ZAG-MaRisk: Die neuen Spielregeln für ZAG-Institute

Delta-Betrachtung und strategische Handlungsfelder

Dominik Siebert
Carola Bader
Muskaan Multani

Juni 2024
Blogpost

Key Facts

- Am 27. Mai 2024 veröffentlichte die BaFin die ZAG-MaRisk, die sofort in Kraft treten und Zahlungs- sowie E-Geld-Institute betreffen
- Die Institute müssen ihre Geschäftsprozesse und Risikomanagementsysteme umgehend überprüfen und anpassen, denn ein umfassendes Risikomanagement, einschließlich ESG-Risiken, ist nun auch für Zahlungs- und E-Geld-Institute vorgeschrieben
- ZAG-MaRisk orientieren sich eng an den MaRisk (BA), enthalten jedoch spezifische Anpassungen für Zahlungs- und E-Geld-Institute
- ZAG-Institute, die Ihre Organisation bereits an den MaRisk Anforderungen orientiert haben, müssen somit dennoch aktiv werden, da es keine vollständige Deckung zwischen den Anforderungen gibt
- ZAG-Instituten ist empfohlen, umgehend eine Gap-Analyse durchzuführen und die Umsetzung von fehlenden Anforderungen zu initiieren

Hintergrund

Am 27. Mai 2024 hat die BaFin die finalen Mindestanforderungen an das Risikomanagement für ZAG-Institute (ZAG-MaRisk) bekanntgegeben. Diese neuen Regelungen beziehen nun auch Zahlungs- und E-Geld-Institute ein, die bisher nicht den umfassenden MaRisk (BA)[1] unterlagen. Aufgrund der sofortigen Gültigkeit und der möglichen Sanktionen ist es zwingend erforderlich, dass betroffene Institute ihre Geschäftsprozesse und ihr Risikomanagement umgehend überprüfen und gegebenenfalls anpassen. Auch wenn die MaRisk (BA) für Zahlungsdienstleister nicht verbindlich galten, haben einige ZAG-Institute diese als Orientierung bei der Etablierung der eigenen Risikomanagementprozesse genutzt und könnten nun davon ausgehen, bereits alle Anforderungen der ZAG-MaRisk zu erfüllen. Da die MaRisk (BA) und die ZAG-MaRisk sich jedoch stellenweise unterscheiden, ist eine detaillierte Deltabetrachtung notwendig.

Von Unsicherheit zu Klarheit: Ziel der neuen ZAG-MaRisk-Regelungen

Zahlungs- und E-Geld-Institute sind gemäß dem Zahlungsdiensteaufsichtsgesetz (ZAG) zu einer ordnungsgemäßen Geschäftsorganisation verpflichtet. Bislang war diese Anforderung im nationalen Recht jedoch nur allgemein in § 27 ZAG enthalten. Die Aufsicht nutzte häufig die MaRisk (BA), die für Kreditinstitute und Finanzdienstleistungsinstitute gelten, als Orientierungspunkt für ZAG-Institute. Diese Praxis führte jedoch zu Unsicherheiten und Interpretationsspielräumen, da die MaRisk (BA) keine formale Geltung für ZAG-Institute hatten.

Obwohl die MaRisk (BA) grundsätzlich nicht auf Zahlungs- und E-Geld-Institute (ZAG-Institute) anwendbar sind, bieten sie dennoch Hinweise auf die Anforderungen, die im Rahmen einer ordnungsgemäßen Geschäftsorganisation gemäß § 27 Abs. 1 ZAG gefordert werden. Am 27. September 2023 hat die BaFin diese Anforderungen konkretisiert und den Entwurf des Rundschreibens zu ZAG-MaRisk zur öffentlichen Konsultation vorgelegt.

