CFGI

WHITEPAPER

Neue Anforderungen an das Risikomanagement von ZAG-Instituten (ZAG-MaRisk)

Neue Risikomanagement-anforderungen an ZAG-Institute

Im Rahmen der Umsetzung der ersten europäischen Zahlungsdienstleisterrichtlinie (PSD 1) in nationales Recht hat der deutsche Gesetzgeber 2009 das Zahlungsaufsichtsgesetz (im Folgenden ZAG) erlassen und einige erlaubnispflichtige Geschäfte einem neuen Aufsichtsregime unterworfen. Nach weiteren Novellierungen und Anpassungen des ZAG durch europäische Richtlinien (u. a. PSD 2) wurden weitere Bankgeschäfte aus dem KWG herausgelöst und dem ZAG hinzugefügt.

In der Praxis gehören zu den ZAG-Instituten in erster Linie Zahlungsdienstleister und E-Geld-Institute. Dabei sind Zahlungsdienstleister (Payment Service Provider, PSPs) Unternehmen, die Zahlungsdienste wie Überweisungen, Lastschriften, Kartenzahlungen oder E-Geld-Zahlungen anbieten. E-Geld-Institute sind Institute, die elektronisches Geld ausgeben und elektronische Geldkonten für Kunden verwalten. Das ZAG beschreibt für ZAG-Institute bestimmte Anforderungen in Bezug auf ihre Geschäftspraktiken, Sicherheitsmaßnahmen, um die Integrität und Sicherheit des Zahlungsverkehrs zu gewährleisten und den Verbraucherschutz fördern.

Am 27. September hat die BaFin den Entwurf eines „Rundschreibens zu den Mindestanforderungen an das Risikomanagement von ZAG-Instituten“ (ZAG-MaRisk) zur Konsultation veröffentlicht. Das Rundschreiben konkretisiert die Anforderungen an die ordnungsgemäße Geschäftsorganisation aus § 27 Abs. 1 ZAG und gibt einen Rahmen für die Ausgestaltung in der Praxis vor. Demnach umfasst eine ordnungsgemäße Geschäftsorganisation interne Kontrollmechanismen und Maßnahmen zur Sicherstellung, dass das Institut seine regulatorischen Verpflichtungen erfüllt.

Darüber hinaus enthält das Rundschreiben präzisierte Anforderungen an die Sicherungsmaßnahmen (§§ 17, 18 ZAG) und das Auslagerungsmanagement (§ 26 ZAG).

Hierbei sind insbesondere die Einführung einer internen Revision, Risiko-Controlling sowie Compliance-Funktion für die meisten ZAG-Institute neu.

Bisher hatte die BaFin zwar kein spezifisches Rundschreiben für ZAG-Institute veröffentlicht, jedoch wurde von der BaFin eine Umsetzung und Berücksichtigung der MaRisk aus dem Aufsichtsregime des KWG den ZAG-Instituten empfohlen.

10 Herausforderungen der ZAG-MaRisk

Der von der BaFin veröffentlichte Konsultationsentwurf der ZAG-MaRisk enthält diverse Konkretisierungen in Bezug auf das Risikomanagement eines ZAG-Instituts. Neu sind hierbei insbesondere die Verpflichtung zur Einführung einer Risikocontrolling-Funktion, Compliance-Funktion und Internen Revision (3-Lines-of-Defence). Daneben enthält die ZAG-MaRisk auch Anforderungen an die Organisationsstruktur des ZAG-Instituts.

Wir empfehlen, einen besonderen Fokus auf die effiziente und prüfungssichere Implementierung der folgenden neuen Anforderungen zu legen:

01 Einrichten einer Risikocontrolling-Funktion

Der Entwurf der ZAG-MaRisk fordert von ZAG-Instituten die Einrichtung einer unabhängigen Risikocontrolling-Funktion [AT 4.4.1 Tz. 1] (2nd Line of Defence). Das Risikocontrolling hat eine Risikoinventur [AT 2.2 Tz. 1] mit geeigneten Indikatoren für die Risikoidentifizierung durchzuführen sowie die Risiken laufend zu überwachen und zu begrenzen [AT 4.1]. Zusätzlich sind Stresstests durchzuführen und eine Risikokultur zu entwickeln sowie zu fördern [AT 3 Tz. 1]. Über die Aktivitäten und Erkenntnissen hat die Risikocontrolling-Funktion an die Geschäftsleitung zu berichten.

