I.M.U.
Institut für Mitbestimmung
und Unternehmensführung

Das I.M.U. ist ein Institut
der Hans-Böckler-Stiftung

Grundlagen und Anwendungsbeispiele

RISIKOMANAGEMENT DER KREDITINSTITUTE

Christiane Kohs

März 2021

Der Begriff Risiko wurde bereits im 16. Jahrhundert verwendet, um kaufmännische Wagnisse und Gefahren zu beschreiben, die unerwartet und nicht vorhersehbar eintraten. Von Anfang an war jedoch schon klar, dass Risiken mit vorausschauendem und klugem Handeln begegnet werden kann und dass sich damit neue Möglichkeiten ergeben können. Seither hat der Risikobegriff in die unterschiedlichsten Disziplinen Eingang gefunden. Im Allgemeinen wird unter Risiko die zufallsbehaftete Möglichkeit einer Veränderung von Ereignissen verstanden, die mit einer eventuellen negativen Auswirkung (Gefahr) verknüpft sind.

Im Rahmen des Kartenstapels wird auf die Kreditinstitute eingegangen.

Nach der Legaldefinition des § 1 Abs. 1 Satz 1 Kreditwesengesetz (KWG) sind Kreditinstitute als Unternehmen definiert, die Bankgeschäfte gewerbsmäßig oder in einem Umfang betreiben, der einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert. Sie umfassen Privatbanken (z.B. Deutsche Bank, Commerzbank), öffentliche Banken (z.B. Sparkassen) sowie Genossenschaftsbanken, die Eigentum ihrer Mitglieder sind. Kreditinstitute sind gegenüber Finanzdienstleistungsinstituten abzugrenzen, die u.a. die Anlagevermittlung, die Anlageberatung, das Factoring und das Finanzierungsleasing erbringen.

MITBESTIMMUNGS-
PORTAL

Inhalt

1 Risikomanagement - Begriffsabgrenzung

In der bankbetrieblichen Literatur wird zumeist zwischen Risikomanagement im weiteren oder umfassenden Sinne und Risikomanagement im engeren Sinne unterschieden. Im umfassenden Sinne wird unter Risikomanagement die Gesamtheit aller Handlungen, die sich mit der Identifikation, Messung, Steuerung und Überwachung von Risiken befassen, verstanden. Das Risikomanagement im engeren Sinne beinhaltet nur die Steuerung oder Bewirtschaftung, d.h. das Managen der Risiken. In dieser engen Begriffsabgrenzung steht dem Risikomanagement das Risikocontrolling gegenüber, welches das Identifizieren, Messen und Überwachen der Risiken beinhaltet.

Gemäß § 25a Abs. 1 KWG ist das Risikomanagement Teil einer ordnungsgemäßen Geschäftsorganisation und umfasst insbesondere:

– die Festlegung von Strategien (Geschäfts- und Risikostrategien),
– die Verfahren zur Ermittlung und Sicherstellung der Risikotragfähigkeit,
– die Einrichtung interner Kontrollverfahren mit einem internen Kontrollsystem und einer Internen Revision,
– eine angemessene personelle und technisch-organisatorische Ausstattung,
– die Festlegung eines angemessenen Notfallkonzepts, insbesondere für IT-Systeme,
– angemessene transparente und auf eine nachhaltige Entwicklung des Kreditinstituts ausgerichtete Vergütungssysteme.

Die Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) präzisieren die Anforderungen des § 25a Abs. 1 und § 25b Abs. 1 KWG und geben somit den Rahmen für die Ausgestaltung des Risikomanagements in deutschen Kreditinstituten vor. Rechtlich gesehen sind die MaRisk ein Rundschreiben, zu dessen Veröffentlichung das Bundesfinanzministerium über § 25a Abs. 4 KWG ermächtigt wird. Die BaFin kann im Rahmen der Prüfungstätigkeit nach § 44 KWG die Einhaltung der MaRisk überwachen und darauf hinwirken, dass die Kreditinstitute die gewünschte Auslegung der MaRisk akzeptieren.

Die MaRisk ist in den Allgemeinen Teil (AT) und den Besonderen Teil (BT) unterteilt. Der Allgemeine Teil umfasst in erster Linie die übergeordneten Anforderungen an die Ausgestaltung des Risikomanagements, bei denen grundsätzlich kein konkreter Bezug zu Geschäftsbereichen besteht. Der Besondere Teil unterteilt sich in

– die Anforderungen an die Aufbau- und Ablauforganisation,
– die Anforderungen an die Risikosteuerungs- und Risikocontrolling-Prozesse und

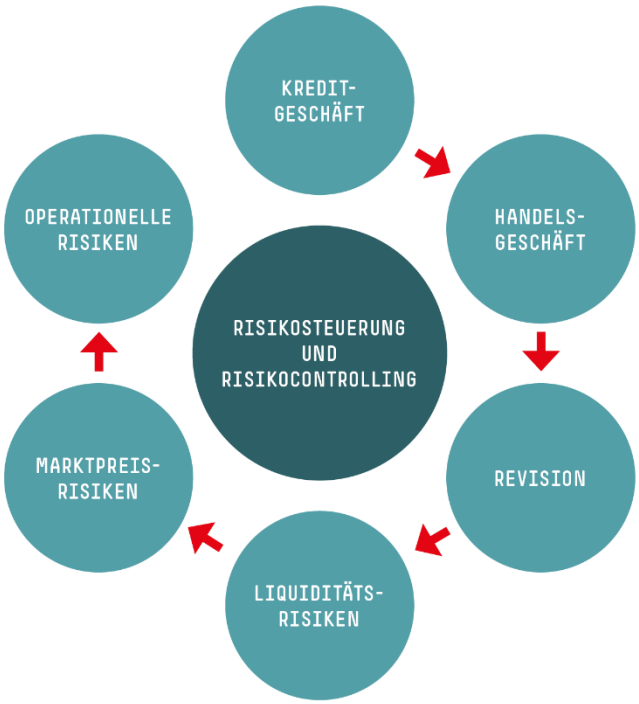
– die besonderen Anforderungen an die Ausgestaltung der Internen Revision sowie der Risikoberichterstattung.

Die MaRisk sind grundsätzlich prinzipienorientiert gestaltet, d.h., dass sie Gestaltungsspielräume für Umsetzungsmöglichkeiten bieten. Nach dem Grundsatz der Proportionalität sind die Anforderungen der MaRisk immer in Relation zur Größe, Risikostruktur und Komplexität des Kreditinstituts zu interpretieren.

Internationale Regulierungsinitiativen erfordern eine häufige Aktualisierung der MaRisk. Die aktuell gültigen Anforderungen stammen aus dem Jahr 2017 (5. Novelle der MaRisk). Am 26. Oktober 2020 wurde der Entwurf der 6. Novelle der MaRisk veröffentlicht, die voraussichtlich in 2021 finalisiert werden.

Die MaRisk spezifizieren nicht, was unter Risiko zu verstehen ist bzw. wie dieses definiert ist. Daher existieren in den Kreditinstituten zum Teil unterschiedliche Risikobegriffe.

Abbildung 1: Wesentliche Elemente der MaRisk



Quelle: Kreditinstitute, Finanzdienstleister und Investmentvermögen – Rechnungslegung und Prüfung, 2020, S. 105: Wesentliche Elemente der MaRisk I.M.U.

2 Geschäfts- und Risikostrategie

Die Geschäftsstrategie bildet den Ausgangspunkt und die Grundlage des Risikomanagementsystems. Die Risikostrategie stellt die bankweite Vorgabe von Zielen zum Umgang mit Risiken dar. Dabei ist die Verzahnung mit der Geschäftsstrategie wichtig. Nur eine gemeinsame Erarbeitung von

Geschäfts- und Risikostrategie stellt die angemessene Berücksichtigung von Zusammenhängen sicher. Strategieänderungen (z.B. im Zusammenhang mit Digitalisierung) müssen zeitgleich angemessen in der Risikostrategie abgebildet werden.

Die Geschäftsleitung ist verantwortlich für die Festlegung und Anpassung der Strategien und hat

– eine nachhaltige **Geschäftsstrategie** festzulegen, in der als Grundlage der Geschäftstätigkeit und unter Beachtung der Risikotragfähigkeit die Ziele des Kreditinstituts für jede wesentliche Geschäftsaktivität sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden,

– eine mit der Geschäftsstrategie und den daraus resultierenden Risiken konsistente **Risikostrategie** festzulegen, die als Grundlage des Risikomanagements die Ziele der Risikosteuerung für die wesentlichen Geschäftsaktivitäten (insbesondere den Risikoappetit für alle wesentlichen Risiken) sowie Maßnahmen zur Erreichung dieser Ziele umfasst sowie

– einen **Strategieprozess** zur Planung, Umsetzung, Beurteilung (inkl. Ursachenanalyse bei Abweichungen) und Anpassung der Strategien einzurichten.

Die Strategien und die dabei getroffenen Annahmen sind gemäß AT 4.2 MaRisk von der Geschäftsleitung regelmäßig und anlassbezogen

– zu überprüfen,

– ggf. an geänderte Rahmenbedingungen für die Geschäftstätigkeit und die Risikosteuerung anzupassen sowie

– dem Aufsichtsorgan des Kreditinstituts zur Kenntnis zu geben und mit diesem zu erörtern.

Dieser Abschnitt basiert insbesondere auf Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, 2020, S. 915 f., Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.), Düsseldorf: IDW Verlag GmbH

2.1 Identifizierung und Beurteilung von Risiken (Risikoinventur)

Zur Festlegung einer Risikostrategie ist es im ersten Schritt erforderlich, eine umfassende Risikoinventur vorzunehmen. Diese hat sich auf den gesamten Geschäftsbetrieb sowie auf zukünftige Veränderungen, die sich aus der Geschäftsstrategie ergeben zu erstrecken.

Grundsätzlich sind zumindest die folgenden Risiken als wesentlich einzustufen (AT 2.2, Tz. 1 MaRisk):

– Adressenausfallrisiken (einschließlich Länderrisiken),

– Marktpreisrisiken,

– Liquiditätsrisiken und

– operationelle Risiken.

Das **Adressenausfallrisiko** (auch Kreditausfallrisiko) bezeichnet die

Gefahr, der eine Bank ausgesetzt ist, wenn sie einen Kredit gewährt. Hierbei besteht das Risiko darin, dass die Tilgungs- und Zinszahlungen des Kreditnehmers nicht rechtzeitig oder überhaupt nicht geleistet werden, er also ausfällt. Je schlechter die wirtschaftliche Situation des Kreditnehmers, desto höher ist das Ausfallrisiko.

Das **Marktpreisrisiko** beschreibt das Risiko, bei der Vermögensanlage Geld zu verlieren, wenn sich die relevanten Marktwerte zum eigenen Nachteil verändern. Bei verzinslichen Wertpapieren könnte dies eine Änderung der Marktzinsen und bei Wertpapieren Änderungen der Börsenkurse sowie bei Fremdwährungen Änderungen der Wechselkurse hervorrufen. Die Entwicklung von Marktwerten ist nicht zuverlässig vorhersehbar und unterliegt ständigen Schwankungen. Diese Unsicherheit kann sich in Gewinnen (Chance) und Verlusten (Risiko) für die Marktteilnehmer niederschlagen.

In der Praxis haben sich Modelle entwickelt, bei denen das Marktpreisrisiko in Zinsänderungsrisiko, Kursänderungsrisiko und Restwertrisiko weiter untergliedert wird.

Mit **Liquiditätsrisiko** wird das Risiko bezeichnet, zum Begleichen fälliger Zahlungen benötigte Zahlungsmittel nicht oder nur zu erhöhten Refinanzierungskosten beschaffen zu können. Es ist zwischen dem Liquiditätsrisiko im engeren Sinne, dem Refinanzierungsrisiko und dem Marktliquiditätsrisiko zu unterscheiden (Deutscher Rechnungslegungs Standard Nr. 20 – Konzernlagebericht, DRS 20 A1.9). Die Auswirkungen unplanmäßiger Entwicklungen, z.B. vorzeitige Kündigungen oder die unvorhergesehene Zahlungsunfähigkeit eines Geschäftspartners werden im Liquiditätsrisiko erfasst (DRS 20 A1.13). Das Refinanzierungsrisiko umfasst das Risiko, bei Bedarf nicht oder nicht zu den erwarteten Konditionen Liquidität beschaffen zu können. Das Risiko aufgrund unzulänglicher Markttiefe oder Marktstörungen Geschäfte nicht oder nur mit Verlusten auflösen bzw. glattstellen zu können, wird als Marktliquiditätsrisiko bezeichnet (DRS 20.11).

Operationelles Risiko ist das Risiko von Verlusten, die durch die Unangemessenheit oder das Versagen von internen Verfahren, Menschen und Systemen oder durch externe Ereignisse verursacht werden (Art. 4 Abs. 1 Nr. 52 Capital Requirements Regulation – CRR, Kapitaladäquanzverordnung). Hierzu gehören somit u.a. Risiken des personellen Bereichs und der Informationstechnologie sowie Rechtsrisiken.

