Point of Compliance
Das Risikomanagement-Magazin

AUSGABE 3 / 2024

PoC

#freiraumsichern

DZ CompliancePartner


Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken
Allein oder vertrauen
Ob Sie Ihrer Verantwortung im Beauftragtenwesen allein gerecht werden oder dafür einem Partner vertrauen, entscheiden nur Sie. Wir sorgen dafür, dass Sie diesen Freiraum nutzen können.
#freiraumsichern
DZ CompliancePartner

#freiraumsichern

Jens Saenger
Sprecher der Geschäftsführung

In der Genossenschaftlichen FinanzGruppe verbinden wir auf einzigartige Weise die Pole unternehmerische Freiheit und strukturelle Solidarität.

Was heißt das für das Beauftragtenwesen? Hier lässt sich die Gesamtverantwortung für die Erfüllung der aufsichtsrechtlichen und gesetzlichen Regularien nicht delegieren, sie verbleibt in der Bank. Aber die Bank hat die Wahl: sich der Verantwortung alleine zu stellen oder dabei einem professionellen Partner zu vertrauen. Dass es diese Auslagerungs- und Unterstützungsoption gibt, ist gelebter Ausdruck des Subsidiaritätsprinzips und damit ureigener Teil unserer Verbund-DNA.

Wir, als Ihr Partner im Beauftragtenwesen, nehmen diese Rolle an, indem wir uns mit allem, was wir tun, in den Dienst der Gemeinschaft stellen und Ihren unternehmerischen Freiraum sichern.

Lesen Sie in dieser Ausgabe der PoC unter anderem, wie Beschwerden zu einem Teil der Lösung werden können (Seite 17), was mit der neuen EU-Geldwäsche-Verordnung auf Sie zukommt (Seite 5) oder wie wir DORA gemeinsam meistern (Seite 14).

Ich wünsche Ihnen eine inspirierende Lektüre.

Herzlichst
Ihr Jens Saenger

Folgen Sie der DZ CompliancePartner GmbH auf Social Media.

IMPRESSUM

PoC – Point of Compliance
Das Risikomanagement-Magazin,
Ausgabe 34, 3/2024
ISSN: 2194-9514
Herausgeber: DZ CompliancePartner GmbH,
Wilhelm-Haas-Platz, 63263 Neu-Isenburg,
Telefon 069 580024-0,
Telefax 069 580024-900, www.dz-cp.de
Handelsregister HRB 11105, Amtsgericht
Offenbach, USt.-IdNr.: DE201150917
Geschäftsführung: Jens Saenger (Sprecher),
Dirk Pagel

Verantwortlich i. S. d. P.: Jens Saenger
Redaktion: Gabriele Seifert, Leitung (red.)
Redaktionsanschrift: DZ Compliance-Partner GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 580024-0, Telefax 069 580024-900, E-Mail: poc@dz-cp.de
Weitere Autoren dieser Ausgabe:
Marc-Timo Brandenburger, Yvonne Debus, Felix Fröhlich, Kevin Lohmann, Giannis Petras, Jens Saenger, Jörg Scharditzky, Lars Schinnerling, Thomas Schröder, Gabriele Seifert, Benjamin Wellnitz

Bildnachweise: DZ CompliancePartner GmbH
Gestaltung: Ralf Egenolf
Druck: Thoma Druck, Dreieich

Redaktionsschluss: 26. September 2024
Auflage: 2.400 Exemplare

Auf dem Weg zur neuen EU-Geldwäsche-Verordnung

Die neue EU-Geldwäsche-Verordnung (EU-GwVO) wurde am 19. Juni 2024 im Amtsblatt der EU veröffentlicht. Die gesetzlichen Regelungen sind drei Jahre nach der Verkündigung – also Mitte 2027 – anwendbar und wirken unmittelbar.

Die EU-Geldwäsche-Verordnung ist ein wesentlicher Teil des sogenannten Single Rulebook, das vier Teile enthält:

- EU-Geldtransfer-Verordnung,
- AMLA-Verordnung (Errichtung einer EU-Aufsichtsbehörde),
- EU-Geldwäsche-Richtlinie und eben die
- EU-Geldwäsche-Verordnung (EU-GwVO).

Die nachstehenden Ausführungen setzen den Fokus auf die Auswirkungen der neuen EU-GwVO – insbesondere für die Genossenschaftliche FinanzGruppe. Dabei wird ein Bogen von den Anfängen der Geldwäschegesetzgebung in Deutschland bis zu den Änderungen durch die – ab Mitte 2027 anzuwendende – EU-GwVO gespannt.

Auf dem Weg zum einheitlichen EU-Rechtsrahmen

Primäres Ziel der oben genannten EU-Gesetzgebungsschritte ist es, die nach wie vor uneinheitliche Umsetzung der bisherigen EU-Geldwäscherichtlinien in den einzelnen Ländern zu beenden und einen EU-einheitlichen Anti-Geldwäsche-Rechtsrahmen inklusive einer entsprechenden Aufsichtsbehörde (Anti-Money Laundering Authority – AMLA) zu implementieren.

Die EU-Geldtransfer-Verordnung ist seit Juni 2023 in Kraft. Die AMLA nimmt planmäßig Mitte 2025 ihre Arbeit in Frankfurt am Main auf und die sechste EU-Geldwäsche-Richtlinie ist bis Mitte 2027 durch die Mitgliedsstaaten in nationales Recht umzusetzen.

Die EU-GwVO selbst entfaltet unmittelbare Rechtswirkung auf die Adressaten in der gesamten EU. Sie bedarf keiner Umsetzung in nationales Recht, wie z. B. bei einer EU-Richtlinie.

Ein Blick zurück

Das deutsche Geldwäschegesetz (GwG) feiert im kommenden Jahr seinen 32. Geburtstag. Deutschland war bei Inkrafttreten des GwG am 1. Januar 1993 gute zwei Jahre wiedervereint. Bundeskanzler der vereinten Republik war Helmut Kohl, der Fußballbundestrainer (der Männer) hieß Anfang 1993 Berti Vogts und die Finanzaufsicht der Banken firmierte noch unter dem Namen BaKred.

Unternehmen wie Amazon und Google mussten erst noch gegründet werden, das Internet machte weniger als ein Prozent der weltweiten Informationsflüsse aus, es gab keinen „App Store“ oder schon gar keine „Fintechs“.

Viele der heute gewohnten geldwäscherechtlichen Begriffe wie Sorgfaltspflichten, PEP-Status, Risikoanalyse oder Internes Kontrollsystem waren vor über 30 Jahren noch nicht im heutigen Maße kodifiziert.

Mit Verabschiedung des ersten GwG Ende 1992 ging es zunächst darum, einen einheitlichen rechtlichen Rahmen in Deutschland zur Bekämpfung von Geldwäsche, insbesondere im Finanzsektor, zu schaffen.

Zu den Eckpfeilern des Ur-GwG zählten und zählen nach wie vor die Pflicht, verdächtige Transaktionen an die zuständigen Behörden zu melden, sowie Identifizierungspflichten bei der Eröffnung von Konten oder der Durchführung bestimmter Transaktionen.

Fünf EU-Geldwäsche-Richtlinien und diverse GwG-Novellierungen später gehören umfassende Sorgfaltspflichten, strenge Dokumentationsanforderungen und die Unterrichtung der Mitarbeitenden zum Status quo der regulatorischen Anforderungen im Bereich der Geldwäsche- und Terrorismusbekämpfung. Ebenso selbstverständlich sind das Betreiben eines internen Kontroll- und Risikomanagementsystems inklusive elektronischem Monitoring und die Sanktionierung von Verstößen gegen das GwG.

Der Blick nach vorn

Durch die neue EU-GwVO bleiben auch ab Mitte 2027 die bekannten und etablierten Strukturen des Geldwäscherechts im Großen und Ganzen erhalten. Auch die Möglichkeit für die Verpflichteten, bestimmte Aufgaben an Dritte auszulagern, wird weiterhin Bestand haben.

Der EU-Verordnungsgeber justiert den rechtlichen Rahmen dennoch an mehreren Stellen neu, schärfer und durchaus auslegungsbedürftig. Diese Auslegungen werden durch die neue Aufsichtsbehörde – die AMLA – erfolgen. Der Verordnungsgeber spricht in diesem Zusammenhang an mehreren Stellen von der Konkretisierung durch technische Standards. Hier bleibt abzuwarten, wie die AMLA die Verordnung gelebt wissen möchte. Sie hat hierbei zwischen zwei und drei Jahre Zeit, um diese Standards fertigzustellen. Daher werden einige dieser Standards durchaus erst kurz vor dem Wirksamwerden der Verordnung im Juli 2027 verkündet werden (können).

Die nachfolgenden Ausführungen orientieren sich am vorliegenden Verordnungstext. Der Fokus liegt dabei insbesondere auf Themenlagen, die die Volksbanken Raiffeisenbanken erwartungsgemäß im Tagesgeschäft betreffen werden und bei denen aus heutiger Sicht Struktur und Auswirkung der gesetzlichen Regelungen relativ klar und wenig auslegungsbedürftig erscheinen.

Für die breite Öffentlichkeit wird sich die neue EU-GwVO vor allem durch die Einführung der **Bargeldobergrenze von 10.000 Euro** bemerkbar machen. Ab Mitte 2027 dürfen gewerblich gehandelte Güter und Dienstleistungen nur bis unter 10.000 Euro bar bezahlt werden. Transaktionen zwischen Privatpersonen, die nicht gewerblich mit dem Kaufgegenstand handeln, sind von der Regelung nicht betroffen – der private Kfz-Verkauf kann also (Stand heute) auch in drei Jahren noch in bar, ohne Betragsgrenze abgewickelt werden.

Weit weniger Aufmerksamkeit wird die **Erweiterung des Verpflichtetenkreises** erregen. Anbieter von Kryptowährungen, Händler von Luxusgütern, Crowdfunding-Dienstleister und sogenannte Investitionsmigrationsberater (Stichwort: goldene Visa) werden in den Anwendungsbereich der Verordnung einbezogen.

Auch **Profifußballvereine und Fußballspielervermittler** gehören bald zu den geldwäscherechtlich Verpflichteten – allerdings erst ab Mitte 2029, wobei die Verordnung nationale Ausnahmeregelungen unter bestimmten Voraussetzungen ermöglicht.