02 Strategieprozess

ZAG-Institute haben im Rahmen eines angemessenen Strategieprozesses das Geschäftsmodell zu analysieren und darauf basierend eine nachhaltige Geschäftsstrategie zu definieren [AT 4.2 Tz. 1]. Der Umgang mit den aus der Geschäftsstrategie resultierenden Risiken sind in einer Risikostrategie inklusive eines Risikoappetits zu bestimmen [AT 4.2 Tz. 2]. Wenn ZAG-Institute investieren, ist eine nachhaltige Investitionsstrategie zu definieren [AT 4.2 Tz. 3].

03 Einrichten einer Compliance-Funktion

Die ZAG-Institute haben neben einer Risikocontrolling-Funktion in der 2nd Line of Defence eine Compliance-Funktion einzurichten, die der Geschäftsleitung direkt unterstellt und berichtspflichtig ist [AT 4.4.2 Tz. 1 und 3]. Der Compliance-Funktion sind uneingeschränkt Zugang zu allen Informationen einzuräumen [AT 4.4.2 Tz. 5]. Die Compliance-Funktion hat die für das Institut relevanten rechtlichen Regelungen und Vorgaben zu identifizieren sowie diese Liste regelmäßig zu aktualisieren [AT 4.4.2 Tz. 2]. Auf der Grundlage der identifizierten rechtlichen Regelungen und Vorgaben hat die Compliance-Funktion Verfahren zur Einhaltung dieser Regelungen zu implementieren und entsprechende Kontrollen zu etablieren [AT 4.4.2 Tz. 1].
Die Compliance-Funktion und der Compliance-Beauftragte haben jährlich und anlassbezogen einen Bericht über die Maßnahmen und Erkenntnisse an die Geschäftsleitung zu erstellen [AT 4.4.2 Tz. 6].

04 Sicherungsmaßnahmen

Das ZAG-Institut hat organisatorische Maßnahmen und Verfahren für Betrugsprävention und die Überwachung, Handhabung und Folgemaßnahmen bei Sicherheitsvorfällen und sicherheitsbezogenen Kundenbeschwerden zu etablieren [BTO 1 Tz. 1]. Darüber hinaus ist eine Kontaktstelle, an die sich Kunden in Betrugsfällen, bei technischen Problemen wenden können, einzurichten [BTO 1 Tz. 2]. ZAG-Institute haben Bearbeitungsgrundsätze für die Prozesse bei Zahlungsdiensten und E-Geld-Geschäften und für die Nutzung von Treuhandkonten zu definieren [BTO 1 Tz. 1 und 2].

Darüber hinaus sind Verwaltungs- und Kontenabstimmungsprozesse [BTO 1 Tz. 1] sowie Kontrollmechanismen bei Investition in sichere, liquide Aktiva [BTO 1 Tz. 2] einzurichten.

05 Interne Revision

Neben einer 2nd Line of Defence ist ein ZAG-Institut verpflichtet eine funktionsfähige Interne Revision als Instrument der Geschäftsleitung, die ihr unmittelbar unterstellt und berichtspflichtig ist, einzurichten [AT 4.4.3 Tz. 1 und 2]. Die Aufgabe der Internen Revision als 3rd Line of Defence ist die risikoorientierte und prozessunabhängige Beurteilung und Prüfung des Risikomanagements, des internen Kontrollsystems und die Ordnungsmäßigkeit aller Aktivitäten und Prozesse [AT 4.4.3 Tz. 3].

Diese Beurteilung und Prüfung hat auf der Basis eines risikoorientierten Prüfungsansatzes zu erfolgen [BT 2.1 Tz. 1]. Dazu hat die Interne Revision einen umfassenden und jährlich fortzuschreibenden risikoorientierten Prüfungsplan (Prüfung aller Prozesse innerhalb von drei Jahren) [BT 2.3 Tz. 1] zu definieren und von der Geschäftsleitung genehmigen zu lassen [BT 2.3 Tz. 5]. Außerhalb der Prüfungen, die auf dem Prüfungsplan basieren, sind durch die Interne Revision kurzfristig notwendige Sonderprüfungen durchzuführen [BT 2.3 Tz. 4]. Über die Erkenntnisse aus den Prüfungen sind schriftliche Prüfungsberichte sowie ein Jahresbericht anzufertigen [BT 2.4 Tz. 1 und 4].