Mit der Veröffentlichung der finalen Version der ZAG-MaRisk am 27. Mai 2024, hat die BaFin nun einen praxisnahen Rahmen geschaffen, der es Zahlungsinstituten und E-Geld-Instituten ermöglicht, ihre Geschäftsorganisation entsprechend den neuen Anforderungen zu gestalten. Dies soll Unsicherheiten beseitigen und einen klaren Handlungsrahmen bieten, der die Institute bei der Einhaltung der regulatorischen Vorgaben unterstützt.

Die neuen Regelungen gelten für alle inländischen Zahlungs- und E-Geld-Institute sowie für inländische Zweigstellen von Unternehmen mit Sitz außerhalb der EU oder des EWR, die Zahlungsdienste anbieten oder im E-Geld-Geschäft tätig sind. Zusätzlich gelten sie für Zweigstellen deutscher Institute im Ausland. Jedoch sind Zweigstellen von Unternehmen aus anderen EWR-Staaten gemäß § 39 ZAG von diesen Anforderungen ausgenommen.

[1] Bankaufsichtliche Anforderungen: Mindestanforderungen an das Risikomanagement

ZAG-MaRisk unter der Lupe: die Anforderungen im Detail

Die Struktur der ZAG-MaRisk gliedert sich in zwei Hauptbereiche: den allgemeinen Teil (Modul AT) und den besonderen Teil (Modul BT).

Im **Allgemeinen Teil (Modul AT)** befinden sich grundlegende Prinzipien für die Ausgestaltung des Risikomanagements, die für alle Zahlungs- und E-Geld-Institute gelten. Dieser Teil legt die Basis für eine einheitliche und umfassende Risikomanagementstrategie.

Der **Besondere Teil (Modul BT)** enthält spezifische Anforderungen an die Organisation der Institute, insbesondere Anforderungen an das interne Kontrollsystem (BT 1), an die Ausgestaltung der Internen Revision (BT 2) und an die Risikoberichtserstattung (BT 3).

Wie in den MaRisk (BA) sind grundsätzlich zahlreiche Öffnungsklauseln inkludiert, die abhängig von Komplexität der Geschäftsaktivitäten und der Risikosituation eine vereinfachte Umsetzung ermöglichen.

Abbildung 1: Übersicht der Anforderungen der ZAG-MaRisk

i. Anwendungsbereich (AT 2)

Die ZAG-MaRisk stellt konkrete Anforderungen für Zahlungs- und E-Geld Institute. Dies soll dazu beitragen, Missstände zu verhindern, die die Sicherheit der anvertrauten Vermögenswerte gefährden könnten. Zudem soll sie sicherstellen, dass Zahlungsdienste und E-Geld-Geschäfte ordnungsgemäß durchgeführt werden und keine erheblichen Nachteile für die Gesamtwirtschaft entstehen.

ii. Gesamtverantwortung der Geschäftsleitung (AT 3)

Alle Geschäftsleiter (§ 1 Abs. 8 ZAG) tragen die Verantwortung für die ordnungsgemäße Geschäftsorganisation und deren Weiterentwicklung, einschließlich ausgelagerter Aktivitäten und Prozesse. Dies umfasst die Beurteilung und Begrenzung von Risiken sowie die Förderung einer angemessenen Risikokultur. Jeder Geschäftsleiter ist zudem für die Einrichtung und Überwachung angemessener Kontrollprozesse in seinem Zuständigkeitsbereich verantwortlich.

iii. Allgemeine Anforderungen an das Risikomanagement (AT 4)

1. Ganzheitliches Risikomanagement (AT 4.1)

Institute müssen regelmäßig eine umfassende Risikoinventur durchführen, die auch ESG-Risiken (Environmental, Social, Governance) berücksichtigt. Dies umfasst die systematische Erfassung aller potenziellen Risiken, die das Institut betreffen könnten. Diese Risiken werden sowohl qualitativ als auch quantitativ bewertet, um deren Ausmaß und Wahrscheinlichkeit zu bestimmen sowie ihre potenziellen Auswirkungen auf das Institut zu quantifizieren. Anschließend sind Maßnahmen zur Steuerung dieser Risiken zu implementieren und deren Entwicklung kontinuierlich zu überwachen.