Häufig werden das Reputationsrisiko sowie strategische Risiken nicht als Teil der operationellen Risiken aufgefasst, sondern als eigenständige Risikoarten.

Nachhaltigkeitsrisiken müssen heute als ein elementarer Bestandteil des Risikomanagements betrachtet werden. Mit dem Merkblatt zum Umgang mit Nachhaltigkeitsrisiken vom 13. Januar 2020 stellt die BaFin ihre Erwartungshaltung klar, dass die beaufsichtigten Unternehmen eine Auseinandersetzung mit Nachhaltigkeitsrisiken sicherzustellen und dies zu dokumentieren haben. Nachhaltigkeitsrisiken gelten demnach lediglich als Unterkategorie der bekannten Risikoarten und sollten insoweit auch schon bisher in die Bewertung, Überwachung, Steuerung und Kommunikation der wesentlichen Risiken nach den jeweils maßgeblichen Vorgaben einbezogen worden sein.

Einen ähnlichen Ansatz verfolgt auch die Europäische Zentralbank (EZB) mit ihren im Mai 2020 zur Konsultation gestellten Leitlinien zu Klima- und Umweltrisiken.

Mit dem so genannten Sustainable Finance Action Plan verfolgt die Europäische Union (EU) drei Ziele (EU-Kommission, Sustainable Finance Action Plan, COM (2018) 97 final vom 8. März 2018):

– Lenkung von Kapitalströmen,

– Integration von Nachhaltigkeitsrisiken in das Risikomanagement der Unternehmen,

– Förderung von Transparenz und Langfristigkeit in Kapitalanlagen.

Der Sustainable Finance Action Plan sieht dazu zehn Maßnahmen mit verschiedenen Regelungen vor, die Finanzmarktteilnehmer – etwa Kreditinstitute, Versicherungen, Kapitalverwaltungsgesellschaften oder Pensionskassen – verpflichten, nachhaltige Investitionen zu fördern, und bestimmte Unternehmen verpflichten, über ihre Nachhaltigkeit zu berichten.

Nachhaltigkeitsrisiken i.S.d. BaFin-Merkblattes sind Ereignisse oder Bedingungen aus den Bereichen Umwelt, Soziales oder Unternehmensführung (Environmental, Social und Governance - ESG) deren Eintreten tatsächlich oder potenziell erhebliche negative Auswirkungen auf die Vermögens-, Finanz- und Ertragslage sowie auf die Reputation eines Unternehmens haben können. Dies schließt klimabezogene Risiken in Form von physischen Risiken und Transitionsrisiken ein.

Unter **physischen Risiken** versteht man die direkten und indirekten Folgen von Extremwetterereignissen wie Stürmen, Starkregen, Hagel, Dürren und extremer Trockenheit.

Bei **Transitions- oder Übergangsrisiken** handelt es sich im Gegensatz dazu um die Auswirkungen der politisch oder gesellschaftlich initiierten Umstellung auf eine nachhaltiger ausgerichtete Wirtschaft, z.B. infolge des Kohleausstiegs oder der Förderung der Elektromobilität.

Neben umwelt- und klimabezogenen Risiken umfassen Nachhaltigkeitsrisiken aber auch Ereignisse, Entwicklungen oder Verhaltensweisen aus den Bereichen **Soziales** und **Unternehmensführung**. Dazu können Fälle aus der jüngeren Vergangenheit zählen, wie beispielsweise hohe Schadensersatzklagen in der Tabak- oder Chemieindustrie aufgrund gesundheitsschädlicher Folgen für die Verbraucher, Reputationsschäden in der Textilindustrie aufgrund der Missachtung von Arbeitsschutzrechten, die Aufdeckung und Verurteilung von Steuerbetrug oder eine unzureichende Geldwäscheprävention im Finanzsektor.

Eine **Risikoinventur** muss regelmäßig, in der Regel einmal jährlich, und anlassbezogen durchgeführt werden, z.B. wenn neue Geschäfte aufgenommen werden, sich die Organisationsstruktur umgestaltet oder wenn sich externe Rahmenbedingungen ändern. Es sind sämtliche für ein Kreditinstitut relevante Risiken aufzunehmen, und zwar zunächst unabhängig davon, ob sie wesentlich sind oder nicht. Neben dem Risikoinventar ist ein zentrales Ergebnis der Risikoinventur auch die Identifizierung der wesentlichen

Risiken. Ob ein Risiko wesentlich ist, soll daran beurteilt werden, ob es die Vermögenslage (einschließlich der Kapitalausstattung), die Ertragslage oder die Liquiditätslage wesentlich beeinträchtigt (AT 2.2, Tz. 2 MaRisk).

2.2 Steuerung von Risiken

An die Identifizierung der Risiken schließen sich die Strategien zu ihrer **Vermeidung** bzw. **Beherrschung** oder **Minimierung** an. Für jedes Risiko, das das Kreditinstitut nicht als für sich unerheblich eingestuft hat, sind derartige Überlegungen anzustellen. Hierbei kommen verschiedene strategische Möglichkeiten in Betracht: Das Kreditinstitut kann beschließen, das identifizierte Risiko zu vermeiden, also z.B. keine entsprechenden Geschäfte abzuschließen. Oder es wird eine Strategie der Risikominderung angestrebt, also beispielsweise der Abbau von Risikoaktiva oder die Reduzierung bestehende Limite für die entsprechenden Geschäfte. Außerdem besteht die Möglichkeit der **Risikoüberwälzung**, häufig durch den Abschluss von Versicherungen. Letztendlich kommt auch die Risikotragung, also die Einräumung oder Ausweitung bestehender Limite, in Betracht. Im Fall von Risiken, die vom Kreditinstitut als unerheblich beurteilt werden, deren Eintrittswahrscheinlichkeit gering ist und die kein hohes Schadenspotenzial aufweisen, ist es auch möglich, diese zu **tolerieren**, also keine Maßnahmen zu ergreifen.

AT 4.3.2, Tz. 5 MaRisk fordert, dass die zur Risikosteuerung und zum Risikocontrolling eingesetzten Verfahren inklusive der Methoden zur Quantifizierung regelmäßig sowie bei sich ändernden Bedingungen auf ihre Angemessenheit zu überprüfen und gegebenenfalls anzupassen sind. Entstehen aufgrund einer Änderung der äußerlichen Bedingungen neue oder zusätzliche Risikotreiber, müssen Kreditinstitute ihre Verfahren zur Risikobeurteilung auf Angemessenheit überprüfen und gegebenenfalls anpassen.

2.2.1 Risikokultur

Risikokultur wurde vom Baseler Ausschuss für Bankaufsicht definiert als die Gesamtheit aller Normen, Einstellungen und Verhaltensweisen in Bezug auf das Risikobewusstsein, die Risikobereitschaft und das Risikomanagement sowie die Kontrollen, die Entscheidungen über Risiken beeinflussen. Die Risikokultur beeinflusst die Geschäftsleitung und die Mitarbeiter beim Umgang mit Risiken im Tagesgeschäft und wirkt sich auf deren Entscheidungen über das Eingehen von Risiken aus.

Wesentliche Elemente der Risikokultur sind:

– Entwicklung, Förderung und Integration der Risikokultur durch die Geschäftsleitung,

– nachhaltiges Risikobewusstsein und risikoangemessenes Verhalten aller Mitarbeiter unter Beachtung des durch die Geschäftsleitung kommunizierten Risikoappetits (= quantitative und qualitative Vorgaben zur Risikobereitschaft),

– nachvollziehbare Entscheidungsprozesse, die unter Berücksichtigung der identifizierten Risiken zu ausgewogenen und nachhaltigen Ergebnissen führen,

– offener Dialog und wertschätzende Kommunikation im Unternehmen zu allen risikorelevanten Fragen.

Mit den Aussagen zum Risikoappetit bringt die Geschäftsleitung zum Ausdruck, wieviel Risiko sie in den einzelnen wesentlichen Risiken oder Geschäftsbereichen einzugehen bereit ist. Die mit dem Risikoappetit im Einklang stehenden Vorgaben müssen klare Steuerungsimpulse für die Mitarbeiter/Bereiche setzen, damit diese ihr Handeln und ihr Tun daran beurteilen und messen können. Hierbei muss es sich nicht zwingend um quantitative Vorgaben (z.B. Limite oder Verlustobergrenzen) handeln. Der Risikoappetit kann auch durch qualitative Vorgaben zum Ausdruck gebracht werden, wie beispielsweise die Vermeidung bestimmter Geschäfte oder die Absicherung betrieblicher Risiken über Versicherungen. Wichtig ist die effektive Verzahnung mit Anreiz- und Sanktionsmechanismen (variable Vergütung, Personalentwicklung, Personalmaßnahmen etc.). Entsprechende Zielvereinbarungen sowie Metriken für die Messung der Zielerreichung müssen mit dem definierten Risikoappetit kompatibel sein.

Es können z.B. Vorgaben darüber gemacht werden, wie hoch der Anteil von Unternehmen im Kreditportfolio oder im Depot sein sollte, deren Wirtschaftsaktivitäten als nachhaltig im Sinne der EU-Taxonomie-Verordnung gelten (Verordnung (EU) 2020/852 vom 18. Juni 2020 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088, ABl. EU Nr. L 198/13 vom 22. Juni 2020). Auch können bestimmte Unternehmen, die in besonderem Maße negativ zum Klimawandel beitragen, als Kreditnehmer ausgeschlossen werden.

Durch einen Verhaltenskodex kann die Risikokultur gefördert werden. So sieht AT 5, Tz. 3g MaRisk vor, dass – abhängig von der Größe des Kreditinstituts sowie der Art, dem Umfang, der Komplexität und dem Risikogehalt der Geschäftsaktivitäten – die Organisationsrichtlinien eines Kreditinstituts einen Verhaltenskodex für die Mitarbeiter enthalten müssen.

Trotz aller Modelle und Technologien sind die Menschen entscheidend für die Risikokultur, sowohl bei der Entstehung von Risiken als auch bei deren Bewältigung.

Dieser Abschnitt basiert insbesondere auf Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, 2020, S. 914 f., Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.), Düsseldorf: IDW Verlag GmbH

2.2.2 Risikotragfähigkeit/Kapital- und Liquiditätssteuerung

Zentrales Element für die operative Begrenzung und Steuerung von Risiken ist das Risikotragfähigkeitskonzept. Mit Hilfe dieses Konzepts bzw. der Risikotragfähigkeitsrechnung ermittelt ein Kreditinstitut, ob es in der Lage ist, eintretende Verluste ohne Bestandsgefährdung und ohne schwerwiegende negative Auswirkungen auf seine Geschäftsaktivitäten auszugleichen. Hierfür steht ein Kreditinstitut das Risikodeckungspotential, d.h. das zum Ausgleich von Risiken intern zur Verfügung stehende Kapital, den wesentlichen

Risiken gegenüber. Risikoappetit und Risikotragfähigkeit müssen konsistent zueinander sein und die aus dem Risikoappetit abgeleiteten Vorgaben und Limite zur operativen Steuerung müssen als strikte Bedingungen die jederzeitige Einhaltung der Risikotragfähigkeit gewährleisten (§ 25a Abs. 1 Satz 3 KWG).

Ein Kreditinstitut ist fähig, seine Risiken zu tragen, wenn den eingegangenen Risiken genügend Deckungsmassen gegenüberstehen. Die Deckungsmasse für Solvenzrisiken ist Kapital, die für Liquiditätsrisiken ist der Liquiditätspuffer.

Weiterführende Informationen hierzu enthält der Kartenstapel „Eigenmittel und Liquidität“.

Bei der Sicherstellung der Risikotragfähigkeit sind sowohl das Ziel der Fortführung des Kreditinstituts als auch der Schutz der Gläubiger vor Verlusten aus ökonomischer Sicht zu berücksichtigen. Hierzu sind interne Risikosteuerungs- und Risikocontrolling-Prozesse einzurichten (AT 4.1 MaRisk).

Besondere Pflichten ergeben sich für die Geschäftsleiter eines Kreditinstituts aus den Anforderungen der EZB an die Ausgestaltung der Prozesse zur Steuerung von Eigenkapital und Liquidität. Hierzu hat die EZB im Herbst 2018 ihre Erwartungen an die Kreditinstitute in zwei umfassenden Leitlinien zur Ausgestaltung der internen Prozesse zur Gewährleistung einer angemessenen Eigenkapital- und Liquiditätsausstattung formuliert. Dabei kommt den Geschäftsleitern die übergeordnete Verantwortung für die Einrichtung und Weiterentwicklung entsprechender Prozesse zu.

Der Betrachtungshorizont im Rahmen des Risikotragfähigkeitskonzepts beträgt üblicherweise ein Jahr, häufig ergänzt um einen dreijährigen Kapitalplanungsprozess. Nachhaltigkeitsrisiken zeichnen sich jedoch unter anderem dadurch aus, dass der Zeithorizont, indem sie eintreten werden, höchst unsicher ist und möglicherweise erst jenseits des einjährigen Betrachtungszeitraums liegt. Kreditinstitute, die in besonderem Maße Nachhaltigkeitsrisiken ausgesetzt sind, benötigen daher neben der eher kurzfristigen Risikotragfähigkeitsbetrachtung einen um einen längeren Zeithorizont ergänzten Steuerungskreis.