Neben den Prüfungen hat die Interne Revision wesentliche Projekte unter Wahrung ihrer Unabhängigkeit zu begleiten [BT 2.1 Tz. 2].

Wenn im Rahmen einer Prüfungstätigkeit Mängel identifiziert werden, hat die Interne Revision die fristgerechte Beseitigung der Mängel zu überwachen (ggf. im Rahmen einer Nachschauprüfung) [BT 2.5 Tz. 1].

06 Interessen-Konfliktmanagement

Durch eine geeignete Gestaltung der Aufbau- und Ablauforganisation sind Interessenkonflikte zu vermeiden [AT 4.3.1 Tz. 1].

07 Dokumentation

ZAG-Institute haben Prozesse, Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege klar zu definieren [AT 4.3.1 Tz. 2] und in Organisationsrichtlinien schriftlich zu fixieren und bekannt zu machen [AT 5 Tz. 3].

Darüber hinaus sind die notwendigen Unterlagen systematisch aufzuzeichnen und aufzubewahren [AT 6].

08 Anforderungen der IT-Systeme

Die Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit der Daten von IT-Systemen und Prozessen sind durch angemessene Maßnahmen sicherzustellen [AT 7.2 Tz. 2]. IT-Systeme sind vor der Inbetriebnahme zu testen und abzunehmen [AT 7.2 Tz. 3]. Ein Notfallkonzept ist zu definieren [AT 7.3]. Die Anforderungen sind ebenfalls hinsichtlich der individuellen Datenverarbeitung (IDV) einzuhalten.

Auch hinsichtlich der Berechtigungen sind regelmäßige und anlassbezogene Überprüfungen von Berechtigungen auf der Basis des Need-to-know-Prinzips durchzuführen [AT 4.3.1 Tz. 2].

09 Änderungen in der Geschäftstätigkeit

Vor der Ausweitung der Geschäftstätigkeit eines ZAG-Instituts in neue Produkte oder neue Märkte ist der Risikogehalt der neuen Aktivität und deren Auswirkungen auf das Gesamtrisikoprofil in einem Konzept zu bewerten [AT 8.1 Tz. 1]. Insbesondere die wesentlichen Konsequenzen für das Risikomanagement sind im Konzept darzustellen [AT 8.1 Tz. 1]. Das Konzept ist durch die Geschäftsleitung zu genehmigen [AT 8.1 Tz. 5].

Bei der Entscheidung, ob es sich bei einer neuen Aktivität um die Ausweitung der Geschäftsaktivität in neue Produkte und neue Märkte handelt und damit die Notwendigkeit eines Konzeptes besteht, ist ein unabhängiger Bereich einzubinden [AT 8.1 Tz. 3].

Über die Produkte und Märkte des ZAG-Instituts ist ein Katalog (der sog. Produktkatalog) vorzuhalten [AT 8.1 Tz. 2].

Auch vor wesentlichen Veränderungen in der Aufbau- und Ablauforganisation sowie in den IT-Systemen sind Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren [AT 8.2 Tz. 1].

10 Auslagerungsmanagement

Für das Management von Auslagerungen an Dritte sind klare Verantwortlichkeiten für die Dokumentation, Steuerung und Überwachung der Auslagerungen zu definieren [AT 9 Tz. 10]. Dabei ist insbesondere ein zentraler Auslagerungsbeauftragter einzurichten, der durch ein zentrales Auslagerungsmanagement unterstützt wird [AT 9 Tz. 12]. Im Rahmen der Auslagerung von Prozessen an Dritte sind im ersten Schritt im Rahmen einer Risikoanalyse die Risiken der Auslagerung zu bewerten und die Auslagerungen auf dieser Basis in wesentliche und unwesentliche Auslagerungen einzuteilen [AT 9 Tz. 2 und 3]. Bei wesentlichen Auslagerungen unterliegt der Auslagerungsvertrag besonderen Anforderungen u. a. hinsichtlich der Kontroll- und Prüfrechte [AT 9 Tz. 6 und 7]. Die Auslagerungen sind zu überwachen und die verbundenen Risiken zu steuern. Bei wesentlichen Auslagerungen hat dies auch anhand von angemessenen KPIs zu erfolgen [AT 9 Tz. 9]. Das Auslagerungsmanagement umfasst auch die Pflicht zum Erstellen eines Auslagerungsregisters sowie einen Jahresbericht über die (wesentlichen) Auslagerungen [AT 9 Tz. 13 und 14].

