Geschäfte abschließen, ohne uns darum zu kümmern, ob wir gegen Vorschriften verstoßen. Diese Mentalität haben wir bereits bei Personen erlebt, die nicht mehr bei der Bank sind und uns dadurch Milliardenstrafen eingebracht haben. Daher ist ein Austausch von Fachwissen und Hintergrundinformationen unerlässlich. Diese Zusammenarbeit kann meiner Meinung nach am besten umgesetzt werden, indem beide Seiten ihr Wissen teilen. So wird vermieden, dass Verdachtsmomente aufkommen.

I3	Status quo: Governance, Risiken und Compliance > Reporting	35	Das Reporting wird zunächst eigenständig vor Ort in den einzelnen Sparten erstellt. Anschließend werden diese Berichte zusammengeführt. Wir haben einen Finanzvorstand, Herr Wolke, der sich die Gesamtsituation anschaut. Ich bitte um Verständnis, dass ich in Bezug auf die genaue Vorgehensweise im Vorstand nicht im Detail informiert bin. Meine Kenntnisse reichen nur bis zu einem gewissen Punkt in der Hierarchie. Ich weiß lediglich, dass es eine Verpflichtung für die Vorstandsmitglieder gibt, sich die Gesamtsituation anzusehen, und dass verschiedene Reporting vorhanden sind. Außerdem ist klar, dass quartalsweise Berichte erstattet werden müssen. Was ich gelesen habe, deutet darauf hin, dass die Vorstandsmitglieder sich die verschiedenen Reporting untereinander ansehen und dass keine isolierten Berichtsstrukturen entstehen dürfen. Die Aufsichtsbehörden würden eine solche Silo-Bildung ebenfalls nicht akzeptieren. Aber ich kann Ihnen keine konkreten Beispiele nennen, da ich in diesem Bereich nicht so involviert bin. Was ich jedoch weiß, ist, dass unser Reporting fortgesetzt wird, da Herr Selig natürlich auch über die Aktivitäten seiner Risikoteams informiert sein möchte. Vor Ort erstellen wir unser eigenes Reporting. Wir erstellen kein spezifisches Reporting für die Corporate Bank, da dies nicht erforderlich ist. Unser Reporting wird dann jedoch auf höherer Ebene zusammengeführt und vom Risikovorstand überprüft. Dabei arbeiten sie eng mit dem Finanzvorstand und dem Governance-Vorstand zusammen.

D Transkripte Experteninterviews

Interview mit Jerome Kögel

I: So, Herr Kögel, ich würde jetzt einmal das Gespräch aufzeichnen. Sind Sie damit einverstanden? #00:00:06#

B: Ja. #00:00:08#

I: Dann kommen wir schon direkt zu der ersten Frage. Bitte stellen Sie sich einmal kurz vor und erläutern Sie Ihre Aufgaben bei der Kreditplus Bank AG. #00:00:32#

B: Ich bin Jerome Kögel, bin 30 Jahre alt. Im Prinzip habe ich mal Controlling studiert, bin dann aber irgendwie in die Wirtschaftsprüfung reingerutscht bei KPMG. War dann ein paar Jahre auch in der Beratung. Ich habe ganz früher meine Bankausbildung gemacht, zurück in den Sparkassen Verbund gegangen. Dort vier Jahre lang die Unternehmenssteuerung für eine Tochter von der Sparkasse mit betreut. Ich bin dann in dem Sinne, es war praktisch ein Institut, das unter WpHG fällt, sehr viel mit Kostenträger. Bin dann praktisch irgendwie in diese Schiene reingerutscht, dass ich viel mit Regulatorik zu tun hatte. Ich habe das interne Kontrollsystem und Ähnliches aufgebaut und dementsprechend nebenher noch mein MBA gemacht und habe dann praktisch über den Headhunter den Job als Leiter MaRisk - Compliance angenommen am Schluss. Das heißt vielleicht zum Hintergrund, also ich habe mich nicht irgendwann mal entschieden, das zu studieren und habe dann angefangen zu arbeiten, sondern ich habe auch das Gefühl, dass ist bei vielen Leuten in dem Umfeld bei uns so, ja, man rutscht da manchmal einfach rein, wenn die Interessen es hergeben. Jetzt bin ich Referatsleiter bei der Kreditplus Bank für MaRisk-Compliance. Ist im Prinzip ganz normale Compliance. Das MaRisk davor kommt nur daher, dass wir zu einem französischen Konzern gehören. Und dort wird Compliance immer auch noch mit Geldwäsche und Risikomanagement gleichgesetzt. Das heißt, ich glaube, die sind da schon ein bisschen in die Richtung unterwegs. Bei uns aber ist es im Prinzip noch klassisch, wie es ja auch die MaRisk- teilweise implizieren. #00:02:29#

I: Sie sind nicht für die Prävention von Geldwäsche zuständig, oder? #00:02:40#

B: Also da wir derzeit die Geldwäschestelle vakant ist übernehme ich praktisch gerade auch einige Aufgaben aus dem Team. Aber im engeren Sinne bin ich eigentlich nur für die klassische Compliance zuständig. #00:02:54#

I: Und was sind dann die klassischen Compliance Aufgaben, die Sie jetzt in der Praxis umsetzen müssen? #00:03:03#

B: Also ganz viel hängt natürlich mit Regulatorik zusammen. Das heißt, wir haben ein System, das bei uns läuft. Ich glaube, da kommen wir nachher noch darauf zu sprechen, wo wir dafür sorgen, dass wir alle regulatorischen Vorgaben auch entsprechend implementieren und umsetzen. Wir sind im Prinzip dafür zuständig, zum Beispiel wenn neue Produkte kommen, dass wir das entsprechend betreuen, diesen ganzen neue Produkteprozess, den wir auch aus der MaRisk kennen. Wir sind oft für Analysen aus Compliance Sicht verantwortlich. Das heißt, wann immer etwas strategisch entschieden wird, wird normalerweise auch eine Compliance Opinion verlangt, wo wir praktisch schauen müssen, vor allem im Sinne Schutz von Kunden, Regulatorik, dass wir uns an die Vorgaben halten. Genau, wo es praktisch eine Meinung von uns geben muss. #00:03:54#

I: Dann kommen wir direkt zur zweiten Frage. Da geht es nämlich um die Entwicklung im Bankensektor. Wenn Sie jetzt in die Gegenwart schauen und die aktuellen Entwicklungen in Bezug auf Governance, Risik und Compliance im Bankensektor betrachten, wie würden Sie denn den derzeitigen Stand des Bankensektors im Jahr 2023 beschreiben? #00:04:20#

B: Ja, habe ich mir die Frage natürlich auch vorher durchlesen und habe mir überlegt, okay, ja gute Frage. Ich würde es mal zusammenfassen, dass wir weiterhin in Entwicklungsstadium sind. Ich meine klar, nach 2009 oder auch schon früher 2001, dann auch erst kürzlich, der Bankensektor hat sich stark verändert in den letzten, ja, im Prinzip... In den letzten 20 Jahren wahrscheinlich noch mehr. Und gefühlt ist es auch, wenn man mal sieht, wie viele neue Anforderungen auf uns zukommen, wo sich Dinge ändern. Wir haben plötzlich ESG überall drin. Das ist ja etwas, was man eigentlich erwarten könnte, dass das schon seit immer eigentlich ein Part davon war. Aber es kommt eigentlich jetzt wirklich erst als eine wirklich fix vorgeschriebene Vorgabe rein. Und daran merkt man, denke ich, dass wir einige Themen, wo man vielleicht denken würde, na ja, wenn man Compliance sich mal als Schaubild malt, dass die Dinge schon drin wären. Und das ist für mich so ein klares Zeichen dafür, dass wir immer

noch dabei sind zu umfassen, was muss Compliance eigentlich alles einfangen am Ende. #00:05:27#

I: Welche Bedeutungen haben regulatorische Anforderungen für die Kreditplus Bank AG und wie wird sichergestellt, dass die gesetzlichen Vorschriften eingehalten werden? Da sind Sie ja als Compliance Manager wahrscheinlich federführend dafür verantwortlich, dass alle gesetzlichen Anforderungen auch eingehalten werden. #00:06:01#

B: Ich glaube, das ist so dieses Chronische, was egal welchen Menschen aus egal welchem Bereich man frägt. Der Bereich, in dem man ist, ist immer unglaublich wichtig, denn sonst würde man da ja nicht arbeiten. Nichtsdestotrotz, Compliance für jemanden, der am Schluss in der Bank steht und irgendwelche Dinge verkauft, wird für ihn nicht so einen hohen Stellenwert haben wie jetzt für mich. Das ist klar. Aber man muss ganz klar sagen und da ist der Gesetzgeber eigentlich auch recht deutlich, ein Compliance Beauftragter - ich bin auch Compliance Beauftragter, hat direkt an den Vorstand zu berichten. Das ist etwas, wo im Prinzip verdeutlichen sollte, es gibt hier nicht noch irgendwelche Umwege, wo Dinge dann verschleiert werden, sondern es ist meine Aufgabe. Ich muss gemeldet werden und der Vorstand muss mich kennen und ich muss mit ihm sprechen. Ich denke, das zeigt eigentlich schon, in welchem Weg wir sind. Und wenn man mal, ich glaube, da kommt nachher auch noch die Frage zu den Reportings, wenn man mal sieht, wie oft ich mit Vorständen, mit Aufsichtsrat und mit unserer französischen Mutter, wie oft wir im Austausch sind. Und wenn ich mal eine rote Ampel melde, wo ich praktisch sage: „wir haben hier ein Problem“ - wenn man sieht, was das für Wellen schlägt. Das zeigt es schon deutlich, dass auch bei uns und ich glaube, das geht wahrscheinlich allen Banken so, vielleicht Wirecard nicht so ganz, aber bei allen, die gut geführt werden, ist es einfach so, dass für den Vorstand mit Sicherheit Compliance eine Stelle ist, die ich regelmäßig lieber mal frage, allein schon aus Selbstschutz. #00:07:39#

I: Berichten die Funktionen Compliance, Risikomanagement und Interne Revision denn separat an den Vorstand? Oder gibt es ein ganzheitliches Reporting von allen drei Bereichen das an den Vorstand geht? #00:08:04#

B: Ja, ich glaube, da sind wir wahrscheinlich schon, ohne es zu wissen, einen gewissen Schritt gegangen in Richtung GRC als gemeinsamen Ansatz. Denn wir berichten tatsächlich zusammen in einer Sitzung der ganzen Vorstandschaft, und zwar quartärlich. Und halbjährlich

sind dann noch die Kollegen von der Gruppe dabei. Genau Wir kommen da direkt hintereinander. Es sind verschiedene Punkte in dieser Präsentation und da kommt eben Compliance, Risk gleich nacheinander. Das heißt vom Reporting her machen wir das schon gemeinsam an die Vorstände und auch an den Aufsichtsrat. Da läuft es ähnlich. #00:08:49#

I: Und welche Vorteile ergeben sich denn durch dieses ganzheitliche Reporting? #00:08:57#

B: Also ein großer Vorteil ist natürlich, wenn wir oder wenn Risk eine Problemstellung identifiziert und sie in dieser Sitzung vorstellt, dann geht die zweite Frage automatisch immer an die jeweils andere Stelle. Das heißt: „was sagt denn ihr dazu?“. Dieser Austausch ist dann auch von Vorstandsseite her im Prinzip der logische Schritt. Und der Vorteil ist, dass eben auch genau für den Vorstand und schließlich müssen die das Unternehmen führen: wenn ein Thema kommt, können sie gleich im Prinzip alle mit verarzten. Sie haben alle direkt beisammen und müssen nicht noch eine extra Sitzung dazu machen. Und dann können sie eben sofort diese Antworten holen, die sie brauchen, um zu entscheiden. #00:09:44#

I: Wie würden Sie denn die Rolle von Governance, Risk und Compliance in der Kreditplus Bank AG beschreiben? Wie wichtig sind denn diese Funktionen? Oder generell diese Thematiken? #00:10:00#

B: Klar, wie gesagt das ist der Fluch der Position. Ich würde natürlich sagen wir haben eine sehr sehr hohe Bedeutung im Unternehmen. Ich sehe das aber auch durchaus gespiegelt. Wir haben jetzt zum Beispiel ein bisschen Bewegung gehabt, wir haben neuen CEO, wir haben einen neuen CFO. In der ersten Terminrunde, die er hatte, war immer auch Compliance dabei, immer bilateral noch die Gespräche, das heißt man merkt das es ist eine hohe Relevanz hat. Das wir bei uns durchaus auch getrieben durch die Gruppe. Frankreich ist in einigen Dingen bisschen strenger als wir andere natürlich auch nicht. Aber dadurch, dass wir einem Riesenkonzern, also der Crédit Agricole angehören, eine der 10 größten Banken der Welt kann man sich vorstellen, es gibt durchaus auch ganz klare Vorgaben aus Frankreich die sagen: „Hey, ihr redet erst wenn Vorstände sagen ihr redet mit Compliance und Ende.“ Es gibt eigentlich kein Vorbeikommen daran. Trotzdem muss man natürlich sagen Compliance ist eine Kostenstelle, wir erbringen keine Erträge und am Schluss sind wir nicht der Motor der Bank, sondern wir sorgen nur dafür, dass wir am Schluss nichts machen, was wir nicht machen dürfen. Und da musst man auch realistisch bleiben. Das Geld wird woanders verdient. #00:11:26#

I: Wie gestaltet sich denn die Zusammenarbeit zwischen den internen Governance-Organen Risikomanagement, Interne Revision, Compliance sowie auch mit den externen Governance Organen, wie zum Beispiel Wirtschaftsprüfer? #00:11:53#

B: Also auch aus meinen vorherigen Stellen, kann ich sagen, es hängt natürlich immer viel mit den Menschen in den Teams ab. Wenn man mit denen gut kann, man, vielleicht sogar im gleichen Flur sitzt, dann ist der Austausch immer ein ganz anderer, als wenn es vielleicht jemand ist, der kurz vor der Rente steht und mit den jungen Leuten, die probieren was zu verändern, nicht so viel anfangen kann. Bei uns jetzt in der Kreditplus habe ich den Vorteil, das Risikomanagement direkt gegenübersitzt, der Leiter ein ähnliches Alter wie ich hat und wir im Prinzip andauernd im Austausch sind. Das heißt, wenn ich irgendwo Probleme mit etwas habe, was er tut, oder andersrum, dann kommt man halt kurz rüber und klärt die Sache und kann auch einfach offen ehrlich miteinander sprechen. Auch wenn einem etwas gegen den Strich geht. Ich denke das ist wichtig. Die Interne Revision ist natürlich auch, für uns immer, so wie im ganzen Unternehmen, die kommen halt prüfen dich und nerven dich dann mit irgendwas. Das ist natürlich absolut notwendig, denn die finden durchaus Sachen, die auch absolut richtig und wichtig sind, dass wir die ändern. Am Ende ist es aber erstmal ein Workload, so ist es ja immer bei der Internen Revision oder beim Wirtschaftsprüfer ist es genau das Gleiche. Ich habe es ein paar Jahren durchgemacht, aber diese Zusammenarbeit im Prinzip, ja, bei uns gibt es eine „Duz-Kultur“, ich glaube das ist ganz wichtig. Und wichtig ist, dass man dann einfach mal hinlaufen kann und das zeigt, glaube ich auch, dass die Zusammenarbeit eigentlich wirklich gut funktioniert, soweit. #00:13:24#

I: Gibt es denn auch zwischen den Schnittstellen einen regelmäßigen Jour-Fix, wo ein Austausch untereinander stattfindet? Jede Schnittstelle gibt ein UpdatΔ@oe, wer gerade an welchem Thema arbeitet und wie man sich eventuell gegebenenfalls sogar unterstützen könnte? #00:13:46#

B: Ist eine gute Idee, gibt es derzeit nicht. Das hängt bei uns, auch davon ab, das im Prinzip, Governance, gut Governance und Risk, bin ich im Prinzip. Aber Risk und die Interne Revision zum Beispiel, wir haben jeweils einen anderen Head of, das heißt, darüber haben wir jetzt den Austausch nicht. Das heißt, wenn wir den gleichen Berichtsweg hätten, an den Head of, dann wäre das wahrscheinlich noch mal ein bisschen anders. Ich bin zum Beispiel mit Legal und

Geldwäsche zusammen, an den gleichen Berichtsweg. Aber nein, wir haben keinen Jour-Fix, sondern eben diese quartärlichen Sitzungen, aber ansonst ist es eher ja, wenn wir es brauche, dann sprechen wir miteinander, wenn nicht, dann nicht. #00:14:35#

I: Welche spezifischen Herausforderungen und Risiken stellen sich denn für Banken in Bezug auf Governance, Risk und Compliance dar? #00:14:49#

B: Also, ich glaub ein großes Problem, dass wir jedenfalls für Governance und Compliance, kann ich sagen haben, dass die Maschinen die Laufen schon lange und Compliance ist erst seit naja 20 - 25 Jahre maximal überhaupt in der Lage, fundiert mal irgendwo nein zu sagen. Sonst hieß es glaub ich früher immer: was Geld bring wird gemacht, Ende. Und das Problem ist eben, wir haben so viele Prozesse, die Laufen, man kann jetzt nicht sagen: ok, wir halten jetzt mal alles an - dann machen wir unsere Compliance Prüfung von allem, und dann machen wir weiter. Denn das dauert 20 Jahre, wir verdient kein Geld in der Zeit. Also, die große Herausforderung ist, zum einen muss man natürlich das laufende Geschäft im Auge behalten. Wenn wir neue Produkte haben, dann müssen wir die prüfen. Wir müssen gucken, wenn eine Regulatorik reinkommt, haben wir die nicht schon umgesetzt. Aber auch da, wenn man mal guckt, wie zum Beispiel die BASEL III Vorschriften oder irgendwann mal BASEL IV oder WpHG, man kann nicht sagen, okay es kommt eine neue MaRisk- Novelle oder WpHG-Novelle und wir prüfen jetzt mal das ganze Gesetz durch. Das geht einfach nicht, da bräuchten wir glaub ich 50 Leute wahrscheinlich dafür, sondern das ist oft ebenso, dass wir nur die Änderungen antizipieren können. Und ich glaube eben, dass das eben ein großes Problem ist, das die Prozesse, die bereits stehen, nicht immer voll geprüft werden können nach den aktuellen Vorgaben und andererseits können wir auch nicht alle Vorgaben, also allein diese Riesenbase, die es gibt an Gesetzten und Vorschriften wir können niemals 100-prozentig sagen: Ja, wir erfüllen alle Vorgaben - sondern es gibt immer ein Risiko damit. Man muss sich eben bewusst sein, es gibt immer ein Risiko, das wir irgendwas nicht einhalten. Das ist inhärent, wir müssen nur versuchen es so klein wie möglich zu halten. #00:17:28#

I: Erfolgt das bei Ihnen anhand von einer regelmäßigen Risikoanalyse? Dass sie sich dann regelmäßig angucken, ok wie hoch ist das Risiko, wie kann man das Mildern oder welche Maßnahmen muss man umsetzen, dass es nicht eintritt. #00:17:47#

B: Ja genau, Op-Risk ist bei uns immer ein Thema, wir müssen uns regelmäßig dazu äußern. Es gibt zum Beispiel auch eine Aufstellung von allen Regularien, die für uns bedeutend sind und dann machen wir zum Beispiel auch jedes Mal, jedes Jahr, nochmal eine eigene operatives Risiko Einschätzung, wo wir praktisch zu jedem wichtigen Gesetz oder wie jeder Regulatorik die wir haben, nochmal sagen: Hey so hoch ist das Risiko tatsächlich am Schluss für uns, aus dieser Regulatorik #00:18:18#

I: Muss ihr quartalsmäßig an das Risikomanagement berichten? Muss jede Funktion bzw. Abteilung an das Risikomanagement ein Update geben muss bezüglich Risiken? #00:18:43#

B: Also, die wirkliche, das Inventar Op-Risk überarbeiten, machen wir nur einmal im Jahr. Da muss man auch sehen, dass dauert halt auch vier Monate, das heißt, viel öfter könnten wir es auch nicht machen. Wir haben aber, um eben dieses unterjährige zu umgehen, haben wir natürlich Ad-hoc-Pflichten, die wir zu erfüllen haben. Das heißt wir machen auch viele Kontrollen, sobald wir irgendwo merken, wir haben hier vielleicht ein Risiko, das wir noch nicht einkalkuliert haben, dann gibt es immer Ad-hoc Berichte. #00:19:15#

I: Okay, gibt es dann auch ein Tool, wo die Abteilungen ihre Risiken erfasst und das Risikomanagement übergreifend auf alle Risiken, die gemeldet worden sind, zugreifen kann? #00:19:28#

B: Genau, es wurde tatsächliche, haben wir jetzt erst seit letztem Jahr ein neues. Das heißt wir füttern das gerade noch, es läuft noch nicht 100-prozentig und, aber da hat der Konzern aber auch ordentlich Geld liegen lassen, damit wir praktisch jetzt ein neues Tool bekommen. Da merkt man glaube ich auch, immer wenn es ums Geld geht, dass es wahrscheinlich auch wichtig ist am Ende. Ich muss sagen, ich verstehe es noch nicht ganz das Tool, aber wenn ich das Zielbild ankucke, dann ist es genau das, wo wir jetzt praktisch daran arbeiten. Was aber auch natürlich, auch immer bedeutet, vielleicht hat man es bis dahin noch nicht so ganz 100-prozentig gut aufbereitet. #00:20:02#

I: Wie heißt das Tool denn? #00:20:06#

B: Q-SAC, aber ich bin mir auch nicht sicher, dadurch dass wir die Gruppe haben. Die kaufen auch gerne mal irgendwas ein und nennen das dann anders. #00:20:20#

I: Auf welche Weise könnte die Zusammenarbeit sowie Kooperationsmechanismen zwischen den Schnittstellen des Risikomanagements, interne Revision und Compliance optimiert werden, um eben Redundanzen und Mehrkosten zu vermeiden? #00:21:10#

B: Ja, also ganz klar ist genau eben, dass wir zum Beispiel Tools nutzen, die wir am besten beide nutzen können. Diese moderneren Tools, die es natürlich auch gibt, sorgen auch dafür, dass das auch von der Bedienung her leichter ist. Also, ich kann ihnen die Risikotools reingucken und verstehe nicht nur Bahnhof, sondern verstehe auch tatsächlich, ich weiß, worauf, worauf ich ungefähr gucken muss, und dann kann man immer noch Fragen und andersrum natürlich auch. Das heißt, da muss man natürlich sagen, da gibt es extrem positive Effekte, die wir daraus haben, sobald wir halt, wenn wir digitaler werden, moderner werden, schneller werden. Aber was, glaube ich, unersetzbar ist, ich glaube, der integrierte Ansatz ist auch genau das, worauf sie, glaube ich, rauswollen. Wenn wir von Grund auf miteinander arbeiten, dann haben wir natürlich genau die Probleme, nicht, dass wir irgendwann mal etwas fertig ist und wir zusammensitzen merken, wir haben viele Dinge doppelt gemacht. Das heißt, ich habe mir Sorgen gemacht um Op-Risk, aber Risiko auch, weil man muss ja sagen, eine Op-Kategorie gehört ja auch immer mir. Das heißt, ich habe sie bei mir drin, sie haben sie bei sich drin, Revision hat es wahrscheinlich auch noch irgendwo drin, und das ist genau das Problem. Jeder hat sich dreimal Gedanken gemacht, wir kommen vielleicht sogar zu etwas unterschiedlichen Ergebnissen, weil wir unterschiedliche Informationsbasis oder einfach das Gefühl, ein anderes ist. Und da ist natürlich wichtig, wenn wir von Anfang an bei allen möglichen Themen einfach uns mal zusammensetzen würden. Ich weiß nicht, ob es immer klappt, wahrscheinlich nicht. Dann hätten wir 100-prozentig Redundanzen würden vermieden werden, und wir bräuchten auch weniger Man-power für einzelne Dinge. #00:22:53#

I: Wie würden sie einen ganzheitlichen GRC-Ansatz definieren? Was ist denn aus ihrer Sicht ein integrierter GRC-Ansatz? #00:23:01#

B: Gute Frage also, ehrlich gesagt, noch gar nicht wirklich, habe ich nur gar nicht so auf dem Schirm gehabt also als Abkürzung. Wenn ich einen integrierten Ansatz mir überlegen müsste, dann wäre das auf jeden Fall, dass wir auf die gleichen Datenbanken zugreifen müssen. Das heißt, wenn wir mal überlegen, gibt es dann im Unternehmen eine Prozesslandkarte, und dann müssten wir eigentlich zu jedem Prozess die gleichen Einschätzungen am Schluss getroffen haben, beziehungsweise das Ergebnis muss das gleiche sein. Und integriert wäre für mich eben genau der Ansatz. Wenn wir einen Prozess verändern oder neu machen, dann müssen wir von Anfang an, an den Tisch sitzen und gemeinsam überlegen, okay, was sind die Auswirkungen

von diesem Prozess? Was wollen wir aus unseren Abteilungen? Wollen wir zum Beispiel bestimmte Kontrollen drauf? Haben wir gewisse sorgen, was das angeht, und ich denke, dass der Austausch da halt zentral ist. #00:24:09#

I: Ich kann ihnen mal die Definition, die in der Literatur steht vorlesen: „GRC ist ein integrierter, holistischer Ansatz einer unternehmensweiten Governance, Risk und Compliance, die dazu dient, sicherzustellen, dass eine Organisation ethisch korrekt und in Übereinstimmung mit ihrer Risikoeignung, internen Richtlinie und externe Anforderungen agiert. Durch eine Abstimmung von Strategie, Prozessen, Technologie und Personal, Strukturen werden Effektivität und Effizienz verbessert. Genau, also das ist eben genau das, dass man halt, was die Strategie angeht, Prozesse, irgendwelche technologischen Tools, wie sie schon gesagt haben, dass es irgendwie eine Datenbank gibt, wo alle Schnittstellen auf Informationen zugreifen können und man nicht halt regelmäßig sich austauschen muss oder Termine vereinbaren. Und dann sprechen irgendwie die anderen Schnittstellen öfter, als sie es eigentlich müssten, und fragen Informationen nach, obwohl man eigentlich das Ganze, dann durch die Datenbank einsehen könnte, und so kann man natürlich auch Zeit sparen. #00:25:40#

B: Ja, ich denke, von der, von der Definition finde ich sich gelungen. Dann ist es ungefähr das, was ich mir auch vorgestellt habe. Ich glaube, natürlich ist es immer schwierig, sich auszusuchen, welche Bereiche nenne ich jetzt. Mit GRC hat man halt dann Governance Risk und Compliance genommen. Man muss natürlich sehen, in jedem Unternehmen gibt es noch andere Themen, die wichtig sind. Manchmal gibt's Compliance noch aufgeteilt in WpHG und Ma-Risk. Wir haben noch Geldwäsche, das teilweise zu Compliance gehört, teilweise auch nicht. Wir haben die Datenschützer. Wir haben ja auch noch die Information Security, was gerade auch absoluter Trend ist. Und zum Beispiel auch ESG, das bei uns zum Beispiel jetzt eine eigene Position bekommen hat, weil guckt man die neue Novelle an, Ma-Risk die jetzt gerade kommt, die schreiben einfach überall ESG rein. Aber dadurch haben wir das Problem nicht gelöst, sondern müssen auch gucken, was macht man denn am Schluss damit? Deshalb ist wahrscheinlich wichtig, dass man eben schon auch klarstellt, dass GRC, das die drei praktisch das wiedergeben sollen, aber natürlich in einzelnen Unternehmen durchaus dann ist eben mal Risk mehr oder Risk weniger, genau wie Compliance auch. #00:27:00#

I: Verfolgt die Kreditplus Bank AG eine integrierte GRC-Strategie? #00:27:57#

B: Ich glaube, von wirklich von einer integrierten Strategie zu sprechen, da fehlt noch einiges. Bei uns sind die Vorgaben schon relativ klar getrennt. Das heißt also, bei uns können sie

gucken, wir haben die Regulatorien, dann haben wir aber auch die Gruppen, Vorgaben, die im Prinzip die Regulatorik teilweise schon enthalten, aber natürlich nicht die nationalen. Da muss man schon noch ganz klar sagen, es gibt Risk, und es gibt Compliance, und es gibt Geldwäsche, und die überschneiden sich natürlich teilweise. Aber aes gibt klare Zuständigkeiten. Ich bin für die Bereiche eben Compliance zuständig und Risk für Risk. Und wenn die scheiß bauen, dann ist das ihr Problem, und wenn ich das tue, ist eben mein Problem und wirklich einen integrierten Ansatz, dass ich zum Beispiel auch, wenn die etwas umsetzen oder ich etwas umsetze, jeweils auch die anderen mit reinnehmen oder vielleicht es eben auch einfach eine Vorgabe ist zukünftig, dass man sagt: Hey, egal was ihr macht, ihr macht zumindest mal noch eine kurze Abstimmung. So ist auf jeden Fall noch nicht. Für mich sind es schon noch sehr klare Trennungen. #00:29:00#