Güterhändler verlieren ihren „Per-se-Verpflichtetenstatus“, es sein denn, es handelt sich um die oben erwähnten Anbieter von Luxusgütern. Hierzu zählen laut Verordnung Edelmetalle und Edelsteine, hochwertige Uhren (ab 10.000 Euro), Kraftfahrzeuge ab 250.000 Euro und Flugzeuge ab 7,5 Mio. Euro.

Deutlicher administrativer Mehraufwand

Für die Kreditwirtschaft und insbesondere die Volksbanken Raiffeisenbanken mit ihrer regionalen Marktausrichtung und ihrer mittelständischen Kundschaft sind die scheinbar kleinen Veränderungen, die die EU-GwVO mit sich bringt, „nicht von Pappe". Einige wichtige Änderungen mit nachhaltigen Auswirkungen auf das Kundengeschäft seien nachstehend aufgelistet.

So verlangt die Verordnung die **Ernennung eines Compliance-Managers** auf Ebene bzw. in der Geschäftsleitung. Dieser ist für die korrekte Umsetzung und Einhaltung der Verordnung zuständig. Dies beinhaltet, neben der Pflicht zur zielgerichteten Ressourcenallokation in Richtung Compliance-Officer, Risikomanagementmaßnahmen und Berichtspflichten.

Die **Kundensorgfaltspflichten** in Bezug auf Schwellenwerte bei Geldtransfers und Bargeschäften sowie im Hinblick auf die Identifizierungsdaten von Kunden, auftretenden Personen und Treugebern werden verschärft. Bei sehr vermögenden Personen mit mindestens 50 Mio. Euro Gesamtvermögen gelten fallweise verstärkte Sorgfaltspflichten.

Die **Anforderungen an die Ermittlung des wirtschaftlichen Eigentums** steigen. Zum einen wird die Schwelle, ab wann wirtschaftliches Eigentum vorliegt, auf 25 % herabgesetzt. Derzeit sind mehr als 25 % Anteilseigentum notwendig, um wirtschaftlich Berechtigter (wB) zu sein. Dabei ist die Beteiligungsquote einer natürlichen Person an einem Unternehmen durch Multiplikation und Addition festzustellen. Damit wird es schwarzen Schafen deutlich erschwert, sich hinter Kaskaden von Beteiligungen zu verstecken.

Für die Volksbanken Raiffeisenbanken wird der administrative Aufwand zunehmen. Denn nicht nur der wB-Ermittlungsaufwand steigt. Kann kein „echter" wB ermittelt werden, müssen alle Personen der Führungsebene des Vertragspartners als fiktive wB erfasst werden. Die AMLA wird – um eine ausufernde Verwaltungspraxis zu verhindern – die Frage beantworten müssen, wie sie die „Führungsebene" definiert.

Leider steigen im Zusammenhang mit der wB-Ermittlung auch die Anforderungen bei der eventuellen Abgabe einer Unstimmigkeitsmeldung.

Ebenfalls statuiert die neue EU-GwVO die Prüfpflicht, ob ein Kunde oder wB Individualsanktionen unterliegt. Es ist darüber hinaus zu prüfen, ob eine sanktionsgelistete Person einen Kunden (juristische Person) kontrolliert oder mindestens eine Mehrheitsbeteiligung hält.

Im Rahmen der Änderungen bei den Kundensorgfaltspflichten werden auch die **Aktualisierungsfristen** auf ein bzw. fünf Jahre bei hohem bzw. normalem Risiko einer Geschäftsbeziehung verkürzt (derzeit zwei bzw. zehn Jahre).

Der **Kreis der politisch exponierten Personen (PEP)** wird vergrößert. Ab Mitte 2027 zählen auch Personen der Führungsriege einer Regierungspartei zu den PEP. Die nicht abschließende Liste umfasst dann auch Positionen auf kommunaler oder regionaler Ebene ab einer Einwohnerzahl von 50.000. Geschwister können teilweise ebenfalls zu den PEP-relevanten Familienangehörigen zählen.

Veränderungen wird es auch bei der Pflicht zur **Abgabe von Verdachtsmeldungen** geben. Prinzipiell verpflichtet der Verordnungsgeber zur Meldung jeden kriminellen Verhaltens. Dies gilt auch dann, wenn zunächst legale Vermögenswerte betroffen sind, wie z. B. der gezahlte Wetteinsatz bei der Teilnahme an illegalem Online-Glücksspiel. Hier bleibt – wie in den anderen Teilbereichen auch – abzuwarten, wie die neue Aufsichtsbehörde (AMLA) die Verordnung auslegt.

Fazit

Die neue EU-GwVO folgt dem übergeordneten und begrüßenswerten Ziel, einen EU-einheitlichen Rechtsrahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung zu schaffen.

Bei der Gestaltung hatte der Verordnungsgeber offenbar insbesondere grenzüberschreitende Kundenbeziehungen, internationale Beteiligungsverflechtungen und finanzsystemrelevante und international agierende Finanzinstitute vor Augen.

Der deutschen Bankenlandschaft mit dem insbesondere im Mittelstand verwurzelten und dem regionalen Markt verbundenen Genossenschaftssektor bürdet der EU-Verordnungsgeber einen beträchtlichen bürokratischen Mehraufwand auf. Ob die verschärften Regelungen zu einem effizienten Mehrwert und Zusatzerfolg bei der Aufdeckung von illegalen Zahlungsströmen und mithin der Verfolgung von Straftätern führen werden, bleibt fraglich.

Seitens der DZ CompliancePartner GmbH haben wir die Umsetzung der Anforderungen der EU-GwVO bereits intern projektiert. Als zentraler Auslagerungsdienstleister in Deutschland werden wir die weitere regulatorische Entwicklung intensiv beobachten und begleiten. Selbstverständlich werden wir bis zum Wirksamwerden der EU-GwVO Mitte 2027 unsere Mandanten über die notwendigen aufbau- und ablauforganisatorischen Änderungen informieren und diese mit ihnen gemeinsam umsetzen. ▬

Thomas Schröder
Abteilungsleiter Geldwäsche- und Betrugsprävention,
E-Mail: thomas.schroeder@dz-cp.de

Ausgestaltung und Auslagerung der MaRisk-Compliance-Funktion

Die Funktion des MaRisk[1]-Compliance-Beauftragten gibt es nun seit über zehn Jahren. Anlass für eine Bestandsaufnahme: Welche Aufgaben sind mit der MaRisk-Compliance-Funktion verbunden, wie grenzt sie sich zu anderen Funktionen ab und welche Anforderungen gibt es an die Auslagerbarkeit?

Grundlage der MaRisk-Compliance sind § 25a Kreditwesengesetz (KWG) und AT 4.4.2 MaRisk. Die Regelungen des § 25a KWG gehen auf die Leitlinien der Europäischen Bankenaufsichtsbehörde und Veröffentlichungen des Baseler Ausschusses für Bankenaufsicht zurück.

Bei den MaRisk selbst handelt es sich um normeninterpretierende Verwaltungsvorschriften zu § 25a KWG, die von der BaFin regelmäßig novelliert und veröffentlicht werden und eine Selbstbindung der Verwaltung darstellen. Die Einhaltung der MaRisk und somit des § 25a KWG wird regelmäßig vom Abschlussprüfer geprüft und kann auch Teil einer Sonderprüfung nach § 44 KWG sein.

Aufgaben

Die Aufgabe der MaRisk-Compliance-Funktion ist es zum einen, den Risiken, die sich aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben ergeben können, entgegenzuwirken, sowie zum anderen, rechtliche Regelungen und Vorgaben mit einem Compliance-Risiko zu identifizieren. Details ergeben sich überwiegend aus den Textziffern 1–7 der AT 4.4.2 MaRisk und teilweise aus anderen Regelungen der MaRisk wie folgt:

1. Implementierung wirksamer Verfahren, AT 4.4.2 Tz. 1, AT 5 Tz. 3 MaRisk

Die Compliance-Funktion hat auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben hinzuwirken. Durch die weiche Formulierung „hinzuwirken" bringt die Aufsicht zum Ausdruck, dass die primäre Verantwortung bei den entsprechenden Fachabteilungen verbleibt und die MaRisk-Compliance-Funktion eher eine koordinierende, beratende Aufgabe ausübt[2]. Klassische Tätigkeit der Compliance-Funktion ist die regelmäßige Überwachung des rechtlichen Umfeldes auf Veränderungen, um frühzeitig Änderungsbedarfe zu adressieren. Darüber hinaus ist darauf zu achten, dass im Institut für alle wesentlichen Regelungen und Vorgaben auch Zuständigkeiten bestehen. Verstößen gegen Vorgaben oder Regelungen ist nachzugehen.

2. Kontrollen, AT 4.4.2 Tz. 1 MaRisk

Gemäß Tz. 1 zu AT 4.4.2 MaRisk hat die MaRisk-Compliance-Funktion auf entsprechende Kontrollen hinzuwirken. Insofern ist strittig, ob die MaRisk-Compliance-Funktion auch selber eigene Kontrollen durchführen

muss. Die Einhaltung gesetzlicher Regelungen und die Implementierung wirksamer Verfahren zur Einhaltung der gesetzlichen Regelungen verbleiben auch gemäß den MaRisk primär in der Verantwortung des jeweiligen Fachbereichs.

Gleichwohl zeigt die Erfahrung, dass es für die Compliance-Funktion sinnvoll ist, eigene Kontrollen durchzuführen: Es gilt, das Risiko für die Bank zu mindern, indem Mängel (z. B. im Beschwerdewesen) frühzeitig erkannt werden. Aus unserer Sicht ist es für das Institut von Nutzen, wenn ein Mangel frühzeitig durch die Compliance-Funktion und deren Kontrollen aufgezeigt und abgestellt wird. Es ist besser, als wenn der Mangel Thema einer Jahresabschlussprüfung oder gar Sonderprüfung nach § 44 KWG ist.