2.2.3 Nachhaltiges Geschäftsmodell

Zudem haben Kreditinstitute eine auf Nachhaltigkeit ausgerichtete Geschäftsstrategie zu formulieren. Zur Geschäftsstrategie ist eine dazu konsistente Risikostrategie zu definieren. Die Risikostrategie ist widerspruchsfrei zur Geschäftsstrategie, wenn sie zu allen wesentlichen, aus der Geschäftsstrategie resultierenden Risiken, Stellung nimmt. Insbesondere muss festgelegt sein, wie die wesentlichen Risiken gemessen werden und in welchem Umfang geplant ist, sie einzugehen.

2.2.4 Kontrollabteilungen

Darüber hinaus ist eine ordnungsgemäße Geschäftsorganisation

gekennzeichnet durch ein internes, von Marktbereichen unabhängiges Kontrollsystem.

Unter „Marktbereichen“ versteht man im Bankwesen die unmittelbar mit Kundenkontakt betrauten Geschäftsbereiche.

Das Kontrollsystem muss mindestens aus Risikocontrolling, Interner Revision und Compliance-Abteilung bestehen. Diese Abteilungen tragen keine Ergebnisverantwortung im Gegensatz zu den Marktbereichen. Die Aufgabenbereiche der Kontrollabteilungen müssen untereinander und in Bezug auf die Marktbereiche klar abgegrenzt sein.

2.2.5 Dokumentation

Eine vollständige Dokumentation der Geschäftstätigkeit, eine angemessene personelle und technische Ausstattung sowie ein Notfallkonzept sind ebenfalls Bestandteil einer ordnungsgemäßen Geschäftsorganisation. Es ist der Aufsicht besonders wichtig, dass das Notfallsystem insbesondere auch die IT-Systeme miteinschließt.

2.3 Gesamtbanksteuerung

Gemäß AT 4.3.2, Tz. 1 MaRisk sind die Prozesse zur Identifizierung, Beurteilung und Steuerung von Risiken in eine gemeinsame Ertrags- und Risikosteuerung einzubinden, um risikoadjustierte Erträge auszuweisen. Des Weiteren müssen die Verfahren zur Risikobegrenzung und Risikosteuerung, insbesondere das Risikotragfähigkeitskonzept, in die Entscheidungsprozesse einer Bank eingebunden werden. Mit Hilfe der Gesamtbanksteuerung sollen auch Wechselwirkungen dargestellt und gesteuert werden. Zum einen sind dies Wechselwirkungen zwischen einzelnen Risiken und den Steuerungsmaßnahmen, zum anderen Wechselwirkungen zwischen einzelnen Risikoarten und Ertragsquellen.

Beispielsweise steigen die physischen Klimarisiken. In Deutschland gab es in den Jahren 2000 bis 2019 mehr als 10.700 Todesopfer und Schäden von 4,27 Mrd. US-Dollar. Damit landet Deutschland im →I Klima-Risiko-Index der Umwelt- und Entwicklungsorganisation Germanwatch auf Platz 18 weltweit, vor allem wegen wiederholter Hitzewellen, Stürmen und Hochwassern an Donau und Elbe. Dies wirkt sich z.B. auf die Werthaltigkeit von Immobiliensicherheiten der Kreditinstitute aus. Es muss gegebenenfalls entschieden werden, in bestimmten Regionen keine Immobilienfinanzierung mehr durchzuführen oder das Risiko durch entsprechende Wertabschläge bei den Beleihungswerten vorwegzunehmen.

3 Internes Kontrollsystem

Ein Kreditinstitut hat zur ordnungsgemäßen Durchführung seiner Geschäftsaktivitäten ein Internes Kontrollsystem einzurichten. Hierzu gehören klare

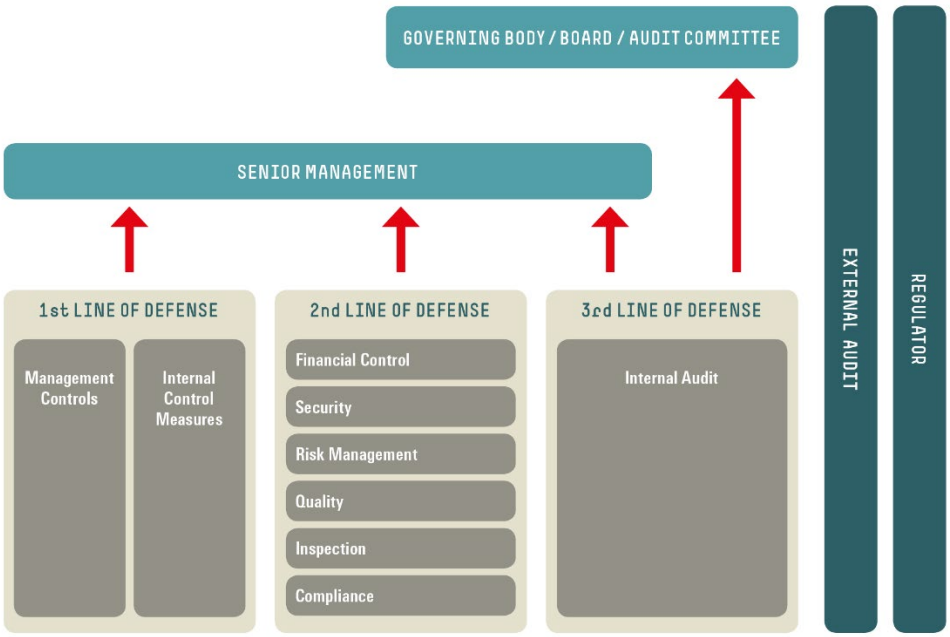
aufbau- und ablauforganisatorische Regelungen für sämtliche Geschäftsprozesse.

Mit dem Three-Lines-of-Defense-Modell ist 2013 vom Institute of Internal Auditors ein systematischer Ansatz zur Verortung von Kontroll- und Risikomanagementverantwortlichkeiten in einer Organisation vorgestellt worden:

– Die erste Verteidigungslinie umfasst die präventiven und detektiven Kontrollen im Tagesgeschäft und die übergreifenden Managementkontrollen in den operativen Geschäftseinheiten.
– Zur zweiten Verteidigungslinie zählen verschiedene Risikomanagement- und Compliance-Funktionen (insbesondere die Risikocontrolling-Funktion, die Compliance-Funktion, der Geldwäschebeauftragte und der Informationssicherheitsbeauftragte). Sie definieren die Kontroll- und Risikomanagementanforderungen und ermöglichen sowie überwachen deren Umsetzung durch die erste Verteidigungslinie.
– Die Interne Revision als dritte Verteidigungslinie überwacht, wie wirksam die erste und zweite Verteidigungslinie eines Kreditinstituts die Risiken beurteilen und steuern und ihre daraus abgeleiteten Aufgaben wahrnehmen.

Dieser Abschnitt basiert insbesondere auf Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, 2020, S. 918 f., Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.), Düsseldorf: IDW Verlag GmbH

Abbildung 2: The Three Lines of Defense Model



Quelle: Adapted from ECIIA / FERMA Guidance on the 8th EU Company Law Directive, article 41

3.1 Regelungen zur Aufbau- und Ablauforganisation

Ein Bestandteil des internen Kontrollsystems sind nach § 25a Abs. 1 Satz 3 Nr. 3a KWG aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortlichkeiten. Es ist grundsätzlich darauf zu achten, dass

– miteinander unvereinbare Tätigkeiten durch unterschiedliche Mitarbeiter durchgeführt werden, um Interessenkonflikte zu vermeiden (Funktionstrennung, AT 4.3.1, Tz. 1 MaRisk) und

– Berechtigungen und Kompetenzen nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) vergeben werden (AT 4.3.1, Tz. 2 MaRisk).

Tätigkeiten sind dann als miteinander unvereinbar anzusehen, wenn sie zu Interessenskonflikten führen können oder wenn ihre Wahrnehmung durch nur eine Person den betreffenden Prozess jeglicher Kontrolle entziehen würde.

Die Funktionstrennung ist auch für den Vertretungsfall zu gewährleisten.

Für Kreditinstitute gilt weiterhin, dass bestimmte Bereiche im Handels- und Kreditgeschäft bis auf die Ebene der Geschäftsleitung aufbauorganisatorisch zu trennen sind.

So sind die Marktbereiche im Kreditgeschäft (Bereiche, die Kreditgeschäfte initiieren) von dem Bereich zu trennen, der bei Kreditentscheidungen über das zweite Votum verfügt (Marktfolge).

Unter „Marktfolge“ versteht man die nicht unmittelbar mit Kundenkontakt betrauten Geschäftsbereiche, die aufbauorganisatorisch von den „Marktbereichen“ zu trennen sind.

Handelsbereiche (Bereiche, die an den Geld- und Kapitalmärkten Geschäfte in Wertpapieren und Derivaten initiieren) sind von den Bereichen zu trennen, die Aufgaben der Abwicklung und Kontrolle von Handelsgeschäften wahrnehmen.

Insgesamt sind die Marktbereiche im Kreditgeschäft sowie die Handelsbereiche von dem Bereich Risikocontrolling aufbauorganisatorisch zu trennen (BTO, Tz. 2 und Tz. 3 MaRisk).

Auch die Überprüfung wesentlicher Rechtsrisiken, d.h. in aller Regel die Tätigkeit der Rechtsabteilung, hat von einer von Markt und Handel unabhängige Stelle zu erfolgen.

Ergänzend stellt AT 5 MaRisk klar, dass jedes Kreditinstitut sicherstellen muss, dass seine Geschäftsaktivitäten auf der Grundlage von Organisationsanweisungen, z.B. in der Form von Handbüchern, Arbeitsanweisungen oder Arbeitsablaufbeschreibungen durchgeführt werden. Wie diese Organisationsrichtlinien letztendlich ausgestaltet sind, steht dem jeweiligen Kreditinstitut offen. Entscheidend ist, dass diese sachgerecht sind und es den Mitarbeitern ermöglichen, auf ihrer Grundlage die ihnen übertragenen Aufgaben ordnungsgemäß zu erfüllen. Im Falle von Veränderungen sind die Organisationsrichtlinien zeitnah an die geänderten Gegebenheiten anzupassen. Sie müssen so detailliert sein, dass die Interne Revision auf ihrer Grundlage

Sachprüfungen durchführen kann.

Dieser Abschnitt basiert insbesondere auf Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, 2020, S. 915 f., Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.), Düsseldorf: IDW Verlag GmbH

3.2 Risikosteuerungs- und Risikocontrolling-Prozesse

Von wesentlicher Bedeutung einer funktionsfähigen Risikomanagement-Organisation sind Risikosteuerungs- und Risikocontrolling-Prozesse, die die

- Identifizierung,
- Beurteilung,
- Steuerung sowie
- Überwachung und Kommunikation

der wesentlichen Risiken und Risikokonzentrationen gewährleisten. Sie dienen der Steuerung und Begrenzung der Risiken und damit der Einhaltung der Risikotragfähigkeit (AT 4.3.2, Tz. 1 MaRisk). Die Risikosteuerungs- und Risikocontrolling-Prozesse sowie die hierbei eingesetzten Methoden müssen regelmäßig sowie anlassbezogen auf ihre Angemessenheit geprüft und ggf. angepasst werden (AT 4.3.2, Tz. 5 MaRisk).

Die Kreditinstitute müssen aussagekräftige Frühwarnindikatoren für alle relevanten Risikoarten identifizieren. Einen wichtigen Frühwarnindikator stellen auch Stresstests dar. Als Frühwarnindikatoren können für die verschiedenen Risikoarten unter anderem herangezogen werden:

Adressenausfallrisiken (einschließlich Länderrisiken)	– Kontoinformationen (Überziehungen, Rückstände) – Wirtschaftliche Verhältnisse – Qualitative Unternehmenskriterien (Managementqualität, Nachfolgeregelungen, Produktpalette, Innovationskraft) – Externe Informationen (Datenbanken, Presse, Internet) – Indizes (CDS-Spreads)
Marktpreisrisiken	– Kurs-Gewinn-Verhältnis – Zins-Spreads – Volatilitäten und diverse Stimmungsindizes
Liquiditätsrisiken	– Geldmengenentwicklung – Entwicklung der Liquiditätsbestände des Kreditinstituts
Operationelle Risiken	– Arbeitsmarktdaten – Studien zu diversen Bereichen – Mitarbeiterfluktuation – IT-Neuerungen

Quelle: Bankenaufsicht – Institutionen, Regelungsbereiche und Prüfung, 2016, S. 134: Frühwarnindikatoren

Ergänzend muss jedes Kreditinstitut über eine angemessene Dokumentation des gesamten Systems verfügen. Darüber hinaus ist es erforderlich, dass die Risikoreports und die Risikohandbücher fortlaufend überarbeitet werden. Das Risikohandbuch sollte sich auf Maßnahmen für Risiken konzentrieren, die im Kreditinstitut auch wirklich genutzt werden können.

