Point of Compliance
Das Risikomanagement-Magazin

AUSGABE 2/2026

PoC

DZ CompliancePartner

Folgen Sie der DZ CompliancePartner GmbH auf Social Media.

IMPRESSUM

PoC – Point of Compliance
Das Risikomanagement-Magazin,
Ausgabe 39, 2/2026
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, Christoph Patzke, Giannis Petras, Jens Saenger, Jörg Scharditzky, Lars Schinnerling, Jacob Schirner, Katja Schlüter, Thomas Schröder, Christian Tipkemper, Justus Tychek, Marina Waidelich, Benjamin Wellnitz

Bildnachweise: iStockphoto.com/Devrimb, www.verbraucherzentrale.de, DZ Compliance-Partner GmbH
Gestaltung: DZ CompliancePartner GmbH
Druck: Thoma Druck, Dreieich

Redaktionsschluss: 31. August 2026
Auflage: 3.500 Exemplare

Veränderte aufsichtsrechtliche Erwartungen,

neue Geschäftsfelder und die zunehmende Bedeutung wirksamer Governance prägen die aktuelle Agenda der Banken.

Jens Saenger
Sprecher der Geschäftsführung

Mit „meinKrypto“ wird Krypto in der Genossenschaftlichen FinanzGruppe zum konkreten Bankgeschäft. Der regulierte Zugang zu Kryptowerten eröffnet neue Möglichkeiten, stellt die Institute aber zugleich vor Anforderungen an Governance, Kundenschutz, Geldwäscheprävention und Compliance. Bestehende Strukturen gilt es gezielt weiterzuentwickeln und die neue Assetklasse verantwortungsvoll in die Organisation zu integrieren (siehe Seite 4).

Mit der AMLR verändert sich der regulatorische Rahmen spürbar. Compliance entsteht zuvorderst dort, wo Menschen Verantwortung übernehmen und Werte im täglichen Handeln sichtbar werden. Die neue Rolle des Compliance-Managers nach AMLR unterstreicht dieses neue aufsichtsrechtliche Verständnis (siehe Seite 17).

Mit der 9. MaRisk-Novelle und DORA rücken zudem Risikosteuerung und operative Resilienz weiter in den Fokus. Krisenfestigkeit wird zur Führungsaufgabe: Klare Verantwortlichkeiten, belastbare Entscheidungswege und regelmäßige Übungen helfen, auch in komplexen Situationen handlungsfähig zu bleiben (siehe Seite 8 und Seite 23).

Ob AMLR, MaRisk oder Krypto – sie alle verändern die Prozesse nicht nur in der Compliance bzw. Marktfolge, sondern auch im Markt. Wie bei allen Veränderungsprozessen ist eine frühzeitige Weichenstellung wichtig. Um sich zu orientieren, empfehlen wir den **Compliance-Kongress 2026 am 2. Oktober 2026 auf Schloss Montabaur.** Dort haben Sie die Möglichkeit, sich mit Experten und Entscheidern im Verbund auszutauschen.

Ich wünsche Ihnen eine anregende Lektüre.

Herzlichst
Ihr Jens Saenger

„A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."

So beginnt das Bitcoin-Whitepaper, das 2008 von Satoshi Nakamoto veröffentlicht wurde.

Bitcoin wurde als dezentrales Zahlungssystem in Reaktion auf die Finanzkrise 2008 entworfen. Das Ziel hinter der Einführung war es, das „Double-Spending-Problem" ohne zentrale Vertrauensinstanz durch die Distributed-Ledger-Technologie (DLT) zu lösen. In der klassischen Finanzwelt wird dieses Problem durch eine zentrale Instanz gelöst: Die Bank führt ein Kontobuch (Ledger) und autorisiert jede Verfügung. Sie stellt sicher, dass ein Guthaben nicht doppelt verausgabt werden kann, da sie über die einzige maßgebliche Wahrheit („welches Konto hat welchen Kontostand") verfügt.

Die technische Innovation von Bitcoin besteht darin, dies über ein Kontobuch darzustellen, das nicht zentral, sondern verteilt, also dezentral, geführt wird. Anstelle einer zentralen Datenbank bei einem vertrauenswürdigen Institut führt jeder teilnehmende Netzwerkknoten eine identische Kopie des gesamten Transaktionsverlaufs. Transaktionen werden in Blöcken gebündelt, die kryptographisch mit dem jeweils vorherigen Block verkettet werden - daher der Name „Blockchain". Die Manipulation eines Blocks würde alle nachfolgenden Blöcke verändern und wäre sofort erkennbar.

Damit sich alle Knoten auf eine einheitliche, gültige Version der Kette einigen, kommt ein Konsensverfahren zum Einsatz: Bei Bitcoin ist es das sogenannte Proof-of-Work-Verfahren (rechenintensives „Mining"), bei vielen jüngeren Netzwerken das sogenannte Proof-of-Stake-Verfahren (Besicherung durch hinterlegte Werteinheiten). Nur die von der Mehrheit der Rechenleistung bzw. des Stakes bestätigte Kette gilt als maßgeblich und korrekt.

Transaktionen werden mit dem privaten Schlüssel des Verfügungsberechtigten signiert und sind für jeden Netzwerkteilnehmer anhand des öffentlichen Schlüssels verifizierbar, ohne dass eine Vertrauensbeziehung zwischen den Parteien bestehen muss.

Im Ergebnis ersetzt das Netzwerk selbst die Kontrollfunktion der Bank: Eine Transaktion gilt erst als bestätigt, wenn sie in einen Block aufgenommen und dieser durch nachfolgende Blöcke bestätigt wurde. Ein Double-Spending-Versuch, also der Versuch, zwei widersprüchliche Transaktionen durchzusetzen, gilt bei hinreichend dezentralen Netzwerken als unwirtschaftlich, da ein einzelner Angreifer eine Mehrheit der Rechenleistung (bzw. des Stakes) aufbringen müsste.

Mit der Einführung programmierbarer Smart Contracts durch Ethereum im Jahr 2015 erweiterte sich das Spektrum von reinen Zahlungstoken um Utility- und Investment-Token. Dies löste in den Jahren 2017 und 2018 einen Boom von Initial Coin Offerings (ICOs) aus. Dieser Boom wurde von erheblichen Anlegerschutzdefiziten begleitet, die später zum regulatorischen Leitmotiv wurden. Es folgten die Etablierung von Stablecoins, wie Tether (USDT) und USDC als Brücke zwischen der Krypto- und der Fiat-Welt, der Boom von Decentralized Finance (DeFi)

in den Jahren 2020 und 2021 sowie eine zunehmende Institutionalisierung durch regulierte Terminmärkte und Verwahrlösungen.

Einen Wendepunkt markierte die Zulassung von Spot-Bitcoin-ETFs in den USA im Jahr 2024, die institutionellen Anlegern erstmals einen regulierten Zugang ohne eigene Verwahrinfrastruktur eröffnete. Parallel dazu reagierte der Gesetzgeber: zunächst mit der FATF Travel Rule und national divergierenden Aufsichtsregimen, schließlich mit der von der EU geschaffenen Markets in Crypto-Assets Regulation, der MiCAR (Verordnung (EU) 2023/1114). Deren Titel III/IV sind bereits seit Juni 2024 anwendbar, ihr Gesamtregime ist seit dem 30.12.2024 vollständig anwendbar. Die Verordnung soll Rechtsklarheit und Rechtssicherheit für Emittenten und Anbieter von Kryptowerten schaffen.

Für den Bankensektor bedeutet dies: Kryptowerte haben den Status eines regulatorisch geduldeten Randphänomens verlassen. Sie sind – reguliert durch MiCAR und flankiert von der aufsichtsrechtlichen Erwartungshaltung der Bafin – zu einer eigenständigen, aufsichtsrechtlich adressierten Assetklasse geworden. Deren Vertrieb im Kommissionsgeschäft unterliegt denselben Wohlverhaltens- und Organisationspflichten wie klassische Finanzinstrumente.

„meinKrypto“ als Lösung der Genossenschaftlichen FinanzGruppe

Kunden der Genossenschaftlichen FinanzGruppe (im Folgenden: GFG) konnten bisher an dieser Entwicklung nicht teilhaben, ohne auf Drittanbieter oder indirekte Investmentvehikel zurückgreifen zu müssen. Dabei handelte es sich leider auch um Anbote sehr unterschiedlicher Seriosität, bis hin zu klassischen Betrügereien, wie der Kollaps der Krypto-Börse FTX im November 2022 als einer der größten Betrugsskandale der Finanzgeschichte zeigte. Dabei wurden ca. 8 Milliarden US-Dollar an Kundengeldern veruntreut. Im Jahr 2022 hat der BVR dann die Notwendigkeit eines eigenen Angebots aus der GFG unterstrichen.

In Kooperation mit der Atruvia AG, der EUWAX AG sowie der Stuttgart Digital Custody GmbH entwickelte die DZ BANK das Selbstentscheiderprodukt „meinKrypto“. Über die Banking-App können Genossenschaftsbanken ihren Kunden so eine Auswahl an Kryptowerten zum Handel anbieten. Jede Genossenschaftsbank kann dabei selbst entscheiden, ob sie das Produkt ins Portlolio aufnehmen möchte oder nicht.

Aufsichtsrechtlich ist das Geschäftsmodell als Kommissionsgeschäft zu sehen und somit als Kryptowertedienstleistung im Sinne der MiCAR zu bewerten. Die Aufnahme von Geschäften ist für Banken notifizierungspflichtig. Das bedeutet, dass der Bafin die Absicht, Kryptowertedienstleistungen anzubieten, angezeigt werden muss. Hierzu sind umfangreiche Angaben zum Geschäftsmodell der Kryptowertedienstleistung, aber auch zu den bankinternen Prozessen, Regelungen sowie zur Institutsstruktur abzugeben. Die Notifizierungspflicht für Kreditinstitute ist in Art. 60 der MiCAR geregelt; die Notifizierung selbst hat spätestens 40 Arbeitstage vor der erstmaligen Erbringung der Kryptowertedienstleistung zu erfolgen. Sobald die Genossenschaftsbank meinKrypto anbietet, ist sie ein Crypto-Asset Service Provider (CASP), für den dann die umfangreichen Vorschriften der MiCAR gelten.

Anpassung von Governance- und Compliance-Strukturen

Die MiCAR stellt Anforderungen an Governance- und Compliance-Vorschriften, die weitreichende Veränderungen in der Bankorganisation und der Prozesslandschaft der Bank mit sich bringen. Eine Bank, die im Rahmen des Selbstentscheiderprodukts „meinKrypto“ den Kommissionshandel mit Kryptowerten anbietet, sollte ihre bestehenden Compliance-Systeme gezielt erweitern.

Kreditinstitute benötigen für Kryptowerte-Dienstleistungen keine gesonderte CASP-Zulassung nach Art. 63 MiCAR, stattdessen können sie gemäß Art. 60 MiCAR eine Notifizierungsanzeige an die Bafin übermitteln. Diese entbindet sie jedoch nicht von den materiellen Organisationspflichten der Art. 66 ff. MiCAR, denn die Notifizierungsanzeige substituiert lediglich die Zulassung, nicht die Compliance-Anforderungen.

Die Compliance-Anforderungen sind in die bestehende Aufbau-/Ablauforganisation zu integrieren. Exemplarisch sind hier jedenfalls die folgenden Punkte aufzuzählen:

- Grundsätze und Verfahren für den ordnungsgemäßen Umgang mit Kundenaufträgen
- Beschwerdemanagement, angepasst an krypto-spezifische Sachverhalte
- Verwahrung von Kundenvermögenswerten
- Sachkunde von Geschäftsleitung, Personal und Aufsichtsrat einschließlich Schulungspflichten zu DLT-Grundlagen, Marktmissbrauch nach MiCAR und produktspezifischen Risiken
- DORA-Überlagerung aufgrund der Nähe von Kryptowerte-Dienstleistungen zu IKT-Systemen
- Marktmissbrauchsüberwachung nach MiCAR

Kundenschutzpflichten

Die MiCAR regelt Kundenschutzpflichten im Wesentlichen auf zwei Ebenen. Erstens sind allgemeine Wohlverhaltens- und Organisationspflichten in den Art. 66 – 74 geregelt und zweitens finden sich dienstleistungsspezifische Pflichten in den Art. 75 – 82. Diese Pflichten sind den Banken grundsätzlich bekannt, da die MiCAR beispielsweise ehrliches, redliches und professionelles Handeln im besten Kundeninteresse, Regelungen zur Unternehmensführung und Behandlung von Interessenkonflikten sowie ein geeignetes Beschwerdemanagement fordert. Diese Vorgaben zeigen Parallelen zu bereits umgesetzten Vorgaben, beispielsweise aus der WpHG- oder MaRisk-Compliance.