2. Klare Strategien (AT 4.2)

ZAG-Institute müssen klare Geschäfts- und Risikostrategien entwickeln und dokumentieren. Diese Strategien sollen sowohl externe als auch interne Faktoren berücksichtigen. Externe Faktoren umfassen Marktbedingungen, regulatorische Änderungen und technologische Entwicklungen, während interne Faktoren die Unternehmensstruktur, Geschäftsmodelle und internen Prozesse umfassen. Die Strategien müssen detaillierte Maßnahmen zur Steuerung und Minimierung der identifizierten Risiken definieren und sicherstellen, dass die strategischen Ziele erreicht werden.

3. Effektives Kontrollsystem (AT 4.3)

Ein effektives Kontrollsystem zur Einhaltung der gesetzlichen Anforderungen muss umgesetzt werden. Die neuen Regelungen betonen die Notwendigkeit der Trennung unvereinbarer Tätigkeiten, um Interessenkonflikte zu vermeiden. Klare Zuständigkeitsregelungen müssen etabliert, und die Risikosteuerungs- und -controllingprozesse müssen regelmäßig überprüft und angepasst werden. Stresstests sind ein weiteres wichtiges Element, die regelmäßig durchgeführt und ausgewertet werden müssen, um die Risikotragfähigkeit unter verschiedenen Szenarien zu bewerten.

4. Einrichtung einer unabhängigen Überwachungsfunktionen (AT 4.4)

Die ZAG-MaRisk verlangen die Einrichtung unabhängiger Überwachungsfunktionen. Dies beinhaltet das Risikocontrolling, das unabhängig vom operativen Geschäft sein muss, sowie die

Compliance-Funktion, die sicherstellt, dass alle gesetzlichen und regulatorischen Anforderungen erfüllt werden. Diese Interne Revision prüft unabhängig und risikoorientiert die Angemessenheit und Wirksamkeit des Risikomanagements und des internen Kontrollsystems und berichtet direkt an die Geschäftsleitung und das Aufsichtsorgan.

iv. Organisationsrichtlinien (AT 5)

Organisationsrichtlinien müssen regelmäßig erstellt, aktualisiert und effektiv kommuniziert werden, um eine klare Struktur und Transparenz innerhalb des Instituts zu gewährleisten. Diese Richtlinien sollen alle relevanten Geschäftsbereiche abdecken und klare Regelungen zur Aufbau- und Ablauforganisation enthalten. Diese Richtlinien müssen regelmäßig überprüft und an neue regulatorische Anforderungen und Marktbedingungen angepasst werden. Zudem ist sicherzustellen, dass alle Mitarbeiter über die aktuellen Richtlinien informiert sind.

v. Umfassende Dokumentation (AT 6)

Eine systematische und nachvollziehbare Dokumentation aller relevanten Unterlagen ist erforderlich. Diese Dokumentation muss mindestens fünf Jahre lang aufbewahrt werden und sicherstellen, dass alle relevanten Informationen im Falle einer Prüfung verfügbar sind.

vi. Zuverlässiges Ressourcenmanagement (AT 7)

Institute müssen sicherstellen, dass ausreichend qualifizierte Mitarbeiter zur Verfügung stehen und dass die technisch-organisatorische Ausstattung regelmäßig überprüft und bei Bedarf angepasst wird. Notfallpläne müssen erstellt und regelmäßig überprüft werden, um sicherzustellen, dass das Institut im Falle eines Notfalls schnell und effektiv reagieren kann.

vii. Flexible Anpassungsprozesse (AT 8)

Institute müssen in der Lage sein, flexibel auf Veränderungen zu reagieren. Dazu gehören Konzepte zur Risikoanalyse und -bewertung neuer Produkte oder Märkte, die regelmäßig überprüft werden müssen. Geplante wesentliche Änderungen in der Organisation und IT-Systemen müssen analysiert und bewertet werden, und die Risiken bei Übernahmen oder Fusionen müssen eingeschätzt und die Strategien entsprechend angepasst werden.