In regelmäßigen Abständen, mindestens aber vierteljährlich, ist ein Risikobericht über die **Adressenausfallrisiken**, in dem die wesentlichen strukturellen Merkmale des Kreditgeschäfts enthalten sind, zu erstellen und der Geschäftsleitung zur Verfügung zu stellen. Der Risikobericht hat die folgenden Informationen zu umfassen (BT 3.2, Tz. 3 MaRisk):

– die Entwicklung des Kreditportfolios, z.B. nach Branchen, Ländern, Risikoklassen und Größenklassen oder Sicherheitenkategorien, unter besonderer Berücksichtigung von Risikokonzentrationen,

– den Umfang der vergebenen Limite und externen Linien; ferner sind Großkredite und sonstige bemerkenswerte Engagements (z.B. Sanierungs- und Abwicklungskredite von wesentlicher Bedeutung, Kredite in der Intensivbetreuung von wesentlicher Bedeutung) aufzuführen und ggf. zu kommentieren,

– ggf. eine gesonderte Darstellung der Länderrisiken,

– bedeutende Limitüberschreitungen (einschließlich einer Begründung),

– den Umfang und die Entwicklung des Neugeschäfts,

– die Entwicklung der Risikovorsorge des Kreditinstituts,

– getroffene Kreditentscheidungen von wesentlicher Bedeutung, die von den Strategien abweichen und

– Kreditentscheidungen im risikorelevanten Kreditgeschäft, die Geschäftsleiter im Rahmen ihrer Krediteinzelkompetenz beschlossen haben, soweit diese von den Voten abweichen, oder wenn sie von einem Geschäftsleiter getroffen werden, der für den Bereich Marktfolge zuständig ist.

Die mit **Marktpreisrisiken** behafteten Positionen des Anlagebuches sind mindestens vierteljährlich, die des Handelsbuchs sind täglich zu bewerten (BTR 2.2, Tz. 2, BTR 2.3, Tz. 1). Der Bericht hat unter Einbeziehung der internen Handelsgeschäfte folgende Informationen zu umfassen (BT 3.2, Tz. 4 MaRisk):

– einen Überblick über die Risiko- und Ergebnisentwicklung der mit Marktpreisrisiken behafteten Positionen,

– bedeutende Limitüberschreitungen,

– Änderungen der wesentlichen Annahmen oder Parameter, die den Verfahren zur Beurteilung der Marktpreisrisiken zugrunde liegen,

– Auffälligkeiten bei der Abstimmung der Handelspositionen (z.B. hinsichtlich der Handelsvolumina, Auswirkungen auf die Gewinn- und Verlustrechnung, Stornoquoten).

Für die **Liquiditätsrisiken** fordert BTR 3.1 MaRisk, dass die Kreditinstitute

für einen geeigneten Zeitraum eine Liquiditätsübersicht erstellen sowie eine Liquiditätsnotfallplanung unterhalten. Ergänzend sind regelmäßig Stresstests durchzuführen und ein Verrechnungssystem zur verursachungsgerechten internen Verrechnung der jeweiligen Liquiditätskosten, -nutzen und -risiken einzurichten. Es ist regelmäßig, mindestens aber vierteljährlich, ein Risikobericht über die Liquiditätsrisiken und die Liquiditätssituation zu erstellen und der Geschäftsleitung zur Verfügung zu stellen (BT 3.2, Tz. 5 MaRisk).

Im Hinblick auf **operationelle Risiken** und bedeutende Schadensfälle ist die Geschäftsleitung mindestens jährlich zu unterrichten (BT 3.2, Tz. 6 MaRisk). Die Berichterstattung hat die Art des Schadens bzw. Risikos, die Ursachen, das Ausmaß des Schadens bzw. Risikos und gegebenenfalls bereits getroffene Gegenmaßnahmen zu umfassen (BTR 4 MaRisk).

3.3 Stresstests

Ein weiteres Instrument zur Identifizierung und Beurteilung von Risiken sind Stresstests, mit denen die Auswirkungen einer erheblichen Veränderung von Risikofaktoren auf die Vermögens-, Ertrags und Liquiditätslage analysiert werden sollen. Stresstests dienen als Ergänzung zu Risikomodellen. Sie sollen extreme Entwicklungen simulieren und insbesondere solche Risiken erfassen, die aufgrund der Datenlage oder in Ermangelung aussagekräftiger Modelle nur ungenügend erfasst werden können. Die MaRisk fordern in AT 4.3.3 die regelmäßige und anlassbezogene Durchführung von Stresstests für alle wesentlichen Risiken und für das Gesamtrisikoprofil.

Dies beinhaltet z.B. auch Sensitivitätsanalysen (bei denen im Allgemeinen nur ein Risikofaktor variiert wird) oder Szenarioanalysen (bei denen mehrere oder alle Risikofaktoren, deren Änderungen sich aus einem vordefinierten Ereignis ergeben, simultan verändert werden) (Erläuterungen zu AT 4.3.3 MaRisk).

Beispiel: Wie funktioniert ein Stresstest?
Ein Kreditinstitut hat annahmegemäß 1.000 Kreditnehmer mit jeweils 100 Mio. € Kreditvolumen, die alle der gleichen Risikoklasse zuzuordnen sind. Erfahrungsgemäß beträgt die Ausfallwahrscheinlichkeit der Kredite (PD = probability of default) in dieser Risikoklasse 1%. Weiter wird angenommen, dass die Kredite identisch besichert sind und über die gleiche Laufzeit verfügen. Die Verlustquote (LGD = loss given default, Differenz zwischen offenem Kreditbetrag und den Sicherheiten) bei Kreditausfall beträgt 25%. Hieraus abgeleitet würde sich der durchschnittlich erwartete Verlust unter Berücksichtigung dieser Annahmen auf 250 Mio. € belaufen ((1% x 1.000 Kreditnehmer) x (25% x 100 Mio. €) = 250 Mio. €).

In einem Stresstest würde nun beispielsweise das Szenario „getestet“ werden, welche Auswirkungen eine starke Rezession hätte. Vorstellbar wäre, dass nicht mehr nur 1%, sondern 3% der Kreditnehmer ausfallen (PD steigt von 1% auf 3%). Darüber hinaus können die Sicherheiten annahmegemäß auch nur noch mit 67%-Abschlägen am Markt verwertet

werden, so dass die Verlustquote statt 25% jetzt 75% beträgt (LGD steigt von 25% auf 75%). Die Folge wäre also, dass der erwartete Verlust auf 2.250 Mio. € steigen würde ((3% x 1.000 Kreditnehmer) x (75% x 100 Mio. €) = 2.250 Mio. €). Im Vergleich zu „normalen“ Zeiten würde sich bei Eintreten dieser extremen Marktentwicklung also ein zusätzlicher Verlust von 2 Mrd. € einstellen, der mittels Eigenkapitalreserven bewältigt werden müsste.

Im Rahmen der Stresstests ist insbesondere zu analysieren, wie sich ein schwerer konjunktureller Abschwung auf das Kreditinstitut auswirkt (AT 4.3.3, Tz. 3 MaRisk).

Unternehmensweite Stresstests, d.h. die Simulation verschiedener Risikoarten und portfolioübergreifende Szenarien, dienen dem Management nicht nur dazu, operative Entscheidungen zur Steuerung akuter Risiken zu treffen, sondern auch dazu, strategische Entscheidungen vorzubereiten.

Neben normalen Stresstests hat jedes Kreditinstitut auch so genannte inverse Stresstests durchzuführen. Dabei wird untersucht, welche Ereignisse das Kreditinstitut in seiner Überlebensfähigkeit gefährden können, d.h. es sind Grenzszenarien zu identifizieren. Ein mögliches Szenario stellt beispielsweise der gleichzeitige Verlust mehrerer Kunden ohne entsprechende Zugänge von Neukunden dar.

Für die aufsichtlich gestiegene Bedeutung von Stresstests stehen die mittlerweile regelmäßig durchgeführten externen Stresstests der European Banking Authority - EBA (Europäische Bankenaufsichtsbehörde) bzw. der EZB.

3.4 Datenmanagement, Datenqualität und Aggregation von Risikodaten

Die Anforderungen hierzu richten sich an systemrelevante Kreditinstitute (AT 4.3.4 MaRisk).

Zur Verbesserung der Risikoberichterstattung hat der Baseler Ausschuss in 2013 die Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung verfasst. Die zukünftigen aufsichtlichen Erwartungen an die Datenhaltung der Kreditinstitute sind sehr hoch:

– Die Risikodaten kommen gebündelt aus einer goldenen Quelle (Data Warehouse).

– Der Risikobericht ist so wenig fehleranfällig wie die Bilanz und Gewinn- und Verlustrechnung.

– Die Erstellung des Risikoberichts erfolgt weitestgehend automatisch.

– Es können schnell benutzerdefinierte Berichte in beliebiger vertikaler Aggregation als auch nach horizontalen Einheiten generiert werden.

Die Datenstruktur und die Datenhierarchie müssen gewährleisten, dass Daten zweifelsfrei identifiziert, zusammengeführt und ausgewertet werden können sowie zeitnah zur Verfügung stehen (AT 4.3.4, Tz. 2 MaRisk).

Das Kreditinstitut hat zu gewährleisten, dass die Risikodaten genau und vollständig sind. Daten müssen nach unterschiedlichen Kategorien auswertbar sein und sollten, soweit möglich und sinnvoll, automatisiert aggregiert werden können (AT 4.3.4, Tz. 3 MaRisk).

Die Risikodaten sind mit anderen im Kreditinstitut vorhandenen Informationen abzugleichen und zu plausibilisieren. Es sind Verfahren und Prozesse zum Abgleich der Risikodaten und der Daten in den Risikoberichten einzurichten, mittels derer Datenfehler und Schwachstellen in der Datenqualität identifiziert werden können (AT 4.3.4, Tz. 4 MaRisk).

Die Datenaggregationskapazitäten müssen hinreichend flexibel sein, um Informationen ad hoc nach unterschiedlichen Kategorien ausweisen und analysieren zu können. Dazu gehört auch die Möglichkeit, Risikopositionen auf den unterschiedlichsten Ebenen (Geschäftsfelder, Portfolios, ggf. Einzelgeschäfte) auszuweisen und zu analysieren (AT 4.3.4, Tz. 6 MaRisk).

3.5 Besondere Funktionen

3.5.1 Risikocontrolling-Funktion

Gemäß § 25a Abs. 1 Satz 3 Nr. 3c KWG muss jedes Kreditinstitut über eine Risikocontrolling-Funktion verfügen (AT 4.4.1, Tz. 1 MaRisk). Die Aufgabe besteht darin, die Risiken des Kreditinstituts als unabhängige Stelle zu überwachen und zu kommunizieren.

Die Risikocontrolling-Funktion ist aufbauorganisatorisch auch in der Geschäftsleitung von den Verantwortungsbereichen zu trennen, die Geschäfte initiieren.

Zu den Aufgaben gehören (AT 4.4.1, Tz. 2 MaRisk):

- Unterstützung der Geschäftsleitung in allen risikobezogenen Fragen, insbesondere bei der Entwicklung und Umsetzung der Risikostrategie sowie bei der Ausgestaltung eines Systems zur Begrenzung der Risiken,
- Durchführung der Risikoinventur und Erstellung des Gesamtrisikoprofils,
- Unterstützung der Geschäftsleitung bei der Einrichtung und Weiterentwicklung der Risikosteuerungs- und Risikocontrolling-Prozesse,
- Einrichtung und Weiterentwicklung eines Systems von Risikokennzahlen und eines Risikofrüherkennungsverfahrens,
- laufende Überwachung der Risikosituation des Kreditinstituts und der Risikotragfähigkeit sowie der Einhaltung der eingerichteten Risikolimite,
- regelmäßige Erstellung der Risikoberichte für die Geschäftsleitung und
- Verantwortung für die Prozesse zur unverzüglichen Weitergabe von unter Risikogesichtspunkten wesentlichen Informationen an die

Geschäftsleitung, die jeweiligen Verantwortlichen und gegebenenfalls die Interne Revision.

Den Mitarbeitern der Risikocontrolling-Funktion sind alle notwendigen Befugnisse und ein uneingeschränkter Zugang zu allen Informationen einzuräumen, die für die Erfüllung ihrer Aufgaben erforderlich sind (AT 4.4.1, Tz. 3 MaRisk).

Bei systemrelevanten Kreditinstituten muss die Risikocontrolling-Funktion grundsätzlich durch einen Geschäftsleiter (Chief Risk Officer - CRO) wahrgenommen werden (AT 4.4.1, Tz. 5 MaRisk).

3.5.2 Compliance-Funktion

Nach § 25a Abs. 1 Satz 3 Nr. 3c KWG muss das interne Kontrollsystem eines Kreditinstituts auch eine Compliance-Funktion umfassen, um den Risiken, die sich aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben ergeben können, entgegenzuwirken (AT 4.4.2, Tz. 1 MaRisk).