Geldwäscheprävention

Die MiCAR schreibt eine aufsichtsrechtliche Erlaubnispflicht für Kryptowerte-Dienstleister vor, lässt das Geldwäscherecht jedoch unberührt. Dieses folgt einem eigenständigen, parallel zu beachtenden Pflichtenregime. Für Institute, die Kryptowerte-Kommissionsgeschäfte betreiben, bedeutet dies eine zweite, ebenso anspruchsvolle Compliance-Ebene neben den MiCAR-spezifischen Wohlverhaltens- und Organisationspflichten.

Nach dem Geldwäschegesetz sind CASPs gemäß § 2 Abs. 1 Nr. 2 GwG als Verpflichtete einzuordnen, soweit sie Kryptowerte im Sinne des § 1 Abs. 29 GwG verwalten oder in ihrem Namen für Rechnung der Kunden erwerben und veräußern. Die geldwäscherechtliche Definition des Kryptowerts orientiert sich dabei an der MiCAR-Terminologie, sodass beide Regelungsregime in ihrer Reichweite eng verzahnt sind, ohne deckungsgleich zu sein.

Für die betroffenen Institute greifen damit die vollen allgemeinen Sorgfaltspflichten, insbesondere die Kundenidentifizierung und die Feststellung des wirtschaftlich Berechtigten. Auch eine auf die spezifischen Risiken von Kryptowerten zugeschnittene Risikoanalyse nach § 5 GwG wird erforderlich. Regelmäßig sind zudem die verstärkten Sorgfaltspflichten nach § 15 GwG zu erfüllen. Deren Anwendbarkeit ergibt sich im Kommissionsgeschäft bereits aus den produktbezogenen Risikofaktoren der Anlage 2 GwG, da diese an die Eigenschaft des Kryptowerts selbst anknüpfen und unabhängig von einem Auslandsbezug einschlägig sind – auch bei rein inländischer Geschäftsstruktur.

Fazit

Mit meinKrypto vollzieht die GFG den Schritt von der reinen Beobachtung des Kryptomarktes hin zur aktiven, regulierten Marktteilnahme. Aufsichtsrechtlich ist dies keine Neuerung, sondern eine konsequente Erweiterung des bereits etablierten Kommissionsgeschäfts auf eine neue Assetklasse mit allen daraus resultierenden Wohlverhaltens-, Organisations- und Geldwäschepräventionspflichten.

Der entscheidende Vorteil des Notifizierungsverfahrens nach Art. 60 MiCAR besteht darin, dass Kreditinstitute ohne separate CASP-Zulassung tätig werden können. Dies entbindet sie jedoch nicht von den materiellen Organisationspflichten der Art. 66 ff. MiCAR. Für die einzelne Genossenschaftsbank bedeutet dies: Wer meinKrypto anbietet, muss bestehende Compliance-Strukturen gezielt und ernsthaft erweitern. Diese Aufgabe erscheint technisch überschaubar, ist organisatorisch aber nicht zu unterschätzen.

Als Umsetzungsempfehlung möchten wir Ihnen daher die folgenden Punkte mitgeben:

1. Bestandsaufnahme statt Neubau: Vorhandene Compliance-Strukturen (insbesondere Kommissionsgeschäft, Beschwerdemanagement und Sachkundeprozesse) sind systematisch auf MiCAR-Kompatibilität zu prüfen, bevor neue Prozesse aufgesetzt werden.
2. Notifizierung frühzeitig einplanen: Die 40-Arbeitstage-Frist nach Art. 60 MiCAR (zzgl. möglicher Nachforderungen durch die Bafin, in Summe bis zu 60 Arbeitstage) sollte als harter Meilenstein vor dem geplanten Produktlaunch im Projektplan verankert werden.
3. Zwei-Ebenen-Compliance mitdenken: MiCAR-Wohlverhaltenspflichten und geldwäscherechtliche Sorgfaltspflichten (inkl. verstärkter Sorgfaltspflichten nach § 15 GwG) laufen parallel und sind getrennt zu dokumentieren.
4. Governance-Sachkunde nicht unterschätzen: Schulungspflichten für Geschäftsleitung, Personal und Aufsichtsrat zu DLT-Grundlagen und MiCAR-Marktmissbrauch sollten nicht als bloße Formsache behandelt werden. ▬

Christoph Patzke
Beauftragter MaRisk-Compliance,
E-Mail: christoph.patzke@dz-cp.de

Christian Tipkemper
Beauftragter WpHG-Compliance,
E-Mail: christian.tipkemper@dz-cp.de

Justus Tychek
Compliance Spezialist,
E-Mail: justus.tychek@dz-cp.de

9. MaRisk-Novelle 2026

Am 30. Juni 2026 hat die Bafin die bereits mit großer Spannung erwartete finale Version der 9. MaRisk-Novelle veröffentlicht[1]. An der Konsultation hat sich sowohl die Geschäftsleitung der DZ CompliancePartner als auch die Fachabteilung über den BVR und die DK beteiligt[2].

Bereits im Vorfeld der Veröffentlichung der finalen MaRisk-Version waren Schlagworte wie „Paradigmenwechsel", „mehr Prinzipienorientierung und weniger Komplexität" oder „weniger Regulierungstiefe bei mehr Verantwortlichkeit im Institut" zu hören. Gleichzeitig hat die Aufsicht betont, dass mit weniger Regulierungstiefe und weniger Komplexität nicht auch weniger Regulierung oder eine Absenkung des Regulierungsniveaus einhergeht.

Die diesjährigen MaRisk beruhen auf der Umsetzung der Aufsichtsmitteilung 2024 zu den EBA-Leitlinien, der Konsultation für die Leitlinien zur Internen Governance (08/2025) sowie auf Erkenntnissen der Aufsicht aus Sonderprüfungen und einer Review der bisherigen MaRisk.

Im folgenden Artikel geben wir Ihnen einen ersten Überblick über die Änderungen in der MaRisk 10.0 mit den Schwerpunkten in Bezug auf die MaRisk-Compliance-Funktion (AT 4.4.2 MaRisk) sowie die Auslagerbarkeit der besonderen Funktionen (AT 9 MaRisk)[3]. Am Ende des Artikels werden die wesentlichen Änderungen aufgrund des BRUBEG[4] dargestellt und wird auf das Non-Paper zum Kleinbankenregime eingegangen. BRUBEG und die daraus erfolgten Änderungen im KWG sind mit den MaRisk als Einheit zu betrachten. Das Kleinbankenregime macht ebenfalls den neuen Aufsichtsansatz deutlich.

1. Formalien

Das Ziel der Aufsicht, die MaRisk weniger komplex zu gestalten, zeigt sich schon an Formalien. Während die MaRisk 9.0 vom Februar 2024 noch 122 Seiten umfassten, haben die aktuellen MaRisk nur noch 82 Seiten[5]: weg von umfangreichen Erläuterungen, Detaillierungen und konkreten Vorgaben hin zu einer Reduzierung der Konkretisierungen und zu Streichungen. Bemerkenswert ist auch, dass bei der Veröffentlichung der finalen Version die Aufsicht zusätzlich eine Vergleichsversion der Konsultations- und der Veröffentlichungsfassung verlautbart hat, was auf deutliche Veränderungen während der Konsultationsphase hinweist. So gab es beispielsweise konsultationsbedingte Änderungen bei der Compliance-Funktion, AT 4.4.2 Tz. 1[6].

2. Wesentliche Änderungen

Nachfolgend werden einige wesentliche Änderungen in den neuen MaRisk beschrieben:

a) Größenordnungen

Es erfolgt eine neue Institutsklassifizierung (aufsteigend)

Less-significant Institutions (LSI)

- Sehr kleine Institute (BS ≤ 1 Mrd. €)
  - ▷ deutliche Erleichterung der MaRisk-Anwendung
- Kleine Institute/SNCI (BS 1 – 5 Mrd. €)
  - ▷ Erleichterung der MaRisk-Anwendung
- Große Institute (i.d.R. ab 5 Mrd. € BS)
  - ▷ volle Anwendung der MaRisk

Significant Institutions (SI)

- Bedeutende Institute: direkte Aufsicht durch die EZB, keine Anwendung der MaRisk, i.d.R. ab 30 Mrd. € BS

Die MaRisk sind grundsätzlich risikoorientiert umzusetzen. Umsetzungstiefe und Ausgestaltung richten sich nach Größe, Risikogehalt und Komplexität des Instituts.

b) Governance

Gemäß AT 3 sind die **Geschäftsleiter** für die ordnungsgemäße Geschäftsorganisation verantwortlich, unabhängig von einer internen Zuständigkeitsregelung. Dies führt zu einer Stärkung der Gesamtverantwortung. Die Geschäftsleiter sind nicht mehr für die „Förderung" der **Risikokultur** verantwortlich, sondern

haben diese „festzulegen und zu genehmigen“. Das Aufsichtsorgan ist mindestens vierteljährlich schriftlich über die Geschäftslage und die Risikosituation zu informieren, der Vorsitzende des Aufsichtsorgans kann direkt bei der IR Auskünfte einholen.

Dies bedeutet eine stärkere Einbindung des Aufsichtsorgans in das Risikomanagement und eine gesteigerte Qualität der Berichte.

c) Kreditgeschäft

Konkretisierungen des Kreditgeschäftes sind insbesondere in BTO 1.1 und 1.21 gegeben. Daraus folgt eine klare Normenstruktur im Kreditprozess. Das Proportionalitätsprinzip hat weiterhin Gültigkeit, und es gibt einen Objektivitätsrahmen sowie Vorgaben zur **Eindämmung von Betrug.** Dies sind keine neuen operativen Vorgaben, doch gehen vertiefte Anforderungen damit einher. Thema sind ferner Bewertung und Überwachung von Sicherheiten. Sicherheiten sind vor Kreditvergabe zu überprüfen, für **kleine Institute** ist eine Überprüfung der **Sicherheitenbewertungsverfahren** nur alle **zwei Jahre** erforderlich. Sehr kleine Institute sind von der Pflicht der Rotation des Bewerters von Immobilien-sicherheiten ausgenommen. Auch erfolgt eine terminologische Vereinheitlichung mit den EBA-Leitlinien zur Bewertung von Sicherheiten. Institute müssen verpflichtend Prozesse zur Überwachung verdächtigen oder betrügerischen Verhaltens im Kreditprozess einführen.

d) Gesamtbanksteuerung

Zentrales Element ist die **Geschäftsstrategie** gemäß AT 4.2. Sie muss tragfähig und langfristig ausgerichtet sein und eine zukunftsgerichtete Geschäftsmodellanalyse enthalten. Die **Risikostrategie** muss konsistent zur Geschäftsstrategie sein, sie konzentriert sich auf die Themen Risikoappetit und Risikokonzentration. In den MaRisk werden die bisherigen detaillierten BAIT-Vorgaben bzw. IKT-strategischen Themen nur noch in gekürzter Form wiedergegeben und durch DORA ergänzt[7]. Insoweit erfolgt eine Trennung, wobei die DORA-Strategie konsistent aus der Geschäftsstrategie abzuleiten ist. In BTR 2.3 werden Anforderungen, die bisher über Verweise auf die EBA-Leitlinien galten (Zinsänderungsrisiko und Einlagenmodellierung), nun direkt in die MaRisk übernommen.

ESG-Risiken wirken sich weiterhin auf alle Risikoarten aus. Sie können nicht mehr ausschließlich historisch betrachtet werden, es ist eine Kombination aus risikopositions-, sektor-, portfolio- und szenario bezogenen Methoden sowie Verfahren für den Portfolioabgleich einzusetzen. Gefordert ist ein Methodenset aus wissenschaftlich fundierten Szenarien mit einem langfristigen Horizont sowie langfristigen Resilienzanalysen. Die Ergebnisse sind in der Strategiefestlegung, dem Geschäftsmodell und den Risikostreuungs- sowie Controlling-Prozessen zu berücksichtigen.