3. Beratung und Unterstützung der Geschäftsleitung, AT 4.4.2 Tz. 1 MaRisk

Die Compliance-Funktion hat die Geschäftsleitung hinsichtlich der Einhaltung der rechtlichen Regelungen und Vorgaben zu unterstützen und zu beraten. Dementsprechend ist die Compliance-Funktion Ansprechpartner und Berater des Vorstandes zu Compliance-Themen.
Die Unterstützung des Vorstandes erfolgt durch

- die regelmäßige Berichterstattung,
- die regelmäßigen Kontroll- und Jahresberichte sowie
- ggf. durch Ad-hoc-Meldungen bei Feststellen schwerwiegender Mängel im Rahmen eigener Kontrollhandlungen.

Ein Beispiel aus unserer Praxis ist die Beratung zur Risikokultur und deren Implementierung im Institut.

4. Identifizierung wesentlicher Regelungen und Vorgaben, AT 4.4.2 Tz. 2 MaRisk

a. Risikoanalyse

Die Identifizierung der wesentlichen rechtlichen und institutsindividuellen Regelungen und Vorgaben, deren Nichteinhaltung zu einer Gefährdung des Vermögens des Institutes führen kann, ist eine der Hauptaufgaben der Compliance-Funktion und hat in regelmäßigen Abständen zu erfolgen. Darauf aufbauend ergeben sich dann die weiteren Schritte zur Risikoüberwachung und -reduzierung, z. B. durch Kontrollen, Schulungen etc.

Welche Regelungen und Vorgaben zu bewerten sind, ist mehrstufig zu prüfen. Zunächst müssen abhängig von dem Geschäftsmodell, den Produkten und Märkten etc. die Regelungen und Vorgaben herausgefiltert werden, die für das Institut nicht einschlägig sind. Darauf aufbauend sind die Regelungen und Vorgaben herauszufiltern, die nicht-finanzbranchenspezifisch sind und daher nicht unbedingt der Bewertung durch die MaRisk-Compliance-Funktion bedürfen. Schließlich gibt es auch Spezialzuständigkeiten bzw. Fachabteilungen mit besonderem Wissen, sodass die MaRisk-Compliance-Funktion hier hinter funktionierende Spezialzuständigkeiten zurücktritt.

Eine wesentliche Arbeitserleichterung ist die vom Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V. (BVR) zur Verfügung gestellte und halbjährlich aktualisierte Muster-Bestandsaufnahme[3]. In dieser werden auf Grundlage des BaFin-Protokolls zur Sitzung des Fachgremiums MaRisk am 24. April 2013 bereits die unwesentlichen rechtlichen Regelungen und Vorgaben sowie auf etwaige Spezialzuständigkeiten eingegangen und aufgelistet.

Die Identifizierung der wesentlichen Regelungen und Vorgaben erfolgt üblicherweise in einer Risikoanalyse und hat mindestens jährlich sowie anlassbezogen zu erfolgen. Gründe für eine anlassbezogene Risikoanalyse können beispielsweise Fusionen, wesentliche eigene Feststellungen der Compliance-Funktion, der Internen Revision oder Erkenntnisse aus dem Prüfungsbericht des Jahresabschlussprüfers oder einer Sonderprüfung nach § 44 KWG sein.

b. Rechtsmonitoring

Darüber hinaus obliegt dem Institut die Überwachung der rechtlich-regulatorischen Regelungen und Vorgaben einschließlich deren Umsetzung. Damit soll sichergestellt werden, dass das Institut die aktuellen Vorschriften und Regelungen, z. B. Gesetze, Urteile, Vorgaben der Aufsicht, in der täglichen Praxis beachtet und umsetzt, wodurch eine Risikoreduzierung herbeigeführt wird.
Notwendig ist somit ein Rechtsmonitoring. Das Institut

selbst kann die entsprechenden einschlägigen Quellen auswerten und ein Rechtsmonitoring erstellen oder aber ein Rechtsmonitoring beziehen, das auf das Geschäftsmodell des Institutes abgestimmt sein sollte. Das heißt, die Rechtsmonitoring-Einträge nebst Handlungsempfehlungen sollten mit dem Geschäftsmodell der Bank korrespondieren und diese abdecken und nicht auch Themen enthalten, die für das Institut nicht einschlägig sind.

5. Berichtspflichten, AT 4.4.2 Tz. 7 MaRisk

In Tz. 7 zu AT 4.4.2 MaRisk ist normiert, dass die Compliance-Funktion mindestens jährlich sowie anlassbezogen über ihre Tätigkeit Bericht zu erstatten hat. Diese Berichterstattung erfolgt üblicherweise über den Jahresbericht und informiert die Geschäftsleitung über die erfolgten Tätigkeiten der MaRisk-Compliance-Funktion. Gleichzeitig wird eine Aussage zur Angemessenheit und Wirksamkeit des Compliance-Risikomanagementsystems getroffen. Damit wird der Vorstand in die Lage versetzt, die Compliance-Risiken zu beurteilen, zu steuern und etwaige Mängel abzustellen.

Ad-hoc-Berichte der Compliance-Funktion können in festgestellten und nicht beseitigten Mängeln, in Verstößen gegen wesentliche Regelungen und Vorgaben oder in wesentlichen Mängeln in Prozessen begründet sein.

Der (Compliance-)Bericht nach Tz. 7 MaRisk umfasst nur MaRisk-Compliance-relevante Themen. Die anderen Compliance-Funktionen, z. B. der WpHG-Compliance, Geldwäsche und Terrorismusfinanzierung, bzw. Datenschutz und Informationssicherheit erstellen eigene Berichte (soweit vorgeschrieben). Es ist nicht Aufgabe der MaRisk-Compliance-Funktion, einen „Gesamt-Compliance-Bericht“ zu erstellen.

Empfänger des MaRisk-Compliance-Berichtes ist zunächst der Vorstand. Die Berichte sind auch an die Interne Revision und das Aufsichtsorgan weiterzuleiten.

6. Einbindung in den Neu-Produkt-Prozess und Einbindung in die Änderung betrieblicher Prozesse oder Strukturen, AT 8.1 und AT 8.2 MaRisk

Die Compliance-Funktion ist auch bei Neu-Produkt-Prozessen und wesentlichen Änderungen einzubinden. Gegenstand der Compliance-Prüfung ist dann z. B.:

- ob die Risiken durch die Fachabteilungen bewertet wurden,
- ob die Produkt-Governance eingehalten wurde,
- ob der Produkt-/Märktekatalog angepasst werden muss bzw.
- ob die Ausführungen zur Wesentlichkeit der Änderung schlüssig und nachvollziehbar sind.

Damit verbunden ist jeweils die Frage, ob die Risikoanalyse unter Berücksichtigung der Bewertung nach AT 8 MaRisk die Risiken noch angemessen wiedergibt oder aber eine Ad-hoc-Risikoanalyse durchzuführen ist.

Befugnisse der Compliance-Funktion, AT 4.4.2 Tz. 3, 6 MaRisk

Die Compliance-Funktion muss schlagkräftig agieren können. Dementsprechend werden ihr spezielle Befugnisse eingeräumt. Sie kann auf andere Funktionen und Stellen zugreifen, sie hat Informationsrechte. Das heißt, sie hat einen uneingeschränkten Zugang zu allen Informationen, die sie für ihre Arbeit benötigt, und ihr gegenüber bestehen Mitteilungspflichten.

Nicht abschließend geklärt ist, ob die MaRisk-Compliance-Funktion auch Weisungs- oder Vetorechte hat, wie es beispielsweise bei anderen Funktionen der Fall ist. Die Aufsicht hat sich im Protokoll zur Sitzung des Fachgremiums MaRisk am 24. April 2013 in Abschnitt 4 dazu nicht abschließend geäußert.

Vor dem Hintergrund, dass die Compliance-Funktion lediglich auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben und entsprechender Kontrollen „hinwirken“ soll, ist es gut vertretbar, ein Veto- und Weisungsrecht zu verneinen. Dafür spricht auch, dass die Geschäftsleitung nach § 25c Abs. 4a Ziff. 3c KWG weiterhin die Gesamtverantwortung trägt und die Compliance-Funktion sich jederzeit an die Geschäftsleitung wenden kann.

1. Organisatorische Stellung der MaRisk-Compliance-Funktion, AT 4.4.2 Tz. 3 MaRisk

Die MaRisk-Compliance-Funktion ist grundsätzlich der Geschäftsleitung unterstellt. Eine Anbindung an andere Einheiten ist möglich, es muss aber immer eine direkte Berichtslinie an die Geschäftsleitung existieren.

Der Wechsel des MaRisk-Compliance-Beauftragten ist dem Aufsichtsorgan unter Angabe der Gründe mitzuteilen, eine Information der Aufsicht ist nicht notwendig.

2. Abgrenzung zu anderen Bereichen

Im Institut gibt es verschiedene Compliance- und Kontrollbereiche. Zu nennen ist u. a. die WpHG-Compliance-Funktion, die Funktion zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen, aber auch die Interne Revision.

Im Hinblick auf WpHG-Compliance und die Funktion des Geldwäschebeauftragten soll die MaRisk-Compliance-Funktion einerseits das Risiko reduzieren und weiße Flecken bzw. Regelungslücken im Institut verhindern und andererseits auf eine einheitliche Compliance-Kultur hinwirken. Daher hat die MaRisk-Compliance-Funktion einen generalistischen Ansatz und stellt keine Superkontroll- oder Superrevisionsinstanz für die anderen Compliance-Bereiche dar[4]. Sofern es spezialisiertes Compliance-Wissen im Institut gibt, sind diese speziellen Compliance-Funktionen primär für die einschlägigen Themen zuständig und nicht die MaRisk-Compliance-Funktion. Entsprechendes gilt auch für das Risiko-Controlling mit dem dort angesiedelten Fachwissen.

Das Verhältnis zur Internen Revision ist durch das Three-Lines-of-Defense-Modell gekennzeichnet. Compliance gehört der zweiten Verteidigungslinie an und prüft prozessabhängig beschränkt auf compliancerelevante Themen, während die Interne Revision der dritten Verteidigungslinie angehört und prozessunabhängig das gesamte Institut einschließlich der Compliance-Funktion prüft.

3. Herausforderungen der letzten Jahre

In den letzten Jahren haben sich das Aufgabenfeld des MaRisk-Compliance-Beauftragten und seine Wahrnehmung im Institut geändert.