Die MaRisk enthalten auch hierzu konkretisierende Regelungen. Da nach den Erläuterungen zu AT 4.4.2, Tz. 1 MaRisk alle sonstigen Vorgaben zur Compliance-Funktion, die sich aus anderen Aufsichtsgesetzen ergeben (insbesondere § 33 WpHG und § 25h KWG jeweils i.V.m. konkretisierenden Verwaltungsvorschriften), unberührt bleiben, wird in der Praxis für die allgemeine Compliance-Funktion auch der Begriff „MaRisk-Compliance“ verwendet.

Mit der Compliance-Funktion soll ein Kreditinstitut für sich selbst nachweisen, dass es alle für sich wesentlichen rechtlichen Regelungen und Vorgaben, insbesondere solcher deren Nichteinhaltung zu einer Gefährdung des Vermögens des Kreditinstituts führen kann, identifiziert und umgesetzt hat.

Die Compliance-Funktion ist nicht verantwortlich für die Einhaltung der genannten Regelungen, die Verantwortung hierfür liegt nicht delegierbar bei der Geschäftsleitung.

Die Compliance-Funktion ist grundsätzlich unmittelbar der Geschäftsleitung zu unterstellen. Eine Anbindung an andere Kontrolleinheiten des Kreditinstituts (z.B. Risikocontrolling, Geldwäschebeauftragter) – mit Ausnahme der Internen Revision – ist zulässig, sofern eine direkte Berichtslinie zur Geschäftsleitung existiert. Systemrelevante Kreditinstitute haben für die Compliance-Funktion jedoch stets eine eigenständige Organisationseinheit einzurichten (AT 4.4.2, Tz. 3 und Tz. 4 MaRisk).

Nach AT 4.4.2, Tz. 5 MaRisk hat jedes Kreditinstitut einen Compliance-Beauftragten zu benennen, der für die Erfüllung der Aufgaben der Compliance-Funktion verantwortlich ist.

Die Compliance-Funktion hat – nach Identifizierung der für das Kreditinstitut wesentlichen rechtlichen Regelungen und Vorgaben – auf die Implementierung wirksamer Verfahren zu deren Einhaltung und entsprechender Kontrollen hinzuwirken. Die eigentliche Implementierung von wirksamen Verfahren

liegt auch in der Verantwortung der jeweils betroffenen Fachbereiche und nicht automatisch bei der Compliance-Funktion.

Ausgangspunkt der Überwachungsaufgaben der Compliance-Funktion ist regelmäßig ein Verzeichnis aller rechtlichen Regelungen und Vorgaben des jeweiligen Kalenderjahres. Auf dieser Basis hat die Compliance-Funktion festzulegen, ob die jeweilige rechtliche Regelung oder Vorgabe für das Kreditinstitut relevant und wesentlich ist.

Die MaRisk-Compliance ist nicht spezialisiert auf einem eingegrenzten Fachgebiet tätig, sondern muss die gesamte Fachbreite des Kreditinstituts abdecken. In den Anwendungsbereich fallen insbesondere die Vorgaben zum Wertpapierhandelsgesetz (WpHG), zur Vermeidung von Geldwäsche und Terrorismusfinanzierung, zur Vermeidung sonstiger strafbarer Handlungen, zum Datenschutz sowie zum Verbraucherschutz.

Der Regulierungsgeber erwartet bei der MaRisk-Compliance-Funktion nicht die Prüfung auf fachlicher Detailebene. Die rechtzeitige und richtige Umsetzung überprüft die Compliance-Funktion daher in der Praxis regelmäßig über ein Risk Assessment, bei dem anhand entsprechender Arbeitsanweisungen sowie Kontrollbeschreibungen und -dokumentationen die Implementierung nachvollzogen wird.

Zur Erfüllung ihrer vorstehenden Überwachungsaufgaben kann die Compliance-Funktion gemäß AT 4.4.2, Tz. 3 und Tz. 6 MaRisk auf andere Funktionen und Stellen zurückgreifen. Den Mitarbeitern der Compliance-Funktion sind

– ausreichende Befugnisse und ein uneingeschränkter Zugang zu allen relevanten Informationen einzuräumen sowie

– die für die Compliance-Funktion wesentlichen Weisungen und Beschlüsse der Geschäftsleitung rechtzeitig bekanntzugeben.

Mindestens einmal im Jahr sowie anlassbezogen ist der Geschäftsführung, dem Aufsichtsorgan und der Internen Revision von der Compliance-Funktion ein Bericht über ihre Tätigkeit sowie die Wirksamkeit und die Angemessenheit der implementierten Compliance-Regelungen vorzulegen, wobei insbesondere auch auf festgestellte Schwachstellen und Maßnahmen zu deren Behebung einzugehen ist (AT 4.4.2, Tz. 7 MaRisk).

Dieser Abschnitt basiert insbesondere auf Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, 2020, S. 920 f., Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.), Düsseldorf: IDW Verlag GmbH

3.5.3 Interne Revision

Die Verpflichtung für Kreditinstitute zur Einrichtung einer Internen Revision ergibt sich aus § 25a Abs. 1 Satz 3 Nr. 3 KWG. Die grundlegenden Anforderungen an die Interne Revision sind in AT 4.4.3 MaRisk festgelegt. Danach ist jedes Kreditinstitut verpflichtet, eine funktionsfähige Interne Revision einzurichten. Im Falle der Unverhältnismäßigkeit im Hinblick auf die Institutsgröße kann diese Funktion durch einen Geschäftsleiter wahrgenommen werden. Um sicherzustellen, dass die Revision ihren Aufgaben nachkommen kann, ist sie aufbauorganisatorisch unmittelbar der Geschäftsleitung zu

unterstellen und dieser berichtspflichtig. Ebenso muss gewährleistet sein, dass der Vorsitzende des Aufsichtsorgans bzw. des Prüfungsausschusses direkt bei dem Leiter der Internen Revision Auskünfte einholen kann (AT 4.4.3, Tz. 2 MaRisk).

Die Aufgabe der Internen Revision hat sich risikoorientiert grundsätzlich auf alle Tätigkeitsbereiche des Kreditinstituts zu beziehen, unabhängig von etwaigen Auslagerungen. Ihre Zielsetzung ist die Beurteilung der Angemessenheit und Wirksamkeit des Risikomanagementsystems mit besonderem Fokus auf dem internen Kontrollsystem (AT 4.4.3, Tz. 3 MaRisk).

Um ihren Aufgaben nachkommen zu können, sind der Internen Revision

– ein vollständiges, uneingeschränktes und jederzeitiges Informationsrecht zu gewähren,
– die notwendigen Unterlagen bereitzustellen und
– Einblick in alle Aktivitäten und Systeme zu ermöglichen (AT 4.4.3, Tz. 4 und 5 MaRisk).

In BT 2 MaRisk sind weitere Anforderungen definiert, die die Aufgaben und Grundsätze der Internen Revision detaillierter regeln und auch aufsichtliche Erwartungen an die Revisionsprozesse – beginnend mit der Prüfungsplanung, über die Prüfungsdurchführung und die Berichterstattung bis hin zur Maßnahmennachverfolgung – konkretisieren. Leitbild ist dabei die unabhängige und selbständige Durchführung der Revisionsarbeit.

Mitarbeiter, die in anderen Organisationseinheiten des Kreditinstituts beschäftigt sind, dürfen grundsätzlich nicht mit Aufgaben der Internen Revision betraut werden. Das schließt jedoch nicht aus, dass in begründeten Einzelfällen andere Mitarbeiter aufgrund ihres Spezialwissens zeitweise für die Interne Revision tätig werden. Beim Wechsel von Mitarbeitern anderer Organisationseinheiten zur Internen Revision sind angemessene Übergangsfristen von in der Regel mindestens einem Jahr vorzusehen, innerhalb derer diese Mitarbeiter keine Tätigkeiten prüfen dürfen, die gegen das Verbot der Selbstprüfung verstoßen (BT 2.2, Tz. 3 MaRisk).

Die jährlich fortzuschreibende und von der Geschäftsleitung zu genehmigende Prüfungsplanung der Internen Revision hat grundsätzlich den gesamten Tätigkeitsbereich des Kreditinstituts abzudecken, wobei dem unterschiedlichen Risikogehalt durch entsprechende Prüfungsintervalle Rechnung zu tragen ist. Die Revisionsplanung hat dabei auch Kapazitätsreserven für unvorhergesehene Mängel bzw. Informationsbedürfnisse (Sonderprüfungen) vorzusehen (BT 2.3 MaRisk).

Über jede Prüfung ist nach BT 2.4 MaRisk zeitnah im Einzelfall zu berichten, wobei das Prüfungsgebiet zu beurteilen sowie Mängel zu vermerken sind. Der Adressatenkreis kann dabei nach Schwere der Feststellungen variieren. Bei schwerwiegenden Mängeln muss der Bericht unverzüglich der Geschäftsleitung vorgelegt werden.

Darüber hinaus sind zusammenfassende Berichterstattungen der Internen Revision (Gesamtbericht) an die Geschäftsleitung und das Aufsichtsorgan ebenso vorgesehen wie eine systematische Mängelverfolgung (BT 2.5

MaRisk). Diese kann auch eine gezielte Nachschauprüfung beinhalten.

Neben den von der BaFin erlassenen MaRisk hat die EBA in den Leitlinien zur internen Governance (EBA/GL/2017/11) Anforderungen an die Interne Revision von Instituten fixiert, die seit dem 30. Juni 2018 anzuwenden sind.

Dieser Abschnitt basiert insbesondere auf Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, 2020, S. 927 f., Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.), Düsseldorf: IDW Verlag GmbH

4 Weitere Komponenten des Risikomanagementsystems (Ressourcen)

4.1 Personelle Ausstattung

Die quantitative und qualitative Personalausstattung des Kreditinstituts hat sich insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation zu orientieren. Dies gilt auch beim Rückgriff auf Leiharbeitnehmer (AT 7.1, Tz. 1 MaRisk).

Die Mitarbeiter sowie deren Vertreter müssen abhängig von ihren Aufgaben, Kompetenzen und Verantwortlichkeiten über die erforderlichen Kenntnisse und Erfahrungen verfügen. Durch geeignete Maßnahmen ist zu gewährleisten, dass das Qualifikationsniveau der Mitarbeiter angemessen ist (AT 7.1, Tz. 2 MaRisk).

4.2 Technisch-organisatorische Ausstattung

Umfang und Qualität der technisch-organisatorischen Ausstattung haben sich vor allem an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation zu orientieren (AT 7.2, Tz. 1 MaRisk).

Anforderungen an die Ausgestaltung der von Kreditinstituten eingesetzten Informationstechnologie ergeben sich bezogen auf die rechnungslegungsrelevanten Aspekte zunächst aus den allgemeinen Anforderungen an die Ordnungsmäßigkeit der Buchführung (§§ 238 f. HGB) sowie aus steuerlichen Vorschriften (§§ 146 ff. AO).

Weitergehende Regelungen für Kreditinstitute, die über die rechnungslegungsbezogenen IT-Systeme hinausgehen, enthält § 25a KWG. Dort wird gefordert, dass ein Kreditinstitut insbesondere über eine angemessene technisch-organisatorische Ausstattung (§ 25a Abs. 1 Satz 3 Nr. 4 KWG) sowie ein angemessenes Notfallkonzept, v.a. für IT-Systeme (§ 25a Abs. 1 Satz 3 Nr. 5 KWG) verfügen muss. Damit wird unmittelbar auf die von den Kreditinstituten eingesetzte IT Bezug genommen. Im Falle einer Auslagerung werden diese Anforderungen an das Kreditinstitut nicht reduziert (§ 25b KWG).

Ausgehend von den gesetzlichen Vorschriften des KWG wird die Erwartungshaltung der BaFin zum Umgang mit IT in den MaRisk (insbesondere AT 7.2 MaRisk) verdeutlicht sowie in den bankaufsichtlichen Anforderungen an die IT (BAIT) in Teilbereichen weiter konkretisiert. Die BAIT umfassen die

Themengebiete „IT-Strategie“, „IT-Governance“, „Informationsrisikomanagement“, „Informationssicherheitsmanagement“, „Benutzerberechtigungsmanagement“, „IT-Projekte und Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen)“, „IT-Betrieb (inkl. Datensicherung)“, „Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen“ sowie „kritische Infrastrukturen“.

Die Erläuterungen zu AT 4.2, Tz. 1 MaRisk heben dazu hervor, dass das Kreditinstitut aufgrund der Bedeutung der IT für das Funktionieren der Prozesse im Kreditinstitut in Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten bei der Festlegung der Geschäftsstrategie auch Aussagen zur künftig geplanten Ausgestaltung der IT-Systeme zu treffen hat. In der Praxis wird deshalb häufig eine gesonderte IT-Strategie aus der Geschäftsstrategie abgeleitet und im Einklang mit dieser formuliert. Die Mindestinhalte sowie weitere Anforderungen an die Erstellung und Pflege der IT-Strategie geben die BAIT im Modul 1 vor.

Zur erfolgreichen Umsetzung der IT-Strategie ist eine sachgerechte IT-Governance erforderlich. Die BAIT (Modul 2) verstehen darunter die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der dazugehörigen IT-Prozesse auf Basis der IT-Strategie und beschreiben die dafür erforderlichen Voraussetzungen. Diese umfassen u.a. die angemessene Personalausstattung, die Vermeidung von Funktionstrennungskonflikten sowie die Festlegung und Überwachung von Key-Performance-Indikatoren.

Die in den AT 5 MaRisk gestellte Anforderung, wonach die Geschäftsaktivitäten auf der Grundlage von Organisationsrichtlinien betrieben werden (z.B. Handbücher, Arbeitsanweisungen oder Arbeitsablaufbeschreibungen), erstreckt sich auch auf die eingesetzte IT. Hier geht es v.a. um die Regelungen für die IT-Aufbau- und IT-Ablauforganisation sowie zur Aufgabenzuweisung, zur Kompetenzordnung und zu den Verantwortlichkeiten und weiteren Regelungen, die die Einhaltung rechtlicher Regelungen und Vorgaben (z.B. Datenschutz, Compliance) gewährleisten.

Umfang und Qualität der technisch-organisatorischen Ausstattung haben sich insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation zu orientieren (AT 7.2 MaRisk). Hierzu ist bei der Ausgestaltung der IT-Systeme und der zugehörigen Prozesse grundsätzlich auf gängige Standards abzustellen.

Der Informationssicherheitsbeauftragte verantwortet vor allem die Festlegung eines so genannten Sollmaßnahmenkatalogs mit Mindestanforderungen an den Schutz der Integrität, Verfügbarkeit, Authentizität sowie Vertraulichkeit von Daten sowie die Prüfung ihrer Einhaltung. Der Bereich „IT“ verantwortet die Festlegung und Umsetzung geeigneter Maßnahmen zur Einhaltung der Mindestanforderungen zum Schutz der Daten. Der Informationssicherheitsbeauftragte ist zur Verhinderung potenzieller Interessenkonflikte aufbauorganisatorisch außerhalb des Bereichs „IT“ anzusiedeln. Die unzureichende Umsetzung von Sollmaßnahmen führt zu einem eingeschränkten Schutz der Daten und damit zu so genannten Informationsrisiken, die in angemessener Weise zu identifizieren, zu steuern und zu berichten sind. Anforderungen an die Ausgestaltung des Informationsrisiko- und

Informationssicherheitsmanagements werden in den Modulen 3 und 4 der BAIT beschrieben.

Das Modul 5 der BAIT umfasst Anforderungen an den Schutz vor vorsätzlichem, aber auch unbewusstem Missbrauch von Zugriffsberechtigungen auf Daten. Dabei haben Prozesse und Kontrollen sicherzustellen, dass Berechtigungen an Benutzer nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) sowie unter Wahrung der Funktionstrennung vergeben werden. Dies betrifft auch den Umgang mit sog. privilegierten Berechtigungen (u.a. administrative Berechtigungen), deren Nutzung durch geeignete Maßnahmen zu überwachen ist.

Anforderungen an die Anwendungsentwicklung sowie die Steuerung von IT-Projekten ergeben sich insbesondere aus dem Modul 6 der BAIT. Kreditinstitute haben angemessene Verfahren zur Entwicklung und Pflege von IT-Systemen inkl. angemessener Test-, Abnahme- und Freigabeprozesse festzulegen. Dies umfasst auch von Endbenutzern der Fachbereiche entwickelte oder betriebene Anwendungen.

Die Auswirkungen von Veränderungen an IT-Systemen auf Kontrollverfahren und die Kontrollintensität sind von den Instituten vor ihrer Durchführung zu analysieren (AT 8.2 MaRisk). Dies geht über das gewöhnliche Testen der Umsetzung der Veränderung deutlich hinaus.

Im Modul 7 geben die BAIT die Mindestanforderungen an einen geordneten IT-Betrieb vor. Dies umfasst u.a. die Inventarisierung aller eingesetzten IT-Systeme und ihrer Schnittstellen untereinander sowie Prozesse zum Umgang mit Störungen im IT-Betrieb und zur Datensicherung.

Für den Fall des vollständigen oder teilweisen Ausfalls des IT-Betriebs, der Dienstleister, des Personals oder der Gebäude (inkl. Rechenzentren) und der damit verbundenen Beeinträchtigung zeitkritischer Aktivitäten und Prozesse sind angemessene Notfallvorsorgekonzepte zu erstellen und regelmäßig im Hinblick auf ihre Wirksamkeit zu testen (AT 7.3 MaRisk).

Bei Auslagerungen und sonstigen Fremdbezügen von IT-Dienstleistungen sind die Anforderungen nach AT 9 MaRisk zu erfüllen. Nach den BAIT umfassen IT-Dienstleistungen alle Ausprägungen des Bezugs von IT, insbesondere die Bereitstellung von IT-Systemen, die Projekte/Gewerke oder die Personalgestellung. Dabei ist es unerheblich, ob die IT-Dienstleistung auf klassischem Weg oder als Cloud-Dienstleistung erbracht wird. Für lediglich als sonstigen Fremdbezug eingestufte IT-Dienstleistungen enthalten die BAIT in Modul 8 aufgrund der grundlegenden Bedeutung der IT für Kreditinstitute eigene Anforderungen. Diese umfassen die Durchführung einer Risikobewertung sowie die Berücksichtigung der hieraus gewonnenen Erkenntnisse beim Managementprozess für die operationellen Risiken sowie bei der Vertragsgestaltung.

Für Kreditinstitute, welche die in § 7 der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) genannten Voraussetzungen erfüllen und kritische Dienstleistungen in den Bereichen „Bargeldversorgung“, „kartengestützter Zahlungsverkehr“, „konventioneller Zahlungsverkehr“ sowie „Verrechnung und Abwicklung von Wertpapier- und Derivatgeschäften“

erbringen, ergeben sich weitere Anforderungen. Betreiber kritischer Infrastrukturen sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Die Betreiber kritischer Infrastrukturen haben die Erfüllung dieser Anforderungen mindestens alle zwei Jahre nachzuweisen. Hierzu kann das Modul 9 der BAIT optional verwendet werden.

Dieser Abschnitt basiert insbesondere auf Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, 2020, S. 928 f., Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.), Düsseldorf: IDW Verlag GmbH

4.3 Notfallkonzept

Für Notfälle in zeitkritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept). Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig durch Notfalltests zu überprüfen (AT 7.3, Tz. 1 MaRisk).

5 Auslagerungen von Aktivitäten und Prozessen

Anforderungen an die Auslagerung von Aktivitäten und Prozessen ergeben sich aus § 25b KWG. Die Anforderungen werden weiter konkretisiert durch AT 9 MaRisk. Spezielle Anforderungen an Auslagerungen finden sich u.a. im WpHG und im Geldwäschegesetz (GwG) sowie den hierzu ergangenen Verlautbarungen der Aufsichtsbehörden (z.B. BAIT, Mindestanforderungen der BaFin an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten - MaComp).

Eine Auslagerung ist in AT 9, Tz. 1 MaRisk definiert als die Beauftragung eines anderen Unternehmens mit der Wahrnehmung von Aktivitäten und Prozessen, die im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen und sonstigen institutstypischen Dienstleistungen stehen und die ansonsten vom auslagernden Kreditinstitut selbst erbracht würden.

Von der Auslagerung abzugrenzen ist der sonstige Fremdbezug von Leistungen (z.B. der einmalige oder gelegentliche Fremdbezug von Gütern und Dienstleistungen).

Grundsätzlich sind Aktivitäten und Prozesse auslagerbar, solange dadurch die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 25a Abs. 1 KWG des auslagernden Kreditinstituts nicht beeinträchtigt wird. Nicht auslagerbar sind die Leitungsaufgaben der Geschäftsleitung. Weitere Restriktionen bestehen für die vollständige Auslagerung der Risikocontrolling-Funktion, der Compliance-Funktion und der Internen Revision, wobei Erleichterungen für gruppeninterne Auslagerungen auf das übergeordnete Kreditinstitut und für kleinere Kreditinstitute bestehen (AT 9, Tz. 4 und 5

MaRisk).

§ 25b KWG regelt insbesondere die Einbeziehung der Auslagerungen in ein angemessenes und wirksames Risikomanagement des auslagernden Kreditinstituts. Die Übertragung der Verantwortung der Geschäftsleiter an das Auslagerungsunternehmen ist dabei ausgeschlossen. Auslagerungen bedürfen einer schriftlichen Vereinbarung, in der die zur Einhaltung der aufsichtsrechtlichen Anforderungen erforderlichen Rechte des Kreditinstituts, einschließlich Weisungs- und Kündigungsrechten, sowie die korrespondierenden Pflichten des Auslagerungsunternehmens festlegt werden. Die Auskunfts- und Prüfungsrechte sowie Kontrollmöglichkeiten der zuständigen Aufsichtsbehörde und des Abschlussprüfers müssen durch geeignete Vorkehrungen gewährleistet werden.

Die sich für wesentliche Auslagerungen ergebenden besonderen Anforderungen bestehen zum einen in Mindestbestandteilen, die im Auslagerungsvertrag zu regeln sind (AT 9, Tz. 7 MaRisk). Zum anderen bestehen sie in organisatorischen Anforderungen wie der Einrichtung eines zentralen Auslagerungsmanagements und der Bestimmung jeweils eines Auslagerungsbeauftragten zur laufenden Überwachung der einzelnen Auslagerungen (AT 9, Tz. 9, 10 bzw. 12, 13 MaRisk). Darüber hinaus sind die Auslagerungen in die Prüfung durch die Interne Revision einzubeziehen (AT 4.4.3, Tz. 4 MaRisk).

Zusätzlich müssen die Kreditinstitute über so genannte Exit-Strategien sowohl für die beabsichtigte oder erwartete als auch für Fälle der unbeabsichtigten oder unerwarteten Beendigung von Auslagerungen verfügen (AT 9, Tz. 5 MaRisk). Für die Auslagerung zeitkritischer Aktivitäten und Prozesse sind außerdem die Notfallkonzepte von auslagerndem Institut und Auslagerungsunternehmen aufeinander abzustimmen (AT 7.3, Tz. 1 MaRisk).

Auf europäischer Ebene hat die Europäische Bankenaufsichtsbehörde (EBA) die Leitlinien zu Auslagerungen erlassen (EBA/GL/2019/02), die seit dem 30. September 2019 zu beachten sind. Die Anforderungen decken sich in weiten Teilen mit denen der MaRisk und der BAIT. Unterschiede bestehen darin, dass die EBA-Leitlinien erhöhte Anforderungen an die Auslagerung sog. kritischer und wichtiger Funktionen stellen. Darüber hinaus fordern die EBA-Leitlinien eine Anzeigepflicht für Auslagerungen gegenüber den Aufsichtsbehörden sowie die Einrichtung eines detaillierten Auslagerungsregisters.

Dieser Abschnitt basiert insbesondere auf Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, 2020, S. 925 f., Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.), Düsseldorf: IDW Verlag GmbH

6 Risikoberichterstattung

Als Grundlage aller Überwachungshandlungen und Steuerungsentscheidungen haben sich die Geschäftsleiter regelmäßig über die Risikosituation berichten zu lassen. Hierzu ist ein System zur Risikoberichterstattung einzurichten, das in nachvollziehbarer, aussagefähiger Art und Weise die Risikosituation des Instituts transparent macht und auch eine Beurteilung der Risikosituation enthält. Die Risikoberichterstattung muss auf vollständigen, genauen und aktuellen Daten beruhen und soll zudem bei Bedarf auch

Handlungsvorschläge, z.B. zur Risikoreduzierung, enthalten (BT 3.1 MaRisk).

In den Risikoberichten sind insbesondere auch die Ergebnisse der Stresstests und deren potenzielle Auswirkungen auf die Risikosituation und das Risikodeckungspotenzial darzustellen (BT 3.1, Tz. 2 MaRisk).

Insbesondere infolge der Vielzahl der der Risikoberichterstattung zugrundeliegenden Informationen sowie der Dynamik in deren Entwicklung im Zeitablauf kommt angemessenen und wirksamen Verfahren, Methoden und Prozessen der Aggregation von Risikodaten eine besondere Bedeutung zu.

Neben der turnusmäßigen Erstellung von Risikoberichten (Gesamtrisikobericht, Berichte über einzelne Risikoarten) muss das Kreditinstitut in der Lage sein, ad hoc Risikoinformationen zu generieren, sofern dies aufgrund der aktuellen Risikosituation des Instituts oder der aktuellen Situation der Märkte, auf denen das Institut tätig ist, geboten erscheint (BT 3.1, Tz. 3 MaRisk).

Die Geschäftsleitung hat das Aufsichtsorgan mindestens vierteljährlich über die Risikosituation in angemessener Weise schriftlich zu informieren. Für das Aufsichtsorgan unter Risikogesichtspunkten wesentliche Informationen sind von der Geschäftsleitung unverzüglich weiterzuleiten (BT 3.1, Tz. 5 MaRisk).

Dieser Abschnitt basiert insbesondere auf Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, 2020, S. 919 f., Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.), Düsseldorf: IDW Verlag GmbH

7 Anforderungen an das Kreditgeschäft

Die BTO 1.2 MaRisk stellen dezidierte Anforderungen an die Prozesse und Verantwortlichkeiten im Kreditgeschäft.