Bei Immobilien, BTO 3, wurde der Schwellenwert auf 40 Mio. EUR (von 30 Mio. EUR) oder 4 % der BS (von 2 % der BS) angehoben.

e) Risiken aus der Ressourcenausstattung

Aus AT 7.2 und 7.3 ergibt sich ein prinzipienorientierter Anforderungsrahmen: Umfang und Qualität der technisch-organisatorischen Ausstattung sind an den internen Erfordernissen, den Geschäftsaktivitäten und der Risikosituation auszurichten. Beim Notfallkonzept liegt der Fokus auf organisatorischen Maßnahmen zur Fortführung kritischer Prozesse.

f) MaRisk-Compliance-Funktion, AT 4.4.2

Hinsichtlich der MaRisk-Compliance-Funktion bringen die neuen MaRisk Veränderungen, die insgesamt zu einer Stärkung der Position führen, vor allem auch im Zusammenhang mit den neuen Regelungen des BRUBEG in den §§ 25a - 25c und 25e KWG (besondere Schlüsselfunktionen).

aa) Hinwirken vs. Sicherstellen

In der Konsultationsfassung erfolgte in Tz. 1 des AT 4.4.2 die Streichung der Formulierung, dass die Compliance-Funktion auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben und entsprechender Kontrollen hinwirken soll. Stattdessen erfolgte die Aufnahme eines Passus, nach dem die Compliance-Funktion die Überwachung der Einhaltung wesentlicher rechtlicher Vorschriften im Rahmen eines strukturierten Prozesses sicherstellt. In der finalen Fassung verblieb es dann bei dem Hinwirken in Bezug auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben und entsprechender Kontrollen. Im Erläuterungstext (rechte Spalte) wird ausgeführt, dass die Compliance-Funktion

- die Risiken aus der Nichteinhaltung wesentlicher rechtlicher Regelungen und Vorgaben identifiziert und
- im Rahmen eines strukturierten Prozesses sicherstellt, dass die jeweils betroffenen Bereiche die Einhaltung dieser Regelungen und Vorgaben überwachen.

Diese sprachliche Differenz führt in der Praxis immer wieder zu unterschiedlichen Interpretationen. Eine Lesart verbindet damit eine weitgehende Haftung der Compliance-Funktion, die an die BGH-Rechtsprechung zur Garantenstellung anknüpft wird[8]. Eine andere Lesart, die auch unserem Verständnis entspricht, sieht die Begriffe „Hinwirken" und „Sicherstellen" nicht im Wettbewerb zueinander:

- Die Compliance-Funktion hat in ihrer Beratungs-, Schulungs- und Kontrollfunktion gegenüber der „ersten Verteidigungslinie" und gegenüber dem Vorstand eine „hinwirkende" Funktion.
- Darüber hinaus hat sie eine gestaltende Aufgabe, für die sie auch einsteht („sicherstellen"). Diese Aufgabe adressiert die methodisch-funktionale Ebene. Die Compliance-Funktion steht dafür ein, dass der methodisch-funktionale Rahmen von ihr beschrieben, kontrolliert und aktuell eingehalten wird.

Für diese Interpretation spricht, dass sie die Stellung der Funktion in der Bankorganisation spiegelt. Ihre schärfste Waffe ist das Berichtswesen. Die Compliance-Funktion verfügt über kein Vetorecht und kann keine Prozesse stoppen, sondern hat „nur" eine direkte Berichtslinie an den Vorstand (und ggf. Aufsichtsrat).

Flankierend treten mit der MaRisk-Novelle nun die Setzung von Fristen zur Mängelbehebung und die Eskalation von nicht behobenen Mängeln bzw. fehlenden Sicherungsmaßnahmen möglicherweise stärker in den Vordergrund.

bb) Nichteinhaltung wesentlicher rechtlicher Regelungen und Vorgaben

Neu ist im Erläuterungsteil unter der Überschrift „Aufgaben der Compliance-Funktion" die Ausführung zur Nichteinhaltung wesentlicher rechtlicher Regelungen und Vorgaben. Danach ist die Compliance-Funktion so auszugestalten, dass Rechtsrisiken aus einer „Non-Compliance" identifiziert und in die Risikosteuerung eingebunden werden. Dies bedeutet einen verstärkten Fokus der Compliance-Funktion auf rechtliche Risiken aus wesentlichen rechtlichen Regelungen, auch in der Risikoanalyse.

cc) Strukturierter Prozess

Die Aufgaben der Compliance-Funktion haben nach den Erläuterungen zu Tz. 1 in einem strukturierten Prozess zu erfolgen. Als strukturierten Prozess kann man einen definierten, dokumentierten und standardisierten Ablauf von Aktivitäten verstehen, die in einer bestimmten Reihenfolge ausgeführt werden, um ein bestimmtes Ziel zu erreichen. Durch einen strukturierten Prozess werden einerseits Unklarheiten und Fehler vermieden sowie andererseits eine Wiederholbarkeit und Vorhersehbarkeit des Ergebnisses am Ende des strukturierten Prozesses möglich.

In Bezug auf die mindestens jährlich zu erstellende Risikoanalyse kann man davon ausgehen, dass institutsindividuell z. B.

- Erkenntnisse OpRisk,
- Erkenntnisse Beschwerden,
- Erkenntnisse anderer Funktionsbereiche/Beauftragtenfunktionen (z. B. WpHG-Compliance, Geldwäsche- und Betrugsprävention, Informationssicherheit und Datenschutz, Hinweisgebersystem, IKT-Risikokontrollfunktion)
- Auswertung der Ergebnisse der externen Prüfung, ggf. Prüfung nach § 44 KWG,
- Vorhandensein und Wirksamkeit von Sicherungsmaßnahmen,
- nicht bearbeitete Rechtsmonitoring-Einträge und
- Ergebnisse eigener Kontrollhandlungen

einfließen sollten. So kann einerseits die Risikosituation angemessen und aktuell beurteilt werden. Andererseits können aber auch zusätzliche Sicherungsmaßnahmen definiert und Kontrollen durchgeführt werden, um festgestellte Risiken zu minimieren. Daher sollte es Standard sein, dass die MaRisk-Compliance-Funktion selbst in den Prozessen bzw. Aktivitäten des Instituts Kontrollen durchführt. Das gilt insbesondere bei den Prozes-

sen und Aktivitäten, bei denen gemäß Risikoanalyse ein erhöhtes Risiko besteht[9]. Durch die Streichung in Tz. 3 zum Rückgriff auf andere Funktionen und Stellen wird unterstrichen, dass die Compliance-Funktion sich ein eigenes Bild von der Risikosituation im Haus machen muss, z. B. durch eigene Kontrollen.

dd) Betroffene Bereiche

In dem Erläuterungstext ist nunmehr die Regelung enthalten, wonach die Compliance-Funktion sicherstellen muss, dass die **jeweils betroffenen Bereiche** die Einhaltung der Regelungen und Vorgaben überwachen. Dieser Passus als Teil der Aufgabenbeschreibung der Compliance-Funktion ist aufgrund der Konsultation in die MaRisk eingefügt worden. Damit wird klargestellt, dass die Compliance-Funktion nicht selbst für die Überwachung operativer Prozesse im Institut verantwortlich ist, sondern originär die Fachbereiche, und dass bei der Compliance-Funktion die Überwachung der Fachbereiche liegt.

ee) Anbindung an andere Funktionen

Nach Tz. 3 kann die Compliance-Funktion bei der Risikocontrolling-Funktion oder anderen geeigneten Funktionen angebunden werden. Andere geeignete Funktionen sind nach den Erläuterungen der GW-Beauftragte oder die IKT-Kontrollfunktion. Die Öffnung ist zu begrüßen. Aufgrund des demografischen Wandels und der hohen Anforderungen an die Funktionen wird es allerdings schwierig sein, geeignete Personen zu finden, die die notwendigen multiplen Qualifikationen in einer Person erfüllen.

ff) Austausch mit der Risikocontrolling-Funktion

Die Pflicht zum Austausch mit der Risikocontrolling-Funktion ist zu begrüßen und häufig schon gelebte Praxis in den Häusern (wie auch der Austausch mit der Internen Revision). Es kann ein persönlicher Austausch, aber auch ein Berichtsaustausch (vierteljährlicher OpRisk-Bericht) erfolgen. So sind für die Compliance-Funktion insbesondere die Berichtsteile interessant, bei denen es Schnittmengen zwischen Risikocontrolling und MaRisk-Compliance gibt, z. B. im OpRisk-Bereich oder beim Thema Nachhaltigkeit.

Aufgrund der gestiegenen und neuen Anforderungen an die Compliance-Funktion gehen wir von einer Änderung der bisherigen Regelungsinhalte aus. Damit hätte eine Umsetzung ab dem 1. Januar 2027 zu erfolgen.

g) Auslagerung, AT 9

aa) Auslagerungsbeauftragter und Auslagerungsregister

Änderungen gab es auch bei AT 9 Auslagerung. Auf den Wegfall des Erfordernisses der Bestellung eines Auslagerungsbeauftragten haben wir schon hingewiesen. Nicht eindeutig sind die Ausführungen zum Auslagerungsregister. Zwar wurde die Tz. 13 des AT 9 des Jahres 2024 ersatzlos gestrichen. Damit entfällt die Notwendigkeit zur Führung eines Auslagerungsregisters aber keinesfalls.

Die Führung des Auslagerungsregisters leitet sich direkt und zwingend aus § 25b Abs. 1 Satz 4 KWG ab. Da die MaRisk lediglich eine behördliche Interpretation des KWG darstellen, können diese die Regelungen des KWG nicht außer Kraft setzen.

Strittig ist derzeit die Konkurrenzsituation zum Register nach DORA. Zum Teil wird argumentiert, dass die Regelungen der DORA-Verordnung als „lex specialis“ die Aufnahmeverpflichtung von IKT-Dienstleistungen in das Auslagerungsregisters nach KWG (MaRisk) verdrängen. Andere Stimmen sehen keine Regelungsgleichheit, sondern eine Regelungsparallelität, so dass beide Register zu füllen wären. Es ist nicht davon auszugehen, dass dieser Streit kurzfristig entschieden sein wird, weshalb wir bis auf Weiteres zu einer parallelen Registerführung raten.

bb) Auslagerung besonderer Funktionen

In AT 9 Tz. 5 hat die Aufsicht die vollständige Auslagerung der Compliance-Funktion oder der Internen Revision nun auf sehr kleine Institute (BS ≤ 1 Mrd. €) beschränkt. Bisher war die Lesart in Bezug auf Auslagerungen, dass Institute mit einer BS bis 5 Mrd. € die besonderen Funktionen auslagern können, sofern nach Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten keine Besonderheiten bestanden. Sowohl in der Sparkassen-Gruppe als auch in der Genossenschaftlichen FinanzGruppe unterscheiden sich die

sehr kleinen und kleinen Institute im Regelfall nur durch die Bilanzsummen. Die Geschäftsaktivitäten und Geschäftsmodelle bzw. Produkte innerhalb der kleinen und sehr kleinen Institute sind überwiegend homogen. Sie werden überwiegend zentral konzipiert bzw. erstellt. Die Institute vertreiben sie lediglich (z. B. Produkte der Union Investment, R+V Versicherung, TeamBank).

Vor diesem Hintergrund und angesichts des oben beschriebenen Dilemmas zur Anbindung der Compliance-Funktion an andere Funktionen beinhaltet diese Regelung der MaRisk eine Herausforderung für „kleine" Institute. Nach dem aktuellen Wortlaut der MaRisk ist für diese die vollständige Auslagerung der Compliance-Funktion nicht mehr möglich.

Alternativen zur vollständigen Auslagerung
Bei einer teilweisen Auslagerung könnte sich das Institut gezielt die Unterstützung ins Haus holen, die benötigt wird. Aus unserer Erfahrung heraus macht eine Teilauslagerung vor allem dann Sinn, wenn das Institut, wie beispielsweise beim Rechtsmonitoring, punktuell fachlich bzw. personell Unterstützung sucht.

Eine weitere, aus unserer Erfahrung heraus sehr praktikable und umfassende Option stellt die (Dauer-)Beratung kleiner Institute dar.

Im Rahmen des Beratungsansatzes erfolgt die Unterstützung des Instituts beim kompletten Compliance-Kreislauf: von der Erstellung der Risikoanalyse über den Jahresüberwachungsplan bis hin zu den Kontrollen und der Berichterstattung.

Insbesondere die Notwendigkeit, einen strukturierten Prozess in der MaRisk-Compliance (s.o. 2 f cc) aufzubauen, wird viele kleine und sehr kleine Institute vor enorme Herausforderungen stellen. Dies kann jedoch im Rahmen einer Beratung vergleichsweise effizient und aufsichtskonform implementiert bzw. geheilt werden. Das Institut profitiert direkt von dem Erfahrungswissen und der Prozesskompetenz der DZ CompliancePartner.