Er trägt heute maßgeblich dazu bei, den Fachabteilungen und somit dem Institut Sicherheit zu geben. Die Compliance-Funktion ist bereits während des laufenden Prozesses in Entscheidungen eingebunden (anders als die Revision, die überwiegend nachgelagert und rückblickend tätig ist). Auch wird die Compliance-Funktion häufig als Gesprächs- und Sparringspartner gesucht, um Prozesse und Verfahren zu optimieren bzw. Sachverhalte frühzeitig zu besprechen.

Für den MaRisk-Compliance-Beauftragten ist das Aufgabenfeld umfassender geworden. Die BaFin hat z. B. die MaRisk-Compliance-relevanten Themen

- ESG AT 2.2, 3, 4.1 MaRisk und
- Immobilien BTO 3 MaRisk

in die MaRisk aufgenommen.

Auch sind durch die Bundesbank Finanzsanktionen nun eine Aufgabe des Compliance-Beauftragten, bei denen sogar eigenständige Kontrollen erwartet werden. Die Themen

- Risikokultur,
- Produktgovernance und leider auch
- die Kriege in der Ukraine und in Nahost

sind ebenfalls MaRisk-Compliance-relevant.

Auslagerung der MaRisk-Compliance-Funktion, AT 9 MaRisk

Die Auslagerung der Funktion des MaRisk-Compliance-Beauftragten ist grundsätzlich zulässig. In AT 9 Tz. 4 MaRisk ist geregelt, dass grundsätzlich alle Funktionen und Prozesse auslagerbar sind, wenn dadurch die Ordnungsgemäßheit der Geschäftsorganisation des Institutes nach § 25a Absatz 1 KWG nicht beeinträchtigt wird. Besondere Maßstäbe gelten für die vollständige oder teilweise Auslagerung der MaRisk-Compliance-Funktion. Nach AT 9 Tz. 5 MaRisk sind zwei Fallkonstellationen denkbar: zum einen bei einem Tochterinstitut innerhalb einer Gruppe und zum anderen bei „kleinen Instituten".

Bei kleinen Instituten ist die vollständige Auslagerung der MaRisk-Compliance-Funktion möglich, sofern deren Einrichtung vor dem Hintergrund der Institutsgröße sowie der Art und des Umfangs, der Komplexität und des Risikogehaltes der betriebenen Geschäftsaktivitäten nicht angemessen erscheint. Eine abschließende Festlegung der Aufsicht, wann ein Institut als klein gilt, gibt es nicht.

Während früher häufig allein auf die Bilanzsumme abgestellt wurde, so wird heute eine Kombination aus Bilanzsumme und Komplexität als Kriterium herangezogen. Bei Bilanzsummen bis zu 30 Mrd. Euro und einem wenig komplexen Geschäftsmodell ist eine Auslagerung der MaRisk-Compliance-Funktion zulässig. Ein wenig komplexes Geschäftsmodell liegt vor, wenn Standardgeschäfte betrieben werden, insbesondere die der Genossenschaftlichen FinanzGruppe. Der Risikogehalt der so betriebenen Geschäfte ist in der Regel gering.

Spätestens wenn ein Institut nicht mehr als „SNCI " (small and non-complex institution) privilegiert ist, dürfte die vollständige Auslagerung nicht mehr möglich sein, eine teilweise Auslagerung aber weiterhin. Vorteile einer vollständigen oder teilweisen Auslagerung der MaRisk-Compliance-Funktion sind

- umfassendes, spezialisiertes Fachwissen der Compliance-Funktion,
- modernes Compliance-Management-System, bei dem u. a. Risikoanalyse, Kontrollen und Rechtsmonitoring miteinander verknüpft sind,
- Reduzierung der Personalkosten im Institut,
- Sicherstellung der Abwesenheitsvertretung des Compliance-Beauftragten,
- Sicherstellung der Aus- und Fortbildung des Compliance-Beauftragten,
- Entfall der Kosten für den gesonderten Bezug eines Rechtsmonitorings, sofern dies im Rahmen der Auslagerung gestellt wird,
- Entfall von Prüfungsleistungen durch die Interne Revision des Institutes, sofern der Dienstleister über ein Testat nach IDW PS 951 Typ 2 verfügt. ▬

Jörg Scharditzky
Abteilungsleiter MaRisk-Compliance,
E-Mail: joerg.scharditzky@dz-cp.de

[1] Die Ausführungen im Text beziehen sich auf die aktuellen Mindestanforderungen an das Risikomanagement (MaRisk), BaFin-Rundschreiben 06/2024 (BA)
[2] Christoph Kunze, MaRisk-Compliance, BVR-Bankenreihe Band 4, 3. Auflage 2024
[3] Wie auch die weiteren Arbeitshilfen des BVR, z. B. Muster-Jahresbericht, Ad-hoc-Musterbericht
[4] Christoph Kunze, a.a.O., Ziff. 1.2.1

ComplianceCollege

ComplianceCollege, das ist praxisorientiertes Compliance-Wissen aus 1.200 Auslagerungsmandaten in der Genossenschaftlichen FinanzGruppe – für Sie und Ihre Bank.

Mit Compliance bzw. dem regulatorischen Beauftragtenwesen verbindet sich zunächst das abstrakte Ziel, aufsichtsrechtliche und gesetzliche Normen umzusetzen. Bei näherer Betrachtung beinhaltet Compliance – neben den funktionalen Aufgaben von der Gefährdungsanalyse über die Kontrollplanung und -durchführung bis zur Dokumentation –, das „Wohlverhalten" jedes Einzelnen in der Bank zu unterstützen bzw. zu befördern. Compliance soll helfen, dass das recht- und ordnungsmäßige Verhalten der Mitarbeiter sichergestellt wird, und so die Bank, ihre Mitarbeiter und ihre Kunden präventiv schützen.

Tatsache ist, dass die ausgeklügeltste Technik nicht vermag, was der Mensch kann: mit einem entsprechenden Problembewusstsein und einer angemessenen Handlungsorientierung Angriffe abwehren.

Deshalb sind Compliance-Sachkundeschulungen und Sensibilisierungsmaßnahmen so ungemein wichtig. Das gilt sowohl für den Fall, dass Sie Ihrer Verantwortung im Beauftragtenwesen allein gerecht werden möchten, als auch dann, wenn Sie dafür auf einen Auslagerungspartner vertrauen.

Um genau diesen Freiraum der Entscheidung zu sichern, haben wir uns entschlossen, mit dem ComplianceCollege den Zugriff auf unser Compliance-Wissen nicht nur unseren Auslagerungskunden, sondern allen Volksbanken Raiffeisenbanken zu ermöglichen. Damit kommen wir einem vielfach an uns herangetragenen Wunsch – in Abstimmung mit unserem Kundenbeirat – nach: Im ComplianceCollege bündeln wir künftig alle Maßnahmen, die auf eine praxisorientierte Wissensvermittlung bzw. Sensibilisierung in der Compliance abzielen.

sicher

Mit den Sachkunde- und Sensibilisierungsmaßnahmen im ComplianceCollege ist die Bank sicher aufgestellt. Als Spezialist für Compliance bzw. Beauftragtenwesen in der Genossenschaftlichen FinanzGruppe kennen wir wie kein anderer die Anforderungen, aber auch die Spielräume.

Wichtig ist: Die Bank erfüllt mit unseren Sachkundeschulungen und Sensibilisierungsmaßnahmen grundsätzlich die jeweiligen aufsichtsrechtlichen Anforderungen und kann dies auch dokumentieren.

Damit das so bleibt, sind wir in einem regelmäßigen Dialog mit den Prüfungsverbänden und der Aufsicht und lassen unsere dienstleistungsbezogenen Prozesse – so auch die Schulungsprozesse – regelmäßig nach IDW PS 951 Typ 2 prüfen.

angemessen

Der Praxisbezug steht immer an erster Stelle. Wir wissen aus unseren täglichen Kontakten zu unseren Kunden, wo die „Schmerzpunkte“ liegen und mit welchem Wissen gute und schnelle Lösungen herbeigeführt werden können. Dabei haben wir das allgemeine Marktgeschehen immer im Blick und können mit unserer tiefen Kenntnis der Genossenschaftlichen FinanzGruppe und ihrer spezifischen Anforderungen fundierte Hilfestellungen geben.

Und noch mehr: Wir entwickeln aus den Erfahrungen unserer Kunden und unserer Beauftragten das Wissen weiter. Damit profitiert die gesamte Gruppe von dieser Wissensbündelung, die wir in unseren Schulungen jedem Teilnehmer zugänglich machen.

Es werden genau die Lerninhalte vermittelt, die für Ihre Bank bzw. Ihre Mitarbeiterinnen und Mitarbeiter wichtig sind. Effizienz, Relevanz und Sicherheit werden für den Lernenden spürbar und erlebbar. Die Umsetzung in die eigene praktische Tätigkeit fällt damit deutlich leichter.

gemeinsam

In den Sachkundeschulungen, die ab 2025 über das ComplianceCollege angeboten werden, stecken das Wissen und die Power der fast 200 Mitarbeiterinnen und Mitarbeiter der DZ CompliancePartner GmbH. Sie bringen, neben ihrem Expertenwissen, die tägliche Erfahrung aus 1.200 Auslagerungsmandaten

- in der Geldwäsche- und Betrugsprävention,
- in der Informationssicherheit,
- im Datenschutz,
- in der MaRisk-Compliance und
- in der WpHG-Compliance mit.

Mehr Praxiswissen geht nicht. ▬

Gabriele Seifert
Bereichsleiterin Kommunikation und Bildung,
E-Mail: gabriele.seifert@dz-cp.de

DORA gemeinsam meistern IKT-Risikokontrolle und Inf

Noch drei Monate – dann sind die DORA-Vorgaben in den Banken umzusetzen. Dazu gehört auch, dass eine IKT-Risikokontrollfunktion einzurichten ist (Art. 6 Abs. 4 DORA). Wie ist diese Funktion praktikabel auszugestalten und wie ist sie mit dem Informationssicherheitsbeauftragten in Einklang zu bringen?

Der bisherige regulative Rahmen

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) fordert in den Ziffern 4.4 BAIT ff. die Einrichtung einer unabhängigen Stelle für die Informationssicherheit (ISB).