Der Lebenszyklus eines Kredits teilt sich in drei wesentliche Phasen auf:

1. Kreditgewährung (Auszahlung)
2. Vertragsmanagement (Rückzahlung)
3. Fälligkeit.

Die erste Phase unterteilt sich in Kreditantrag, Kreditbeurteilung, Kreditentscheidung und Auszahlung/Dokumentation.

In der Phase zwei werden auf der Einzelvertragsebene die Rückzahlung und Indikatoren für eine Bonitätsverschlechterung überwacht. Falls notwendig, wird gegebenenfalls das interne Rating des Kunden angepasst. Eine wesentliche Verschlechterung des Ratings führt zu einer Reklassifikation des Kredits in die Intensivbetreuung, die Sanierung oder die Abwicklung.

Die Beendigung der Kredite (Phase drei) umfasst die Abwicklung und Liquidation der Sicherheiten bei den ausgefallenen Krediten bzw. die Archivierung und der Folgevertrag bei den ordnungsgemäß zurückgezahlten Verträgen.

Im Sinne der AT 2.3, Tz. 2 MaRisk gilt als Kreditentscheidung jede Entscheidung über Neukredite, Krediterhöhungen, Beteiligungen, Limitüberschreitungen, die Festlegung von kreditnehmerbezogenen Limiten sowie von

Kontrahenten- und Emittentenlimiten, Prolongationen und Änderungen risikorelevanter Sachverhalte, die dem Kreditbeschluss zugrunde lagen (z.B. Sicherheiten, Verwendungszweck). Dabei ist es unerheblich, ob diese Entscheidung ausschließlich vom Kreditinstitut selbst oder gemeinsam mit anderen Kreditinstituten getroffen wird (so genanntes Konsortialgeschäft).

Der gesamte Abschnitt basiert insbesondere auf Bankenaufsichtliches Risikomanagement – Grundlagen und Anwendung regulatorischer Anforderungen, 2018, S. 387 ff., Andrae, Silvio/Hellmich, Martin/Schmaltz, Christian, Stuttgart: Schäffer-Poeschel Verlag

7.1 Funktionstrennung und Votierung

Maßgeblicher Grundsatz für die Ausgestaltung der Prozesse im Kreditgeschäft ist die klare aufbauorganisatorische Trennung der Bereiche Markt und Marktfolge bis einschließlich der Ebene der Geschäftsleitung (BTO 1.1, Tz. 1 MaRisk).

Das Kreditinstitut muss definieren, ab welchem Gesamtvolumen ein Kreditgeschäft risiko- oder nicht risikorelevant ist. Eine oft gewählte Grenze ist 250.000 €. Nicht risikorelevantes Geschäft braucht nur ein positives Votum. Alle anderen Kredite müssen – bevor sie gewährt werden – ein positives Votum aus dem Marktbereich und eines aus der Marktfolge vorweisen. Unbeschadet dessen können Geschäftsleiter weiterhin ihre Krediteinzelkompetenz ausüben. Es muss darüber hinaus transparent kommuniziert sein, wer Kreditgeschäfte bis zu welchem Volumen allein bzw. zusammen mit anderen gewähren darf. Bei abweichenden Voten zwischen Markt und Marktfolge muss der Kredit abgelehnt werden oder zur Eskalation eine Entscheidungsstufe höher gegeben werden.

Sicherheiten sind nicht im Marktbereich zu bewerten (BTO 1.1, Tz. 7 MaRisk).

7.2 Anforderungen an die Prozesse im Kreditgeschäft

Zwingend einzurichten sind die folgenden Teilprozesse im Kreditgeschäft (BTO 1.2, Tz. 1 MaRisk):

– Kreditbearbeitung,
– Bonitätsbeurteilung,
– Kreditbearbeitungskontrolle,
– Kreditweiterbearbeitung,
– Intensivbetreuung,
– Sanierung und Abwicklung (Problemkredite),
– Risikovorsorge.

Kreditbearbeitung

Die Bearbeitungsschritte für eine Kreditgewährung, inklusive der Sicherheitenbewertung, müssen von der Organisation definiert und dokumentiert werden.

Neben der wirtschaftlichen Betrachtung sind insbesondere auch die technische Machbarkeit und Entwicklung sowie die mit dem Objekt/Projekt verbundenen rechtlichen Risiken in die Beurteilung einzubeziehen. Dabei kann auch auf die Expertise einer unabhängigen sach- und fachkundigen Organisationseinheit zurückgegriffen werden (BTO 1.2, Tz. 5 MaRisk).

Das Kreditinstitut hat standardisierte Kreditvorlagen zu verwenden, soweit dies in Anbetracht der jeweiligen Geschäftsarten möglich und zweckmäßig ist, wobei die Ausgestaltung der Kreditvorlagen von Art, Umfang, Komplexität und Risikogehalt der Kreditgeschäfte abhängt (BTO 1.2, Tz. 10 MaRisk).

Bei allen Kreditengagements muss es eine initiale und im weiteren Verlauf mindestens jährliche Beurteilung der Risiken des Engagements geben. Die Konditionen sollten sich mit steigendem Risiko des Engagements verteuern. Außerdem muss es ein Mahnverfahren für fehlende Unterlagen geben.

Bonitätsbeurteilung

Vor der Kreditgewährung muss die Kapitaldienstfähigkeit des Kreditnehmers bzw. des Objekts beurteilt werden. Bei Immobiliar-Verbraucherdarlehen sind auch zukünftige, als wahrscheinlich anzusehende Einkommensschwankungen in die Beurteilung der Kapitaldienstfähigkeit einzubeziehen (BTO 1.2.1, Tz. 2 MaRisk).

Die Werthaltigkeit und der rechtliche Bestand von Sicherheiten muss vor der Kreditgewährung überprüft werden. Wenn die Werthaltigkeit wesentlich von einem Dritten abhängt, ist das Kreditrisiko des Dritten zu bewerten (BTO 1.2.1, Tz. 3 und 4 MaRisk).

Kreditbearbeitungskontrolle

Es muss prozessabhängige Kontrollen geben, insbesondere bezüglich der Einhaltung der Kreditvergabekompetenzen (BTO 1.2.3 MaRisk).

Kreditweiterbearbeitung

Während der Vertragslaufzeit muss das Kreditinstitut das vertragskonforme Verhalten des Kreditnehmers überwachen. Bei zweckgebundenen Kreditvergaben ist zu kontrollieren, ob die valutierten Mittel der vereinbarten Verwendung zukommen (Kreditverwendungskontrolle) (BTO 1.2.2, Tz. 1 MaRisk).

Das Ausfallrisiko muss mindestens jährlich überprüft werden und die Sicherheitenüberprüfung in angemessenen Abständen erfolgen. Außerordentliche Überprüfungen sind vorzunehmen, wenn das Kreditinstitut Informationen von einer wesentlichen Verschlechterung der Risikoeinschätzung erhält (BTO 1.2.2, Tz. 3 und 4 MaRisk).

Intensivbetreuung

Das Kreditinstitut muss Kriterien festlegen, nach denen ein Engagement intensiv beobachtet werden muss. Diese Kriterien können nicht im Marktbereich entwickelt werden. Die der intensiven Beobachtung zugeführten Engagements müssen regelmäßig auf ihren Status hin untersucht werden (BTO 1.2.4 MaRisk):

– weitere Intensivbetreuung,

– Rückführung in die Normalbetreuung und

– Abgabe an die Sanierung oder Abwicklung (Rechtsabteilung).

Sanierung und Abwicklung

Bei einer erfolglosen Intensivbetreuung muss das Engagement ggf. saniert werden. Für den Übergang von der Intensivbetreuung zur Sanierung muss das Kreditinstitut interne Kriterien festlegen. Wenn ein Engagement ein Sanierungsfall wird, muss das Kreditinstitut vom Kreditnehmer ein Sanierungskonzept anfordern, welches die Chancen einer erfolgreichen Sanierung beurteilt (BTO 1.2.5, Tz. 1 bis 5 MaRisk).

Für den Fall der Abwicklung eines Engagements ist ein Abwicklungskonzept zu erstellen. In den Prozess der Verwertung der Sicherheiten sind Mitarbeiter oder ggf. externe Spezialisten mit entsprechenden Kenntnissen einzubeziehen (BTO 1.2.5, Tz. 6 MaRisk).

Risikovorsorge

Es müssen Kriterien festgelegt werden, nach denen wertberichtigt, abgeschrieben bzw. Rückstellungen zugeführt werden. Die Risikovorsorge ist zeitnah zu ermitteln (BTO 1.2.6 MaRisk).

Verfahren zur Früherkennung von Risiken

Jedes Kreditinstitut muss ein Verfahren zur Früherkennung von Risiken haben. In einfachen Fällen kann es auch ein um vorausschauende Elemente erweitertes Risikoklassifizierungsverfahren sein. Bei der Früherkennung geht es nicht darum, einen Ausfall so früh wie möglich zu erkennen. Vielmehr sollen Kunden, die möglicherweise Schwierigkeiten haben, ihre Raten zu zahlen, frühzeitig aus dem Gesamtbestand herausgefiltert werden. Die zu modulierende Wahrscheinlichkeit ist also keine Ausfallwahrscheinlichkeit, sondern die Wahrscheinlichkeit von Zahlungsstörungen (BTO 1.3 MaRisk).

Risikoklassifizierungsverfahren

Ein Kreditinstitut muss aussagekräftige Risikoklassifizierungsverfahren haben. Ergebnis dieser Verfahren sind die internen Ratings. Die Verwendung externer Bonitätseinschätzungen enthebt das Kreditinstitut nicht von seiner Verpflichtung, sich ein Urteil über das Adressenausfallrisiko zu bilden und dabei eigene Erkenntnisse und Informationen in die Kreditentscheidung einfließen zu lassen (BTO 1.2, Tz. 4 MaRisk). Die Risikoklassifizierungsverfahren dürfen nicht vom Marktbereich entwickelt worden sein. Darüber hinaus müssen die internen Ratings entscheidungsrelevant sein. Verwendung finden sollten sie unter anderem für:

– die Kreditentscheidung,

– die Bepreisung eines Kredits,

– die Bildung von Wertberichtigungen sowie

– die Kapitalunterlegung.

Wichtig ist außerdem, dass das Klassifizierungsverfahren sowohl auf quantitativen als auch auf qualitativen Kriterien basiert (BTO 1.4 MaRisk).

8 Anforderungen an das Handelsgeschäft

Handelsgeschäfte sind grundsätzlich alle Abschlüsse, die ein (AT 2.3, Tz. 3 MaRisk):

- Geldmarktgeschäft,
- Wertpapiergeschäft,
- Devisengeschäft,
- Geschäft in handelbaren Forderungen (z.B. Handel in Schuldscheinen),
- Geschäft in Waren oder
- Geschäft in Derivaten

zur Grundlage haben und die im eigenen Namen und für eigene Rechnung abgeschlossen werden. Als Wertpapiergeschäfte gelten auch Geschäfte mit Namensschuldverschreibungen sowie die Wertpapierleihe. Handelsgeschäfte sind auch Vereinbarungen von Rückgabe- oder Rücknahmeverpflichtungen sowie Pensionsgeschäfte.

Der gesamte Abschnitt basiert insbesondere auf Bankenaufsichtliches Risikomanagement – Grundlagen und Anwendung regulatorischer Anforderungen, 2018, S. 393 ff., Andrae, Silvio/Hellmich, Martin/Schmaltz, Christian, Stuttgart: Schäffer-Poeschel Verlag

8.1 Funktionstrennung

Die Trennung in Markt und Marktfolge aus dem Kreditgeschäft setzt sich im Handelsgeschäft fort, nur dass die Marktfolge „Abwicklung und Kontrolle“ genannt wird. Bei geringem Handelsvolumen muss die Trennung nicht bis zur Geschäftsleitungsebene durchgehalten werden (BTO 2.1 MaRisk).

8.2 Anforderungen an die Prozesse im Handel

Bei Abschluss des Geschäfts müssen alle Konditionen vereinbart worden sein und standardisierte Vertragstexte verwendet werden. Die Konditionen müssen marktgerecht sein. Nicht-marktgerechte Abschlüsse müssen die Ausnahme bleiben. Sie dürfen nur aufgrund des expliziten Kundenwunsches bzw. aufgrund interner Vorgaben erfolgen. In jedem Fall ist dem Kunden die Nicht-Marktgerechtigkeit offen zu legen. Die Geschäftsabschlüsse dürfen nur in begründeten Ausnahmefällen außerhalb des Handelsraums getätigt werden. Die Geschäfte sind unverzüglich zu erfassen, in der Position zu berücksichtigen und die Unterlagen an die Abwicklung und Kontrolle weiterzuleiten. Mitarbeiter des Handels dürfen auf Zahlungsverkehrskonten nur zusammen mit einem Mitarbeiter aus handelsunabhängigen Bereichen zugreifen können. Pro Jahr muss jeder Händler an mindestens zehn aufeinander folgenden Handelstagen nicht auf seine Handelsposition zugreifen dürfen. Während dieses Zeitraums wird die Position von einem anderen Händler geführt. Diese Regelung zielt darauf ab, Unregelmäßigkeiten aufzudecken, die ein einzelner Händler unter Umständen noch vertuschen kann (BTO 2.2.1 MaRisk).