3. BRUBEG – (besondere) Schlüsselfunktionen

Insgesamt geht mit dieser 9. MaRisk-Novelle eine deutliche Veränderung einher, die zu einer Stärkung der Compliance-Funktion führt. Diese Stärkung wird durch das BRUBEG unterstützt, dessen Regelungen überwiegend am 1. April 2026 in Kraft traten und zu Veränderungen des KWG führten.

Durch die Herausnahme von Regelungen aus den MaRisk als normeninterpretierende Verwaltungsvorschriften und die Implementierung in das KWG als Gesetz unterstreicht der Gesetzgeber die Bedeutung dieser Veränderungen.

Das BRUBEG hat u.a. Auswirkungen auf die Beschlussfassung zu Großkrediten, Organtransaktionen, Offenlegung, Anzeigepflichten einschließlich Beteiligungsanzeigen, Beteiligungen, Verschmelzungen und Fusionen, Corporate Governance, ESG-Risiken, das Risikomanagement und Schlüsselfunktionen.

In Bezug auf die **Compliance-Funktion** ergibt sich Folgendes: Die Compliance-Funktion gehört zu den **internen Kontrollfunktionen** i. S. d. § 1 Abs. 2a KWG. **Leiter der internen Kontrollfunktionen** sind Personen, die auf der höchsten Hierachieebene – mit Ausnahme der Geschäftsleiter – für die tatsächliche Leitung des Tagesgeschäftes der internen Kontrollfunktionen zuständig sind, § 1 Abs. 2c KWG. Inhaber **besonderer Schlüsselfunktionen** sind gemäß § 1 Abs. 2d KWG **Personen,** die **besondere Funktionen** wahrnehmen. Hierzu zählen die Leiter der internen Kontrollfunktionen sowie der Leiter Finanzen, soweit sie nicht Geschäftsleiter sind.

Somit zählen die **Leiter der Compliance-Funktion** zu den Inhabern **besonderer Schlüsselfunktionen,** § 1 Abs. 2 Nr. 22 S. 2 KWG.

Aus den §§ 25a – 25c und 25e KWG ergibt sich, dass die Kontrollfunktionen unabhängig auszugestalten sind. Leiter der Kontrollfunktionen müssen über eine hinreichende Autorität verfügen. Sie erhalten das Recht, unabhängig von der Geschäftsleitung unmittelbar an das Aufsichtsorgan zu berichten und insbesondere zu riskanten Entwicklungen Warnungen auszusprechen, § 25c Abs. 4a Nr. 3 KWG. Die Leitungen der Kontrollfunktionen können zukünftig nur mit Zustimmung des Verwaltungs- oder Aufsichtsorgans von ihren Aufgaben entbunden werden, § 25c Abs. 4a Nr. 3i KWG. Bislang sahen die

MaRisk lediglich eine Vorabinformation an das Aufsichtsorgan vor, nun ist eine ausdrückliche Zustimmung notwendig.

Die Inhaber von Schlüsselfunktionen müssen fachlich geeignet und zuverlässig sein, was durch die Institute fortlaufend sicherzustellen ist. Bei Missständen kann die Bafin verlangen, dass eine Schlüsselfunktion nicht übertragen oder entzogen wird bzw. seitens des Instituts Maßnahmen ergriffen werden, damit die Anforderungen erfüllt werden.

4. Non-Paper Kleinbankenregime

Das gemeinsame Non-Paper von Bafin und Deutscher Bundesbank aus dem Jahr 2025 schlägt ein vereinfachtes EU-Regulierungsregime für kleine, nicht-komplexe Banken mit einer Bilanzsumme bis zu 10 Mrd. € vor. Kern des Vorschlags ist es, komplizierte, risikobasierte Kapitalregeln durch eine einfachere, ungewichtete Verschuldungsquote (Leverage Ratio) zu ersetzen. Es bleibt abzuwarten, ob ein Kleinbankenregime eingeführt und wie dieses weiter ausgestaltet wird. Das Kleinbankenregime zeigt deutlich den Ansatz der Aufsicht zu einer verschlankten, aber gleichwohl effektiven Regulatorik und Aufsicht, so wie er mit der 9. MaRisk-Novelle initiiert wurde.

5. MaRisk-QuickCheck

BRUBEG und 9. MaRisk-Novelle führen zu Veränderungen in der Compliance. Um Sie neben unseren klassischen Beratungsangeboten zusätzlich bei diesen Veränderungen zu unterstützen, haben wir einen MaRisk-QuickCheck entworfen, der Sie insbesondere bei der Umsetzung der neuen MaRisk unterstützt.

Der QuickCheck beruht auf den finalen MaRisk vom Juni 2026 ergänzt um Ausführungen dazu, ob es sich um Neuerungen oder Klarstellungen handelt und welche Umsetzungsfristen gelten, und macht konkrete Vorschläge zur Umsetzung. Gleichzeitig können Sie Umsetzungsverantwortlichkeiten hinterlegen und Bearbeitungsstände sowie die Umsetzung dokumentieren.

Den QuickCheck stellen wir unseren Auslagerungskunden in der MaRisk-Compliance kostenlos zur Verfügung. ▬

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

[1] Dieser Artikel hat den Stand 21.07.2026.

[2] Die Chronologie der MaRisk stellt sich wie folgt dar: RS 18/2005, Anlage 1, Mai 2006, 1. Novelle 2007, 2. Novelle 2009, 3. Novelle 2010, 4. Novelle 2012, 5. Novelle 2017, 6. Novelle 2021, 7. Novelle 2023, 8. Novelle 2024, 9. Novelle 2026.

[3] Im Rahmen dieses Formates ist es nicht möglich, sämtliche Änderungen oder Klarstellungen der MaRisk-Novelle darzustellen, daher wird der Schwerpunkt auf die Compliance-Funktion und Auslagerbarkeit gesetzt.

[4] Umsetzung der CRD VI in nationales Recht im Rahmen des Bankenrichtlinienumsetzungs- und Bürokratieentlastungsgesetzes (BRUBEG).

[5] Jeweils im Querformat.

[6] Sofern im Folgenden kein Gesetz etc. angegeben ist, bilden die MaRisk die Grundlage.

[7] Damit einhergehend fällt die Bestellung eines Zentralen Auslagerungsbeauftragten weg, das Zentrale Auslagerungsmanagement bleibt weiterhin bestehen. Ausgelagerte bzw. fremdbezogene IKT-Dienstleistungen i.S.v. DORA, die dem IKT-Drittparteienmanagement unterliegen, fallen nicht mehr in den Anwendungsbereich des AT 9 MaRisk.

[8] BGH-Urteil vom 17.07.2009, 5 StR 394/08, BGHSt 54,44 Berliner Stadtreinigungsbetrieb: Einen Compliance-Officer kann eine strafrechtliche Haftung nach § 13 StGB treffen, wenn ihm konkrete Kontroll-, Überwachungs- oder Eskalationspflichten übertragen wurden und diese nicht eingehalten wurden. Zivilrechtlich sind Ansprüche nach § 93 AktG bzw. § 43 GmbHG bei Organstellung möglich sowie aus § 280 BGB als Arbeitnehmer. Aus § 130 OWIG kann sich ein Bußgeld ergeben. Gegen zivilrechtliche Ansprüche schützt eine D&O Versicherung, strafrechtliche Haftung ist nicht durch Versicherungen abdeckbar.

[9] Oder es sonst zu Auffälligkeiten gekommen ist.

Krisen bewältigen, Handlungsfähigkeit sichern, Resilienz steigern

Was sagt die DORA zum Umgang mit Krisen?

Vor dem Hintergrund zunehmender Cyber-Bedrohungen, geopolitischer Unsicherheiten und wachsender regulatorischer Anforderungen hat die operationelle Resilienz von Finanzinstituten deutlich an Bedeutung gewonnen. Mit dem Digital Operational Resilience Act (DORA) hat die Europäische Union einen verbindlichen Rahmen geschaffen, der Institute dazu verpflichtet, ihre Fähigkeiten zur Vermeidung, Bewältigung und Nachbereitung von IKT-bezogenen Störungen und Krisen umfassend zu stärken (vgl. Art. 5, 6, 11 DORA).

Während sich in der Vergangenheit viele Maßnahmen auf präventive Kontrollen und klassische Business-Continuity-Management-Ansätze (BCM) konzentrierten, erweitert DORA die Perspektive deutlich. Neben dem Schutz kritischer Systeme wird insbesondere die Fähigkeit in den Fokus gerückt, schwerwiegende Vorfälle effektiv zu managen und die Handlungsfähigkeit auch unter Krisenbedingungen aufrechtzuerhalten (vgl. Art. 17 DORA).

Reicht das bisherige BCM als Maßnahme aus? Was ist darüber hinaus zu beachten?

In zahlreichen Instituten hat sich BCM als essenzieller Bestandteil etabliert und fokussiert sich insbesondere auf die Aufrechterhaltung kritischer Geschäftsprozesse in Notfallsituationen. In der Praxis zeigt sich jedoch, dass Pläne allein nicht ausreichen, wenn sich ein isolierter Notfall zu einer komplexen Krise entwickelt. Situationen dieser Art sind oft durch eine hohe Dynamik, unvollständige Informationslagen, bereichsübergreifende Abhängigkeiten sowie erheblichen Entscheidungs- und Kommunikationsdruck geprägt. DORA bezieht diese Entwicklung ein, indem neben Notfallvorsorge und Wiederanlauf insbesondere auch Incident Management, Krisenkommunikation und Governance-Strukturen stärker in den regulatorischen Fokus rücken (vgl. Art. 5, 11, 13, 17 DORA).

Ein wesentlicher Aspekt ist dabei die eindeutige Festlegung von Rollen, Verantwortlichkeiten und Entscheidungswegen. Leitungsorgane sind explizit dazu angehalten, angemessene Strategien und Lösungsoptionen zu definieren sowie deren Wirksamkeit regelmäßig zu überprüfen (vgl. Art. 5, 6 DORA). Darüber hinaus fordert DORA regelmäßige Tests, Übungen und Reviews, um die tatsächliche Funktionsfähigkeit der etablierten Maßnahmen sicherzustellen (vgl. Art. 24 DORA).

Vor diesem Hintergrund gewinnen integrierte Ansätze an Bedeutung, die technische, organisatorische und personelle Aspekte miteinander verzahnen. Zu den zentralen Handlungsfeldern zählen dabei:

- die Integration von Informationssicherheit, BCM und Krisenmanagement,
- der Aufbau klar strukturierter Krisenstabsorganisationen,
- die Etablierung belastbarer Kommunikations- und Eskalationsprozesse,
- die Durchführung regelmäßiger, realitätsnaher Übungen
- sowie die gezielte Befähigung von Führungskräften zur Entscheidungsfindung unter Unsicherheit.

Kann ein solch komplexer integrierter Ansatz zum Krisenmanagement in der Praxis umgesetzt werden und wenn ja, wie? Welche zentrale Lösung gibt es in der Genossenschaftlichen FinanzGruppe?

Der Ansatz sollte durch die Kombination eines spezialisierten Cybersecurity-Services mit einem strukturierten Krisenmanagementrahmen umgesetzt werden.

Beispiel eines möglichen integrativen Ansatzes in der Praxis

Atruvia hat hierzu infolge einer Beiratsinitiative den Service agree21OpSec-CSIRTaaS erarbeitet. CSIRTaaS (kurz für: Computer Security Incident Response Team as a Service) ist eine spezialisierte Unterstützungsleistung zur strukturierten Bewältigung von Cybervorfällen. Der Service adressiert insbesondere die Anforderungen an Reaktions- und Wiederherstellungsfähigkeit. Im Kern ergänzt der Ansatz präventive Maßnahmen mit operativen Incident-Response-Fähigkeiten durch ein dediziertes Expertenteam. Im Falle eines schwerwiegenden Cyberangriffs übernimmt ein zentrales CSIRT die Koordination verschiedener Maßnahmen. Dazu zählen die initiale Lagebewertung, Eindämmung und forensische Analyse. Zusätzlich wird ein strukturierter „Werkzeugkoffer“ an Notbetriebsmaßnahmen bereitgestellt. Er ermöglicht auch unter Worst-Case-Bedingungen, etwa bei vollständiger Isolation der IT-Systeme, kritische Geschäftsprozesse innerhalb kurzer Zeit wieder aufzunehmen.