Handlungsbedarf für ZAG-Institute (Proportionalitätsprinzip)

Grundsätzlich enthalten die ZAG-MaRisk ein breites Spektrum an neuen und konkretisierten Anforderungen. Jedoch kann der Umsetzungsaufwand zwischen den betroffenen Unternehmen sehr unterschiedlich sein. Dies hängt insbesondere von der ggf. bereits freiwilligen Berücksichtigung der KVG MaRisk und der Komplexität der Geschäftsaktivitäten des ZAG-Institutes ab.

In der Vorbemerkung des Rundschreibens (AT 1) betont die BaFin das Proportionalitätsprinzip, um die heterogenen Institutsstrukturen angemessen zu berücksichtigen. So beinhaltet das Rundschreiben Öffnungsklauseln, die gerade von ZAG-Instituten mit weniger komplexen Prozessen eine vereinfachte Umsetzung ermöglichen sollen und andererseits für komplexe Institute eine Erweiterung und vertiefte Umsetzung der Anforderungen vorsieht.

Daher empfiehlt sich im ersten Schritt für alle ZAG-Institute ein Scoping um die eigene Betroffenheit zu beurteilen und die spezifischen Anforderungen entsprechend zu adaptieren. In den folgenden Schritten sind dann das Zielbild zu definieren, ein Abgleich mit der Aufbau- und Ablauforganisation durchzuführen sowie Umsetzungsmaßnahmen abzuleiten.

Bei der Umsetzung der neuen Anforderungen der ZAG-MaRisk sollte auf die Expertise aus der Umsetzungspraxis, inklusive Lessons Learned, Best Practices und Quick-Wins der MaRisk (KWG), zurückgegriffen werden, da sich eine Vielzahl der Anforderungen in beiden Rundschreiben wiederfinden. Dies ist insbesondere bei der Umsetzung der Anforderungen in Bezug auf Compliance, Risikocontrolling und die Interne Revision der Fall.

CFGI als Partner bei der erfolgreichen Umsetzung

Scoping der Anforderungen

CFGI unterstützt euch beim Scoping der MaRisk-Anforderungen unter Anwendung des Proportionalitätsgrundsatzes und greift dabei auf jahrelange Prüfungs- und Beratungsexpertise zurück. Die Anforderungen werden in einen angemessenen Projektplan überführt.

Revisionssichere Prozesse

CFGI unterstützt euch bei der Gestaltung, Implementierung und Optimierung der MaRisk bezogenen Prozesse. Wir helfen euch dabei revisionssichere Kontroll-handlungen in die Prozesse einzubinden.

Prüfer Dry Runs

CFGI führt Dry Runs der relevanten Prozesse mit den Mitarbeitern und Jahresab-schlussprüfern durch. Unser MaRisk Team verfügt über umfangreiche Big Four Prüfungserfahrung und begleitet seit vielen Jahren erfolgreich BaFin Prüfungen.

Quick Wins und Lessons Learned

Unser MaRisk Team bringt 20 Jahre Erfahrung bei der Umsetzung und Optimierung von BaFin-MaRisk-Anforderungen mit und ermöglicht euch damit eine effiziente und prüfungssichere Umsetzung der ZAG-MaRisk.

Auslagerung

Funktionen und Prozesse, die durch die MaRisk gefordert sind, können durch CFGI übernommen werden. Unsere Expertise kann bei der Auslagerung der Internen Revision, der Compliance und des Risikomanagements eine sinnvolle Alternative sein.

Eure Ansprechpartner

SAM SALEHI
Senior Manager

@ ssalehi@cfgi.com
+49 (0) 160 980 182 58

NELE JÜRGENS
Manager

@ njuergens@cfgi.com
+49 (0) 160 968 840 80

CFGI

Supporting CFOs
In All Critical Functions

Who is CFGI?

We are a leading global accounting and business advisory firm. We partner with our clients on their most important regulatory, transaction, and business improvement initiatives.

Our team of over 1000 former Big 4 professionals brings expertise across technical accounting, capital markets, tax, valuation, ESG, transaction advisory, restructuring, cybersecurity and technology solutions — all delivered with an independent and roll-up-the-sleeves approach. CFGI was founded in 2001 and serves thousands of global clients from our 28 offices throughout the Americas, Europe, and Asia Pacific regions.

Call or email us today to begin a dialogue. We'll show you how a consulting relationship with CFGI can provide both immediate benefits and lasting effects.

---

cfgi.com/de | in