Die wichtigste Anforderung der BaFin an den Informationssicherheitsbeauftragten ist die Mitwirkung bei der Entwicklung und die Überwachung der Informationssicherheitsstrategie des Unternehmens. Er hat darauf zu achten, dass die geltenden Sicherheitsvorgaben umgesetzt werden. Um nicht in Interessenkonflikte zu geraten, muss der ISB unabhängig agieren können (BAIT Tz. 4.5).
Es ist sicherzustellen, dass er über die notwendige fachliche Kompetenz und Ressourcen verfügt (BAIT Tz. 4.5), die erforderlich für die Bewertung des aktuellen Zustandes der Informationssicherheit sind und ihm erlauben, Maßnahmen zu beschreiben oder zu ergreifen, um die Sicherheitslage zu verbessern. Er berichtet direkt an die Geschäftsführung oder den Vorstand (BAIT Tz. 4.10).

Der ISB berät darüber hinaus die Unternehmensführung in Fragen der Informationssicherheit und informiert sie regelmäßig über den aktuellen Sicherheitsstatus (BAIT Tz. 4.4). Wie die Prüfungspraxis gezeigt hat, legt die BaFin großen Wert darauf, dass der ISB über aktuelle Entwicklungen im Bereich Informationssicherheit informiert ist, denn nur so kann sichergestellt werden, dass Sicherheitsvorfälle schnell erkannt, gemeldet und bearbeitet werden. Zudem sind regelmäßige Risikoanalysen und Schwachstellenprüfungen durch den ISB durchzuführen, um potenzielle Sicherheitsrisiken frühzeitig zu identifizieren und zu beheben.

Schlussendlich darf der ISB zur Sicherung seiner Unabhängigkeit und zur effektiven Wahrnehmung seiner Aufgaben weder in der ersten, noch in der dritten Verteidigungslinie (i.S.d. Modells der „drei Verteidigungslinien“) angesiedelt werden. Er ist ganz klassisch der zweiten Verteidigungslinie zuzuordnen, die neben der kontrollierenden auch eine beratende und schulende Aufgabe innehat.

Der zukünftige regulative Rahmen

DORA (Digital Operational Resilience Act) fordert in Art. 4 Abs. 6 DORA die Einrichtung einer IKT-Risikokontrollfunktion und lässt dabei die Funktion des Informationssicherheitsbeauftragten zunächst unerwähnt. Was heißt das konkret für den ISB und wie muss die IKT-Risikokontrollfunktion ausgestaltet werden.

Aufgaben des Informationssicherheitsbeauftragten
Um es deutlich herauszustellen: Die BaFin hält am ISB fest, obwohl sie die BAIT nach eigener Angabe ersatzlos aufgeben wird (vgl. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_0708_Interview_Kosche_Steinbrecher.html;jsessionid=31C8B0960EAADB8EE49F593980254EE1.internet981?nn=19669324, abgerufen am 26.09.2024).

– Beauftragter
formationssicherheit

KI-gestützter VertragsCheck auf DORA-Konformität

Die „größte Herausforderung" in diesem Jahr ist DORA und dort die „Überprüfung bestehender Dienstleisterverträge", so das Ergebnis der aktuellen Bankenumfrage 2024 des Genoverbandes e.V. Das deckt sich mit unserer Einschätzung: Die manuelle Prüfung der Verträge ist enorm zeit- und arbeitsaufwendig.

Wir haben deshalb eine KI-gestützte Vollständigkeitsprüfung entsprechend den DORA-Klauseln entwickelt. Das Vertragswerk mit IKT-Drittparteien wird systematisch und nachvollziehbar auf DORA-Konformität untersucht, fehlende Passagen werden erkannt und entsprechende Formulierungsvorschläge aus den BVR-Musterklauseln ausgegeben.

Die Vorteile liegen auf der Hand: Die Bank profitiert

- von einer deutlichen Steigerung der operativen Effizienz;
- von einer sicheren Lösung: Die Vertragsprüfung erfolgt auf Systemen der DZ CompliancePartner GmbH. Es bedarf somit keiner aufwendigen Bewertung eines externen Cloud-Dienstleisters;
- von einer klaren Verbundorientierung: Analysen und Ausgaben basieren einerseits auf Verbundempfehlungen, andererseits auf unserer Expertise aus mehr als 100 Mandaten in der Informationssicherheit.

Das Tool ist bereits im Rahmen unserer DORA-Umsetzungsbegleitung und -beratung im Einsatz. Zukünftig wird es als eine integrale Standardleistung der Auslagerung „Beauftragter IKT-Risikokontrolle und Informationssicherheit" (IKT-Risikokontrollfunktion) angeboten.

Rechtlicher Hinweis: Die Dienstleistung umfasst den Abgleich der relevanten Vertragsklauseln unter Einsatz von KI. Sie stellt keine rechtliche Beratung, Bewertung oder Einschätzung der DORA-Konformität gemäß § 2 des Rechtsdienstleistungsgesetzes (RDG) dar. Die Interpretation der Ergebnisse, rechtliche Bewertungen und Anpassungen von Verträgen liegen in der Verantwortung des Kunden.

DORA fordert ausdrücklich (Art. 5 Abs. 2 lit. c DORA), dass Finanz-institute klare Verantwortlichkeiten für alle IKT-bezogenen Funktionen festlegen. Zwar ändert sich mit DORA der Blickwinkel, die Verordnung folgt einer strikten Risikoperspektive (im Gegensatz zu den BAIT, die eine Sicherheitsperspektive eingenommen hatten). Aber DORA betrachtet die gleichen Inhalte wie die BAIT. Tatsächlich betont sie sogar die Anforderungen an die Informationssicherheit als „den zentralen Baustein der Operativen Resilienz", um das Schutzziel eines verbesserten IKT-Risikomanagements zu erreichen. Insoweit ist nachvollziehbar, warum die BaFin und auch der BVR die in DORA statuierte „IKT-Risikokontrollfunktion" **als ergänzende Aufgabenstellung des bisherigen ISB formulieren.**

Die Beibehaltung des ISB lässt sich darüber hinaus aus der ISO-Norm 27001 herleiten: Die ISO/IEC 27001 verlangt, dass ein Unternehmen eine klar definierte Verantwortung für das Management der Informationssicherheit hat. Das bedeutet, dass bestimmte Aufgaben und Zuständigkeiten für die Informationssicherheit formal festgelegt werden müssen. Dazu gehört die Einrichtung eines Informationssicherheitsmanagementsystems (ISMS). In Klausel 5.3 der ISO 27001 wird zudem festgelegt, dass Rollen und Verantwortlichkeiten für die Informationssicherheit klar benannt werden müssen. Damit ist

nichts anderes als eine ISB-Funktion gemeint.

Des Weiteren sind die vierteljährlichen Berichtspflichten zur Informationssicherheit (MaRisk AT 4.3.2 Tz. 3) weiterhin und somit auch nach dem 17. Januar 2025 vorzunehmen. Die BaFin hat angekündigt, zur Funktion des ISB nochmal gesondert Stellung zu nehmen.

Zusammenfassend werden mit Inkrafttreten von DORA die Anforderungen an den ISB eher erweitert. Der ISB wird im Zusammenspiel mit der IKT-Risikokontrollfunktion eine wichtige Rolle spielen, die EU-weiten Anforderungen aus DORA umzusetzen und damit schlussendlich die operative Resilienz der Bank sicherzustellen.

Aufgaben der IKT-Risikokontrollfunktion

Die IKT-Risikokontrollfunktion (Art. 6 Abs. 4 DORA) ist eine zentrale Komponente von DORA. Sie bezieht sich auf die organisatorischen und prozessualen Maßnahmen, die ein Finanzinstitut ergreifen muss, um die Risiken im Zusammenhang mit der IT-Infrastruktur, den IT-Prozessen und der Cybersicherheit zu kontrollieren und zu überwachen.

Gemäß Art. 6 Abs. 4 S. 2 DORA ist die IKT-Risikokontrollfunktion – genau wie der ISB – in der „zweiten Verteidigungslinie“ anzusiedeln und mit entsprechenden Mitteln und Befugnissen auszustatten.

Versteht man diese Funktion also sachgerecht als Weiterentwicklung der bisherigen ISB-Funktion nach BAIT (s.o.), so bleiben nur ergänzende Aufgaben. Zentrale Punkte sind hierbei

- die Bewertung der Risikoposition gegen Cyberrisiken und
- die Bewertung der Resilienz bzw. Widerstandsfähigkeit der IKT-Risiken sowie
- die entsprechende Berichterstattung (Art. 6 Abs. 5 DORA).

Es sind ergänzende „High-Level“ Risikokontrollen einzuführen und zu berichten, um hieraus Maßnahmen ableiten zu können (inkl. Umsetzungsstand der Maßnahmen). Die Funktion bildet damit die Überwachung des IKT-Risikomanagementrahmens mit ab.

Fazit

Das bewährte System der ISB-Funktion kann und sollte beibehalten und durch die Aufgaben der IKT-Risikokontrollfunktion ergänzt werden.
Dies spart ein Neuaufsetzen an sich bewährter Prozesse und ermöglicht eine nahtlose Zusammenführung der Aufgaben – ohne System- und Prozessbrüche. Die neue Funktion ist am besten als „Beauftragte(r) IKT-Risikokontrolle und Informationssicherheit“ zu verstehen. Die Stellenbeschreibung des bisherigen ISB ist entsprechend anzupassen.
Die DZ CompliancePartner GmbH wird ab dem 17. Januar 2025 den Beauftragten IKT-Risikokontrolle und Informationssicherheit (IKT-Risikokontrollfunktion) in der Vollauslagerung anbieten. ▬

Marc-Timo Brandenburger
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: marc-timo.brandenburger@dz-cp.de

Benjamin Wellnitz
Bereichsleiter Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de

Beschwerdemanagement – im Sinne des Kunden

Der Gesetzgeber hat im Wertpapiergeschäft auf unionsrechtlicher und nationaler Ebene Mindestanforderungen an das Beschwerdemanagement sowie den dazugehörigen Beschwerdebericht formuliert. Hierbei handelt es sich um zwingende Pflichten. Bei Verstößen drohen Prüfungsfeststellungen, gegebenenfalls Sonderprüfungen und hohe Bußgelder.