viii. Überwachung von Auslagerungen (AT 9)

Die neuen Anforderungen legen besonderen Wert auf die Überwachung von Auslagerungen durch ZAG-Institute. Dienstleistungen oder Waren, die einmalig oder gelegentlich bezogen werden und typischerweise von beaufsichtigten Unternehmen stammen, die sie selbst nicht erbringen können, werden weiterhin nicht als Auslagerung betrachtet. Es liegt in der Verantwortung der Institute, durch eigene Risikoanalysen zu bestimmen, wie diese Leistungen zu qualifizieren sind. Bei einfachen Auslagerungen müssen die allgemeinen Anforderungen des

ZAG für eine ordnungsgemäße Geschäftsorganisation eingehalten werden. Bei wesentlichen Auslagerungen hingegen sind umfassendere Pflichten zu erfüllen.

Es bleibt zwingend erforderlich, dass die Leitungsaufgaben der Geschäftsführung nicht ausgelagert werden können. Hierbei muss stets sichergestellt sein, dass die aufsichtsrechtlichen Pflichten eingehalten werden und der Auslagerungsdienstleister den Weisungen des beaufsichtigten Instituts unterliegt.

ix. Spezifische Anforderungen an Zahlungsdienste E-Geld-Geschäfte (BTO 1 bis 3)

Die neuen ZAG-MaRisk formulieren spezifische Anforderungen für Zahlungsdienste und E-Geld-Geschäfte, die sich auf drei Hauptbereiche konzentrieren:

Der erste Aspekt betrifft die Sicherung von Haftungsfällen, einschließlich der Verwaltung von Treuhandkonten und der Einführung geeigneter Kontrollmechanismen (BTO 1). Das neue Rundschreiben berücksichtigt dabei, dass Zahlungs- und E-Geldinstitute im Gegensatz zu Kreditinstituten nicht berechtigt sind, Kundengelder zu halten. Um den gesetzlichen Sicherungsanforderungen zu entsprechen, bietet das ZAG den Instituten drei Optionen: die Hinterlegung auf einem Treuhandkonto, die Anlage in sichere liquide Aktiva mit niedrigem Risiko nach Abstimmung mit der BaFin oder die Absicherung durch eine Versicherung oder gleichwertige Garantie. Die BaFin konkretisiert im Rundschreiben die Anforderungen, die ein Treuhandkonto erfüllen muss. Diese Vorgaben zielen darauf ab, eine klare Trennung zwischen Kunden- und Institutsgeldern zu gewährleisten, um den Schutz der Kundengelder sicherzustellen und eine Vermischung zu verhindern.

Zweitens konkretisiert die BaFin die Anforderungen an den Umgang mit betrügerischen Handlungen, Sicherheitsvorfällen und Kundenbeschwerden (BTO 2). ZAG-Institute müssen organisatorische Maßnahmen und Verfahren implementieren, die eine effektive Betrugsprävention gewährleisten und sicherstellen, dass auf Sicherheitsvorfälle sowie sicherheitsbezogene Kundenbeschwerden schnell und angemessen reagiert wird. Dies beinhaltet die Überwachung und Handhabung von Sicherheitsvorfällen sowie die Einleitung notwendiger Maßnahmen. Zusätzlich müssen Institute eine geeignete Kontaktstelle für sicherheitsrelevante Kundenbeschwerden einrichten, die Beschwerden zeitnah und wirksam bearbeiten kann. ZAG-Institute müssen ferner Verfahren zur Erfüllung der gesetzlichen Meldepflichten einrichten und dokumentieren, um Interessenskonflikte im Meldeprozess zu vermeiden.