Ergänzend zu der beschriebenen operativ-technischen Komponente bietet Atruvia einen ganzheitlichen Beratungsansatz (Produktfamilie: Krisenmanagement 360), der insbesondere die organisatorische und führungsbezogene Ebene adressiert. Ziel ist es, Institute dazu zu befähigen, auch in komplexen und dynamischen Krisensituationen strukturiert, koordiniert und entscheidungssicher zu agieren.

Dieser Ansatz umfasst modulare Leistungsbausteine, die je nach Reifegrad und Zielbild kombiniert werden können. Dazu zählen u.a.:

- **Krisenstabsübungen:** Simulation realistischer Szenarien zur Überprüfung von Entscheidungs-, Eskalations- und Kommunikationsprozessen. Vor Ort in den Instituten gemeinsam mit dem Krisenstab.
- **Notbetriebstests:** Erprobung technischer und organisatorischer Abläufe unter Ausfallbedingungen zur Sicherstellung der Betriebsfähigkeit im Notfall.
- **Assessments:** Strukturierte Analyse des Reifegrads in den Bereichen Informationssicherheit, BCM und Compliance im Kontext regulatorischer Anforderungen anhand eines standardisierten Bewertungsbogens.
- **Krisenstabstrainings:** Individuell zugeschnittene Workshops u. a. zur Stärkung von Rollenverständnis, Führungsverhalten und Kommunikationsfähigkeit in Krisensituationen sowie zur Vertiefung spezifischer Bedarfsfelder.
- **VR-TrainingLab:** Praxisnahe Simulation in einer virtuellen Umgebung zur realitätsgetreuen Abbildung von Stress- und Entscheidungssituationen als innovativer, immersiver Trainingsansatz.

Vorteile eines integrativen Ansatzes beim Krisenmanagement

Generell ist hier eine regelmäßige Durchführung verschiedener Maßnahmen zu empfehlen, um eine kontinuierliche Weiterentwicklung der Resilienz sicherzustellen. Dies unterstützt insbesondere die regulatorische Anforderung nach regelmäßiger Überprüfung und Verbesserung der Maßnahmen (vgl. Art. 24 DORA).

Der Mehrwert eines integrierten Ansatzes liegt vor allem in der Stärkung der Handlungsfähigkeit im Krisenfall. Durch klar definierte Strukturen, trainierte Entscheidungsprozesse und etablierte Kommunikationswege können Reaktionszeiten verkürzt und Fehlentscheidungen

reduziert werden. Gleichzeitig wird die organisationsweite Koordination verbessert, was insbesondere bei bereichsübergreifenden Krisenlagen entscheidend ist.

Zudem ermöglicht ein solcher Ansatz die systematische Identifikation von Schwachstellen in Prozessen, Technologien und Organisationsstrukturen. Dies schafft die Grundlage für eine kontinuierliche Verbesserung und stärkt die langfristige Resilienz des Instituts.

Weiterhin wird durch die Implementierung strukturierter Übungen, umfassender Assessments und sorgfältiger Dokumentationen eine fundierte Grundlage für den Nachweis gegenüber Aufsichtsbehörden geschaffen. Die Anforderungen aus DORA sowie aus nationalen Regelwerken wie MaRisk und KWG können auf diese Weise nachvollziehbar adressiert werden. Im Rahmen der Implementierung von Maßnahmen gewinnt die Nachweisfähigkeit der Wirksamkeit zunehmend an Bedeutung.

Fazit

Zusammenfassend wird deutlich, dass modernes Krisenmanagement weit über die reine technische Absicherung und klassische Notfallkonzepte hinausgeht. Die regulatorischen Anforderungen, insbesondere durch DORA, erfordern eine ganzheitliche Betrachtung der operationellen Resilienz. Integrierte Ansätze, die technische Fähigkeiten mit organisatorischer Vorbereitung und gezielter Befähigung von Entscheidungsträgern verbinden, leisten dabei einen wesentlichen Beitrag zur Sicherstellung der Handlungsfähigkeit in zunehmend komplexen Krisenszenarien. ▬

Jacob Schirner
Consultant Informationssicherheit bei ATRUVIA, Schwerpunkt BCM
E-Mail: jacob.schirner@atruvia.de

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

Anforderungen der Aufsicht und genossenschaftliche Wertewelt – Rolle des zukünftigen Compliance-Managers

Vertrauen entsteht nicht allein durch Gesetze, Verordnungen oder Regulatorik. Vertrauen entsteht durch Menschen, durch Entscheidungen, durch Verantwortung. Genau darin liegt der Kern einer guten Compliance-Kultur und zugleich eine zentrale Aufgabe des zukünftigen Compliance-Managers.

Der Begriff „compliant“ bedeutet „regelkonform“, „konform“ oder „im Einklang mit etwas“. Aber mit was genau stehen oder handeln wir im Einklang, wenn wir compliant sind? Compliance und die gelebte Compliance-Kultur beginnen nicht mit einem Gesetz oder einer Verordnung. Sie beginnen mit einer Haltung. Mit der Überzeugung, dass regelkonformes und verantwortungsvolles Handeln selbstverständlich sein sollte – auch dann, wenn keine eindeutige Vorgabe existiert.

Compliance ist deshalb mehr als die Einhaltung von Regeln. Sie ist Ausdruck eines Miteinanders, das auf Werten wie Vertrauen, Respekt und Verantwortung basiert. Gerade in einer Zeit, in der kurzfristige Interessen und individuelle Vorteile häufig stärker in den Vordergrund rücken, gewinnt diese Haltung wieder an Bedeutung.

Die Frage, ob wir compliant – im Einklang mit etwas - sind und handeln, bemisst sich insofern gerade nicht an der Anzahl der Kontrollen oder Richtlinien. Sie zeigt sich im täglichen Handeln. Dort entscheidet sich, ob Regeln gelebt oder lediglich erfüllt werden.

Compliance-Kultur

Jede Bank lebt vom Vertrauen ihrer Kunden, Mitglieder und der Gesellschaft. Dieses Vertrauen ist nicht selbstverständlich. Es muss jeden Tag neu verdient werden.

Compliance ist deshalb weit mehr als die Umsetzung regulatorischer Anforderungen. Sie ist Teil einer guten – und im Wortsinn: vorbildlichen – Unternehmensführung und einer gelebten Risikomanagementkultur. Sie gibt Orientierung und unterstützt uns dabei, verantwortungsvolle Entscheidungen zu treffen.

Dabei entsteht Compliance primär gerade nicht in der Compliance-Abteilung. Sie hat ihre Basis überall dort, wo Menschen in Unternehmen, in Banken und ganz allgemein: im gesellschaftlichen Miteinander Verantwortung übernehmen.

Anforderungen der Aufsicht

Überfliegen wir die Presseberichte über unsere Branche oder unsere Gruppe, darf es nicht verwundern, dass sich die Erwartungen der Bafin als Aufsichtsbehörde verändert haben. Es geht in der Regulatorik heute nicht mehr allein darum, ob Vorgaben erfüllt werden oder wurden. Im Mittelpunkt steht zunehmend die Frage, ob Compliance wirksam ist und ob Risiken in der Bank tatsächlich verstanden und gesteuert werden.

Jede Bank, jedes genossenschaftliche Institut muss das eigene Risikoprofil kennen und daraus zielgerichtete Maßnahmen ableiten, um den jeweiligen Risikofeldern adäquat zu begegnen. Dabei entscheidet nicht die Größe eines Instituts über Quantität und Umfang der Compliance, sondern die individuelle Risikosituation der Bank in Verbindung mit den entsprechenden Risikomanagementmaßnahmen.

Vor diesem Hintergrund ist es nachvollziehbar, dass für die Aufsicht Proportionalität im Sinne von Größenabhängigkeit nicht weniger Compliance bedeutet, sondern Angemessenheit des institutsspezifischen Risikomanagements, das Erkennen und Kennen von Risiken und das Entwickeln und Implementieren von angemessenen Maßnahmen.

Genossenschaftliche Wertewelt

In den Volksbanken Raiffeisenbanken sind Verantwortung, Transparenz, Solidarität und Nachhaltigkeit tief verwurzelt. Sie gehören seit jeher zum genossenschaftlichen Selbstverständnis und Wertekanon. Die genossenschaftliche Idee steht für ein Miteinander, das nicht allein vom eigenen Vorteil geprägt ist, sondern vom Gedanken der gemeinsamen Verantwortung.

Die Erwartungen der Aufsicht und die genossenschaftliche Wertewelt stehen dabei nicht im Widerspruch. Im Gegenteil: Genossenschaftliches Selbstverständnis und genossenschaftliche DNA sind im gesamtgesellschaftlichen und erst recht im finanzwirtschaftlichen Kontext eine wesentliche Grundlage moderner Compliance-Überlegungen.

Wo die genossenschaftlichen Werte gelebt werden, muss Compliance nicht ständig eingefordert werden. Sie ist Teil des täglichen Handelns. Nicht aus gesetzlicher oder regulatorischer Pflicht, sondern aus Überzeugung.

Umsetzung der AMLR

Die AMLR tritt im Juli 2027 in Kraft. Bis dahin sind auch die Genossenschaftsbanken gefordert, personelle und organisatorische Anpassungen zu planen.

- Welches Mitglied der Geschäftsleitung soll die neue Funktion des Compliance-Managers in der Bank bekleiden?
- Welche Aufgaben muss der Compliance-Manager in seiner neuen Funktion übernehmen?
- Wie ist das Zusammenspiel der neuen Funktion des Compliance-Managers mit anderen Bereichen zu gestalten?
- Wie ist das bankinterne Geldwäsche-Compliance-Management-System nach den neuen Vorgaben zu gestalten?

Diese und weitere Fragen hierzu werden wir gemeinsam mit Ihnen auf dem Compliance Kongress 2026 am 2. Oktober 2026 in Montabaur erörtern. Als weitere Vertiefung in dieses wichtige Thema werden wir noch im vierten Quartal zu der Rolle und den Aufgaben des Compliance-Managers Online-Seminare anbieten.

Ab Anfang 2027 unterstützen wir Sie zusätzlich mit einem fachlichen Qualifizierungsprogramm für die Rolle und die Aufgaben des Compliance-Managers. Unabhängig hiervon unterstützen wir Sie hausindividuell bei der Implementierung der neuen Funktion des Compliance-Managers.

Die Rolle des zukünftigen Compliance-Managers nach der neuen EU-Geldwäscheverordnung

Die regulatorischen Anforderungen der vergangenen Jahre – von § 25a KWG über die MaRisk und die EBA-Leitlinien zur internen Governance bis hin zur neuen EU-Geldwäscheverordnung (AMLR) – verdeutlichen, dass Compliance heute als wesentlicher Bestandteil einer wirksamen Governance verstanden wird. Diese Entwicklung spiegelt sich nicht zuletzt auch in den Vorgaben der AMLR wider. Mit der neuen Rolle des Compliance-Managers wird die Compliance-Funktion nochmals deutlich gestärkt und ausdrücklich auf Ebene der Leitungsorgane verankert.

Nach den neuen Vorgaben, welche zum 10. Juli 2027 in Kraft treten, ist demnach künftig ein Mitglied der Geschäftsleitung als Compliance-Manager zu benennen. Mit dieser Funktion geht die Gesamtverantwortung für die Einhaltung der geldwäscherechtlichen Anforderungen einher. Die Hauptaufgabe soll darin bestehen, sicherzustellen, dass die institutsinternen Strategien, Grundsätze, Verfahren und Kontrollen dem individuellen Risikoprofil entsprechen, wirksam umgesetzt werden und hierfür ausreichende personelle sowie sachliche Ressourcen zur Verfügung stehen.

Die AMLR zeigt damit, dass eine wirksame Geldwäsche-Compliance noch stärker als integraler Bestandteil einer verantwortungsvollen Unternehmensführung und Governance gesehen und vor allem gelebt werden muss.

Nicht die Größe einer Bank entscheidet dabei über die Ausgestaltung der Compliance, sondern die Risiken ihres Geschäftsmodells und die Wirksamkeit der getroffenen Maßnahmen.

Fazit

Compliance ist kein Selbstzweck. Sie schafft den Rahmen für Vertrauen. Compliance entsteht nicht allein durch Richtlinien oder Kontrollen, sondern dort, wo Menschen Verantwortung übernehmen und Werte im täglichen Handeln sichtbar werden.

Im genossenschaftlichen Bankwesen ist dies kein neuer Gedanke. Verantwortung, Verlässlichkeit und gemeinschaftliches Handeln gehören seit jeher zu unserem Selbstverständnis.

Die regulatorischen Entwicklungen der vergangenen Jahre greifen diese Werte auf und übertragen sie in konkrete organisatorische Anforderungen. Mit Blick auf die AMLR wird dies besonders anhand der neu geschaffenen Rolle des Compliance-Managers deutlich. ▬

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

Justus Tychek
Compliance Spezialist,
E-Mail: justus.tychek@dz-cp.de

Wertpapier-Aufsichtsrecht – praxisnah und kompakt

Die regulatorischen Anforderungen im Wertpapiergeschäft sind anspruchsvoll und entwickeln sich kontinuierlich weiter. Für Banken bedeutet das: Mitarbeitende müssen die maßgeblichen Vorschriften nicht nur kennen, sondern auch in der täglichen Arbeit sicher und nachvollziehbar anwenden. Die Bank muss ein entsprechendes Schulungskonzept vorhalten, das den aufsichtsrechtlichen Anforderungen an die Sachkunde gemäß WpDVerOV entspricht. Genau hier setzt unser Schulungsangebot im Wertpapierbereich an.

Wir verbinden fundierte Fachexpertise in der WpHG-Compliance mit der langjährigen Erfahrung aus unserer Tätigkeit als führender Auslagerungsdienstleister innerhalb der Genossenschaftlichen FinanzGruppe. Unsere Spezialisten kennen sowohl die aufsichtsrechtlichen Erwartungen als auch die konkreten Fragestellungen, die im Vertrieb, in den Fachbereichen und in den Kontrollfunktionen der Institute auftreten. Die Inhalte unserer Sachkunde-Schulungen beruhen damit nicht allein auf theoretischem Wissen, sondern auch auf den Erkenntnissen aus unserer täglichen Praxis.

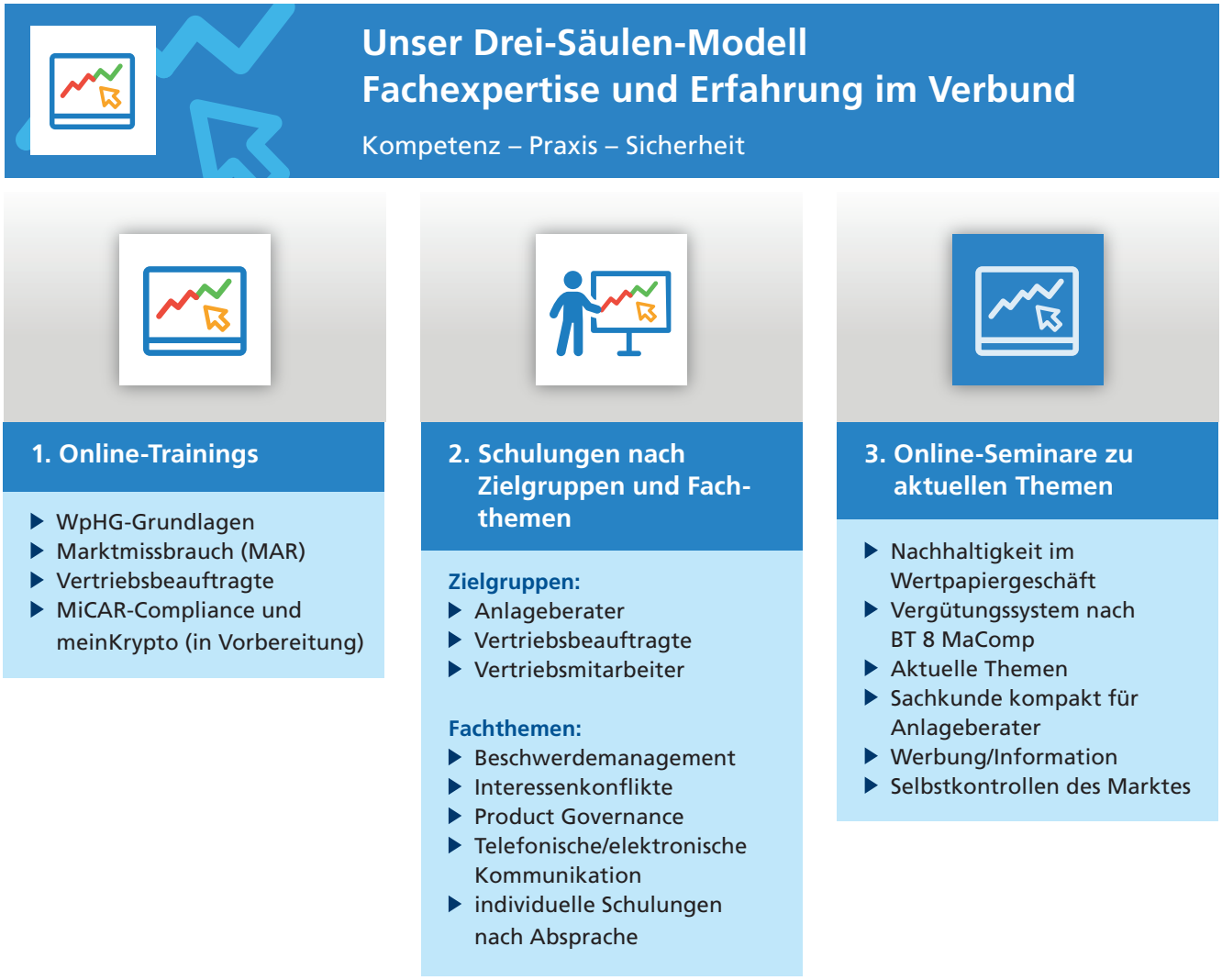
Unser Ziel ist es, anspruchsvolle Sachverhalte einfach und transparent darzustellen. Daher sind unsere Schulungen so konzipiert, dass sie komplexe Gesetze, Verordnungen und aufsichtsrechtliche Vorgaben in verständliche Handlungsempfehlungen übersetzen. Dafür haben wir ein Drei-Säulen-Modell entwickelt, das Grundlagenwissen, zielgruppenspezifische Vertiefungen und ausgewählte Fachthemen sinnvoll miteinander verbindet.

Erste Säule: Online-Trainings (WBT)

Die erste Säule unseres Schulungskonzepts bilden die Online-Trainings bzw. WBTs. Als Basiswissen für die WpHG-Compliance dient unsere Grundlagenschulung, die allen Bankmitarbeitern die wesentlichen Verhaltensregeln anschaulich vermittelt. Die Teilnehmenden lernen hierbei, warum WpHG-Compliance relevant ist und wie sie sich im Alltag im Umgang mit Beschwerden, Interessenkonflikten und Mitarbeitergeschäften aufsichtskonform verhalten. Unsere Vertiefungsmodule zum Marktmissbrauch (MAR) und für Vertriebsbeauftragte eignen sich aufbauend auf der Basisschulung für Mitarbeitende in relevanten Positionen und bieten spezifisches Wissen für genau diese Zielgruppen.

Durch das digitale Format können sich die Teilnehmenden zeit- und ortsunabhängig Wissen aneignen oder vertiefen. Dies ist insbesondere dann von Vorteil, wenn größere Mitarbeitergruppen geschult oder einheitliche fachliche Grundlagen innerhalb eines Instituts geschaffen werden sollen.

Neue Mitarbeitende, Auszubildende oder Beschäftigte, die in einen wertpapierrelevanten Bereich wechseln, können sich so strukturiert mit den maßgeblichen Anforderungen vertraut machen. Gleichzeitig eignen sich die Trainings zur regelmäßigen Auffrischung bereits vorhandener Kenntnisse. Verständliche Beispiele, typische Praxissituationen und klare Kernaussagen erleichtern dabei den Wissenstransfer. Alle Teilnehmenden erhalten fachlich



geprüfte und einheitlich aufbereitete Inhalte, können das Lerntempo jedoch an ihren persönlichen Arbeitsalltag anpassen.

Zweite Säule: Schulungen nach Zielgruppen und Fachthemen

Nicht jede Tätigkeit im Wertpapiergeschäft stellt dieselben Anforderungen an die jeweils erforderliche Sachkunde. Anlageberater benötigen andere Vertiefungen als Vertriebsmitarbeitende, Vertriebsbeauftragte oder Beschäftigte innerhalb der Compliance-Funktion. Die zweite Säule unseres Modells besteht daher aus speziellen, bankindividuellen Schulungen, die sich an den konkreten Aufgaben und Verantwortungsbereichen der jeweiligen Zielgruppe orientieren.

In den zielgruppenspezifischen Veranstaltungen greifen unsere Spezialisten genau die Anforderungen auf, die für die Teilnehmenden in ihrer jeweiligen Funktion relevant sind. Diese Schulungen eignen sich für einen kleineren Personenkreis, damit auf die Fragen und Wünsche der Teilnehmer individuell eingegangen werden kann (pro Schulung max. 20 Teilnehmende).

Beispielsweise lernen Teilnehmende unserer Schulung für Anlageberater die aufsichtsrechtlichen Grundlagen und Tätigkeiten in der WpHG-Beratung, die notwendig für die Qualifizierung gem. § 14 WpDVerOV sind. Neben den theoretischen Grundlagen geht es im Praxisteil anschließend schwerpunktmäßig um die Pflichten innerhalb der Wertpapierberatung. Mit Fallbeispielen und konkreten Vorschlägen zur Fehlervermeidung erhalten die Teilnehmenden hier auch einen starken Praxisbezug, der mit ihrer Tätigkeit eng verknüpft ist. Abgerundet wird die Schulungsveranstaltung durch die Möglichkeit, spezifische Fragen und Fallkonstellationen mit unseren Spezialisten zu besprechen.

Daneben bieten wir auch Veranstaltungen zu bestimmten Fachthemen an. Diese können bedarfsorientiert frei miteinander kombiniert werden. Vom Beschwerdemanagement über Product Governance, Vergütungssysteme

nach BT 8 MaComp, Werbung bis zur telefonischen/elektronischen Kommunikation oder Anforderungen bei professionellen Kunden bieten wir zu sämtlichen WpHG-relevanten Fachthemen ein entsprechendes Schulungsmodul an.

Die Schulungen finden grundsätzlich online und damit ebenfalls ortsunabhängig statt, können auf Wunsch aber auch in Präsenz gehalten werden. Das Format kann dabei passend zum Teilnehmerkreis, zum Themenumfang und zu den organisatorischen Rahmenbedingungen des Instituts ausgewählt werden. Der unmittelbare Austausch der Teilnehmenden mit unseren Spezialisten schafft einen Mehrwert, der über die reine Vermittlung von Fachwissen hinausgeht.

Im Anschluss erhalten die Teilnehmenden ein Zertifikat, das als Nachweis zur Sachkunde gemäß den Anforderungen der WpDVerOV dienen kann.

Dritte Säule: Online-Seminare

Ergänzend zu unseren Online-Trainings und zielgruppen- sowie fachspezifischen Schulungen bieten wir mehrmals pro Jahr Online-Seminare zu aktuellen aufsichtsrechtlichen Themen des Wertpapierrechts an. Die Online-Seminare sind als kompakte Formate (Dauer meist 60 Min.) ausgestaltet und lassen sich somit gut in den Arbeitsalltag integrieren. Im Mittelpunkt unserer Seminare steht ebenfalls nicht nur die Vermittlung regulatorischer Vorgaben, sondern insbesondere deren praktische Umsetzung im Arbeitsalltag. Anhand konkreter Fallbeispiele und typischer Fragestellungen aus der Compliance-Praxis zeigen wir auf, welche Anforderungen sich daraus für Institute ergeben und worauf es bei einer rechtssicheren Umsetzung ankommt.

Beispielsweise lernen die Teilnehmenden in unserem Online-Seminar zu den aufsichtsrechtlichen Anforderungen an Informationen und Werbung, worauf bei der Prüfung und Dokumentation selbst erstellter Marketingmitteilungen konkret zu achten ist. Neben Dokumentationsmustern gehen wir hierbei auch auf „Best Practice"-Fälle und häufige Fehlerquellen ein, die uns in unserer langjährigen Erfahrung als Mehrmandantendienstleister regelmäßig begegnen.

Im Anschluss an die Veranstaltungen erhalten die Teilnehmenden ein Teilnahmezertifikat als Fortbildungsnachweis.

Sicher durchs Aufsichtsrecht mit uns als Partner

Unser umfangreiches Qualifizierungsangebot in der Wertpapier-Compliance ermöglicht es Ihnen, Ihr bestehendes Sachkundekonzept zu optimieren. Dabei schaffen die Online-Trainings ein einheitliches Basiswissen, das durch zielgruppen- und fachspezifische Schulungen vertieft werden kann. Mit unseren regelmäßigen, kompakten Online-Seminaren zu aktuellen aufsichtsrechtlichen Themen greifen wir darüber hinaus neue regulatorische Entwicklungen und ausgewählte Fachthemen auf und unterstützen Sie dabei, Ihr Wissen und Ihre Sachkunde dauerhaft auf dem aktuellen Stand zu halten. ▬

Marina Waidelich
Beauftragte WpHG-Compliance,
E-Mail: marina.waidelich@dz-cp.de

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

Operative Resilienz ist eine Führungsaufgabe

Warum bereichsübergreifende Governance zum Erfolgsfaktor wird: Von der Umsetzung zur Wirksamkeit

Ein internationaler Flughafen zählt zu den komplexesten Organisationsstrukturen überhaupt. Täglich greifen zahlreiche Bereiche mit unterschiedlichen Aufgaben und Verantwortlichkeiten ineinander, um einen sicheren und stabilen Betrieb zu gewährleisten. Dabei sind Verantwortlichkeiten, Kommunikationswege und Aufgaben klar und geregelt.

Ein ähnlicher Grundsatz gilt für Finanzinstitute. Auch hier entsteht operative Resilienz nicht durch einzelne Maßnahmen oder isolierte Funktionen, sondern durch bereichsübergreifende Zusammenarbeit unter einer „Leitzentrale".

Bereits kleine Störungen an den organisatorischen Schnittstellen können Auswirkungen auf den gesamten Betriebsablauf haben. Umgekehrt entsteht Stabilität dort, wo Prozesse ineinandergreifen, Informationen rechtzeitig verfügbar sind und Entscheidungen auf einer gemeinsamen Grundlage getroffen werden.

Die Umsetzung des Digital Operational Resilience Act (DORA) hat diese Zusammenhänge in dem vergangenen Jahr besonders deutlich werden lassen. Im Mittelpunkt standen zunächst regulatorische Anforderungen, neue Prozesse und organisatorische Anpassungen.

Mit etwas Abstand zur Einführungsphase zeigt sich jedoch eine weitergehende Erkenntnis: Die nachhaltige Wirkung regulatorischer Anforderungen entsteht nicht allein durch deren Umsetzung, sondern durch ihre Verankerung in der täglichen Unternehmenssteuerung.

Die entscheidende Frage lautet daher nicht nur: „Haben wir die Anforderung umgesetzt?" Sondern vielmehr: „Sind wir als Institut in der Lage, Risiken ganzheitlich zu steuern, um auch unter herausfordernden Bedingungen handlungsfähig zu bleiben?"
Operationale Resilienz ist damit nicht ausschließlich eine regulatorische Anforderung. Sie ist ein wesentlicher Bestandteil wirksamer Unternehmenssteuerung und lässt Themen, welche Schnittstellen zueinander haben, zusammenwachsen.

1. Operative Resilienz entsteht im Zusammenspiel

Operative Resilienz wird häufig zunächst einzelnen Themenfeldern oder Fachbereichen zugeordnet – z. B. der Informationssicherheit, dem IKT-Risikomanagement oder dem Notfallmanagement.

Diese Betrachtung greift jedoch zu kurz. Die Fähigkeit eines Instituts, auch unter außergewöhnlichen oder belastenden Rahmenbedingungen stabil und handlungsfähig zu bleiben, ist keine isolierte Aufgabe einzelner Bereiche. Sie ist vielmehr Ausdruck einer ganzheitlichen Steuerungsfähigkeit der Organisation.

Mit Einführung von DORA ist dieses Verständnis stärker in den Mittelpunkt gerückt. Die Verordnung fordert nicht nur belastbare Prozesse und Kontrollen, sondern stärkt vor allem den Anspruch an eine bereichsübergreifende und wirksame Unternehmenssteuerung.
Der Fokus verschiebt sich damit von der isolierten Erfüllung einzelner **Anforderungen hin zur gesamtheitlichen Steuerung der Risiken im Risikomanagement der Bank.**

Managementimpulse

- Verstehen wir operative Resilienz als gemeinsame Aufgabe der gesamten Organisation?
- Werden wesentliche Risiken aus unterschiedlichen Perspektiven betrachtet und zusammengeführt?
- Verfügen wir über eine gemeinsame Grundlage für strategische Entscheidungen?

2. Schnittstellen entscheiden über Resilienz

Die Leistungsfähigkeit komplexer Organisationen entscheidet sich häufig nicht innerhalb einzelner Bereiche, sondern am Zusammenspiel.

Dies kann nur zuverlässig funktionieren, wenn Informationen und Ergebnisse zwischen den beteiligten Bereichen rechtzeitig verfügbar sind, Verantwortlichkeiten klar geregelt sind und Entscheidungen auf einer gemeinsamen Grundlage getroffen werden. Gerade an diesen Schnittstellen zeigt sich, ob das Gesamtsystem funktioniert.

DORA beinhaltet klare Regelungen für eine resiliente Organisation. Sie entsteht jedoch nicht von selbst. Sie ist das Ergebnis des abgestimmten Zusammenwirkens verschiedener Steuerungs- und Kontrollfunktionen.

Informationssicherheit/IKT-Risikokontrolle, Datenschutz, BCM, Compliance oder Auslagerungsmanagement erfüllen jeweils einen eigenständigen Auftrag und bringen ihre spezifische Expertise und ihren Blick auf Risiken mit ein.

Sehen wir die Umsetzung der DORA-Verordnung als Chance – so entsteht ein Mehrwert nicht durch die isolierte Betrachtung der einzelner Themenfelder, sondern durch die Fähigkeit, unterschiedliche Perspektiven zusammenzuführen und ein gemeinsames Verständnis von Risiken, Auswirkungen und Handlungsbedarfen zu entwickeln.

Die praktische Umsetzung regulatorischer Anforderungen hat gezeigt, dass Herausforderungen häufig nicht innerhalb einzelner Verantwortungsbereiche entstehen, sondern dort, wo Übergaben stattfinden und eine wirksame Verzahnung sicherzustellen ist.
Beispiele hierfür sind:

- Unterschiedliche Risikobewertungen
- Fehlende gemeinsame Informationsgrundlage
- Unklare Verantwortlichkeit bei bereichsübergreifenden Themen
- Verzögerung bei Entscheidungen

Die Qualität einer Institution bemisst sich nicht allein an der Leistungsfähigkeit ihrer einzelnen Funktionen. Entscheidend ist vielmehr, wie gut diese miteinander vernetzt sind und gemeinsam zur Steuerungsfähigkeit des Instituts beitragen.

Managementimpulse

- Wo liegen in Ihrem Institut die entscheidenden Schnittstellen – und wie stellen Sie sicher, dass dort Informationen und Verantwortlichkeiten wirksam ineinandergreifen?
- Sind Verantwortlichkeiten und Entscheidungswege über Bereichsgrenzen hinweg wirksam ausgestaltet?

3. Aus Ereignissen lernen: Governance zeigt sich im Ernstfall

Auch komplexe Systeme wie ein Flughafen entwickeln sich kontinuierlich weiter: Ereignisse werden analysiert, Abläufe überprüft und Verbesserungen umgesetzt. Hier ist es von essenzieller Bedeutung, Verbesserungen über das Gesamtsystem umzusetzen, um keine Lücken im Zusammenspiel zu schaffen. Genau dieser Gedanke ist auch für die operative Resilienz von Finanzinstituten entscheidend: Zum Beispiel der Umgang mit IKT-Vorfällen verdeutlicht dies besonders.

Die strukturierte Erfassung und Dokumentation eines Vorfalls ist eine wichtige Grundlage. Sie schafft Transparenz und ermöglicht Nachvollziehbarkeit.

Der eigentliche Mehrwert entsteht jedoch erst dann, wenn die gewonnenen Erkenntnisse genutzt werden:

- Welche Ursachen lagen zugrunde?
- Welche Prozesse haben funktioniert?
- Wo bestanden Schwachstellen?
- Welche Maßnahmen verbessern die Widerstandsfähigkeit nachhaltig?

Ein Vorfall sollte daher nicht ausschließlich als abgeschlossenes Ereignis betrachtet werden, sondern als Möglichkeit zur Weiterentwicklung der Organisation. Dabei spielt wiederum die Zusammenarbeit verschiedener Funktionen eine zentrale Rolle. Erst durch die gemeinsame Betrachtung von technischen, organisatorischen und regulatorischen Aspekten entsteht ein ganzheitliches Bild.

Dokumentation schafft Transparenz. Erst die gemeinsame Auswertung schafft Resilienz.

Managementimpulse

- Nutzen Sie die Erkenntnisse aus Vorfällen und Risiken systematisch zur Weiterentwicklung Ihrer Organisation?
- Sehen Sie die Erkenntnisse als Chance zur Verbesserung Ihrer Resilienz?

4. Governance als Führungsaufgabe

Operative Resilienz ist kein isoliertes Fachthema und keine rein regulatorische Verpflichtung. Sie ist ein wesentlicher Bestandteil einer zukunftsfähigen Unternehmenssteuerung.

Die Rolle des Leitungsorgans besteht dabei nicht darin, sämtliche operativen Details zu steuern. Vielmehr gilt es, eine Organisationsstruktur zu schaffen, in der Verantwortung klar verankert ist, Risiken transparent bewertet werden und fundierte Entscheidungen auf einer Grundlage getroffen werden können.

Wie bei dem komplexen System des Flughafens entsteht Stabilität nicht durch die Optimierung einzelner Einheiten, sondern durch das abgestimmte Zusammenspiel aller Beteiligten.

Die Umsetzung regulatorischer Anforderungen entfaltet daher ihren nachhaltigen Wert erst dann, wenn sie nicht nur formal erfüllt, sondern in die tägliche Steuerung der Organisation integriert wird.

Eine wirksame Governance zeigt sich nicht in der Anzahl vorhandener Regelwerke oder Kontrollen. Sie zeigt sich darin, ob eine Organisation auch unter veränderten Rahmenbedingungen handlungsfähig bleibt und Entscheidungen auf einer belastbaren Grundlage treffen kann.

Managementimpulse

- Haben wir ein gemeinsames Verständnis darüber, welche Faktoren unsere operative Resilienz maßgeblich beeinflussen?
- Sind unsere Governance-Funktionen so miteinander verzahnt, dass Risiken ganzheitlich betrachtet werden?
- Nutzen wir regulatorische Anforderungen als Impuls zur Weiterentwicklung unserer Unternehmenssteuerung?

Fazit – von der Regulierung zur gelebten Resilienz

Die Umsetzung von DORA hat viele Institute dazu veranlasst, bestehende Strukturen, Prozesse und Verantwortlichkeiten kritisch zu hinterfragen und weiterzuentwickeln.

Die wichtigste Erkenntnis geht dabei jedoch über einzelne regulatorische Anforderungen hinaus:

Operative Resilienz entsteht nicht allein durch Regelwerke, Prozesse oder Kontrollen. Sie entsteht dort, wo Verantwortung übernommen wird, Informationen wirksam zusammengeführt werden und unterschiedliche Bereiche gemeinsam zur Stabilität der Organisation beitragen.

Vielleicht liegt genau darin die wichtigste Erkenntnis aus der Umsetzung von DORA: Der Blick muss sich vom einzelnen Prozess und der einzelnen Anforderung hin zur ganzheitlichen Steuerung des Gesamtsystems verändern.

Stabilität entsteht nicht durch die isolierte Optimierung einzelner Bereiche, sondern durch das abgestimmte Zusammenspiel aller Beteiligten. Regulatorik schafft den Rahmen. Wirksame Unternehmenssteuerung schafft Resilienz. ▬

Katja Schlüter
Beauftragte Informationssicherheit & Datenschutz,
E-Mail: katja.schlueter@dz-cp.de

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

Allein oder vertrauen

Ob Sie Ihrer Verantwortung im Beauftragtenwesen allein gerecht werden oder dabei einem Partner vertrauen – wir unterstützen Sie, Ihre Entscheidung erfolgreich umzusetzen: **www.dz-cp.de**

#freiraumsichern

DZ CompliancePartner

ISO-Zertifizierung dokumentiert Qualität und Sicherheit

Informationssicherheit ist heute eine zentrale Voraussetzung für Vertrauen und erfolgreiche Zusammenarbeit. Mit der Zertifizierung nach ISO/IEC 27001:2022 dokumentiert die DZ CompliancePartner die Wirksamkeit ihres Informationssicherheitsmanagements und setzt ein klares Zeichen für Qualität und Sicherheit.

Die Digitalisierung verändert die Prozesse im Finanzsektor grundlegend. Gleichzeitig steigen die Anforderungen an die Sicherheit und Widerstandsfähigkeit von IT-Systemen und Geschäftsprozessen. Cyberbedrohungen, komplexe IT-Landschaften und die zunehmende Einbindung spezialisierter Dienstleister machen Informationssicherheit zu einem zentralen Bestandteil verantwortungsvoller Unternehmensführung.

Diesen Nachweis hat die DZ CompliancePartner erbracht und wurde nach erfolgreichem Audit durch den TÜV SÜD zertifiziert, dass ihr Informationssicherheitsmanagementsystem (ISMS) die Anforderungen der internationalen Norm ISO/IEC 27001:2022 erfüllt.

Mit dieser Zertifizierung bestätigt die DZ CompliancePartner die Wirksamkeit ihres Informationssicherheitsmanagements sowie ihren strukturierten Umgang mit Informationssicherheitsrisiken. Gleichzeitig unterstreicht sie den Anspruch, Informationen von Kunden, Partnern und Mitarbeitenden verantwortungsvoll und nach anerkannten internationalen Standards zu schützen.

Informationssicherheit gewinnt regulatorisch weiter an Bedeutung

Gerade im Finanzsektor kommt der Informationssicherheit eine besondere Rolle zu. Mit dem Digital Operational Resilience Act (DORA) hat der europäische Gesetzgeber die Anforderungen an das Management von Informations- und Kommunikationstechnologien (IKT) sowie an die Steuerung von Drittparteienrisiken weiter konkretisiert. Kapitel V der Verordnung befasst sich mit dem Management des IKT-Drittparteienrisikos. Artikel 28 Absatz 5 sieht vor, dass Finanzunternehmen nur mit IKT-Drittdienstleistern zusammenarbeiten sollen, die angemessene Informationssicherheitsstandards einhalten. Werden kritische oder wichtige Funktionen ausgelagert, müssen Institute zudem berücksichtigen, ob ihre Dienstleister aktuelle und anerkannte Qualitätsstandards für Informationssicherheit anwenden.

Für auslagernde Unternehmen gewinnen damit nachvollziehbare und unabhängige Nachweise über das Sicherheitsniveau ihrer Dienstleister zunehmend an Bedeutung. Eine Zertifizierung nach ISO/IEC 27001:2022 schafft hierfür eine international anerkannte Grundlage.

ISO/IEC 27001:2022 als anerkannter Standard

Die internationale Norm ISO/IEC 27001:2022 definiert Anforderungen an ein Informationssicherheitsmanagementsystem. Ziel ist es, Informationssicherheit systematisch zu steuern und kontinuierlich weiterzuentwickeln. Dabei umfasst Informationssicherheit weit mehr als technische Schutzmaßnahmen. Ebenso berücksichtigt werden organisatorische Prozesse, Verantwortlichkeiten, Risikomanagement sowie Maßnahmen zur Sensibilisierung der Mitarbeitenden. Im Mittelpunkt stehen die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

Für Kunden und Geschäftspartner bietet eine Zertifizierung den Vorteil, dass die Wirksamkeit des Managementsystems durch eine unabhängige Stelle überprüft wurde und regelmäßig erneut überprüft wird.

„Informationssicherheit ist für unsere Kunden ein wesentlicher Bestandteil einer vertrauensvollen Zusammenarbeit. Die Zertifizierung bestätigt, dass wir unser Informationssicherheitsmanagement konsequent an einem international anerkannten Standard ausrichten und kontinuierlich weiterentwickeln“, sagt Jens Saenger, Sprecher der Geschäftsführung der DZ CompliancePartner.


ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

ZERTIFIKAT

Zertifikat-Registrier-Nr.: 12 310 70724 TMS / Auftrags-Nr.: 707204760

Die Zertifizierungsstelle
der TÜV SÜD Management Service GmbH
bescheinigt, dass die Organisation

DZ CompliancePartner

DZ CompliancePartner GmbH
Wilhelm-Haas-Platz
63263 Neu-Isenburg
Deutschland

für den Geltungsbereich

Übernahme der Beauftragtenfunktion für
Finanzinstitute und andere Dienstleistungsunternehmen
auf den Gebieten Geldwäsche- und Betrugsprävention (Zentrale Stelle),
IKT-Risikokontrolle und Informationssicherheit, Datenschutz,
Wertpapierhandelsgesetz-Compliance
inklusive Single-Officer, MaRisk-Compliance, KI-Compliance,
Beratungs- und Unterstützungsdienstleistungen im Beauftragtenwesen
einschließlich der Standorte gemäß Anlage

ein Informationssicherheitsmanagementsystem gemäß
„Erklärung zur Anwendbarkeit“ eingeführt hat und anwendet.
Durch ein Audit wurde der Nachweis erbracht,
dass die Forderungen der

ISO/IEC 27001:2022

erfüllt sind.
Dieses Zertifikat ist gültig vom 23.04.2026 bis 22.04.2029.
Version der Erklärung zur Anwendbarkeit: v4 24.02.2026

Fred Wenke
Leiter der Zertifizierungsstelle
München, 23.04.2026

Seite 1 von 2

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuvsud.com/de-certificate-validity-check

Erfolgreiches Audit bestätigt die Wirksamkeit des Managementsystems

Der Zertifizierungsprozess erfolgte in mehreren Stufen. Im ersten Audit bewerteten die Auditoren des TÜV SÜD die Dokumentation des Informationssicherheitsmanagementsystems, die organisatorischen Rahmenbedingungen sowie die definierten Prozesse.

Im anschließenden Hauptaudit überprüften sie an den verschiedenen Standorten die praktische Umsetzung. Im Fokus standen dabei sowohl technische und organisatorische Sicherheitsmaßnahmen als auch Verantwortlichkeiten, interne Abläufe und die Umsetzung der Informationssicherheit im Unternehmensalltag.

„Informationssicherheit entfaltet ihren Nutzen erst dann vollständig, wenn sie im täglichen Handeln verankert ist. Deshalb standen im Audit nicht nur dokumentierte Prozesse, sondern insbesondere deren praktische Umsetzung im Mittelpunkt“, erläutert Sandra Sitter, Bereichsleiterin IT und Prozesse der DZ CompliancePartner.

Nach Abschluss der Audits wurden die Ergebnisse durch die zuständigen Stellen bewertet. Erst nach erfolgreicher Prüfung wurde das Zertifikat erteilt. Dieses Verfahren gewährleistet eine objektive und unabhängige Bestätigung der Erfüllung aller Anforderungen der ISO/IEC 27001:2022.

Mehr Transparenz und Sicherheit für Kunden

Für Kunden der DZ CompliancePartner schafft die Zertifizierung zusätzliche Transparenz und Sicherheit in der Zusammenarbeit. Die Informationssicherheit ist systematisch in Prozessen, Verantwortlichkeiten und kontinuierlichen Verbesserungsmaßnahmen verankert.

Gerade im Auslagerungsmanagement unterstützt dieser unabhängige Nachweis Unternehmen dabei, regulatorische Anforderungen nachvollziehbar zu erfüllen und Dienstleister anhand anerkannter Standards zu bewerten.

„Unsere Kunden erwarten nachvollziehbare und belastbare Nachweise für den sicheren Umgang mit Informationen. Die Zertifizierung stärkt diese Transparenz und schafft eine verlässliche Grundlage für eine langfristige Zusammenarbeit“, erklärt Jens Saenger.

Die Zertifizierung ist dabei kein einmaliger Meilenstein. Das Informationssicherheitsmanagementsystem wird kontinuierlich überprüft und weiterentwickelt. Risiken werden regelmäßig bewertet, Maßnahmen angepasst und Prozesse fortlaufend verbessert, um auf neue technologische Entwicklungen, Bedrohungslagen und regulatorische Anforderungen reagieren zu können.

„Informationssicherheit ist eine gemeinsame und dauerhafte Aufgabe. Die erfolgreiche Zertifizierung ist das Ergebnis des Engagements vieler Mitarbeitender und zugleich Ansporn, unser Sicherheitsniveau kontinuierlich weiterzuentwickeln“, so Sandra Sitter.

Die Zertifizierung nach ISO/IEC 27001:2022 dokumentiert damit nicht nur die erfolgreiche Erfüllung eines international anerkannten Standards. Sie stärkt das Vertrauen von Kunden und Partnern, erhöht die Transparenz des Informationssicherheitsmanagements und unterstreicht den Anspruch der DZ CompliancePartner, Informationen verantwortungsvoll und nachhaltig zu schützen. ▬ *(red.)*

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 CP steht im Einklang mit den Anforderungen der novellierten MaRisk AT 4.4.3. Wir haben die neuen MaRisk geprüft, woraus sich nur unwesentlicher Anpassungsbedarf ergibt. Diesen werden wir unmittelbar in Umsetzung bringen.

Seit der letzten Berichterstattung in der Point of Compliance (1/2026, S. 26) wurden aus der von der Geschäftsführung genehmigten Jahresprüfungsplanung 2026 die Prüfungen Hinweisgebersystem, MaRisk-Compliance, WpHG-Compliance und die Innenrevisionsprüfung im IT-Bereich abgeschlossen. Da alle diese Prüfungen dienstleistungsbezogen waren, wurden sie jeweils den entsprechenden Mandanten zur Verfügung gestellt. Da die Innenrevisionsprüfung der IT der DZ CompliancePartner potentiell alle Mandanten betrifft, wurde diese Bericht an alle Mandanten, die im Berichtszeitraum unsere Kunden waren, versandt.

Die Quartalsberichte für das erste und zweite Quartal 2026 der Internen Revision wurden fristgerecht erstellt und den Mandanten, die im Zeitraum zu unseren Kunden gehörten, zur Verfügung gestellt.

Weiterhin wurde turnusgemäß je ein Follow-Up Quartalsbericht für Q1 und Q2 2026 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.

Neben den Mandanten erhält die ZAM regelmäßig alle dienstleistungsbezogenen Prüfberichte, die Quartalsberichte und eine Aufstellung eines Sachstandes aller offenen und erledigten Punkte zu den getroffenen dienstleistungsbezogenen Feststellungen.

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 wirtschaftliche Lage der DZ CompliancePartner ist stabil und mit +707 T€ über Plan. Hierzu haben die leicht über Plan liegenden Erlöse (+212 T€ über Plan) sowie eine geringe Unterschreitung des Aufwands (68 T€ unter Plan) beigetragen.

Die neue Regulatorik (MaRisk, AMLR) hat im ersten Halbjahr Mehraufwand verursacht. Dieser zeigt sich nicht nur in gestiegenen Personalaufwand, sondern auch durch deutlich gestiegene Rechts- und Beratungskosten. Die Aufwände werden im zweiten Halbjahr weiter ansteigen, insbesondere durch ein besonderes Engagement in der verbundübergreifenden Umsetzung des europäischen Geldwäscherechts AMLR.

Trotz des steigenden Aufwandes ist weiterhin von einem positiven Ergebnis im Geschäftsjahr auszugehen. ▬

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

Freitag, 2. Oktober 2026
Schloss Montabaur

Topthema: AMLR (gültig ab 10.07.27)

Der Compliance-Kongress 2026

Keynote: **Der europäische Blick auf Deutschland**

Handlungsfähigkeit entsteht dort, wo Freiheit und Ordnung zusammengedacht werden.

Dr. Thomas de Maizière Bundesminister a. D., Vorsitzender Dt. Telekom Stiftung

Externer Impuls: **Beobachten statt Bewerten**

Die schnelle Bewertung auffälliger Aspekte einer Tat ist verlockend – und sehr häufig falsch.

Alexander Horn Fallanalytiker und Profiler von Weltrang

Fachimpulse AMLR: **Die EU-Regulatorik für die Bekämpfung von Geldwäsche- und Terrorismusfinanzierung**

Fachimpulse Krypto: **meinKrypto und Regulatorik als Katalysator für Innovation**

Vorstandsforum: **AMLR – Relevanz für mich als Vorstand**

Fachforum: **Compliance-Radar**

Erfahren Sie mehr und melden Sie sich jetzt an:
www.dz-cp.de/compliance-kongress

ComplianceCollege

ComplianceCollege ist eine Marke der DZ CompliancePartner