I: Welche potenziellen Vorteile könnte sich denn eben ergeben, wenn man von vornherein sagt: Okay, wir haben eine ganzheitliche GRC-Strategie im Unternehmen? #00:29:32#

B: Also genau klar, die Redundanzen sind wichtig, auch die Manpower ist wichtig, die man vielleicht einsparen könnte, was aber auf jeden Fall auch wichtig ist, und dass man man natürlich sehen, größere Unternehmen, vor allem aber auch kleinere, es geht immer auch darum, um diese Machtspielchen. Also habe ich als der kleine Compliance Beauftragte, der mit seinen 30 Jahren herumspringt und meint, er könnte irgendwie den Alten erklären, dass es gerade so nicht geht. Es ist immer auch wichtig, dass man eine gemeinsame Machtbasis in Anführungszeichen hat, und eben auch, weil, wenn jetzt der Compliance Beauftragte, der Geldwäsche beauftragte, und der Risk, der Op-Risk Beauftragte, wenn die zusammenkommen und sagen: hey so geht’s nicht. Dann habe ich eine ganz andere Argumentationsgrundlage, als wenn eben nur einer von denen ankommt, weil die anderen vielleicht überhaupt gar nicht Bescheid wissen. Wenn praktisch die alle zusammenkommen, gibt es meiner Meinung nach keinen Vorstand der Welt, der sagt: ja ja…komm passt schon. Was natürlich bei den Einzelnen auch nicht passieren sollte. Es ist auf jeden Fall wichtig, wenn da diese Allianz zusammenkommt und wenn man eine integrierte Strategie hat, dann hat man das immer schon, dann hat man komplett andere Möglichkeiten eben Sachen auch mal klarzustellen, mal zu Fordern und den Leuten nicht auch noch hinterher rennen muss, damit man seine Bedenken praktisch irgendwie gelöst bekommt #00:31:05#

I: Welche technologischen Lösungen und Tools könnte denn in Betracht gezogen werden, um einen integrierten GRC-Ansatz praktisch zu unterstützen? Habt ihr ein Tool oder eine

Softwarelösung, wo eben alle Schnittstellen auf Informationen zugreifen können bzw. auch Daten erfassen können, dass es übergreifend ist? #00:31:43#

B: Wir haben so etwas, vor allem geht mein halbes Budget meine Abteilung im Prinzip immer für ein Tool drauf. Da sind wir aber auch Vorreiter. Ich war vor einem Monat in Frankreich und habt auch mit den anderen Ägypten, Irland, Spanien gesprochen und da sind wir wirklich absoluter Vorreiter und die einzigen die sowas haben. Wir haben ein Tool, das heißt Radar, Teamradar. Da kommen praktisch alle Regulationen, die wir haben, das heißt sei es von Europa, Deutschland, die kommen praktisch wie in so einen großen Filter rein in dieses Tool. Dann ist da eine Musterbank hinterlegt, das heißt wir geben an, haben wir mit Immobilien zu tun? Nein. Haben wir mit WphG zu tun? Nein. Haben wir mit MaRisk zu tun? Ja. Das wird dann praktisch vorgefiltert. Und alles, was am Schluss noch relevant für uns ist, kommt in dieses Tool und wird dann von Compliance bearbeitet. Das heißt da kommt jetzt neue Eva-Guidelines zum Beispiel, die kommen darüber rein. Erstmals, wir erfahren davon. Ich hoffe Eva-Guidelines hätten wir auch so erfahren. Aber zumindest bei kleineren Anpassungen, geht das durch aus, flutscht das mal durch. Wir haben die Information sichergestellt und wenn es da reinkommt, gucken wir es uns in Compliance an, verteilen es dann alle Interessengruppen, von denen wir denken, wahrscheinlich betrifft es euch. Dann müssen die alle in diesen Tools zurückmelden – „betrifft uns nicht“ oder „haben wir schon umgesetzt“ oder „wir setzen das bis zum 30.6. um“. Und dann fragen wir praktisch nochmal am 1.7. nach: „Hey wie sieht es aus, habt ihr es schon umgesetzt?“. Und wenn ja, dann haben wir sichergestellt, wir kennen alle Regulationen die neu reinkommen und sich ändern. Und wir haben einen revisionssicheren, prüfersicheren Prozess, wo wir darstellen können: „Hier, jede von den Abteilungen hat das für sich umgesetzt“. Und man kann sich vorstellen, alles, was oben in diesen Topf reinfällt, denn wir kriegen, in einem Jahr bestimmt 1500 oder noch mehr Regulation rein. Es ist nur Aufwand, dass überhaupt mal so zu kriegen, dass nur noch die ankommen, die wir brauchen. Aber dadurch, dass wir da immer besser werden, ist es ein krass wichtiges Tool und ich könnte auch nur jeder Bank, die in unserer Größenordnung zumindest ist, empfehlen, sich mit so einem Tool, das muss ja jetzt nicht unbedingt das sein, aber irgend sowas auseinanderzusetzen, weil das hat bei uns dafür gesorgt dass Op-Risk wirklich deutlich gesunken ist. #00:34:27#

I: Ja, dann lohnt sich ja meistens auch die Investition. Vor allen Dingen, wenn diese Softwarelösungen, ja, wie sie jetzt schon gesagt haben, viel Budget dann auch verbrauchen. #00:34:38#

B: Genau, also das ist natürlich immer verbunden, alles was technologisch ist und was taugt kostet meistens ordentlich Geld. Ich meine jetzt auch QSAC von den Kollegen im Risikomanagement, das kostet sicherlich auch einiges an Budget. Aber ja, ich kenne jetzt SAP nicht, aber wenn wir praktisch da mal einen kleinen Haushalt an Tools hat, die einem dabei helfen, dann kann man schon diese tägliche Arbeit, die man hat und die im Zweifel auch einfach nur Zeit kosten, kann das natürlich schon extrem dabei helfen. Wenn wir Abteilungsbudgets zusammenlegen würden, und es Tool gibt die uns beiden helfen, ist es sicherlich auch nochmal etwas was, wenn wir beide uns mit dem gleichen Tool auskennen, was hilft, wenn es eben richtig integrierte Tools gibt #00:35:27#

Interview mit Ulrich Probst

I: Ich würde einmal mit der Aufzeichnung starten. Herr Probst, sind Sie damit einverstanden? #00:00:08#

B: Ja, ich bin einverstanden. #00:00:10#

I: Bitte stellen Sie sich einmal kurz vor und erläutern sie ihre Aufgaben bei der ING Bank. #00:00:52#

B: Ich bin der Ulrich Probst und habe eine Reihe verschiedener Rollen in der ING Diba AG, so ist es Handelsregisterlich korrekt. Gut, eigentlich habe ich seit fast 25 Jahren einen ganz normalen Arbeitsvertrag als Bankangestellter, bin aber in verschiedenen Rollen. Ich bin seit über 20 Jahren im Betriebsrat. Ich bin Vorsitzender der Haustarif Kommission für die GBV-Gewerkschaft, dort auch im Bundesvorstand. Und zu guter Letzt, und das ist eben der Trigger für dieses Interview: ich sitze auch im Aufsichtsrat der ING Diba AG mit Gewerkschaftsmandat. #00:01:46#

I: Okay. #00:01:47#

B: Ich bin Arbeitnehmer und gleichzeitig delegiert der DBV-Gewerkschaft im Aufsichtsrat, und da sitze ich auch in drei Ausschüssen des Prüfungsausschusses, Vergütungskontrollausschuss und ESG-Ausschuss. Und das ist, wenn Sie Compliance Berührungspunkte haben, vielleicht auch interessant. Ich bin für die Region Deutschland der zentrale Whistleblowing-Officer. #00:02:15#

I: Ah okay, das ist spannend! Seit wann machen Sie das? #00:02:21#

B: Seit 2016. Seit erster Wahl im Aufsichtsrat. Ich bin gerade wiedergewählt worden, und gemäß Geschäftsordnung des Aufsichtsrats benennt der Aufsichtsrat bzw. der Prüfungsausschuss des Aufsichtsrats, ernennt einen Whistleblowing-Officer für die Region Deutschland, und da hat bis vor kurzem noch Lande dazugehört. Die wurden jetzt aber letztes Jahr mit uns verschmolzen, also Finanzierungsvermittler für SMI und die Interviews. Wenn dir der Begriff was sagt, die gibt's auf jeden Fall auch in Augsburg die Interviews. Vermittler von Immobilienfinanzierung. #00:03:09#

I: Üben sie dann auch eine Beratungsfunktion aus? #00:04:08#

B: Nein, gar nicht. Das ist eine interne Geschichte. Die wird auch gar nicht nach außen kommuniziert, und ich tu's auch gar nicht. Also in meinen Profilen, da LinkedIn und Xing, da steht vom Whistleblowing-Officer nichts drinnen. Bank Intern ist es natürlich breit kommuniziert, weil das muss, ja oder soll ja sein, sonst bringt es nichts. #00:04:39#

I: Ja, stimmt. #00:04:40#

B: Als Meldekanal da bin ich regelmäßig in Compliance und Risk Culture Schulungen. Da bin ich mindestens im Abspann immer hinten mit drin, also alles, was Kultur, Risiko und Compliance betrifft. Bin ich immer mit inhärent #00:04:58#

I: Thema Entwicklung: Wenn sie jetzt in die Gegenwart schauen und die aktuellen Entwicklungen bezogen auf Governance, Risk Compliance im Banksektor sich anschauen, wie würden Sie den derzeitigen Stand im Banksektor im Jahr 2023 beschreiben, vor allen Dingen im Vergleich zum Jahr 2007, 2008? Was hat sich da verändert? #00:05:58#

B: Da hat sich mit Sicherheit einiges geändert, also wenn ich den ganzen Sektor auf jeden Fall betrachte, Governance, Risk und Compliance waren logischerweise schon immer Themen, aber die wurden eher, also subjektiver Eindruck von mir natürlich, die wurden eher stiefmütterlich und wachstums- und ertragshemmend betrachtet und da empfinde ich auf jeden Fall jetzt einen erheblichen Wechsel von 2007/ 08 bis heute. Also die GRC-Themen, die werden mittlerweile erstmal als insgesamt sogar sehr riskant betrachtet, wenn ich nicht compliant bin und die Risiken nur als Wachstumshemmer betrachte, also die Bedeutung der drei Begriffe ist erheblich gewachsen. Und die Gesamtheit der der drei Begriffe, die würde ich jetzt eher also für den ganzen Sektor als Grundlage für ordentliches, nachhaltiges Geschäft mit Wachstum und stabilen Erträgen betrachten. Früher eher Hemmnis, jetzt tendenziell deutlich stärker die Grundlage fürs Geschäft. #00:07:25#

I: Ja, man merkt finde ich auch, dass es einfach ein sehr wichtiges Thema ist und dass man das hätte auch schon früher besser integrieren müssen, eigentlich. #00:07:38#

B: Viele haben gerne drüber weggesehen, haben Risiken in Kauf genommen, ausgesprochen starken Risikoappetit gezeigt und vielleicht auch noch drüber raus. Und die Geldbußen, Geldstrafen bei Compliance und Geldwäsche und ähnlichem, die haben natürlich auch einige auf den Boden der Tatsachen zurückgebracht. Fast alle. #00:08:01#

I: Was haben denn regulatorische Anforderungen für eine Bedeutung in der ING Bank? Wie wird sichergestellt, dass gesetzliche Vorschriften eingehalten werden? #00:09:36#

B: Also, da haben wir abgeleitet aus gesetzlichen Vorgaben und abgeleitet aus Konzernvorgaben, weil unsere Konzernmutter, also in ING Deutschland oder ING Diba AG, ist ja 100-prozentige Tochter der ING Group mit Sitz in Amsterdam. Die hat wieder ihre eigenen Richtlinien, die abgeleitet sind aus europäischem Recht, aus niederländischem Recht, und wir machen dann genau das gleiche hier in Deutschland. Und zwar für alles, also für alle Bereiche, Risk, Compliance, alles, was die Unternehmensführung und die Line-of-defense betrifft. Wir schreiben dann wieder abgeleitet unsere eigenen Richtlinien und Arbeitsanweisungen, und, die Zusammenarbeit, ich gehe dann gleich mal ein Stück weiter, die Zusammenarbeit mit den Regulatoren, die ist auch ausgesprochen intensiv. Also das kriege ich jetzt bei uns, in der ING Diba, kriege ich es auf jeden Fall auch intensiv mit über die Aufsichtsratssitzungen, insbesondere wenn ich im Prüfungsausschuss teilnehme. Also da ist auf jeden Fall immer eingeladen die Bafin und Bundesbank, und das gleiche natürlich dann auch für die großen Aufsichtsratssitzungen insgesamt. Also, da herrscht reger Austausch und ist auch intensiver Dialog. #00:11:21#

I: Okay, und wie erfolgt die Zusammenarbeit? Also zwischen den internen Governance-Organen und den externen Governance-Organe wie zum Beispiel Wirtschaftsprüfer? Gibt es eventuell auch Absprachen zwischen interne Revision und Wirtschaftsprüfung, dass man sich da gegenseitig unterstützt? #00:11:50#

B: Also die externen, die sind auf jeden Fall dauerhaft bei uns im Haus, ist auch mit Sicherheit erforderlich, weil wir ja auch als systemrelevant eingestuft sind, und ich denke, das ist Branchen Standard. Inwieweit allerdings die Wirtschaftsprüfer mit unserer internen Revision oder dann auch mit den Prüfern in Amsterdam und der Group Revision zusammenarbeiten, also sicherlich

im Rahmen der Erfordernisse. Aber inwieweit die sich dann im täglichen Doing austauschen, da kann ich nichts dazu sagen, weil ich es schlicht nicht weiß. #00:12:40#

I: Ich kenne es so von uns aus, dass die interne Revision dann versucht, einfach gewisse Dinge abzudecken, die vom Wirtschaftsprüfer nicht angeguckt werden im Rahmen der Jahresabschlussprüfung. Also wenn es Sinn macht, letztendlich. #00:13:05#

B: Ja gut, guter Hinweis. Im Aufsichtsrat laufen da verschiedene Themen zusammen. Da berichtet eben auch die die interne Revision und legt auch ihren Prüfungsplan vor, und von Regulatoren her, bekommen wir ja auch Schwerpunkte zugewiesen, die dann der Wirtschaftsprüfer intensiver prüft. Also, da findet schon Austausch statt, also so, dass logischerweise vermieden ist oder vermieden wird, genau die gleiche Stelle doppelt zu prüfen, es sei denn, es macht aus fachlichen Gründen Sinn, aus zwei Perspektiven rauszugehen. #00:13:54#

I: Wie erfolgt die Zusammenarbeit zwischen den internen Governance-Organen, also Compliance, Risikomanagement und interne Revision? Gibt's da eventuell ein GRC-Reporting, wo die Einheiten regelmäßig an den Vorstand oder auch Aufsichtsrat berichten? #00:14:27#

B: Also, im Aufsichtsrat läuft auch an der Stelle viel zusammen, weil da quartalsweise auf jeden Fall ausführlich berichtet wird. Und zusätzlich dazu dann natürlich noch die, die Jahres berichtet. #00:14:43#

I: Ah, Okay, aber diese quartalsweise Berichterstattung, läuft die dann von allen Funktionen separat, oder haben die einen Bericht, den sie zusammen erstellen? #00:14:56#

B: Also, einen integrierten Bericht gibt's nicht. #00:14:58#

I: Okay, also, jede Funktion berichtet quasi selbstständig. #00:15:02#

B: Ja #00:15:03#

I: Wie erfolgt denn der Austausch zwischen Compliance, Interne Revision, Risikomanagement? Weiß du sprechen die Schnittstellen im Rahmen eines regelmäßigen Jour-Fix miteinander? Um eben Doppelarbeiten zu vermeiden und sich bewusst auszutauschen und ggf. zu unterstützen. #00:16:01#

B: Austausch findet auf jeden Fall statt. Nur Doppelarbeiten bin ich mir also, ohne jetzt Details zu kennen und zu nennen. Aber ich bin mir sicher, dass Doppelarbeiten auch stattfinden, weil

es, weil es durchaus auch Sinn machen kann, aus verschiedenen Perspektiven zu betrachten, weil es gibt ja dann auch noch interne Revision der Gruppe Amsterdam, die sich dann auch bei uns hier in Deutschland Vorgänge anschauen. Also, es kann durchaus sein, dass die Group, also die ING Group an der deutschen Kasse vorbei hier rein bei uns prüft. #00:16:52#

I: Ah, ja, okay. #00:16:54#

B: Also, es geht nie komplett an der an der deutschen Kasse vorbei, aber eben auf eigene Initiative. #00:17:02#

I: Wie viele Mitarbeiter hat denn der Compliance Bereich oder Risikomanagement oder Interne Revision? Das sind wahrscheinlich ziemliche viele Mitarbeiter bei euch? #00:17:15#

B: Ja, tendenziell auch noch wachsen. Wobei das bei uns schon immer relativ breit aufgestellt war. #00:17:26#

I: Okay, glauben Sie denn, es würde Sinn machen, dass diese Funktionen bzw. Schnittstellen sich einmal im Monat, vielleicht in einem Meeting, zusammenrufen und zusammen abstimmen/absprechen? #00:17:43#

B: Also, ich bin mir sicher, da heißt Center Of Expertise, also nach der agilen Struktur Aufbauorganisation sind, also integrated risk und Compliance sind beides Center Of Expertise, und die laufen relativ. Also die laufen nicht Hand in Hand, aber relativ eng nebeneinander. #00:18:16#

I: Ah, Okay! #00:18:17#

B: Also, Austausch findet da auf jeden Fall statt. #00:18:21#

I: Okay. #00:18:22#

B: Zumal, weil die beiden unter Risk, also unter der Risiko Vorständin hängen. #00:18:27#

I: Ah, ja, okay, dann ist es ein deutlich leichterer weg, oder? #00:18:34#

B: Ja, ja, also, die können gar nicht unabhängig voneinander arbeiten, weil sie regelmäßig, und zwar direkt an dem gleichen Risiko Vorstand berichten. #00:18:45#

I: Welche spezifischen Herausforderungen und Risiken stellen sich denn jetzt für Banken in Bezug auf Governance, Risk und Compliance? #00:19:07#

B: Also, es sind die sich regelmäßig und relativ schnell hintereinander ändernden rechtlichen Anforderungen, und da müssen auf jeden Fall die Aufbau- und die Ablauforganisation darauf zugeschnitten sein, auch personell. Und die die Aufmerksamkeit seitens Regulatoren und andere Stakeholder, also auch Kunden. Ich denke, das ist gerade bei Banken, die sich früher relativ wenig Gedanken drum gemacht haben, in der Masse zumindest das ist eine spezifische Herausforderung in der Bankenbranche. Und der sich verändernde Wettbewerb in Banken. #00:20:31#

I: Bezüglich der immer steigenden regulatorischen Anforderungen habt ihr aktuell eine Software mit der ihr arbeitet? #00:20:40#

B: Ja, also bei uns, bei den nenne ich mal alteingesessenen Mitspielern in der in der Bankenbranche. Wir sind gewohnt, eng getrackt und reguliert zu werden, und die Wettbewerber, die neu am Markt aufpoppen, die sind deutlich weniger reguliert, und das halte ich für eine spezielle Herausforderung in der Bankenbranche. Die anderen werden sich dran gewöhnen müssen, dass Risk und Compliance im Finanzdienstleistungsbereich extrem wichtig sind. Wir, wir sind an der Stelle eigentlich mehr mit uns beschäftigt, keine, keine Fehler zu machen und compliant zu sein, und wenn wir es irgendwann oder irgendjemand in der in der Branche nicht sein kann oder will, dann muss es auf jeden Fall in jeder Richtung sehr gut erklären können, wobei, das ist jetzt gar nicht so spezifisch für Banken. Aber bei uns ist es eben ein Thema, weil die die Bankenbranche insgesamt, die lebt natürlich auch stark von der Reputation. Ansonsten sind die, die Banken, relativ einfach austauschbar untereinander. Wir sind kein Rohstofflieferant, auf denen eine nicht verzichten kann. Also, wir sind erheblich leichter zu substituieren als Lieferanten für seltene Erden. #00:22:14#

I: Okay, habt ihr denn genau eben was so diese regulatorischen Anforderungen, die immer mehr dazukommen, habt ihr denn irgendwie eine Software zum Beispiel, die dazu dient, um das Ganze einzufangen, um das irgendwie ja zu tracken. Dass vielleicht sich irgendwelche Bereiche erklären müssen, dass sie eben compliant handeln oder eben gesetzlichen Anforderungen oder auch interne Kontrollen dokumentieren können? #00:22:57#

B: Also da mit absoluter Sicherheit also dieses IKS, also interne Kontrollsystem, das gibt es, und zwar sowohl auf der nationalen, also deutschen Ebene als auch im Konzern, also das ist also das alles, was da gemacht werden muss und gemacht wird, das ist so weit als möglich Software unterstützt. Und das geht weit über Excel hinaus. #00:23:24#

I: Auf welche Weise könnte denn die Zusammenarbeit oder ebenso Kooperationsmechanismen integriert werden zwischen den Schnittstellen Risikomanagement, Interne Revision, Compliance, um Mehrkosten und Redundanzen zu vermeiden? #00:24:13#

B: Also so wie bei den Prüfungsplänen empfiehlt sich auf jeden Fall, sich auszutauschen, um auch vom anderen zu wissen, was er eigentlich gerade tut. Ansonsten würde ich aber nicht mit, also nicht immer mit mit der vollen Begeisterung Redundanzen und Mehrkosten vermeiden wollen, weil das kann durchaus gut investiert sein, wenn ich, eben weil die Bereiche sind ja nicht ohne Grund voneinander getrennt, also die, die Cas und Compliance und Risk, die haben ja alle alleinstehend ihre Berechtigung, und dieses auch gegenseitig oder redundant unter Inkaufnahme von Mehrkosten zu prüfen - das kann durchaus sinnvoll sein und sollte auch gewollt sein, aus unterschiedlichen Winkeln die gleiche Sache zu betrachten. #00:25:14#

I: Was stellen sie sich denn unter einem integrierten GRC-Ansatz vor? Wie könnte ein integrierter GRC-Ansatz aussehen? #00:25:56#

B: Also mit dem Ziel, aus einer letztendlich Organisationseinheit alle, alle Themen vollumfänglich abzudecken. Das, das wäre für mich der der integrierte Ansatz. #00:26:45#

I: Dann lese ich Ihnen mal die Definition vor, die in der Literatur zu finden ist. GRC ist ein integrierter, holistischer Ansatz einer unternehmensweiten Governance, Risk und Compliance, die dazu dient, sicherzustellen, dass eine Organisation ethisch korrekt und in Übereinstimmung mit ihrer Risikoneigung, internen Richtlinien und externe Anforderung agiert. Durch eine Abstimmung von Strategie, Prozessen, Technologie und Personal, Strukturen werden Effektivität und Effizienz verbessert. Also dass man halt eben sich anguckt, okay, wir sind eine Schnittstelle. Was habt ihr für Prozesse, was haben wir für Prozesse? Wie kann man sich halt gegenseitig irgendwo unterstützen, wo es halt eben Sinn macht, wenn man halt ja einfach gleiche Themen hat, genauso wie vielleicht, dass man eben auch so ein GRC Reporting ect. macht? #00:28:00#

B: Das ist perfekt ausformuliert, das, was ich gemeint habe. Alle, alle drei oder alle drei sitzen in einem Raum. Jeder schreibt auf Sideboard, was er haben muss, und dann wird abgeglichen, was die anderen dazu liefern können und wo es vielleicht Limitierungen gibt, und im Endergebnis werden alle Anforderungen erfüllt. #00:28:29#

I: Verfolgt die ING Bank einen integrierten GRC-Ansatz? #00:28:58#

B: Also genau das an sich ist, ist eigentlich und natürlich auch in Klammern ist, ist wichtig, weil bei uns arbeiten die Org-Einheiten schon zusammen, aber eben nicht als eine Org-Einheiten. Aber vorhin bin ich am Rand ja drauf zu sprechen gekommen, so wie Compliance und Risk, also integrated compliance, integrated risk und was dann da alles drunter fällt. Die sitzen nebeneinander unterm gleichen Vorstand. Also faktisch geht's schon in Richtung eines integrierten GRC-Ansatzes, aber in der Organisation ist es so nicht abgebildet. #00:29:44#

I: Welche potenziellen Vorteile könnten sie sich denn vorstellen, die sich ergeben könnte, wenn man eine integrierte GRC-Strategie definiert, dass jeder im Unternehmen weiß, ah, Okay, die arbeiten zusammen, wir haben eine GRC-Strategie. Würde das Sinn machen in ihren Augen? #00:30:21#

B: Ja, das sind eigentlich die die letzten Begriffe aus deiner Definition, die du gerade gezeigt hattest. Das wäre die die Steigerung oder Maximierung der Effektivität und der Effizienz. Also das auf jeden Fall mit weniger Leuten am Ende des Tages sogar noch mehr erreichen. Durch Vermeidung von Redundanzen. Das wäre der Idealtypus. Allerdings sehe ich da wieder Risiken, aber gut, das ist nicht die Frage, ne? #00:31:00#

I: Welche Risiken könnten sich denn dadurch ergeben? #00:31:05#

B: Ja, nämlich dass bei einer Gruppe, wie hast du es gesagt, holistischer Ansatz integriert, also alle, alle zusammen die individuelle Expertise nicht mehr so zum Tragen kommen wie in einer aufgeteilten Organisation. Die Formel getrennt, aber letztendlich natürlich auf Zusammenarbeit angewiesen, auch zusammenarbeitet. Und die, die Komplexität, die Abstimmungen sind, oder die Komplexität, ist natürlich auch um einiges größer. Wenn ich, wenn ich eine Org-Einheit aufsetze, die sehr unterschiedliche Themen bearbeiten soll, kann, kann gut funktionieren, wie eben in deiner Definition, mit Effizienz und Effektivität, aber dass das Risiko in Kurzform ist, möglicherweise untergehende individuelle Kompetenzen und Reibungsverluste. Und dass Konkurrenzen entstehen, die ich an der Stelle definitiv nicht brauche. #00:32:37#

I: Welche technologischen Lösungen und Tools könnten denn in Betracht gezogen werden, um einen integrierten GRC- Ansatz in Banken zu unterstützen? #00:32:55#

B: Ja, also, egal welcher technologische Ansatz, er muss auf jeden Fall transparent für alle sein. Und wie es immer so ist bei technologischen Lösungen und Tools, er muss von der ersten Sekunde an Rund um die Uhr gepflegt sein. Ansonsten ist mir der technologische Ansatz oder die technologische Lösung ist mir schon fast egal. Weil, wenn eine Woche keine reinschaut,

also Transparenz, auch aktiv reinschauen und natürlich auch Informationen wirklich transparent zur Verfügung stellen. Und das andere ist ohne akribische Datenpflege, egal in welchem Bereich, ohne die funktioniert keine technologische Lösung. #00:33:56#

I: Ja, das stimmt, da muss man auf jeden Fall dahinter sein, und es pflegen. Genau das war's tatsächlich schon. Vielen Dank für die Beantwortung der Fragen. Ich würde jetzt mit der Aufzeichnung einmal stoppen. #00:34:19#

Interview mit Klaus Abel

B: Genau, ich bin einverstanden mit der Aufzeichnung. Falls sie das irgendwo dokumentiert brauchen. #00:00:06#

I: Bitte stellen sie sich kurz vor und erläutern sie ihre Aufgaben bei der Deutsche Bank AG. #00:00:24#

B: Ja, sehr gerne, also mein Name ist Klaus Abel. Ich bin seit 24 Jahren bei der Deutschen Bank vornehmlich im Kreditgeschäft tätig, dort im Risikomanagement - Kreditrisikomanagement. Ich habe damals als Trainee angefangen. Dann habe ich schwerpunktmäßig Problemkreditbetreuung erst für Großkunden gemacht und bin dann vor ungefähr 20 Jahren auf das Retail Segment gewechselt. Dort habe ich Betreuung gemacht und hatte dann die Chance in die Zentrale zu gehen und mich dort schwerpunktmäßig mit Regulatoren Themen im Kreditgeschäft und mit Aufsichtsrechtlichen Themen zu befassen. Das ist im wesentlichen Regulatorik. Das habe ich dann auch sehr lange in Frankfurt gemacht nämlich von 2007 bis 2023. Ich hatte dann zwischendrin mal eine Stage im Regulatory Management im direkten Kontakt mit der europäischen Zentralbank für ungefähr anderthalb Jahre. Ich bin dann aber wieder ins Kreditgeschäft zurückgekehrt und war da wieder Workout-Management. Der Anfang war Workout-Management, dann kam Regulatorik allgemein, dann kam Regulatory Management mit der EZB als Kontaktperson zu Kreditrisikomanagement. Und dann kam die Rückkehr als Teamleiter und das ist die Stelle, die ich heute begleite im Workout-Bereich aus Risk Sicht. Ich bin vor allem für das Technisieren von Regelwerken, für die Kommunikation mit Wirtschaftsprüfern und für Kreditentscheidungen zuständig. Die müssen eine bestimmte Qualität haben, weil wir in der Deutschen Bank den Ansatz gewählt haben, dass Teile unseres Kunden Workout-Managements, also das Relationship-Management, die sind in der sogenannten first-line-of-defence. Das heißt die sind in einem anderen Bereich angeordnet. Wohingegen bestimmte Funktionen die auch regulatorisch Charakter haben, im

Risikomanagement angesiedelt sind. Man hat das irgendwann geteilt, um personell ein cut zu machen. Wir arbeiten da sehr eng mit den Kollegen zusammen. Die Kollegen sind auch gut qualifiziert. Die sind nicht im Risikomanagement tätig, sondern im Operations-Bereich. Wir sind dann sozusagen die Sparringspartner für die. Wir reden nicht mit den Kunden aber wir kriegen dann auch Kreditanträge und wir sind für die gesamten Governance, Kreditentscheidung und Regulatorik zuständig und da bin ich der Teamleiter dafür. Mein Team sitzt in Hamburg. Das kurz zu meiner Person: Ausbildung, Banklehre gemacht und dann Jura studiert auch zwei Examina gemacht und bestanden und dann als Trainee wieder zur Bank zurückgehrt. #00:03:36#

I: Wenn sie sich jetzt mal die Gegenwart anschauen und die aktuellen Entwicklungen in Bezug auf Governance, Risk und Compliance im Banksektor anschauen, was würden sie denn sagen? Was ist denn der derzeitige Stand aktuell im Banksektor im Jahr 2023, vielleicht auch im Vergleich zum Jahr 2007, 2008? Was hat sich da im Vergleich verändert? #00:05:15#

B: Bedingt durch die Bankenkrise hat sich natürlich dramatisch bei den Banken auch die Auffassung verändert es sind natürlich sehr viele Sachen festgestellt worden. Da gab es erheblichen regulatorischen Druck seitens des Gesetzgebers und seitens der Aufsichten. Das ist ja nicht nur hier die europäische Bank und die deutschen Aufsichten. Sondern das sind die internationalen Bankaufsichtsbehörden, die darauf gedrängt haben, dass sich bei den Banken dramatisch was verändert und verbessert. Und diese dramatische Veränderung die zeigt sich heute sehr deutlich. Das heißt, die Banken haben auch, weil sie es mussten, aber auch, weil sie es wollten, natürlich sehr viel gemacht, sehr viel neues eingeführt. Und wenn man das vergleicht mit der Situation vor der Bankenkrise 2007 ist das wirklich ein Verhaltenswechsel. #00:06:13#

I: Und welche Bedeutungen haben regulatorische Anforderungen für die Deutsche Bank? Wie wird sichergestellt, dass gesetzliche Vorschriften eingehalten werden? #00:06:27#

B: Extrem hohe Bedeutung! Die Deutsche Bank ist bekanntermaßen das größte deutsche Kredit Institut und damit natürlich auch im Fokus der europäischen Zentralbank. Sie ist natürlich auch im Fokus der FED und der Wertpapieraufsicht in den USA. Wir sind ja in den USA an der Börse gelistet und müssen deswegen auch die amerikanischen Vorgaben einhalten, was zum Beispiel auch Kontrollen und Governance betrifft. Unabhängig davon, ob wir jetzt in Deutschland sitzen und deutsches Geschäft machen, müssen wir zum Beispiel die sogenannten SOX-Vorschriften, das ist Sarbanes-Oxley Act einhalten und müssen das auch in Deutschland praktizieren. Das

müssen wir machen, um festzuhalten, ob Kontrollen durchgeführt werden. Die Kontrollen müssen wir auch immer wieder prüfen und testen und das wiederholt sich jedes Jahr. Das ist eine sehr aufwendige Geschichte. Anders ausgedrückt, es hat eine extrem hohe Bedeutung. Die Aufsichtsbehörden sowie die Wirtschaftsprüfer, derzeit bei uns EY, überwachen dies äußerst genau. Sie achten darauf, dass die Einhaltung gewährleistet wird – dies betrifft primär den Kreditbereich, aber auch andere Geschäftsbereiche und natürlich auch das Management. Das heißt, es werden hier intern auch immer wieder Schulungen, Pflichtschulungen durchgeführt, die man auch absolviert haben muss, und es wird natürlich auch drauf geguckt, dass man möglichst wenig Findings kriegt hinsichtlich regulatorischer Lücken, Governance Lücken, Kontrolllücken. Da reagiert man in Management mittlerweile sehr, sehr sensibel darauf. Es wird sofort aufgenommen, und man muss dann recht schnell, ideal ist wenn man keine Findings hat, aber wenn man welche haben sollte, sollte man recht schnell für Abhilfe sorgen. #00:08:13#

I: Okay, dann würde ich in diesem Zusammenhang zur Frage fünf springen. Wie gestaltet sich denn die Zusammenarbeit zwischen den internen Governance Organen, also Risikomanagement und interne Revision, Compliance, sowie den externen Governance Organ wie jetzt beispielsweise Wirtschaftsprüfern? Wie erfolgt da der Austausch, die Zusammenarbeit? #00:08:35#

B: Sehr eng und intensiv, natürlich auch vertrauensvoll, wobei man sagen muss, natürlich sind hier unterschiedliche Interessen und natürlich auch Neutralitätsaspekt zu betrachten. Wir können nicht erwarten, dass ein Wirtschaftsprüfer sich mit uns hier zusammensetzt und uns im Zweifel Rechtsrat erteilt. Das ist klar, dass muss man selber hinbekommen. Andererseits ist es natürlich ein enger Austausch, das heißt, wir kommunizieren, unsere Politik hier im Haus war schon immer „offen“. Und wenn die Auffassung des Wirtschaftsprüfers zumindest hinterfragbar ist, treten wir natürlich auch an und gehen in die Diskussion. Da findet dann ein offener Dialog statt. Und zum Schluss akzeptieren wir natürlich, wenn uns ein Wirtschaftsprüfer mit guten Argumenten sagt, dass er das anders sieht. Dann akzeptieren wir natürlich auch das Finding und sind dann auch schnell dabei, teilweise schon während der Prüfung. Es ist jetzt nicht so, dass die jedes Mal kommen und z.b. 35 Punkte nicht stimmen. Aber sie sind selber im Audit Bereich in der Revision tätig, die finden immer was. Wir freuen uns natürlich, wenn das dann richtig gewichtet wird. Es ist wichtig, dass man nicht, um es umgangssprachlich auszudrücken, aus einer Mücke einen Elefanten macht. Gleichzeitig ist es wichtig, dass uns klar erklärt wird, warum eine bestimmte Vorgehensweise gewünscht ist und uns dann ein Stück weit Guidance gibt. Natürlich nicht in der Art, dass wir später behaupten könnten: "Wir haben es genauso

gemacht, wie uns der Prüfer das gesagt hat." Das dürfen die auch nicht. Es ist wichtig das Feld ganz klar zu definieren damit wir wissen, wo wir uns bewegen müssen und um im Zweifelsfall Signale zu erhalten, ob wir auf dem richtigen Weg sind. Das sollte jedoch keinesfalls nach dem Motto geschehen: "Der Wirtschaftsprüfer hat gesagt, dass wir jetzt bei allen Kunden fünf Kontrollen durchführen müssen." Die Kontrollen werden nicht einfach von ihm vorgegeben; stattdessen legt er fest, welche Kontrollen bei den Kunden notwendig sind. Das ist unsere Verpflichtung und Verantwortung das in der Praxis mit Leben befüllt, die dürfen sich nicht ins laufende Tagesgeschäft einmischen. Jedoch freuen wir uns über klare Anweisungen und einen offenen Dialog. Wir sehen Revisionsprüfungen und auch externe Prüfungen als Chance.

Natürlich wehren wir uns im Zweifel, wenn wir merken es ist juristisch nicht haltbar, was der sagt. Dann führen wir konstruktive Gespräche, und bisher haben wir immer Lösungen gefunden. Die Wirtschaftsprüfer zeigen sich auch offen für Argumente. Wenn sie sagen, es ist vertretbar, dann schreiben sie das auch so rein. Wir wollen aber auf der anderen Seite natürlich auch Dinge annehmen, weil die klare Auffassung unseres Hauses ist: Wirtschaftsprüfer sollen nicht mit dem goldenen Ring durch die Arena geführt werden, sondern die sollen uns auch ein Stück weit sagen, wo wir besser werden können. Das ist etwas, was wir sehr ernst nehmen. Gleichzeitig treten wir natürlich auch an, um unseren Ansatz Argumentativ zu begründen und auch zu verteidigen. Bisher hat sich in solchen Fällen, auch während unserer langjährigen Zusammenarbeit mit KPMG, stets ein äußerst konstruktiver Dialog entwickelt. Es war sehr erfreulich zu sehen, wie wir voneinander lernen konnten. Ich habe auch persönlich eine Lernkurve bei Prüfern beobachtet, die teilweise als Junior begonnen haben. Es gab Momente, wo man ihnen die Basics erklären musste. Beeindruckend war jedoch zu beobachten, wie sie mit der Zeit das Wirtschaftsprüfungs-Examen bestanden haben und wie sich dadurch auch die Qualität der gestellten Fragen verändert hat. Diese Entwicklung hat uns besonders Freude bereitet. Wir sagen auch gerne Dinge, die banal sind. Doch wenn ein Wirtschaftsprüfer genau den Punkt anspricht, bei dem wir möglicherweise Anregungen benötigen und eine Diskussion notwendig ist – wenn man sagen kann, dass es eine andere Perspektive gibt – dann betrachten wir das als Bereicherung. Wir nehmen die Findings natürlich ernst, auch wenn sie nicht immer Jubelstürme auslösen. Aber es ist auch sehr oft so, dass man auch Anregungen bekommt, noch mal in sich zu gehen, und das zum Schluss Schaden abgewandt wird für die Aktionäre und dass wir nachher bei der europäischen Zentralbank als unseren Haupt Regulator dann auch mit einer guten Story antreten können. Also für uns ist es natürlich manchmal auch eine Herausforderung, denen das zu erklären, warum sie vielleicht nicht Recht haben. Auf der anderen Seite nehmen wir gerne Argumente auf, wichtigen Argumente, und ich schätze den konstruktiven Dialog mit

den Wirtschaftsprüfern. Weil da kriegen sie von außen, von Menschen, die nicht in dieser Mühle sind. Kriegen sie manchmal wertvolle Hinweise, neue Blickwinkel und auch manchmal Kritik, aber Kritik muss man dann konstruktiv nehmen. #00:13:30#

I: Genau, das ist natürlich auch für mich als Revisoren immer schön zu hören, weil wir auch bei uns im Unternehmen immer sagen, dass man das eigentlich eher als Chance sehen sollte. #00:14:09#

B: Das ist ein Punkt, den man unbedingt berücksichtigen muss. Im Gesetz steht viel, und natürlich könnte man argumentieren: "Gib mir einfach 100 Millionen mehr, dann kann ich noch 20 weitere Mitarbeiter einstellen, die alles erledigen." Es ist jedoch oft die Herausforderung, mit den vorhandenen Ressourcen und Systemen zurechtzukommen. Es wäre leicht zu sagen: "Kauft ein neues System, das wird alles verbessern." Aber das ist nicht immer möglich und man kann auch nicht einfach dem Vorstand sagen: „investiere eine Milliarde in das Privatkundengeschäft, dann wird auch alles gut“. Dann wird der Vorstand sagen: „vielen Dank für den wichtigen Hinweis.“ Man muss also häufig abwägen, welche Möglichkeiten die internen Systeme der Bank hergeben und wie man dennoch den Vorgaben entsprechen kann. Es erfordert auch ein gewisses Maß an Pragmatismus, denn besonders im Retail Geschäft müssen viele Dinge standardisiert werden. Wenn man im Retail Geschäft ankommt und sagt: "Ich werde hier individuelle Bearbeitung und Analysen für jeden Fall durchführen", dann macht das Geschäft keinen Sinn mehr. Hier ist es notwendig, eine Vielzahl von Fällen zu standardisieren und kluge standardisierte Entscheidungen zu treffen. Das ist auch manchmal das, was den Prüfer passiert, die individuelle Betreuung aus dem Großkundengeschäft auf Retail ansetzten. Dann wundern sie sich darüber, dass wir gewisse Dinge standardisiert und vereinfacht haben. Dennoch können wir nachweisen, dass es konform mit den Risikostandards ist. Dies ist die Aufgabe des Risikomanagements: aufzuzeigen, dass wir trotz einer gewissen standardisierten und automatisierten Bearbeitung die Risiken im Griff haben. #00:15:53#

I: Wie würden sie denn generell die Rolle von Governance, Risk und Compliance in der Deutsche Bank AG beschreiben? #00:16:08#

B: Ja, es sind unterschiedliche Bereiche. Wir haben ja einen großen Chief Administration Office, das unter der Leitung von Herrn Professor Dr. Simon ist. Er verantwortet federführend als versierter Jurist diese Bereiche unter einem Dach. Da ist Legal mit Governance und Compliance zusammen wohingegen der Risikobereich einen eigenen Vorstand hat, weil es dort nämlich auch um konkrete Risiken geht und deren Management. Und es ist aber so, dass es ein

miteinander ist, nämlich auch ein wechselseitiger Austausch von Kow-How und ein Zuliefern. Wir sind natürlich für die konkreten Risiken zuständig im Risikomanagement. Ich kann mich nicht hinstellen und behaupten, dass Governance schuld ist, wenn es zu Problemen bei zahlreichen Krediten kommt, weil ich die Vorgaben nachlässig oder zu tolerant definiert und interpretiert habe. Aber der Anstoß für zum Beispiel neue Vorschrift kommt natürlich aus dem Compliance Bereich, da wir stets darüber informiert sein müssen, welche Veränderungen sich ergeben haben. Es gibt Konsultationen zum Beispiel für neue Vorgaben. Auch bezüglich der Umsetzungen und bis zu welchem Zeitpunkt die Umsetzung erfolgen muss. Beispiel dafür ist die Definition of Default, die neue Ausfall Definition. Der Anstoß zu neuer Regel kommt von Compliance. Compliance informiert uns mittels eines stark institutionalisierten und systematischen Verfahrens über neu erlassene Vorschriften. Anschließend greifen wir den Ball auf, der uns zugeworfen wird, und sind verpflichtet, die Umsetzung aus Risiko Sicht anzugeben. Wir sind sozusagen auch die Praktiker und die Risikomanager an sich. Aber die Vorgaben, die wir erfüllen müssen, die kriegen wir, wenn sich da was tut, dann über die Compliance schiene mitgeteilt und wir müssen dann sozusagen den Ball aufnehmen und in unsere Prozesse umsetzen. #00:18:16#

I: Und wie erfolgt dann die Meldung wieder zurück zu Compliance? Also gibt es einen regelmäßigen Jour-Fix, wo ihr bestätigen bzw. erläutern müsst, wie die Umsetzung erfolgt ist? Oder wie erfolgt die Kommunikation genau? #00:18:41#

B: Ich muss da leider gestehen, dass ich mit Compliance da weniger zu tun habe, sondern wir haben da noch mal Abteilungen installiert in Risk, die von Compliance den Ball sozusagen zugespielt bekommen, das dann aufbereiten und die dann aber uns auch challengen und erst mal informieren und dann mit uns auch die Umsetzung angeht. Wir müssen denen dann zeigen, wie und was wir bis wann umsetzen wollen oder umgesetzt haben. Das wird also dann den Risk dann nochmal intern aufgenommen. Das wir natürlich auch Compliance zurückspielen: „Wir wissen, dass es sich um eine Vorschrift handelt, die uns betrifft und wir werden da auch die Umsetzung prüfen. Wir werden eine Analyse machen, wir werden dann auch die Lücken schließen, sofern vorhanden, und wir werden das an die entsprechenden Bereiche tragen.“ Es gibt Kreditrisiken sowohl für die Corporate Bank als auch für die Privatbank. Diese Risiken existieren in verschiedenen Ländern wie Italien, Spanien und anderen, da wir global tätig sind. Die jeweiligen Abteilungen müssen dann ihre Ergebnisse, wie sie die neuen Vorschriften umgesetzt haben, entsprechend zurückspielen. Das heißt, die können das nicht zur Kenntnis nehmen und sagen, schön, wir dürfen ab sofort das und das nicht mehr machen, wir lassen jetzt

einfach mal liegen und hoffen, dass keiner vorbeikommen. Genau das wurde durch diesen neuen Prozess erreicht. Er wurde mehr oder weniger nach der Bankenkrise institutionalisiert. Dadurch können wir nun aus verschiedenen Quellen Informationen beziehen, insbesondere natürlich von den Aufsichtsbehörden, aber auch von Gesetzes-Homepages oder dem Bundesgesetzblatt. Wenn sie sich Regelungen und BGB ändern, müssen wir ja auch in Zweifel die Verträge umstellen. Aber aus Quellen, die zugänglich sind, wird es dann erst mal vorsortiert, vorgeprüft. Am Anfang war es ein bisschen holprig, weil da haben sie natürlich erst mal überall noch dem Wort Kredit und Risk gesucht und haben dann Kredit-Risk daraus gemacht. Da musste man dann auch sehr vieles prüfen und dann als nicht relevant einstufen. Aber auch das ist wichtig. Mir ist lieber, ich kriege eine Regel zu viel als eine zu wenig, und da hat sich aber jetzt auch der Dialog entwickelt. Das heißt, die kriegen jetzt auch ein bisschen mehr Know-How in Compliance, dass wir wissen, was interessiert uns eigentlich, und dass wir uns dann auch speziell darauf hinweisen. Wir greifen die Aufgabe auf und analysieren die neuen Regelwerke oder nehmen an Konsultationen teil. In solchen Fällen können wir auch immer in Kontakt mit Bankenverbänden treten. Dann geben wir den Ball zurück, indem wir präsentieren, wie wir die erhaltenen Informationen umgesetzt haben. Das ist ein ganz wesentliches Feld, das wir mit Compliance beackern. Neue Vorschriften rechtzeitig erkennen - wir haben ja auch Vorlaufzeiten, die müssen wir einhalten. Wir können nicht einfach sagen: "Das ist ja schon seit einem halben Jahr in Kraft, ganz toll!". Wenn die Umsetzung nicht sofort erfolgt, erhalten wir möglicherweise ein Finding und die Revision frohlockt auch, weil sie sagt, da habt ihr mal wieder geschlafen. Obwohl so etwas eigentlich nicht passiert. Dennoch müssen wir sicherstellen, dass wir rechtzeitig unsere Prozesse und Arbeitsabläufe an das neue Recht anpassen. Hierbei stehen wir im Austausch mit der Compliance, aber natürlich auch mit Legal und den Praktikern aus dem Marktseite. Wir müssen es letztendlich in die Praxis umsetzen. Das ist dann sozusagen eine ganzheitliche Betrachtungsweise. Der Impuls dazu kommt jedoch von der Compliance. Sie informieren uns beispielsweise darüber, dass sich die Vorschriften zur Eigenkapitalregulierung ändern, was für viele Banken sozusagen das Grundgesetz ist. Hierbei sind viele Aspekte direkt auf uns zugeschnitten. Ein weiteres Beispiel ist die neue MaRisk, welche unser alltägliches Handwerkszeug darstellt. In diesen Situationen machen wir uns Gedanken darüber, wie wir diese Vorgaben in unsere Prozesse übersetzen können, sodass die Personen, die später damit arbeiten müssen, es auch verstehen. Wir können nicht einfach die MaRisk kopieren und einfügen, da wir dann genauso gut das Gesetzesbuch überreichen könnten, in dem alles steht. Unsere Aufgabe ist es, die Übersetzung für die Praktiker zu liefern, die nicht alle Regulierungsexpertinnen und -experten sind. Von der Compliance-Ebene erhalten

wir dann quasi auf übergeordneter Ebene den Hinweis: "Hier gibt es etwas, mit dem ihr euch befassen müsst." #00:23:22#

I: Gibt es bei in der Deutsche Bank technologische Tools oder eine Software, mit der alle gesetzlichen Vorgaben erfasst werden können und anschließend alle Bereiche dort zurückmelden können, dass sie hiermit bestätigen, dass sie diese gesetzlichen Vorgaben umgesetzt haben bzw. in die Prozesse implementiert haben? #00:23:57#

B: Es ist schon automatisiert. Jedoch kann ich Ihnen nicht mit Sicherheit sagen, ob es sich dabei um ein normales Excel-Dokument handelt oder ob es ein eigenes Tool ist. Aber da bitte ich um Verständnis. Da bin ich leider nicht nah genug dran. Ich erhalte von unserer Fachabteilung eine umfassende Präsentation in Form einer ansprechenden PowerPoint, in der jede Regel zusammen mit einer kurzen Analyse aufgeführt wird. Dabei werden dann die verantwortlichen Personen zu benannt, die sich um die Umsetzung kümmern müssen. Diese Personen füllen dann entsprechende PowerPoint Templates aus, um darzulegen was wir getan haben oder noch tun wollen. Es gibt ein Tool, mit der die neuen Vorschriften erfasst werden und an uns weitergeleitet werden, und dann kommen die Bereiche ins Spiel, die das sozusagen dann für die einzelnen Risikoabteilungen aufnehmen. Das hilft mir auch nichts, wenn ich jetzt über Operation Risk 15 Vorschriften kriege. Da sag ich: „schön; toll! Ich habe mich weitergebildet aber betrifft mich nicht!“. Mein Vorgesetzter leitet das bereits ein, datiert es und entfernt es aus dem System – es ist also auch systembasiert. Das ist hier nicht nach dem Motto: ich schicke einmal allen eine Mail wo drinsteht: „hey passt mal auf - ich habe da gestern was gelesen.“ Es wird systematisch erfasst und systematisch weitergeleitet. Und wie das genau geht, da bin ich leider nicht direkt an der Quelle. #00:25:33#

I: Wie erfolgt denn die generelle Zusammenarbeit mit den Schnittstellen Compliance, Interne Revision? Wie erfolgt der regelmäßige Austausch? Habt ihr eventuell ein regelmäßiger Jour-Fix, wo sich gegenseitig upgedated wird? Wer arbeitet an was genau gerade oder in welchem Format erfolgt denn dieser regelmäßige Austausch? Oder ruft man da bei Bedarf einfach mal an? #00:26:06#

B: Also, auf Managementebene ist das sicherlich ein regelmäßiger Austausch in Exkurs in diesen Gremien, wo natürlich auch der Head of Compliance mit drinsitzt. Auf Arbeitsebene, zu der ich mich jetzt mal erzählen möchte, ist es jetzt nicht so, dass wir alle vier Wochen mit denen reden, sondern wir sind dann im Gespräch, wenn die eine Prüfungsplanungen mit uns machen, das heißt, die kommen irgendwann auf uns zu und sagen wir wollen eueren Bereich prüfen.

Wann passt's? Natürlich passt es einem nie. Das muss man ja dann zeitlich ermöglichen. Genauso ist es auch mit den Wirtschaftsprüfern. Da hat man natürlich auch regelmäßige Meetings, aber da bin nicht ich dabei. Wenn ich kein Thema habe, setze ich mich nicht mit EY zusammen und reden über Gott und die Welt. Das machen dann die Bereiche, die halt die Prüfungskoordination machen. So ist es auch mit Group Audit. Die haben dort mit denen regelmäßig ein Austausch auch über die Planung. Wir kommen dann, ich nehme jetzt mal das Problem Kredit Betreuungssegment. Wir kommen dann ins Spiel, wenn wir auch wirklich Themen haben, das heißt Prüfungsplanung, Prüfungsdurchführung und dann natürlich, falls vorhanden, Finding und auch Finding Schließung. Und der Finding Schließungsprozess folgt dann auch wieder einem toolbasierten, sehr, sehr strukturierten Prozess. Das bedeutet, dass wir verschiedene Aspekte berücksichtigen müssen. Zuerst müssen wir eine Lösung finden, das hat erstmal Priorität. Anschließend ist es notwendig, diese Lösung dem entsprechenden Management vorzustellen, sie dort zur Genehmigung vorzulegen und bei einer bestimmten Schwere des Problems auch die Zustimmung von Group Audit einzuholen. Wenn wir ein schwerwiegendes Finding hätten mit einer hohen Variety, dann haben wir natürlich auch die Pflicht, vor der Schließung auch noch einmal Rücksprache mit Group Audit zu halten, um sicherzustellen, ob die die Schließung auch mittragen. Dies gilt sowohl intern als auch extern. Wir informieren die Wirtschaftsführung über unsere Vorgehensweise. Falls diese nicht richtig wäre, würden sie uns darauf hinweisen, dass es nicht ihren Vorstellungen entspricht. Sie greifen jedoch nicht so detailliert in die Angelegenheit ein. Die mischen sich natürlich nicht so im Detail ein. Was sie jedoch regelmäßig tun, ist, wenn wir im vorherigen oder im aktuellen Bericht eine Feststellung hatten, dann überprüfen sie im nächsten Jahr erneut, ob die empfohlene Maßnahme umgesetzt wurde. Sie sehen sich die Fälle an und möchten verstehen, wie wir diese in der Praxis konkret umsetzen. Man kann vieles in einen Prozess reinschreiben, wichtig ist, dass es auch von den Beteiligten befolgt wird. Wie bereits erwähnt, hat es in der operativen Praxis keine Wirkung, wenn nicht alle sich daranhalten. Es ist wenig nützlich, beeindruckende Regelwerke mit dem Markenzeichen der Deutschen Bank in Umlauf zu bringen, wenn sie von niemandem beachtet werden oder wenn keiner über die Neuerungen informiert ist. Daher ist es meine Aufgabe, die Mitarbeiter zu informieren und sie gegebenenfalls zu schulen, sobald es neue Entwicklungen gibt – sei es, um Fehler zu korrigieren oder um neue Vorschriften einzuführen. Die Angestellten müssen wissen, was sie tun müssen. Besonders im Retail ist es von großer Bedeutung, klare Anweisungen zu geben, wie standardisierte Verfahren durchgeführt werden sollten. Es geht darum zu erklären, wo und wie sie auf die Systeme zugreifen müssen, um sicherzustellen, dass die gleichen Abläufe befolgt werden. Wir müssen

äußerst präzise Prozesse entwerfen, die auch von Personen umgesetzt werden können, die nicht unbedingt BWL studiert haben, sondern vielleicht eher einen kaufmännischen oder anlernenden Hintergrund haben. Dies ist notwendig, um sicherzustellen, dass sie die Vorgaben wirklich umsetzen können. #00:29:51#

I: Welche spezifischen Herausforderungen und Risiken stellen sich jetzt denn für Banken in Bezug auf Governance, Risk und Compliance da? #00:30:03#

B: Das ist die künstliche Intelligenz, weil das wird kommen. Ich bin zwar kein Experte auf diesem Gebiet, sondern spreche hier allgemein, aber Künstliche Intelligenz ist ein Thema, über das sich auch Banken Gedanken machen müssen, wie sie es effektiv einsetzen können. Seit Freitag gibt es eine neue Veröffentlichung der EBA, die äußerst aufschlussreich ist. In dieser Veröffentlichung wurde eine Umfrage durchgeführt, um herauszufinden, wie Künstliche Intelligenz verwendet wird. Künstliche Intelligenz stellt eine Herausforderung dar, da sie dazu dient, Prozesse zu vereinfachen. Sie ist oft schneller und fehlerfrei, und sie kann viele Aufgaben übernehmen, die bisher von Menschen erledigt wurden – das ist uns allen bekannt. Das ist jedoch nur ein Aspekt. Man kann ja viel programmieren, aber das andere ist dann, und das spielt genau in die Governance rein. Wie können sie das dann so überwachen, und wie können sie die menschliche Intervention sicherstellen? Vor allem müssen Sie verstehen, was Künstliche Intelligenz bewirkt. Wenn Sie sich darauf verlassen, dass die KI-Entscheidungen allein trifft, basierend auf Black-Box denken, verlieren Sie die Kontrolle. Wenn Sie nicht verstehen, wie die KI ständig dazulernt und welche Prozesse sie genau ausführt, werden die Aufsichtsbehörden wahrscheinlich sofort einschreiten. Ihr könnt hier nicht loslegen und nicht den Algorithmus von irgendeiner ähnlichen Firma machen lassen, die bei euch gar nicht wegen des Copyrights sagt, was sie da programmiert hat. KI bietet enorme Chancen, da sie schnell und effizient einfache Abläufe bewältigen kann, was letztlich Kosten spart. Auf der anderen Seite muss man die Kontrolle behalten, die Algorithmen verstehen können, in der Lage sein, einzugreifen und ausreichend Personal haben, um die KI gegebenenfalls zu überstimmen und vor allem zu überwachen. Es nützt mir nichts, wenn Sie sagen: "Ja, sie treffen für mich diese wunderschönen Entscheidungen", und später stürzt meine Portfolioperformance ab. Das könnte sowohl das Management als auch mich betreffen. Denn ich habe Vertrauen in dieses System, ohne zu wissen, was diese Algorithmen eigentlich tun. Wenn Sie so etwas umsetzen möchten, müssen Sie auch die Anforderungen der EZB berücksichtigen. In diesem Fall kann ich Ihnen wirklich keine weiteren Informationen geben ob und wie die Deutsche Bank das plant, das ist einfach meine persönliche Auffassung, und ich glaube, dass es die KI gibt. Es gibt zweifellos

Bestrebungen in diese Richtung, das ist mir bewusst. Die Künstliche Intelligenz wird jedoch unausweichlich kommen, und dann wird es unvermeidlich sein. Die Chance liegt in der Vereinfachung von einfachen Aufgaben oder solchen, die schnell erlernt werden können. Die KI übernimmt diese Tätigkeiten, während der menschliche Faktor nach wie vor vonnöten ist. Allerdings wird ein noch höheres Maß an Expertenwissen erforderlich sein. Man muss sich in der IT auskennen und vor allem verstehen, wie der Algorithmus funktioniert. Zudem ist es unerlässlich, ein Verständnis für das Kreditgeschäft zu haben. Wenn der Algorithmus Entscheidungen trifft, die gegen jede logische Kreditvergabe-Strategie verstoßen, dann können sie das nicht die KI machen lassen. Governance kommt dann ins Spiel, das ist nachher das, was die Menschen machen müssen. Ich kann die Governance nicht auch noch von der KI erledigen lassen, da wäre ich außen vor. Das wäre, als würde ein autonom fahrendes Auto gegen die Wand fahren, während ich darin sitze – in diesem Fall sicherlich nicht fröhlich, sondern eher gestikulierend. Die Governance wird vor diesem Hintergrund noch bedeutend wichtiger werden, als sie es ohnehin schon ist. Sie ist der Schlüssel dazu. Denn wenn man Algorithmen einsetzt, muss man in der Lage sein, immer noch zu wissen, was sie tun. Man muss sie stoppen, anpassen und stets den Überblick darüber behalten können, was gerade geschieht. Das wird dann zur Herausforderung für die Governance. In den kommenden Jahren, bis zum Ende des Jahrzehnts, werden wir wahrscheinlich eine Revolution erleben, nicht nur in Banken, sondern auch in anderen Bereichen. Wir müssen dann schlussendlich der Aufsicht erklären können, warum wir so viele Kreditausfällen haben. Wenn wir einfach sagen, dass hat die geniale elektronische KI entschieden und wir haben es aber auch nicht verstanden, aber wir haben die KI es dennoch machen lassen. Wenn wir so antreten, dann wird der Laden geschlossen. Dann wird die andere KI in der EZB sagen, ihr habt sie doch nicht mehr alle. #00:34:37#

I: Dann würde ich mal direkt zur achten Frage kommen. Wie würden sie denn einen integrierten GRC - Ansatz definieren? #00:35:01#

B: Es muss so ablaufen wie eigentlich ein perfektes Getriebe. Die Zahlenräder müssen ineinandergreifen greifen. Die Tätigkeiten, die einfach Compliance nicht leisten kann, müssen von uns übernommen werden. Wir müssen hier Hand in Hand arbeiten. Von Compliance müssen die Anstöße kommen hinsichtlich des gesamten Rahmenwerks, gesetzliche Vorgaben und von uns muss dann die Ausarbeitung kommen. Wir können das nicht Compliance überlassen, weil da sind die auch nicht dafür ausgebildet. Ich kann einen Compliance-Experten haben, der mir eine Menge Vorschriften detailliert und umfassend erklären kann. Aber am Ende kann ich ihn nicht das Kreditgeschäft für mich erledigen lassen. Hier komme ich ins Spiel. Ich

muss die Vorschriften so interpretieren können, dass sie zu meinem Handlungsfeld passen und ich sie einhalten kann. Gleichzeitig muss ich sicherstellen, dass ich sie so umsetze, dass es letztendlich profitabel ist – schließlich wollen wir mit Krediten Geld verdienen. Manchmal wird vergessen, dass wir das Kreditgeschäft nicht nur betreiben, dass sich Compliance- und Governance-Personal freuen oder den Wirtschaftsprüfern Arbeit zu verschaffen. Unser Endziel ist natürlich auch die Erwirtschaftung von Erträgen. Das kann jedoch nur funktionieren, wenn wir die Vorschriften korrekt anwenden und sie so nutzen, dass wir am Ende auch einen Mehrwert erzielen. Ein einheitlicher Ansatz im Bereich Compliance erfordert natürlich Verständnis für unsere spezifischen Bedürfnisse. Gleichzeitig müssen wir für Compliance ebenfalls Verständnis aufbringen. Wir können die Vorgaben nicht einfach ignorieren, noch können wir sagen, dass unsere Mitarbeiter dazu nicht in der Lage sind und es daher auslassen. Ein solches Verhalten ist natürlich nicht akzeptabel. Dennoch können wir stets Lösungen erarbeiten, indem wir analysieren, was wir zur Verfügung haben, wie wir Anforderungen erfüllen können und dabei Kosten sparen, ohne sofort Milliarden investieren zu müssen – schließlich sind solche Summen nicht jedes Jahr verfügbar. Wir müssen mit den vorhandenen Ressourcen und dem vorhandenen Personal versuchen, unser Unternehmen stabil auf Kurs zu halten. Das ist zweifellos eine Herausforderung, ich kann auch sagen, dann stellen wir halt nochmal 20000 ITler ein, die machen uns das alles fein hier. In Bezug auf finanzielle Angelegenheiten und betriebswirtschaftliche Aspekte ist es nicht so einfach, die erforderlichen Ressourcen zu rekrutieren. Das Management mag sagen, Herr Abel, das ist eine großartige Idee, aber genau das ist der Knackpunkt. Wie können wir unsere Systeme optimieren, um die Vorgaben zu erfüllen? Wie können wir effiziente Abläufe erreichen? Dies wird letztendlich dazu führen, dass Erträge generiert werden, und das ist das treibende Element. Ein integrierter Ansatz, auch mit Group Audit, ist meiner Meinung nach unerlässlich. Natürlich müssen wir unabhängig sein, das ist klar. Aber letzten Endes werden auch die Einnahmen, die der Vertrieb generiert, dazu verwendet, sie zu finanzieren. Bisher habe ich noch nicht gehört, dass Group Audit Erträge erwirtschaftet hat. Diese Aussage treffe ich jedoch ohne abwertende Absichten gegenüber meinen Kollegen.Aber letztendlich müssen sie auch versuchen, lösungsorientiert vorzugehen. Wir müssen das Recht beachten und die Vorgaben der Aufsicht und die Findings der Prüfer ernstnehmen und schließen. Wir müssen auch stets berücksichtigen, ob es sich am Ende des Tages für uns lohnt. Wie können wir das so gestalten, dass die Prüfer zustimmen und gleichzeitig unsere Abläufe letztendlich zu einem positiven Deckungsbeitrag führen? Unser Ziel ist es, mit Krediten Geld zu verdienen. Wir wollen nicht unbedingt Immobilien über Zwangsverkäufe erwerben – das ist eigentlich nicht unser Bestreben. Vielmehr möchten wir

Kunden haben, die pünktlich ihre Raten zahlen, ohne Diskussionen, und in ein paar Jahren vielleicht ein weiteres Geschäft mit uns abschließen, ohne darüber nachdenken zu müssen, wie sie ihr Haus verkaufen können, weil das Geld nicht ausreicht. Diese Kunden sollen Zinsen und Tilgungen begleichen, und wir wollen nur noch Positives hören – dass alles reibungslos abgelaufen ist und dass sie nun auch Vermögensverwaltung mit uns betreiben möchten. Tatsächlich will eine Bank in Bezug auf Kredite eigentlich keine weiteren Probleme, sondern einfach, dass sie fließen und einen schönen Ertrag einbringen. #00:39:07#

I: Ich kann ihnen dazu gerne mal die Definition vorlesen, die ich in der Literatur gefunden habe: GRC ist ein integrierter, holistischer Ansatz einer unternehmensweiten Governance, Risk und Compliance, die dazu dient, sicher zu stellen, dass eine Organisation ethisch korrekt und in Übereinstimmung mit ihrer Risikoneigung, internen Richtlinien und externe Anforderungen agiert. Durch eine Abstimmung von Strategie, Prozessen, Technologie und Personal und Strukturen werden Effektivität und Effizienz verbessert. #00:40:17#

B: Genau, wir dürfen auch nicht versuchen, die Revision zu kopieren. Dies mag in einigen Fällen sinnvoll sein, vor allem wenn es hohe Ausfälle gibt. Jedoch sollte das nur punktuell geschehen, wenn es einen konkreten Bedarf gibt. Insbesondere dann, wenn man merkt, dass die im Vertrieb zu viel alleine machen, wenn man sie alleine lässt, was die große Sorge der Aufsicht ist. Obwohl unsere Vertriebsmitarbeiter erfahren und kompetent sind – schließlich sind sie qualifizierte Bankfachleute und keine unseriösen Drückerkolonnen – erhalten sie ihre Entlohnung auf Grundlage ihrer Abschlüsse, die sie machen. Natürlich besteht die Gefahr, dass bei dieser Art der Vergütung die Tendenz entsteht, Kredite anzubieten, auch wenn dies nicht immer angemessen ist. Daher müssen wir möglicherweise durch Stichprobenkontrollen überwachen, was sie produzieren. Dennoch können wir nicht einfach den Ansatz von Group Audit auf den Vertrieb übertragen, da die Aufgaben von Group Audit eine andere Schwerpunktsetzung haben. Stattdessen müssen wir eine engere Zusammenarbeit zwischen den Bereichen ermöglichen. Dies erfordert einen kontinuierlichen Austausch, gelegentliche Prüfungen und möglicherweise auch Schulungen für unsere Vertriebsmitarbeiter, um sicherzustellen, dass die Qualität der Kreditvergaben gewährleistet ist. Es ist stets von Vorteil, wenn jemand in der Revision tätig ist, der zuvor bereits praktische Erfahrung im Geschäftsbereich gesammelt hat und nicht nur rein theoretisch ausgebildet ist. Auf diese Weise könnt die auch ein besseres Gespür dafür bekommen, was die Leute bewegt, warum sie bestimmte Handlungen ausführen und wie ich ihnen mit konstruktiver Kritik helfen kann. Dabei ist es wichtig, Kritik so anzubringen, dass sie als Anregung für Verbesserungen

verstanden wird, anstatt einfach alles als falsch abzustempeln, ohne jedoch eine Lösung anzubieten. Denn es ist nicht hilfreich, lediglich darauf hinzuweisen, dass etwas nicht funktioniert, ohne gleichzeitig einen Lösungsvorschlag zu präsentieren. Gleichzeitig müssen wir aber auch beachten, dass wir nicht die Rolle von Group Audit beeinträchtigen. Group Audit muss eigenständig und unabhängig bleiben. Dennoch müssen wir uns bewusst sein, dass wir alle von einem erfolgreichen Unternehmen abhängen, das Gewinne erzielt, die deutlich höher sind als die Kosten. Daher müssen wir gemeinsam daran arbeiten. Dies bedeutet, dass wir uns an die Vorschriften halten müssen, um drastische Strafen zu vermeiden, die das Unternehmen erheblich belasten könnten. Das wurde in der Vergangenheit schmerzlich deutlich, und es hilft niemandem, wenn man sich komplett an die Regulatorik hält, aber gleichzeitig keine Geschäfte mehr abschließen kann. Die Herausforderung besteht darin, eine Balance zu finden zwischen der Anerkennung der Regulatorik und dem Streben nach Gewinn. Dies ist das spannende Dilemma, in dem wir uns bewegen. Wir müssen die Vorschriften beachten, aber gleichzeitig müssen wir auch Wege finden, um Einnahmen zu generieren. Denn wenn wir zu vorsichtig agieren und keine Kredite mehr vergeben, werden wir unser Geschäft nicht aufrechterhalten können – das ist die Realität. Dieser Balanceakt erstreckt sich auch auf das Risikomanagement. Wir müssen sicherstellen, dass die Risiken beherrschbar sind. Für mich bedeutet Risikomanagement jedoch nicht, Risiken komplett zu vermeiden, sondern sie zu managen und vorausschauend zu agieren. Denn letztendlich birgt jeder Kredit ein gewisses Risiko. Schließlich können wir im Voraus nicht sicher wissen, ob der Kunde in der Lage sein wird, seine Schulden zurückzuzahlen. #00:43:30#

I: Wird ein integrierter GRC-Ansatz als definierte Strategie in der Deutschen Bank verfolgt? Also gibt es da eventuell eine niedergeschriebene Strategie was die Zusammenarbeit und Prozesse der Schnittstellen angeht definiert? Oder verläuft es eher intuitiv, dass man eben weiß: Okay, das macht Sinn, dass man sich eben regelmäßig mal austauscht? #00:44:18#

B: Also, intuitiv auf keinen Fall! Wir sind verpflichtet, unsere Strategie regelmäßig zu entwickeln und der Aufsicht vorzulegen. Wenn wir einfach intuitiv vorgehen würden, das würde die Aufsicht sagen: „intuitiv hier, euch helfen wir ja – wir sind das größte deutsche Institut.“ Das würde schiefgehen. Ich habe jedoch nicht genug Einblick in die Strategieentwicklung, um hier weitere Informationen zu liefern.

Ich kann Ihnen jedoch mitteilen, dass es im Außenverhältnis interessante Entwicklungen in Bezug auf die Strategie gegeben hat. Insbesondere der erwähnte Professor Simon, dessen Schwerpunkt im Bereich Chief Administration liegt, ist nicht nur für formale Angelegenheiten

zuständig, sondern er verantwortet auch die Bereiche Legal, Governance und Compliance unter sich. Zusätzlich hat er nun auch die Rolle des Länderchefs für Amerika übernommen. Ich zitiere hier lediglich Informationen, die öffentlich zugänglich sind, und bitte Sie, nicht anzunehmen, dass ich über besonderes Insiderwissen verfüge – das ist ohnehin nicht der Fall, da ich mich auf Deutschland beschränke. Es scheint, dass diese Änderungen in der Strategie von oben nach unten umgesetzt werden, wobei Herr Simon nun auch für die USA verantwortlich ist. In diesem Bereich müssen nicht nur Vorschriften eingehalten werden, sondern es ist auch erforderlich, mit Kunden zu interagieren. Man strebt an, eine Person mit starkem regulatorischem Hintergrund in der Organisation zu haben, um eine ganzheitliche Betrachtung sicherzustellen und entsprechend umzusetzen. Aktuell gibt es noch Verbesserungsbedarf in diesem Bereich, wie aus den Medienberichten hervorgeht. Es gab unterschiedliche Meinungen und Reaktionen, aber der Auslöser für diese Veränderung war, einen Experten für Governance in den USA einzusetzen, um eventuelle Schwachstellen zu schließen. Dies dient dazu, sicherzustellen, wie diese Strategie im Vorstand tatsächlich umgesetzt wird. Hierbei möchte ich betonen, dass ich selbstverständlich nicht persönlich mit jedem einzelnen Mitglied des Vorstands gesprochen habe. Dennoch sehe ich dies als sichtbaren Beweis dafür, dass die Strategie rasch umgesetzt wird. Herr Simon ist seit diesem Jahr für die USA verantwortlich und bringt insbesondere Fachwissen im Bereich Legal und Governance ein. Zudem besteht eine enge Zusammenarbeit mit Herrn Olivier, unserem Risikovorstand. Unsere Bereiche sind natürlich eigenständig, da wir sicherstellen müssen, dass wir die Kreditstrategie in der Praxis umsetzen und die Risiken ordnungsgemäß steuern. Das Rahmenwerk wird von den Abteilungen Risk und Governance bereitgestellt. #00:47:24#

I: Welche potenziellen Vorteile könnten sich ergeben wenn Banken einen integrierten GRC-Ansatz verfolgen? #00:47:44#

B: Im besten Fall, wenn ein reibungsloser Austausch stattfindet und alles nahtlos zusammenpasst, entsteht eine Art ideale Welt. Hierbei entwickeln die Compliance-Manager ein besseres Verständnis für die Realitäten im Kreditgeschäft. Genauso wichtig ist es jedoch, dass die Personen, die über Kreditentscheidungen verantwortlich sind, ein umfassendes Verständnis für die Einhaltung von Compliance-Richtlinien haben. Es darf nicht mehr vorkommen, dass wir Geschäfte abschließen, ohne uns darum zu kümmern, ob wir gegen Vorschriften verstoßen. Diese Mentalität haben wir bereits bei Personen erlebt, die nicht mehr bei der Bank sind und uns dadurch Milliardenstrafen eingebracht haben. Daher ist ein Austausch von Fachwissen und Hintergrundinformationen unerlässlich. Diese Zusammenarbeit kann meiner Meinung nach am

besten umgesetzt werden, indem beide Seiten ihr Wissen teilen. So wird vermieden, dass Verdachtsmomente aufkommen. Wenn Compliance oder Governance beispielsweise unter dem Dach des Risikobereichs wären, bestünde die Möglichkeit, dass die Dinge im Hintergrund so gelenkt werden könnten, wie es einem gerade passt. Das sollte vermieden werden, denn hier sollte ein Vorstandsmitglied dem anderen ganz klar seine Erwartungen mitteilen, sei es in positivem oder negativem Sinne. Es ist wichtig, dass hier eine Trennung erfolgt, ähnlich wie bei der früheren Kombination von Kreditentscheidung und Kreditverkauf unter einem Dach und der eine, der war Chef vom anderen, der hat zudem im Zweifel gesagt: du kannst gerne entscheiden, wie du willst, aber dein Bonus solltest du nicht aus dem Blick verlieren. Solche Situationen führten oft dazu, dass Menschen entsprechend handelten. Diese Praktiken gehören der Vergangenheit an, aber sie verdeutlichen, dass eine Trennung notwendig ist. Heutzutage sind Governance, Compliance und Risiko getrennt, was eine positive Entwicklung ist. Diese Abteilungen verfolgen zwar gemeinsame Ziele, legen jedoch unterschiedliche Schwerpunkte. Ein intensiver Austausch zwischen ihnen ist wichtig, ebenso wie mit der Internen Revision, die unabhängig sein muss und das ist auch gut so, weil die Revision die hier Gefährlichkeit Prüfungen macht, die kann man sich schenken. Das würde kein einziger Prüfer akzeptieren. #00:50:21#

I: Gibt es denn ein ganzheitliches GRC- Reporting, indem diese Funktionen einmal im Quartal oder einmal im Jahr zusammen an den Vorstand berichten? Oder berichtet jede Funktion separat? #00:51:25#

B: Das Reporting wird zunächst eigenständig vor Ort in den einzelnen Sparten erstellt. Anschließend werden diese Berichte zusammengeführt. Wir haben einen Finanzvorstand, Herr Wolke, der sich die Gesamtsituation anschaut. Ich bitte um Verständnis, dass ich in Bezug auf die genaue Vorgehensweise im Vorstand nicht im Detail informiert bin. Meine Kenntnisse reichen nur bis zu einem gewissen Punkt in der Hierarchie. Ich weiß lediglich, dass es eine Verpflichtung für die Vorstandsmitglieder gibt, sich die Gesamtsituation anzusehen, und dass verschiedene Reportings vorhanden sind. Außerdem ist klar, dass quartalsweise Berichte erstattet werden müssen. Was ich gelesen habe, deutet darauf hin, dass die Vorstandsmitglieder sich die verschiedenen Reportings untereinander ansehen und dass keine isolierten Berichtsstrukturen entstehen dürfen. Die Aufsichtsbehörden würden eine solche Silo-Bildung ebenfalls nicht akzeptieren. Aber ich kann Ihnen keine konkreten Beispiele nennen, da ich in diesem Bereich nicht so involviert bin. Was ich jedoch weiß, ist, dass unser Reporting fortgesetzt wird, da Herr Selig natürlich auch über die Aktivitäten seiner Risikoteams informiert

sein möchte. Vor Ort erstellen wir unser eigenes Reporting. Wir erstellen kein spezifisches Reporting für die Corporate Bank, da dies nicht erforderlich ist. Unser Reporting wird dann jedoch auf höherer Ebene zusammengeführt und vom Risikovorstand überprüft. Dabei arbeiten sie eng mit dem Finanzvorstand und dem Governance-Vorstand zusammen. Wir haben auch ein Reporting für Kreditausfälle, dass das Interesse des Finanzbereichs weckt. Sollten regulatorische Probleme auftreten, interessiert sich natürlich auch Herr Professor Simon, der für diesen Bereich zuständig ist. In solchen Fällen treten die verschiedenen Vorstände sofort in den Dialog miteinander. #00:53:38#

I: Okay, ja, wir sind tatsächlich schon durch mit den Fragen. Dementsprechen würde ich jetzt mit der Aufzeichnung stoppen. #00:53:49#

E Einverständniserklärung der Experten

Hochschule Neu-Ulm
University of Applied Sciences

Einverständniserklärung zur Erhebung und Verarbeitung von Interviewdaten

Erläuterung

Sie erklären sich dazu bereit, im Rahmen der Bachelorarbeit **„Die Bedeutung der Integration von Governance, Risk und Compliance (GRC) im Banksektor: Eine Analyse der ganzheitlichen Betrachtung von GRC"** von Frau Emilia Steinhauer an einem Interview teilzunehmen. Sie wurden über Art, Umfang und Ziel sowie den Verlauf des o. g. Forschungsvorhabens informiert.

Das Interview wird mit einem Aufnahmegerät aufgezeichnet und sodann in Schriftform gebracht.

Für die weitere wissenschaftliche Auswertung des Interviewtextes werden alle Angaben, die zu einer Identifizierung Ihrer Person oder von im Interview erwähnten Personen und Institutionen führen könnten, anonymisiert. Das Transkript des Interviews dient nur zu Analysezwecken und wird lediglich in Ausschnitten zitiert.

Ihre personenbezogenen Kontaktdaten werden von Interviewdaten getrennt für Dritte unzugänglich gespeichert und vertraulich behandelt.

Einverständnis

Sie sind damit einverstanden, im Kontext des o. g. Forschungsvorhabens an der Befragung teilzunehmen. Darüber hinaus akzeptieren Sie die o. g. Form der anonymen Weiterverarbeitung und wissenschaftlichen Verwertung des geführten Interviews und der daraus entstehenden Daten.

Ihre Teilnahme an der Erhebung und Ihre Zustimmung zur Verwendung der Daten sind freiwillig. Durch die Ablehnung entstehen Ihnen keine Nachteile. Ihnen ist bekannt, dass Sie diese Einwilligung jederzeit gegenüber Frau Emilia Steinhauer widerrufen können mit der Folge, dass die Verarbeitung Ihrer personenbezogenen Daten, nach Maßgabe der Widerrufserklärung, für die Zukunft unzulässig wird. Dies berührt die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung jedoch nicht.

Unter diesen Bedingungen erklären Sie sich bereit, das Interview zu geben und sind damit einverstanden, dass es aufgezeichnet, verschriftlicht, anonymisiert und ausgewertet wird.

Jason Koegel

Vorname, Nachname in Druckschrift

Ditzingen, 13.06.2023 J. Koegel

Ort, Datum / Unterschrift

Hochschule Neu-Ulm
University of Applied Sciences

Einverständniserklärung zur Erhebung und Verarbeitung von Interviewdaten

Erläuterung

Sie erklären sich dazu bereit, im Rahmen der Bachelorarbeit **„Die Bedeutung der Integration von Governance, Risk und Compliance (GRC) im Banksektor: Eine Analyse der ganzheitlichen Betrachtung von GRC**“ von Frau Emilia Steinhauer an einem Interview teilzunehmen. Sie wurden über Art, Umfang und Ziel sowie den Verlauf des o. g. Forschungsvorhabens informiert.

Das Interview wird mit einem Aufnahmegerät aufgezeichnet und sodann in Schriftform gebracht.

Für die weitere wissenschaftliche Auswertung des Interviewtextes werden alle Angaben, die zu einer Identifizierung Ihrer Person oder von im Interview erwähnten Personen und Institutionen führen könnten, anonymisiert. Das Transkript des Interviews dient nur zu Analysezwecken und wird lediglich in Ausschnitten zitiert.

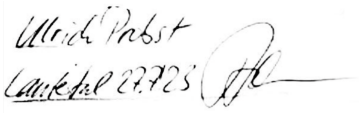
Ihre personenbezogenen Kontaktdaten werden von Interviewdaten getrennt für Dritte unzugänglich gespeichert und vertraulich behandelt.

Einverständnis

Sie sind damit einverstanden, im Kontext des o. g. Forschungsvorhabens an der Befragung teilzunehmen. Darüber hinaus akzeptieren Sie die o. g. Form der anonymen Weiterverarbeitung und wissenschaftlichen Verwertung des geführten Interviews und der daraus entstehenden Daten.

Ihre Teilnahme an der Erhebung und Ihre Zustimmung zur Verwendung der Daten sind freiwillig. Durch die Ablehnung entstehen Ihnen keine Nachteile. Ihnen ist bekannt, dass Sie diese Einwilligung jederzeit gegenüber Frau Emilia Steinhauer widerrufen können mit der Folge, dass die Verarbeitung Ihrer personenbezogenen Daten, nach Maßgabe der Widerrufserklärung, für die Zukunft unzulässig wird. Dies berührt die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung jedoch nicht.

Unter diesen Bedingungen erklären Sie sich bereit, das Interview zu geben und sind damit einverstanden, dass es aufgezeichnet, verschriftlicht, anonymisiert und ausgewertet wird.



Ort, Datum / Vorname, Nachname in Druckschrift und Unterschrift

HNU
Hochschule Neu-Ulm
University of Applied Sciences

Einverständniserklärung zur Erhebung und Verarbeitung von Interviewdaten

Erläuterung

Sie erklären sich dazu bereit, im Rahmen der Bachelorarbeit **„Die Bedeutung der Integration von Governance, Risk und Compliance (GRC) im Banksektor: Eine Analyse der ganzheitlichen Betrachtung von GRC"** von Frau Emilia Steinhauer an einem Interview teilzunehmen. Sie wurden über Art, Umfang und Ziel sowie den Verlauf des o. g. Forschungsvorhabens informiert.

Das Interview wird mit einem Aufnahmegerät aufgezeichnet und sodann in Schriftform gebracht.

Für die weitere wissenschaftliche Auswertung des Interviewtextes werden alle Angaben, die zu einer Identifizierung Ihrer Person oder von im Interview erwähnten Personen und Institutionen führen könnten, anonymisiert. Das Transkript des Interviews dient nur zu Analysezwecken und wird lediglich in Ausschnitten zitiert.

Ihre personenbezogenen Kontaktdaten werden von Interviewdaten getrennt für Dritte unzugänglich gespeichert und vertraulich behandelt.

Einverständnis

Sie sind damit einverstanden, im Kontext des o. g. Forschungsvorhabens an der Befragung teilzunehmen. Darüber hinaus akzeptieren Sie die o. g. Form der anonymen Weiterverarbeitung und wissenschaftlichen Verwertung des geführten Interviews und der daraus entstehenden Daten.

Ihre Teilnahme an der Erhebung und Ihre Zustimmung zur Verwendung der Daten sind freiwillig. Durch die Ablehnung entstehen Ihnen keine Nachteile. Ihnen ist bekannt, dass Sie diese Einwilligung jederzeit gegenüber Frau Emilia Steinhauer widerrufen können mit der Folge, dass die Verarbeitung Ihrer personenbezogenen Daten, nach Maßgabe der Widerrufserklärung, für die Zukunft unzulässig wird. Dies berührt die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung jedoch nicht.

Unter diesen Bedingungen erklären Sie sich bereit, das Interview zu geben und sind damit einverstanden, dass es aufgezeichnet, verschriftlicht, anonymisiert und ausgewertet wird.

Klaus Abel

Vorname, Nachname in Druckschrift

Hamburg, 28.2023 K. Abel

Ort, Datum / Unterschrift