Für die Aufsichtsbehörde scheint das Beschwerdemanagement ein guter Indikator für Missstände in den Instituten zu sein. Eingeleiteten BaFin-Sonderprüfungen gingen oftmals Auffälligkeiten im Beschwerdemanagement des jeweiligen Institutes voraus. Hieraus lässt sich die Relevanz eines ordnungsgemäßen, effektiven und funktionierenden Beschwerdemanagements ableiten. Die ordnungsgemäße Bearbeitung von Beschwerden wirkt sich zudem erfahrungsgemäß positiv auf die Kundenbeziehung aus. Werden die Vorgaben jedoch nicht oder nur unzureichend umgesetzt, drohen hier Feststellungen durch die externe Prüfung, gegebenenfalls sogar Sonderprüfungen und hohe Bußgelder. Im Ergebnis führen diese Regelungen zu einem hohen Umsetzungsaufwand im Institut, im Speziellen für die Compliance-Funktionen (insbesondere WpHG- und MaRisk-Compliance).

Beschwerdebegriff

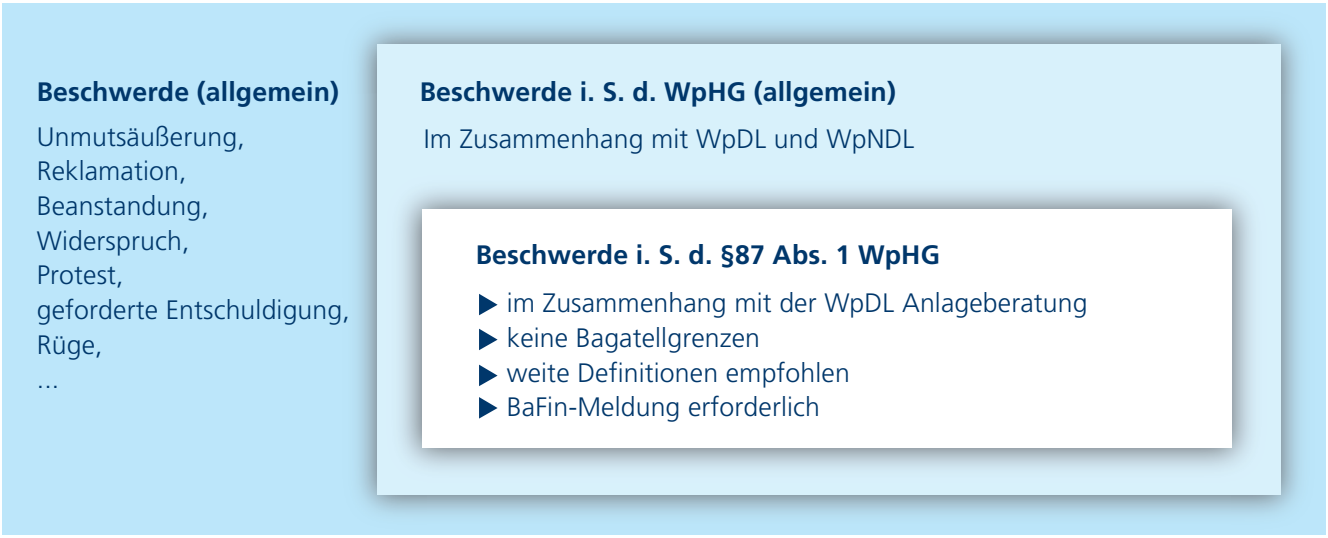
Zur Erleichterung der Rechtsanwendung hat die BaFin in BT 12.1 MaComp den Begriff der Beschwerde legaldefiniert. **Hiernach ist eine Beschwerde jede Äußerung der Unzufriedenheit, die ein Kunde i. S. d. § 67 Abs. 1 WpHG oder ein potenzieller Kunde (Beschwerdeführer) an ein Wertpapierdienstleistungsunternehmen im Zusammenhang mit dessen Erbringung einer Wertpapierdienstleistung oder einer Wertpapiernebendienstleistung richtet.**

Der Begriff „Beschwerde“ muss nicht zwingend durch den Beschwerdeführer genutzt werden. Eine Beschwerde bedarf laut den MaComp zudem keiner bestimmten Form. Relevantes Abgrenzungsmerkmal zu anderen an das Institut gerichteten Beschwerden ist hierbei der Zusammenhang mit der „Erbringung der Wertpapierdienstleistung oder Wertpapiernebendienstleistung“. Hiervon sind im Weiteren Beschwerden zu differenzieren, die sich auf die Tätigkeit eines Anlageberaters (aktiv oder inaktiv) i. S. d. § 87 Abs. 1 WpHG beziehen und von einem Privatkunden gemäß § 67 Abs. 3 WpHG erhoben werden.

Darunter fallen z. B. Beschwerden über folgende Sachverhalte:

- unterbliebene oder fehlerhafte Einholung der Kundenangaben,
- keine oder unzureichende Aufklärung (z. B. über Kosten, Zuwendungen etc.),
- keine oder fehlerhafte Dokumentation der Beratungsgespräche bzw. keine Zurverfügungstellung der Beratungsdokumentation,
- fehlerhafte Eingabe oder Weiterleitung einer Wertpapierorder durch den Anlageberater, sofern diese im Zusammenhang mit der Beratung steht.

Abb. 1. **Beschwerdebegriffsunterteilung**



Quelle: eigene Darstellung

Alle Beschwerden in diesem Zusammenhang sind schließlich gemäß § 87 Abs. 1 S. 4 WpHG i. V. m. § 8 Abs. 4 WpHGMaAnzV der BaFin gesondert, innerhalb von sechs Wochen nach Beschwerdeerhebung, über die Melde- und Veröffentlichungsplattform (MVP) mit folgenden Informationen zu melden:

- Datum der Beschwerdeerhebung,
- Name des Mitarbeiters, aufgrund dessen Tätigkeit die Beschwerde erhoben wird, sowie dessen eindeutige interne Kennnummer,
- gegebenenfalls die zugehörige Zweigstelle/-niederlassung oder sonstige Organisationeinheit des Instituts.

Entsprechend empfiehlt es sich in der Praxis als Institut – aus Gründen der Rechtssicherheit – sämtliche eingehenden Beschwerden zu erfassen, auszuwerten und somit keine Risiken einzugehen. Schließlich gehen Auslegungsfehler bei der Frage, ob es sich um eine aufzeichnungspflichtige Beschwerde handelt oder nicht, im Zweifelsfall zu Lasten des jeweiligen Instituts.

Folglich ist im Hinblick auf die Möglichkeit einer direkten Beschwerde bei der BaFin und der damit einhergehenden erhöhten Aufmerksamkeit durch die Aufsicht davon abzuraten, Beschwerden wegen vermeintlich „fehlender Relevanz“ nicht zu erfassen. Wichtig ist hierbei, dass auch potenzielle Kunden Beschwerden artikulieren können. Eine aktive Geschäftsbeziehung ist keine zwingende Voraussetzung für das Einreichen einer Beschwerde.

Vorgaben zur Beschwerdebearbeitung

In den MaComp wird beschrieben, welche internen Vorkehrungen zur Beschwerdebearbeitung anhand eines sogenannten Beschwerdemanagements vorgenommen werden müssen. Differenziert wird hierbei zwischen „internen Vorkehrungen“ und „internen Verfahren“.

a. Interne Vorkehrungen

Vorausgesetzt wird gemäß Art. 26 Abs. 1 S. 1 Delegierte Verordnung (EU) 2017/565 (im Folgenden DV genannt) ein wirksames und transparentes Verfahren, das eine unverzügliche Abwicklung von Beschwerden gewährleistet. „Unverzüglich“ ist hierbei ein Rechtsbegriff, der in § 121 Abs. 1 S. 1 BGB mit der Beschreibung „ohne schuldhaftes Zögern“ legaldefiniert ist. Beschwert sich Kunde K z. B. an einem Montag, dürfte „Unverzüglichkeit“ bei Erfassung der Beschwerde am darauffolgenden Montag nicht mehr vorliegen. Aus BT 12.1 MaComp ergibt sich ferner, dass die Grundsätze für das Beschwerdemanagement eindeutige, genaue und aktuelle Informationen über das Verfahren zur Abwicklung von Beschwerden enthalten müssen sowie dass die Geschäftsleitung die Grundsätze gemäß Art. 26 Abs. 1 S. 4 DV bestätigen muss. Die Beschwerdebearbeitung ist außerdem schriftlich zu dokumentieren. Fundamentaler Bestandteil der internen Vorkehrungen ist die vorgeschriebene Einrichtung einer

Beschwerdemanagementfunktion. Dieser obliegt die Zuständigkeit für die Prüfung der Beschwerden, was ein Ausdruck des Prinzips der wirksamen Grundsätze und Verfahren für das Beschwerdemanagement ist. Hierdurch werden außerdem mögliche Interessenkonflikte vermieden.

Kernpunkte der internen Vorkehrungen sind daher:

- Einrichtung einer Beschwerdemanagementfunktion,
- Sicherstellung des internen Informationsflusses,
- schriftliche Dokumentation der Beschwerdebearbeitung,
- Einbindung der Geschäftsleitung,
- wirksame und transparente Grundsätze und Verfahren,
- Vermeidung von Interessenkonflikten.

b. Interne Verfahren

Laut Art. 26 Abs. 1 S. 2 DV sind die eingegangenen Beschwerden aufzuzeichnen und Maßnahmen zur Lösung zu treffen. Hieraus resultiert die Pflicht zur Etablierung eines internen Beschwerderegisters. Gemäß § 9 Abs. 4 WpDVerOV beträgt die Dauer der Aufbewahrung von Kundenbeschwerden mindestens fünf Jahre. Sollten Aufbewahrungen über fünf Jahre durchgeführt werden, sind die spezifischen Anforderungen der EU-DSGVO zu beachten. Aus dem Wortlaut des BT 12.1.3 Nr. 4 und 5 MaComp wird zudem deutlich, dass das Beschwerdemanagement insgesamt kein bürokratischer Selbstzweck ist. Vielmehr soll über das Beschwerdemanagement eine Funktion etabliert werden, die anhand von Indikatoren Missstände innerhalb eines Instituts aufdeckt. Deswegen ist es gemäß BT 12.1.3 Nr. 4 MaComp erwünscht, dass durch die Überprüfung der Compliance-Funktion eine ordnungsgemäße Abwicklung der Beschwerden innerhalb der Institute gewährleistet wird und ferner „Risiken und Probleme" ermittelt werden.