8.3 Abwicklung und Kontrolle

Unmittelbar nach dem Abschluss müssen die Geschäftsbestätigungen und Abrechnungen durch die Abwicklung und Kontrolle ausgestellt werden. Die Bestätigungen sind unverzüglich und schriftlich an den Handelspartner zu schicken. Der unverzügliche Eingang der Gegenbestätigung ist zu überwachen und beim Ausbleiben gegebenenfalls zu reklamieren. Die Gegenbestätigung muss zuerst und auf direktem Wege in die Abwicklung gelangen. Auf die Gegenbestätigung kann verzichtet werden, wenn

– es ein automatisches Matching zwischen den Handelspartnern gibt,

– beide Handelspartner jederzeit Zugriff auf die Abschussdaten haben und diese Daten kontrolliert werden.

Die Handelsgeschäfte sind bezüglich der Vollständigkeit, Limite und Marktgerechtigkeit laufend zu kontrollieren. Unstimmigkeiten und Auffälligkeiten müssen durch einen handelsunabhängigen Bereich unverzüglich geklärt werden. Die im Handel ermittelten Positionen müssen mit den Positionen in nachgelagerten Systemen der Abwicklung, des Rechnungswesens und des Risikocontrollings abgeglichen werden. Zwischen- und Auffangkonten sind dabei besonders aufmerksam zu prüfen (BTO 2.2.2 und 2.2.3 MaRisk).

9 Vergütungssysteme

Kreditinstitute haben nach § 25a Abs. 1 S. 3 Nr. 6 KWG angemessene, transparente und auf eine nachhaltige Entwicklung des Instituts ausgerichtete Vergütungssysteme für Geschäftsleiter und Mitarbeiter einzurichten. Weitere Konkretisierungen hierzu finden sich in den §§ 25a Abs. 5 bis Abs. 5c und 25n KWG sowie in der Institutsvergütungsverordnung (InstitutsVergV) und der hierzu von der BaFin veröffentlichten Auslegungshilfe zur Institutsvergütungsverordnung in der Fassung vom 15. Februar 2018.

Die deutschen Rechtsvorschriften setzen die Vorgaben in der Capital Requirements Directive – CRD (Eigenkapitalrichtlinie, Richtlinie 2013/36/EU) sowie den der EBA-Leitlinien für eine solide Vergütungspolitik (EBA/GL/2015/22) um. Für die Identifikation der Risikoträger als Adressaten bestimmter Anforderungen und zur Regelung der Anforderungen an die als variable Vergütung in Betracht kommenden Instrumente bestehen unmittelbar anzuwendende Verordnungen der EU-Kommission.

Die InstitutsVergV enthält neben einem für alle Institute anwendbaren allgemeinen Teil Anforderungen, die lediglich auf bedeutende Institute im Sinne der Vorschrift anwendbar sind. Der allgemeine Teil regelt neben Definitionen u.a. des Vergütungsbegriffs insbesondere

– Anforderungen an die Verantwortlichkeiten für die Vergütungsstrategie und Vergütungssysteme,

– das Erfordernis einer regelmäßigen Überprüfung der Vergütungssysteme unter Beteiligung der Kontrolleinheiten,

– die Verpflichtung zur Einrichtung eines transparenten und nachvollziehbaren Verfahrens zur Ermittlung des Gesamtbetrags der variablen Vergütungen (Bonuspool) unter Berücksichtigung der regulatorischen Kennzahlen sowie

– die Verpflichtung zur Offenlegung von Angaben zur Vergütung.

Die Regulierung betrifft grundsätzlich nur die variable Vergütung, während die Kreditinstitute die fixe Vergütung weitgehend frei festlegen können. Durch einen so genannten Bonus Cap wird die variable Vergütung grundsätzlich auf jeweils 100% der fixen Vergütung für jeden einzelnen Geschäftsleiter oder Mitarbeiter begrenzt; durch Beschluss der Anteilseigner ist eine Anhebung auf bis zu 200% möglich (§ 25a Abs. 5 KWG).

Kreditinstitute, deren Bilanzsumme im Durchschnitt zu den jeweiligen Stichtagen der letzten drei abgeschlossenen Geschäftsjahre 15 Mrd. € erreicht oder überschritten hat, gelten nach § 25n KWG grundsätzlich als bedeutende Institute. Sie sind nach § 25a Abs. 5b verpflichtet, auf der Grundlage einer Risikoanalyse so genannte Risikoträger zu ermitteln, zu denen insbesondere auch die Geschäftsleiter gehören. Für die Risikoträger bestehen besondere Anforderungen an das Verfahren zur Bemessung der variablen Vergütung (Ex-ante-Risikoadjustierung nach § 19 InstitutsVergV). Zur Ex-post-Risikoadjustierung der Vergütung von Risikoträgern sind nach § 20 InstitutsVergV

– von der variablen Vergütung – u.a. abhängig von Stellung, Aufgaben und Höhe der variablen Vergütung – zwischen 40 bis 60% einzubehalten und über einen Zurückbehaltungszeitraum von drei bis fünf Jahren auszuzahlen, sofern eine nachträgliche Überprüfung bestätigt, dass die ursprüngliche Ermittlung der variablen Vergütung gemäß § 19 InstitutsVergV auch rückblickend noch zutreffend erscheint; im Fall einer negativen Abweichung des Überprüfungsergebnisses ist die zurückbehaltene variable Vergütung entsprechend zu reduzieren (Nachhaltigkeitskomponente),

– für mindestens 50% der variablen Vergütung Instrumente, die den Wert bzw. die Bonität des Kreditinstituts nachhaltig widerspiegeln und die jeweils eine Sperrfrist von mindestens einem Jahr haben, zu vereinbaren,

– Vereinbarungen über die Möglichkeit einer Rückforderung der variablen Vergütung (Claw Back) für den Zeitraum von zwei Jahren nach der Auszahlung zu treffen.

Auf diese Weise soll sichergestellt werden, dass die Kreditinstitute die Möglichkeit einer rückwirkenden Vergütungsanpassung aufgrund nachträglich erkannter negativer Entwicklungen haben.

Weiterführende Informationen enthält der Kartenstapel „Vorstandsvergütung in Banken“.

Dieser Abschnitt basiert insbesondere auf Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, 2020, S. 924 f., Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.), Düsseldorf: IDW Verlag GmbH

10 Weitere Komponenten einer ordnungsgemäßen Geschäftsorganisation

10.1 Managementinformationssystem

Nach § 25a Abs. 1 Satz 6 Nr. 1 KWG sind angemessene Regelungen zu implementieren, anhand derer sich die finanzielle Lage des Kreditinstituts jederzeit mit hinreichender Genauigkeit bestimmen lässt. Die finanzielle Lage umfasst die Liquiditäts-, Vermögens- und Ertragslage.

Die konkrete Ausgestaltung des Managementinformationssystems hängt von Art und Umfang der betriebenen Geschäfte, der Risikobereitschaft des Kreditinstituts, seiner finanziellen Situation und von externen Faktoren ab. Das hat zur Konsequenz, dass das Managementinformationssystem fortlaufend daraufhin zu untersuchen ist, ob es in seiner konkreten Ausgestaltung sachgerecht ist oder ob Anpassungen aufgrund veränderter Rahmenbedingungen erforderlich sind.

10.2 Hinweisgebersystem

Eine ordnungsgemäße Geschäftsorganisation umfasst darüber hinaus einen Prozess, der es den Mitarbeitern unter Wahrung der Vertraulichkeit ihrer Identität ermöglicht, Verstöße gegen die CRR oder gegen das KWG oder gegen aufgrund des KWG erlassene Rechtsverordnungen sowie etwaige strafbare Handlungen innerhalb des Unternehmens an geeigneter Stelle zu berichten (Hinweisgebersystem oder Whistleblowing) (§ 25a Abs. 1 Satz 6 Nr. 2 KWG).

Ein Hinweisgebersystem ist hilfreich, um Fehlverhalten insbesondere auf Managementebene zu begegnen. Es ermöglicht Mitarbeitern die anonyme, sanktionsfreie Weitergabe von Informationen. Dies soll eine offene Kommunikationskultur nicht ersetzen, sondern lediglich ergänzen.

Die Stelle muss nicht unbedingt innerhalb des Kreditinstituts angesiedelt sein, es ist auch möglich, dass diese Funktion beispielsweise durch einen beauftragten Rechtsanwalt wahrgenommen wird. Ergänzend haben die Kreditinstitute sicherzustellen, dass diesen Meldungen Beachtung geschenkt wird, d.h. den Hinweisen nachgegangen wird und gegebenenfalls erforderliche Konsequenzen aus den festgestellten Verstößen gezogen bzw. Verbesserungsmaßnahmen eingeleitet werden.

11 Risikomanagement auf Gruppenebene

Soweit Geschäftsleiter in ihrer Funktion für ein übergeordnetes Unternehmen einer Institutsgruppe oder einer Finanzholding-Gruppe verantwortlich sind, erstreckt sich die Verantwortung auf die angemessene Ausgestaltung des Risikomanagements in der Gruppe. Im Einzelnen bedeutet dies, dass zumindest Vorgaben und Leitlinien für die Ausgestaltung der

Risikomanagement-Organisation zu formulieren sind, auf deren Umsetzung i.d.R. mit gesellschaftsrechtliche Möglichkeiten hingewirkt werden muss (§ 25a Abs. 3 KWG, AT 4.5 MaRisk).

Verantwortlich für das Risikomanagement auf Gruppenebene sind die Geschäftsleiter des übergeordneten Unternehmens.

Die besonderen Funktionen sollten auch auf Gruppenebene angesiedelt sein, d.h. in Form einer Konzernrevision, eines gruppenweiten Risikocontrollings und einer gruppenweiten Compliance-Funktion.

Das Managementinformationssystem ist gruppenweit aufzubauen. Ebenso muss gewährleistet sein, dass die Auswirkungen einer plötzlichen und unerwarteten Zinsänderung auf die Anlagenbuchinstrumente gruppenweit betrachtet werden.

Ebenso muss für alle gruppenangehörigen Unternehmen ein Hinweisgebersystem bestehen.

12 Quellenverzeichnis und weiterführende Literatur

Andrae, Silvio/Hellmich, Martin/Schmaltz, Christian: Bankenaufsichtliches Risikomanagement – Grundlagen und Anwendung regulatorischer Anforderungen, Stuttgart: Schäffer-Poeschel Verlag, 2018.

Brixner, Joachim/Schaber, Mathias: Bankenaufsicht – Institutionen, Regelungsbereiche und Prüfung, Stuttgart: Schäffer-Poeschel Verlag, 2016.

Bopp, Robert E./Weber, Max: Sustainable Finance – Auswirkungen des Klimawandels auf das Risikomanagement von Banken, Stuttgart: Schäffer-Poeschel Verlag, 2020.

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ➔I Auslegungshilfe zur Institutsvergütungsverordnung 2018

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ➔I Bankaufsichtliche Anforderungen an die IT (BAIT) 2017

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ➔I Merkblatt zum Umgang mit Nachhaltigkeitsrisiken 2020

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ➔I Mindestanforderungen an das Risikomanagement - MaRisk 2017

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ➔I Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten - MaComp 2018

Deutsches Rechnungslegungs Standards Committee e.V. (Hrsg.): Deutsche Rechnungslegungs Standards (DRS), Stuttgart: Schäffer-Poeschel Verlag, 2020.

Hopt, **Klaus J./Binder, Jens-Hinrich/Böcking, Hans-Joachim**: Handbuch Corporate Governance von Banken und Versicherungen, 2. Auflage, München: Verlag C. H. Beck, 2020.

Institut der Wirtschaftsprüfer in Deutschland e.V. (Hrsg.): Kreditinstitute, Finanzdienstleister und Investmentvermögen - Rechnungslegung und Prüfung, Düsseldorf: IDW Verlag GmbH, 2020.

Ansprechpartnerin im I.M.U.

Maxi Leuchters

Über die Autorin

Wirtschaftsprüferin Steuerberaterin Dipl.-Wirtschafts-ingenieurin Christiane Kohs, Geschäftsführerin der CARA GmbH Wirtschaftsprüfungsgesellschaft, Berlin, und Inhaberin einer Steuerberaterpraxis. Sie ist Sachverständige auf den Gebieten der nationalen und internationalen Rechnungslegung sowie des Steuerrechts und berät in wirtschaftlichen Angelegenheiten u.a. Arbeitnehmervertreter im Aufsichtsrat.

Kontakt

Impressum

Erschienen im Mitbestimmungsportal, dem Infoservice der Hans-Böckler-Stiftung für die Mitbestimmungspraxis.

Online-Fassung und weitere Themen unter www.mitbestimmung.de

Kontakt:
Michael Stollt
Hans-Böckler-Stiftung
Georg-Glock-Straße 18
40474 Düsseldorf
mitbestimmungsportal@boeckler.de

Hans-Böckler-Stiftung,
März 2021