Drittens beziehen sich die Anforderungen auf die Inanspruchnahme von Agenten, wobei die Zuverlässigkeit und Eignung der Agenten sowie die Erfüllung gesetzlicher Vorgaben im Fokus stehen (BTO 3). Die dargestellten Anforderungen betreffen im Wesentlichen die organisatorischen Regelungen beim Einsatz von Agenten und wiederholen weitgehend die bereits im ZAG festgelegten Regelungen.

Deltabetrachtung ZAG-MaRisk und MaRisk (BA): Wo liegen die Unterschiede?

Während es zwischen beiden Rundschreiben aufgrund der Anlehnung aneinander große inhaltliche Überschneidungen in den Anforderungen gibt, lassen sich wesentliche Unterschiede im Detail erkennen, die ZAG-Institute nicht außer Acht lassen dürfen, um Rechtskonformität mit den ZAG-MaRisk sicherzustellen. Diese Unterschiede lassen sich sowohl im Modul AT als auch Modul BT identifizieren.

Delta Betrachtung: In der Ausgestaltung des Risikomanagements unterscheiden sich die ZAG-MaRisk nur in Details zu den MaRisk (BA)

Erleichterungen in ZAG-MaRisk | Gleiches Anforderungslevel | Erweiterte Anforderungen in ZAG-MaRisk

ZAG-MaRisk	MaRisk (BA)	Wesentliche Unterschiede	Vergleich
I AT 2 Anwendungsbereich	AT 2 Anwendungsbereich	ZAG-MaRisk gilt für Zahlungs- und E-Geld-Institute, MaRisk (BA) für Kredit- und Finanzdienstleistungsinstitute	=
II AT 3 Gesamtverantwortung der Geschäftsleitung	AT 3 Gesamtverantwortung der Geschäftsleitung	MaRisk (BA) dehnt Verantwortung der Geschäftsleiter auch auf die Gruppenebene und Finanzholding-Gruppen aus	+
III AT 4 Allgemeine Anforderungen an das Risikomanagement	AT 4 Allgemeine Anforderungen an das Risikomanagement	• AT 4.1: ZAG-MaRisk fokussiert auf Abschirmung von Risiken, MaRisk (BA) detailliert Risikotragfähigkeit • AT 4.3.4 Datenmanagement, Datenqualität, und Aggregation von Risikodaten, AT 4.3.5 Verwendung von Modellen und AT 4.5 Risikomanagement auf Gruppenebene aus MaRisk (BA) in ZAG-MaRisk nicht enthalten • Unterschiede liegen in der Spezifikation der Anforderungen an Zahlungs- und E-Geld-Institute	+
IV AT 5 Organisationsrichtlinien	AT 5 Organisationsrichtlinien	MaRisk (BA) verlangt Risikodatenaggregation, ZAG-MaRisk den Umgang mit sensiblen Zahlungsdaten	=
V AT 6 Dokumentation	AT 6 Dokumentation	-	=
VI AT 7 Ressourcen	AT 7 Ressourcen	ZAG-MaRisk erlaubt den Notfallbericht durch den Informationssicherheitsbeauftragten	+
VII AT 8 Anpassungsprozesse	AT 8 Anpassungsprozesse	AT 8.1 MaRisk (BA) erfordert eine Testphase und detailliertere Prüfungen bei Fehlern im Neu-Produkt-Prozess, während ZAG-MaRisk allgemeinere Anforderungen an die Einbindung von Organisationseinheiten und Kontrollfunktionen stellt	+
VIII AT 9 Auslagerung	AT 9 Auslagerung	MaRisk (BA) erlaubt vollständige Auslagerung der Internen Revision unter bestimmten Bedingungen, während ZAG-MaRisk dies nicht erlaubt und strengere IT-Sicherheits- und Dokumentationsanforderungen hat	!

Abbildung 2: Deltabetrachtung Allgemeiner Teil zwischen den ZAG-MaRisk und den MaRisk

Neben dem offensichtlichen Unterschied der Anwendungsbereiche (AT 2) von MaRisk (BA) und ZAG-MaRisk, gibt es weitere wesentliche Unterschiede: Bei der Gesamtverantwortung der Geschäftsleitung (AT 3) erweitern die MaRisk (BA) die Verantwortung der Geschäftsleiter auch auf die Gruppenebene und Finanzholding-Gruppen, während die ZAG-MaRisk diesen Aspekt nicht berücksichtigen. Dies bedeutet, dass die ZAG-MaRisk weniger umfassende Anforderungen an die organisatorische Struktur der Geschäftsleitung stellen.

Die allgemeinen Anforderungen an das Risikomanagement (AT 4) zeigen weitere Unterschiede auf. Während die ZAG-MaRisk sich auf die Abschirmung von Risiken fokussieren, bieten die MaRisk (BA) detaillierte Vorgaben zur Risikotragfähigkeit. Zudem enthalten die MaRisk (BA) spezielle Anforderungen an das Datenmanagement, die Datenqualität und die Aggregation von Risikodaten (AT 4.3.4) sowie an die Verwendung von Modellen (AT 4.3.5) und das Risikomanagement auf Gruppenebene (AT 4.5). Diese spezifischen Anforderungen fehlen in den ZAG-MaRisk vollständig, was die unterschiedlichen Schwerpunkte der beiden Regelwerke verdeutlicht. Für ZAG-Institute gibt es hier somit eine Erleichterung der Anforderungen bezüglich des Umgangs mit Daten.

Die Regelungen zu den Organisationsrichtlinien (AT 5) unterscheiden sich ebenfalls. MaRisk (BA) verlangen eine detaillierte Risikodatenaggregation, während die ZAG-MaRisk den Umgang mit

sensiblen Zahlungsdaten stärker betonen. Dies zeigt sich insbesondere in den Anforderungen an die Dokumentation und den Schutz dieser Daten.

Bei den Anforderungen zu Ressourcen (AT 7) erlaubt ZAG-MaRisk die Berichterstattung durch den Informationssicherheitsbeauftragten, was in den MaRisk (BA) nicht vorgesehen ist.

Im Bereich der Anpassungsprozesse (AT 8) verlangen die MaRisk (BA) eine detaillierte Testphase und Prüfungen bei Fehlern im Neu-Produkt-Prozess, während die ZAG-MaRisk allgemeinere Anforderungen an die Einbindung von Organisationseinheiten und Kontrollfunktionen stellen.

Schließlich erlauben die MaRisk (BA) unter bestimmten Bedingungen die vollständige Auslagerung der Internen Revision, während dies bei den ZAG-MaRisk nicht gestattet ist. Die ZAG-MaRisk legen strengere IT-Sicherheits- und Dokumentationsanforderungen fest, um sicherzustellen, dass die spezifischen Risiken im Zahlungs- und E-Geld-Bereich angemessen adressiert werden.

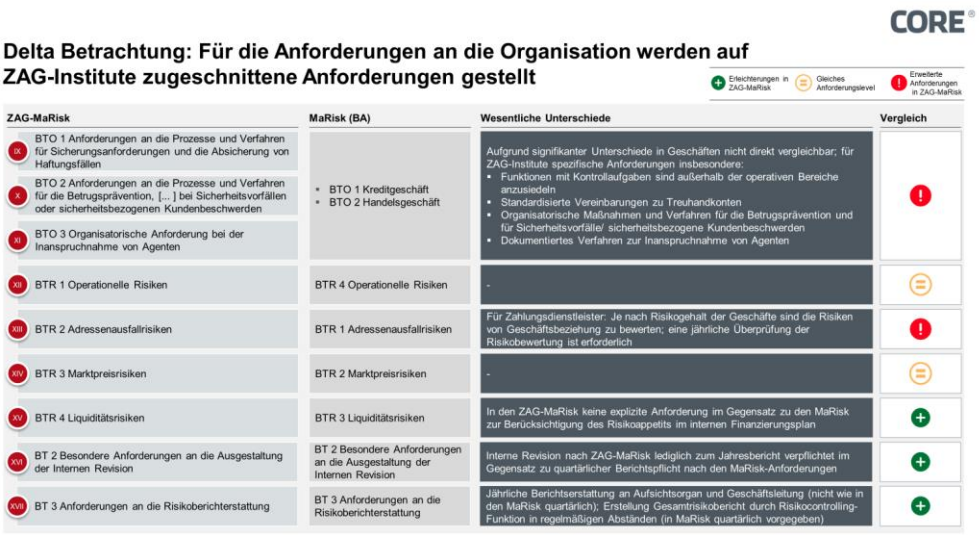

Abbildung 1: Deltabetrachtung Besonderer Teil zwischen den ZAG-MaRisk und den MaRisk

Besonders deutlich werden die Unterschiede im Bereich der speziellen Anforderungen (Modul BT). Die ZAG-MaRisk umfassen Anforderungen an die Prozesse und Verfahren für Sicherungsanforderungen und die Absicherung von Haftungsfällen (BTO 1), die MaRisk (BA) hingegen nicht. Weiterhin legen die ZAG-MaRisk detaillierte Anforderungen an die Betrugsprävention und den Umgang mit Sicherheitsvorfällen und Kundenbeschwerden (BTO 2) fest. Zudem definieren sie organisatorische Anforderungen bei der Inanspruchnahme von Agenten (BTO 3), was bei MaRisk (BA) keine direkte Entsprechung findet.

Auch im Umgang mit operationellen Risiken (BTR 1) und Adressenausfallrisiken (BTR 2) gibt es Unterschiede. Für Zahlungsdienstleister ist es erforderlich, die Risiken je nach Risikogehalt der

Geschäfte zu bewerten und jährlich zu überprüfen. Diese spezifischen Anforderungen sind in den MaRisk (BA) nicht enthalten.

Im Bereich der Risikoberichterstattung unterscheiden sich die MaRisk (BA) und ZAG-MaRisk ebenfalls. In den MaRisk (BA) müssen Risikoberichte insbesondere die Ergebnisse der Stresstests und deren potenzielle Auswirkungen auf die Risikosituation und das Risikodeckungspotenzial darstellen. Ebenso müssen die den Stresstests zugrunde liegenden wesentlichen Annahmen und die potenziellen Auswirkungen von Risikokonzentrationen gesondert dargestellt werden. Diese konkreten Anforderungen sind in den ZAG-MaRisk nicht geregelt. Hier besteht lediglich die Pflicht Risikoberichte zu erstellen, die nicht nur die Risikosituation darstellen, sondern auch bewerten. Die Berichte sollen auf vollständigen, genauen und aktuellen Daten basieren und eine zukunftsorientierte Risikoeinschätzung enthalten, die über aktuelle und historische Daten hinausgeht. Bei Bedarf sind in den Risikoberichten auch Handlungsvorschläge, beispielsweise zur Risikoreduzierung, zu integrieren.

Eine wesentliche Erleichterung findet sich für ZAG-Institute in der Frequenz der Berichtserstattung. Während nach den MaRisk (BA) die Geschäftsleitung das Aufsichtsorgan mindestens vierteljährlich über die Risikosituation informieren muss, kommt auf ZAG-Institute diese Pflicht nur jährlich zu. Auch die Interne Revision ist lediglich zu einem Jahresbericht nach den ZAG-MaRisk verpflichtet und nicht quartärlich wie in den MaRisk gefordert. Für den Gesamtrisikobericht der Risikocontrolling-Funktion wird gänzlich auf eine Frequenzvorgabe verzichtet. In den ZAG-MaRisk ist lediglich von „in angemessenen Abständen“ die Rede während in den MaRisk (BA) klar auch hier quartärliche Berichte gefordert werden.

Fazit

Die Veröffentlichung der ZAG-MaRisk durch die BaFin stellt einen bedeutenden Meilenstein für Zahlungs- und E-Geld-Institute dar, indem sie erstmals eine klare und verbindliche Richtlinie zur ordnungsgemäßen Geschäftsorganisation liefert. Diese neuen Regelungen, die speziell auf die Geschäftsmodelle und Risikoprofile dieser Institute zugeschnitten sind, betonen die Notwendigkeit einer umfassenden Risikoabschirmung, insbesondere in Bezug auf operative, Liquiditäts- und Geschäftsmodellrisiken. Darüber hinaus gewinnen Themen wie Sicherungsanforderungen und Auslagerungsmanagement zunehmend an Bedeutung.

Die Implementierung dieser Vorschriften erfordert eine gründliche Überprüfung und Anpassung der bestehenden Geschäftsprozesse. Hier sollten ZAG-Institute umgehend eine Gap-Analyse durchführen, um Lücken in Ihrem Risikomanagement zu identifizieren und Maßnahmen abzuleiten. Wie die Deltabetrachtung zeigt, sind selbst Institute, die bereits alle Anforderungen der MaRisk erfüllen zum Handeln verpflichtet, weil es keine vollständige Deckung zwischen den Anforderungen gibt. Insbesondere sollte sichergestellt werden, dass ein „Three-Lines-of-Defence-Modell“ sauber verankert ist und Rollen klar abgrenzbar sind, eine umfassende schriftlich fixierte Ordnung besteht und ein end-to-end Risikomanagementprozess etabliert und dokumentiert ist.

Trotz der damit verbundenen Herausforderungen bietet die Umsetzung der ZAG-MaRisk jedoch auch zahlreiche Chancen: Die Institute können ihr Risikomanagement optimieren, um potenzielle Risiken frühzeitig zu erkennen und geeignete Maßnahmen zu ergreifen, die interne Transparenz erhöhen und ihre Compliance stärken, was langfristig zu einer stabileren und vertrauens-würdigeren Geschäftsorganisation führt.

In jedem Fall sind die notwendigen Anpassungen umgehend einzuleiten, da andernfalls neben empfindlichen finanziellen Schäden auch Reputationsschäden drohen, vor allem wenn im Rahmen potenzieller BaFin-Prüfungen Lücken gegenüber den neuen Vorgaben festgestellt werden.

Abbildungsverzeichnis

Authors

Dominik Siebert ist Managing Partner bei CORE und blickt in der Finanzindustrie auf fundierte Erfahrungen bei komplexen Transformationsvorhaben, von der strategischen Konzeptionierung bis zur Umsetzungssteuerung zurück. Bei CORE fokussiert sich Dominik auf Projekte zur Entwicklung und strategischer Positionierung digitaler Bezahllösungen.

Mail: dominik_siebert@epam.com

Carola Bader ist Expert Associate bei CORE und verfügt über umfassende Erfahrung in den Bereichen Compliance und Risikomanagement in der Finanzindustrie. Sie fokussiert sich auf die Beratung von Finanzdienstleistern bei der Umsetzung effektiver Compliance-Strategien, der Einhaltung regulatorischer Anforderungen und der Bekämpfung von Finanzkriminalität.

Mail: carola_bader@epam.com

Muskaan Multani ist Transformation Fellow bei CORE. Mit ihrer Expertise und Erfahrung im Compliance-Bereich fokussiert sie sich auf die Begleitung von Compliance-Projekten vorranging in der Finanzindustrie von der strategischen Konezptionierung bis zur Umsetzung. Sie ist verantwortlich für die Unterstützung von Projektteams und Kunden bei geschäftskritischen Technologietransformationen.

Mail: muskaan_multani@epam.com

COREtransform GmbH
Kurfürstendamm 194
10707 Berlin | Deutschland
https://core.se/
Telefon: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Telefon: +41 44 261 0143
office@core.se

COREtransform Ltd.
9 Devonshire Square, 5th Floor
London EC2 4YF
Großbritannien
https://core.se/
Telefon: +44 20 328 563 61
office@core.se