Die bloße Ermittlung reicht jedoch nicht aus, weswegen explizit eine Behebung der aufgetretenen Risiken und Probleme gefordert wird. Für die Behebung gemäß Art. 26 Abs. 7 DV werden seitens der Aufsicht beispielhafte Maßnahmen aufgeführt:

- Ursachenermittlung,
- Identifizierung von Parallelen,
- Prävention für zukünftige Prozesse und Produkte.

Im Rahmen des internen Verfahrens des Beschwerdemanagements ist zudem sicherzustellen, dass Kunden Beschwerden kostenlos einreichen können und in einfach verständlicher Sprache, zeitnah über den Prozess ins Bild gesetzt werden. Kommt es z. B. zu Verzögerungen, ist dies dem jeweiligen Kunden mitzuteilen (vgl. BT 12.1.3 Nr. 10 MaComp). Hierbei ist der Kunde über seine Möglichkeit, die Beschwerde an eine Stelle zur alternativen Streitbeilegung weiterzuleiten oder eine zivilgerichtliche Klage zu erheben, aufzuklären (vgl. BT 12.1.3 Nr. 11 und 12 MaComp). Am Ende des Beschwerdeprozesses ist das Institut in der Pflicht, zur Beschwerde Stellung zu beziehen und dem Beschwerdeführer seinen Standpunkt mitzuteilen. Zusammengefasst lässt sich festhalten, dass die internen Vorkehrungen im Zusammenspiel mit dem jeweiligen Verfahren ein wirksames Beschwerdemanagement i. S. d. WpHG gewährleisten müssen.

Rolle des Beschwerdeberichts

Der Beschwerdebericht nach Art. 26 Abs. 6 DV i. V. m. BT 12.2 MaComp ist das Mittel der Aufsicht, um sich ein Bild über ein Institut und auch – nachgelagert – vom Markt zu verschaffen.

Form, Aufbau und Inhalt sind gemäß der Anlage „BT 12.2 – Beschwerdebericht nach Art. 26 Abs. 6 der Delegierten Verordnung (EU) 2017/565" vorgegeben. Weitere Ausführungen zum Inhalt sind dem BT 12.2 Nr. 3 MaComp zu entnehmen.

Da diese Anlage bereits aus Datenschutzgründen nicht alle Daten zur Weiterleitung einer Beschwerde (z. B. Kundendetails) beinhaltet bzw. fordert, ist der Umkehrschluss, dass das interne Beschwerderegister neben den relevanten

Daten wie Kundendetails mindestens auch die geforderten Angaben aus der Anlage erfasst.

Bei der Erfassung von Beschwerden ist wiederum nach BT 12.2 Nr. 4 MaComp zu beachten, dass alle Beschwerden – auch Beschwerden von potenziellen Kunden wie auch Beschwerden, die bei vertraglich gebundenen Vermittlern (im Folgenden vgV genannt) eingehen – zu berücksichtigen sind. Folglich muss ein Institut dafür Sorge tragen, dass die eingesetzten vgV entsprechende Beschwerdeaufzeichnungen tätigen und diese zur Auswertung an das Institut bzw. die Beschwerdemanagementfunktion weiterleiten. Des Weiteren empfiehlt sich eine entsprechende Aufschlüsselung nach diesen Unterscheidungskriterien im Beschwerderegister.

Die Einreichung des Beschwerdeberichts hat schließlich gemäß BT 12.2 Nr. 1 MaComp einmal jährlich bis zum 1. März für das vorangegangene Kalenderjahr zu erfolgen. Die BaFin sieht die Einreichung über das MVP-Portal vor.

Fazit

Beschwerden sind für die Aufsicht ein wichtiges Indiz, inwiefern Kundeninteressen gewahrt werden und der ordnungsgemäße Geschäftsbetrieb gewährleistet ist. Deswegen sollte das Thema nicht unterschätzt werden. Beschwerden sollten hierbei auch nicht als Makel am eigenen Institut verstanden werden, sondern als Teil der Lösung. Gleichzeitig vermittelt ein funktionierendes Beschwerdemanagement dem Kunden eine hohe Wertschätzung gegenüber seinem Feedback. Letztlich ist Beschwerdemanagement immer Vertrauensarbeit. ▬

Felix Fröhlich
Beauftragter WpHG-Compliance,
E-Mail: felix.froehlich@dz-cp.de

Giannis Petras
Beauftragter WpHG-Compliance,
E-Mail: giannis.petras@dz-cp.de

Mobiles Arbeiten – auch eine Frage der Compliance

Die Welt der Arbeit hat sich in den letzten Jahren stark verändert. Durch die fortschreitende Digitalisierung ist dabei auch der Begriff „New Work" vermehrt aufgekommen. „New Work" steht für eine zeitgemäße Arbeitsphilosophie, die eine flexible und ortsunabhängige Arbeitsumgebung fördert – ob im Büro, zu Hause oder unterwegs. Diese moderne Form des Arbeitens ermöglicht den Mitarbeitenden, ihre Tätigkeiten effizient an unterschiedliche Umgebungen anzupassen, ganz gleich, wo sie sich befinden. Doch wie verhält es sich mit der Compliance im Hinblick auf mobiles Arbeiten? Welche Regeln und Richtlinien gilt es dabei zu beachten? Und wie verändern sich unsere Produktivität und Work-Life-Balance durch das mobile Arbeiten?

Die Bedeutung von Compliance beim mobilen Arbeiten

Für unsere Mitarbeiter ist die Balance zwischen Job und Privatleben ein hohes Gut. Durch die generelle Einführung von mobilem Arbeiten bieten wir eine hohe Flexibilität, um den Beruf besser mit der individuellen Lebenssituation in Einklang zu bringen. Durch den flexiblen Arbeitsort innerhalb Deutschlands wirkt sich die individuelle Arbeitsgestaltung vor allem auf die Produktivität positiv aus. Im Detail lassen sich die Produktivitätsgewinne auf den Wegfall von Arbeitswegen und die eigenverantwortliche Arbeit zurückführen. Dies ist sowohl aus Arbeitnehmer- als auch aus Arbeitgebersicht eine sichtbar positive Veränderung. Das Thema Compliance ist hierbei von zentraler Bedeutung, auch für uns im Unternehmen. Während wir bemüht sind, unseren Tätigkeiten im Beauftragtenwesen innerhalb des Compliance-Bereichs nachzukommen, sind wir natürlich auch bestrebt, alle festgeschriebenen Regelungen einzuhalten, um mobiles Arbeiten möglich zu machen. Diese Regularien dienen dazu, rechtliche Risiken zu minimieren und ein faires, sicheres Arbeitsumfeld zu gewährleisten. So sind vor allem Themen wie Datenschutz und IT-Sicherheit von hoher Relevanz. Zudem muss sichergestellt werden, dass bei der flexiblen Arbeitsplatzgestaltung arbeitsrechtliche Vorgaben, wie Arbeitszeitgesetze oder Pausenregelungen, eingehalten

werden. Andernfalls können Verstöße nicht nur rechtliche Konsequenzen nach sich ziehen, sondern auch das Vertrauen der Mitarbeitenden in die Integrität des Unternehmens destabilisieren. Der Schlüssel zu einer Compliance-konformen Umsetzung von mobilem Arbeiten liegt in klar formulierten, verbindlichen Richtlinien. Diese sollten in Abstimmung mit der Rechtsabteilung, dem Verantwortlichen für Datenschutz, der Informationssicherheit und auch dem Verantwortlichen für Arbeitssicherheit erarbeitet und regelmäßig überprüft werden. Die Einhaltung von Compliance-Vorgaben liegt aber nicht nur beim Unternehmen, sondern auch bei den Mitarbeitenden selbst. Regelmäßige Schulungen und Sensibilisierung sind notwendig, um ein
Bewusstsein für mögliche Risiken zu schaffen und die Relevanz der Einhaltung zu verdeutlichen.

Fazit

Zusammenfassend bietet mobiles Arbeiten eine einzigartige Möglichkeit, den Job flexibler an die individuelle Lebenssituation anzupassen. Es fördert eine gesteigerte Work-Life-Balance, steigert die Produktivität, unterstützt die Eigenverantwortung und ermöglicht eine berufliche Mobilität. Mobiles Arbeiten wirkt sich positiv auf die Attraktivität unseres modernen Unternehmens aus und führt zu Talentgewinnungs- und Bindungspotenzialen im Rekrutierungsbereich. Mit klaren Richtlinien, regelmäßigen Schulungen und einer unterstützenden technologischen Infrastruktur lässt sich mobiles Arbeiten nicht nur effizient, sondern auch sicher und regelkonform gestalten. Compliance und Flexibilität müssen dabei keine Gegensätze sein – im Gegenteil: Sie ergänzen sich, wenn die richtigen Rahmenbedingungen geschaffen werden. ▬

Kevin Lohmann
Bereichsleiter Unternehmenssteuerung,
E-Mail: kevin.lohmann@dz-cp.de

DORA-Umsetzung

Bereits im Februar 2024 haben wir das DORA-Umsetzungsprojekt in der DZ CompliancePartner GmbH gestartet. Sechs Teams aus unterschiedlichen Fachbereichen beschäftigen sich seitdem intensiv mit der Umsetzung der Inhalte.

Dabei gilt es vor allem, die Kundensicht mit der Perspektive des IKT-Drittdienstleisters zu vereinen.

Weiterentwicklung des Dienstleistungsangebots

Priorität hatte zunächst die Weiterentwicklung des Dienstleistungsangebots, insbesondere das Angebot für die Umsetzungsbegleitung der Kunden. Ziel war und ist, unseren Kunden pragmatische Lösungen für die praktische Umsetzung anbieten zu können.

Dafür werden im Projekt Informationen aus verschiedensten Quellen gesichtet, verarbeitet und weiterentwickelt, um sie als Umsetzungshilfen oder in Form zielgruppengerechter Schulungsangebote den Kunden zur Verfügung zu stellen.

Beispielsweise wurde ein Tool zur systematischen Umsetzung und Dokumentation der DORA-Inhalte auf Basis der GAP-Analyse des BVR entwickelt, das bereits in zahlreichen Kundenprojekten eingesetzt wird. Zudem wurde eine Seminarreihe für Verantwortliche – mit Hilfestellungen für die Umsetzung – und dann auch für Vorstände entwickelt, in denen ein fachlicher Gesamtüberblick bzw. die vorstandsrelevanten Handlungsfelder vermittelt wurden. Weitere bedarfs- und zielgruppenorientierte Webinare sind in Planung, bereits bestehende Web Based Trainings (WBT) werden DORA-konform aktualisiert.

Sowohl bei der Gestaltung der Kundenprozesse als auch bei der internen Umsetzung sind die zentralen Muster und Hilfestellungen aus dem Verbund handlungsleitend.

Einen großen Stellenwert im Projekt hat die Weiterentwicklung unserer eigenen IT-Anwendungen und deren Anpassung an die Anforderungen von DORA.

ISI kompakt und BCM kompakt werden fristgerecht vor dem Inkrafttreten von DORA am 17. Januar 2025 DORA-ready sein und somit aufsichtsrechtlich konform sein.

Dabei wird sehr viel Wert auf eine umfangreiche Vorbefüllung, z. B. mit Bewertungshilfen, gelegt. Sie stellt für die Umsetzungsverantwortlichen in der Bank eine große Hilfestellung dar und entlastet somit spürbar die bankinternen Ressourcen.

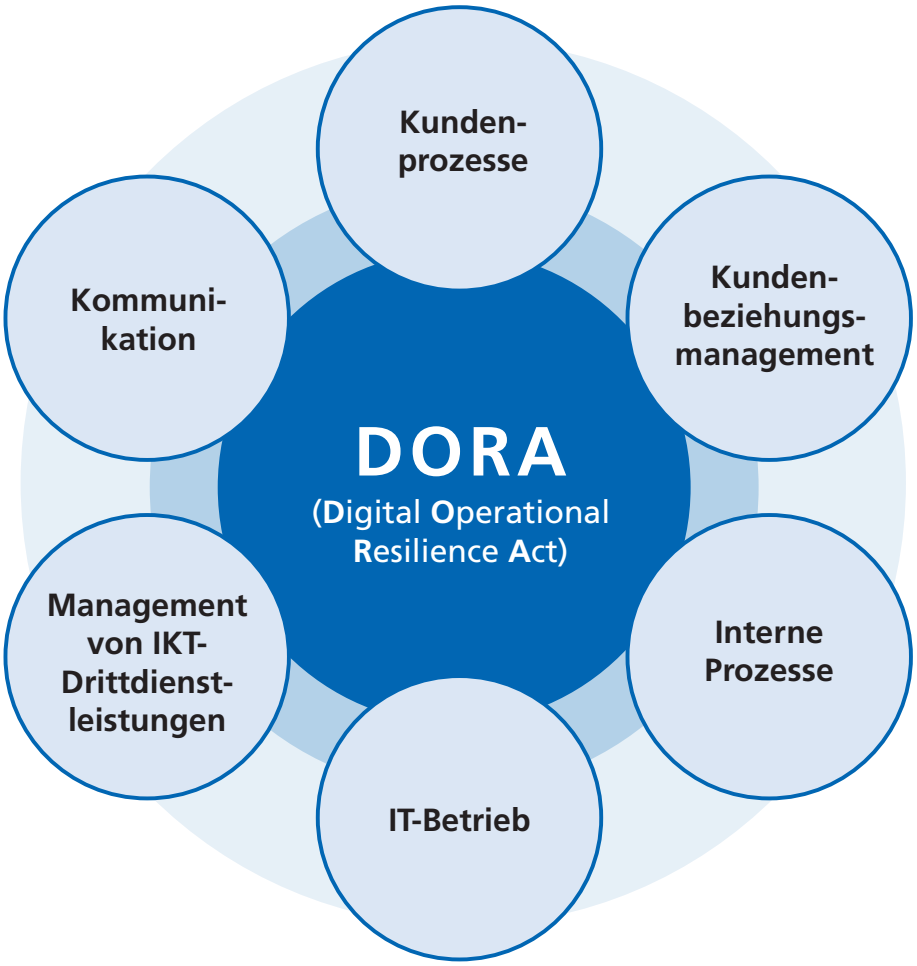
Um noch ressourcenschonender arbeiten zu können und sowohl die Kunden als auch die internen Mitarbeitenden zu entlasten, setzen wir ein Tool zum KI-gestützten VertragsCheck in Bezug auf DORA-Konformität ein (siehe auch S. 15).

Als IKT-Dienstleister passen auch wir alle bestehenden Dienstleistungsverträge mit unseren Kunden an: Noch in diesem Jahr erhalten alle Bestandskunden DORA-konforme Vertragsdokumente.

Ergänzend werden auch die bestehenden Produkte um neue Leistungsbausteine ergänzt. So wird u. a. die Funktion des Informationssicherheitsbeauftragten zum neuen Jahr um die Aufgaben der IKT-Risikokontrollfunktion erweitert (siehe auch S. 14).

Als IKT-Drittdienstleister, der kritische und wichtige Funktionen in Banken unterstützt, überprüfen wir ebenfalls alle internen Prozesse im IT-Betrieb, in der Informationssicherheit und im Notfallmanagement. Es bleibt dabei nicht nur bei der Anpassung der Prozesse. Mithilfe geeigneter Testverfahren werden diese geprüft. Derzeit wird eine Zertifizierung nach ISO 27001 vorbereitet.

In Bezug auf das IKT-Drittparteienmanagement folgen wir grundsätzlich der Strategie, möglichst autark zu agieren. Gerade im IT-Betrieb wird großer Wert auf die Unabhängigkeit von Dritten gelegt. Da sich aber nicht alle Leistungen aus eigener Hand erbringen lassen, stellen wir auch an unsere IKT-Dienstleister höchste Anforderungen an die Informationssicherheitsstandards. Derzeit erfolgt eine Ab-



stimmung mit den Vertragspartnern, um auch dort die fristgerechte Einhaltung der relevanten Anforderungen nach DORA sicherzustellen.

Im Fazit bleibt festzuhalten: Informationssicherheit ist für uns kein einmaliges Projekt – sie ist fest verankert in all unseren Prozessen. DORA bietet hier einen neuen Orientierungsrahmen und ist in der Praxis ein guter Anlass, bewährte Strukturen und Prozesse zu prüfen und nachhaltig zu verbessern. ▬

Ansprechpartner:
Yvonne Debus, *Referentin Projektmanagement,*
E-Mail: yvonne.debus@dz-cp.de

Interne Revision

Regelmäßig berichten wir an dieser Stelle über die Interne Revision der DZ CompliancePartner GmbH. Wir möchten Ihnen damit einen Überblick über die Qualität der unterschiedlichen Auslagerungsdienstleistungen geben und Sie in Ihrem Auslagerungscontrolling unterstützen. Die durchgeführte Revisionstätigkeit der DZ CompliancePartner GmbH genügt den Anforderungen gemäß MaRisk AT 4.4.3 und BT 2.

Seit der letzten Berichterstattung in der Point of Compliance (2/2024, S. 27) wurden aus der von der Geschäftsführung genehmigten Jahresprüfungsplanung 2024 die Prüfungen der Bereiche „MaRisk-Compliance“, „WpHG-Compliance“ und „Produkte und Prozesse“ abgeschlossen, wobei die beiden ersten an die Mandanten der jeweiligen Auslagerungen versandt wurden. Der letztgenannte Prüfungsbericht ist nicht dienstleistungsbezogen und wurde daher intern veröffentlicht.

Der Quartalsbericht Q2 2024 der Internen Revision wurde fristgerecht erstellt und den Mandanten, die im Zeitraum zu unseren Kunden gehörten, zur Verfügung gestellt.

Weiterhin wurde turnusgemäß ein Follow-up-Quartalsbericht für das zweite Quartal 2024 erstellt und der Geschäftsführung der DZ CompliancePartner GmbH vorgelegt. In den Follow-up-Berichten wird die Abarbeitung der von internen und externen Prüfern getroffenen Maßnahmen / Empfehlungen dokumentiert. Offene Punkte werden durch die Interne Revision konsequent nachgehalten.

Als weiterer Informationsaustausch finden zwischen dem Sprecher der Geschäftsführung der DZ CompliancePartner GmbH und der Internen Revision regelmäßige Jours Fixes statt. ▬

Ansprechpartner:
Lars Schinnerling, *Bereichsleiter Interne Revision,*
E-Mail: lars.schinnerling@dz-cp.de

Wirtschaftliche Lage

Die DZ CompliancePartner GmbH wächst unvermindert. Zum Jahreswechsel wird die Beschäftigtenzahl die 200er-Grenze überschritten haben. Damit gelingt es uns weiterhin, auch im knappen Fachkräftemarkt unsere Kolleginnen und Kollegen zu binden und neue Mitarbeitende zu rekrutieren. Ein herzliches Dankeschön an das bestehende Team für diesen Erfolg!

Das kumulierte Ergebnis am Ende des dritten Quartals 2024 ist positiv. Mit einem Erlös von 17.139 TEuro liegen wir gut 6 % über dem geplanten Erlösziel von 16.146 TEuro. Wesentlicher Treiber hierbei sind Erlöse aus der DORA-Umsetzungsberatung, die das Unternehmensergebnis insgesamt positiv beeinflussen. Aber auch alle anderen Bereiche erreichen oder überschreiten das geplante Ziel zu Q3 leicht. Dem steht derzeit eine Aufwandsunterschreitung von 542 TEuro gegenüber, die sich aber wegen der hohen internen Aufwendungen für die DORA-Umsetzung und -Umsetzungsberatung bis Jahresende deutlich verringern wird.

Insgesamt gehen wir im Jahr 2024 von einem Ergebnis von ca. 2 Mio. Euro vor Steuern aus. Damit werden wir das geplante Jahresergebnis von 1,745 Mio. Euro übertreffen.

Ansprechpartner:
Jens Saenger, *Sprecher der Geschäftsführung,*
E-Mail: jens.saenger@dz-cp.de

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken