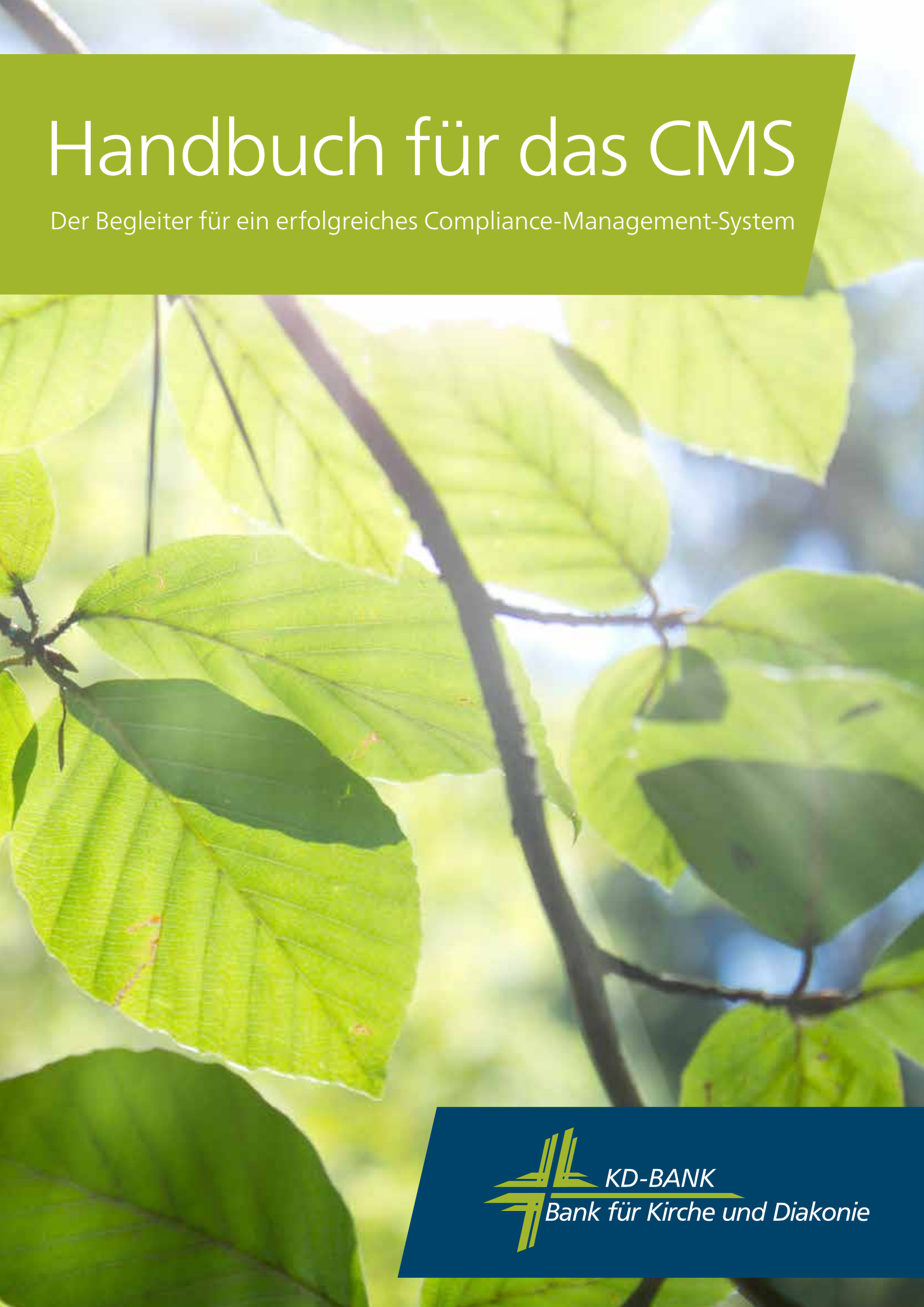
Handbuch für das CMS

Der Begleiter für ein erfolgreiches Compliance-Management-System



KD-BANK
Bank für Kirche und Diakonie

Der Inhalt des Handbuchs richtet sich nach dem Standard für Compliance-Management-Systeme TR CMS 101:2011

Das Handbuch und die enthaltenen Vorgaben zum Compliance-Management-System wurden vom Vorstand der Bank für Kirche und Diakonie in der Erstfassung ursprünglich am 18. April 2016 in Kraft gesetzt und sind für alle Mitarbeitenden der Bank für Kirche und Diakonie eG verbindlich. Es erfolgt eine fortlaufende Anpassung der Inhalte des Handbuchs entsprechend der für das Compliance-Management-System relevanten Anforderungen.

Der Vorstand der Bank für Kirche und Diakonie eG – KD-Bank ist für die Einrichtung, Aufrechterhaltung und ständige Verbesserung des Management-Systems zur Erfüllung der Compliance-Anforderungen verantwortlich.

Grundlage für das implementierte Compliance-Management-System (CMS) der Bank für Kirche und Diakonie bildet die von Vorstand und Aufsichtsrat in der Gesamtbankstrategie aufgenommene Regelung:

> *„Wir bekennen uns zu einer gelebten Compliance-Kultur in unserer Bank für Kirche und Diakonie. Die Grundeinstellungen und Verhaltensweisen des Vorstands, der leitenden Mitarbeitenden sowie die Rolle des Aufsichtsorgans prägen diese Kultur und beeinflussen somit die Grundhaltung, die die Mitarbeitenden der Beachtung von Regeln beimessen und damit die Bereitschaft zu regelkonformem Verhalten."*

Angesichts der Bedeutung von Compliance und der möglichen Folgen von Verstößen gegen Compliance-Anforderungen handelt es sich beim Compliance-Management-System um ein eigenständiges Management-System. Die wesentlichen, auf die Inhalte der Gesamtbankstrategie abgestimmten, übergreifenden Compliance-Regelungen wurden in der Teilstrategie für das Compliance-Management-System zusammengefasst. Durch fest implementierte Verfahren und Verantwortlichkeiten werden die Einrichtung, Aufrechterhaltung und ständige Verbesserung des Compliance-Management-Systems erfüllt.

1. Anwendungsbereich *Seite 6*

2. Ziele des Compliance-Management-Systems *Seite 6*

3. Begriffe *Seite 6*

4. Compliance-Management-System *Seite 8*

- 4.1 Allgemeine Anforderungen
- 4.2 Dokumentationsanforderungen
  - 4.2.1 Allgemeines
  - 4.2.2 Lenkung von Vorgabedokumenten
  - 4.2.3 Lenkung von Nachweisdokumenten

5. Verantwortung der Leitung *Seite 10*

- 5.1 Verpflichtung der Leitung
- 5.2 Verantwortung, Befugnis und Kommunikation
  - 5.2.1 Verantwortung und Befugnis
  - 5.2.2 Compliance-Beauftragter MaRisk und WpHG
  - 5.2.3 Interne Kommunikation
- 5.3 Managementbewertung
  - 5.3.1 Allgemeines
  - 5.3.2 Eingaben für die Bewertung
  - 5.3.3 Ergebnisse der Bewertung

6. Management von Ressourcen *Seite 16*

- 6.1 Bereitstellung von Ressourcen
- 6.2 Personelle Ressourcen
  - 6.2.1 Allgemeines
  - 6.2.2 Kompetenz, Schulung und Bewusstsein
- 6.3 Infrastruktur

7. Compliance-Prozesse und Umsetzung *Seite 19*

7.1 Spezifische Compliance-Risiken der Organisation

7.2 Anwendbare Compliance-Anforderungen

7.3 Entscheidung über die angemessenen Maßnahmen zur Erfüllung der Compliance-Anforderungen

7.4 Integration der Compliance-Anforderungen in die Arbeitsabläufe

7.5 Umgang mit compliance-relevanten Interessenskonflikten

7.6 System von Freigaben, Genehmigungen und Berechtigungen

7.7 Hinweisgebersystem

7.8 Anti-Korruptionsrichtlinie

7.9 Beratung, Unterstützung

7.10 Umgang mit compliance-relevanten Vorgängen

7.11 Externe Dienstleister

8. Systemüberwachung, -analyse und -verbesserung *Seite 25*

8.1 Interne Audits

8.2 Überwachung

8.3 Verbesserung

8.3.1 Ständige Verbesserung

8.3.2 Korrekturmaßnahmen

8.3.3 Vorbeugungsmaßnahmen

1. Anwendungsbereich

Diese Richtlinie erstreckt sich auf alle Leitungs- und Mitarbeiterebenen, alle Funktionsbereiche und Prozesse sowie alle Rechtsordnungen und Rechtsgebiete und alle unternehmensinternen Vorschriften, Richtlinien, Anweisungen.

2. Ziele des Compliance-Management-Systems

Ziel des über die Teilstrategie und über das Compliance-Handbuch dokumentierten Compliance-Management-Systems ist es, systematisch Voraussetzungen dafür zu schaffen, dass Verstöße gegen Compliance-Anforderungen vermieden bzw. wesentlich erschwert und eingetretene Verstöße erkannt und angemessen behandelt werden können.

3. Begriffe

Compliance-Kultur

Die Compliance-Kultur stellt die wesentliche Grundlage für jede Organisation dar. Dies bedeutet, dass das Management/die Geschäftsleitung erst durch aktives Vorleben die Voraussetzung für das Annehmen, die Beachtung und das Umsetzen der Compliance-Vorgaben durch die Mitarbeitenden schafft.

Führung

Führungskräfte haben eine Vorbildfunktion und müssen sich zur Einhaltung gesetzlicher, regulatorischer und ggf. auch eigener ethischer Vorgaben verpflichten und dies durch entsprechendes Verhalten vorleben. Genauso strikt müssen sie dies auch von ihren Mitarbeitenden einfordern (Führungsgrundsätze der Bank für Kirche und Diakonie).

Einbeziehung der Mitarbeitenden

Auf allen Ebenen werden Mitarbeitende im täglichen Arbeitsleben mit gesetzlichen Anforderungen direkt oder indirekt konfrontiert. Oftmals ist es dem Einzelnen nicht immer hinreichend bewusst, dass seine Tätigkeit gesetzlichen Vorgaben genügen muss. Deshalb müssen die Mitarbeitenden sensibilisiert werden. Sie sind es, die zum überwiegenden Teil die gesetzlichen Vorgaben im Unternehmen berücksichtigen und umsetzen bzw. einhalten müssen.

Administration des Compliance-Systems durch den Compliance-Beauftragten

Jedes funktionierende System bedarf eines gewissen administrativen Aufwands, damit wesentliche überwachende Aufgaben, steuernde Aktivitäten sowie Auswertungs- und Berichterstattungstätigkeiten vollzogen werden. Dies geschieht nicht von selbst, daher ist eine Stelle erforderlich, die diese Funktionen und Aufgaben wahrnimmt, der Compliance-Beauftragte MaRisk.

Compliance-Risikoanalyse

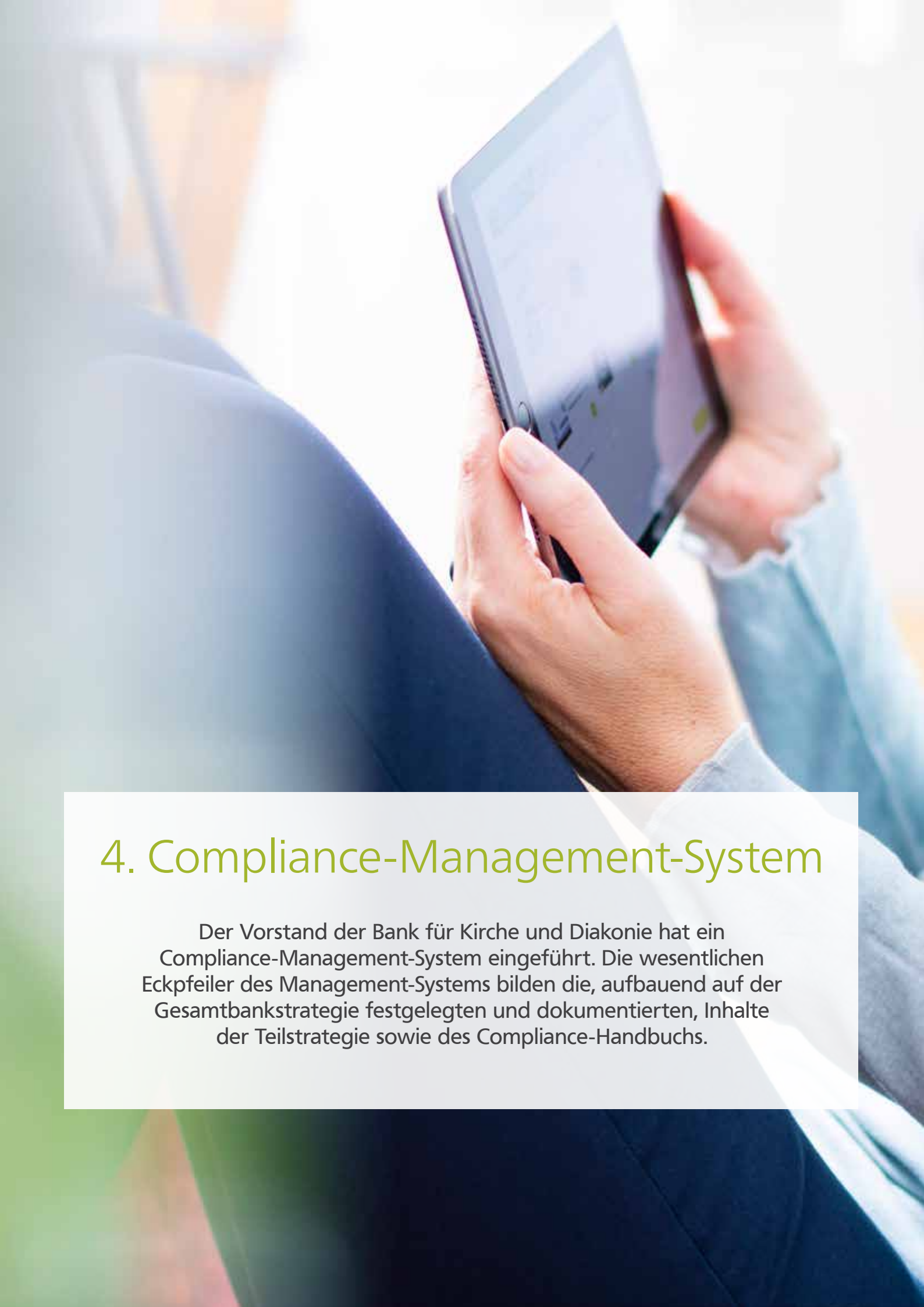
Ohne eine Standortbestimmung wird es jeder Organisation schwerfallen, die richtigen Entscheidungen zu treffen. Dies gilt umso mehr, wenn es um Gesetzeskonformität geht. Die Organisation muss sich einen Überblick über ihr organisatorisches Umfeld (Rechtsform der Gesellschaft, Produkte bzw. Dienstleistungserbringung, nationales oder internationales Agieren etc.) verschaffen, um die sich daraus ergebenden Compliance-Risiken richtig zu bewerten. Nur wenn man sich der Risiken bewusst ist, kann man dementsprechende Vorkehrungen zur Vermeidung bzw. zur Minderung der Compliance-Risiken treffen. Diese Vorkehrungen müssen dann in die entsprechenden Prozesse und Arbeitsabläufe integriert werden.

Systemorientierter Managementansatz

Ermitteln, verstehen, leiten und lenken von miteinander in Wechselbeziehung stehenden Prozessen als Systemansatz tragen zur Wirksamkeit und Effizienz der Compliance-Ziele bei. Compliance sollte kein Zufallsprodukt, sondern ein Ergebnis von klaren Vorgaben und deren Umsetzung sein. Nur ein systematischer Ansatz, der Transparenz der Vorgaben und Nachweise garantiert, ist belastbar und kann zur Entlastung der Organisation und des Managements herangezogen werden.

Systemüberwachung, -analyse und -verbesserung

Die ständige Verbesserung der Gesamtleistung der Organisation stellt ein permanentes Ziel der Organisation dar. Dazu trägt das Compliance-Management-System durch verschiedenste Maßnahmen bei, wie z.B. durch interne Compliance-Audits, -Tests der internen Kontrollen (gesetzte Maßnahmen oder Einrichtung zur Erkennung von Compliance-Verstößen), -Überwachung durch externe Prüfer/Prüfstellen. Die Analyse aller verwertbaren Informationen sollte dann zur Verbesserung des Compliance-Management-Systems genutzt werden. Letztlich sollte jede Organisation das Ziel anstreben, Compliance-Verstöße zu verhindern und durch entsprechende Maßnahmen den Schaden für die Organisation oder die Gesellschaft so gering wie möglich zu halten.



4. Compliance-Management-System

Der Vorstand der Bank für Kirche und Diakonie hat ein Compliance-Management-System eingeführt. Die wesentlichen Eckpfeiler des Management-Systems bilden die, aufbauend auf der Gesamtbankstrategie festgelegten und dokumentierten, Inhalte der Teilstrategie sowie des Compliance-Handbuchs.

4.1 Allgemeine Anforderungen

Die vom Vorstand beschlossenen und in Kraft gesetzten Regelungen zum Compliance-Management-System sowie die daraus resultierenden internen sowie ausgelagerten Prozesse sind für alle Mitarbeitenden verbindlich. Die Abfolge und Wechselwirkung der verschiedenen Prozesse werden hierbei beachtet. Um das wirksame Durchführen und Lenken dieser Prozesse sicherzustellen, bestehen unterschiedliche Kriterien, Methoden und Vorgaben. Des Weiteren wird die Verfügbarkeit von Ressourcen und Informationen sichergestellt, um die Durchführung und Überwachung dieser Prozesse umsetzen zu können. Der Vorstand leitet und lenkt die Prozesse in Übereinstimmung mit den gesetzlichen, insbesondere den bankaufsichtsrechtlichen Anforderungen sowie sonstigen Vorgaben. Im Falle der Auslagerung von Prozessen wird die Lenkung der Prozesse über diesbezügliche vertragliche Regelungen und Vorgaben, insbesondere Organisationsanweisungen geregelt.

4.2 Dokumentationsanforderungen

4.2.1 Allgemeines

Alle zum Compliance-Management-System zählenden Vorgabe- und Nachweisdokumente werden revisionssicher dokumentiert. Dies erfolgt im Regelfall über ein elektronisches Organisationshandbuch, das allen Mitarbeitenden standortübergreifend uneingeschränkt zur Verfügung steht. Alle den Compliance-Bereich betreffenden Unterlagen, wie zum Beispiel Aufzeichnungen über Ergebnisse von Compliance-Audits, Compliance-Berichten, Risikoanalysen und -bewertungen, Aufzeichnungen über Kennzahlen zur Messung von Compliance, Vorstandsprotokolle über Compliance-Angelegenheiten, Dokumente über Compliance-Schulungen sowie Dokumente über Compliance-Verstöße und die im Einzelfall ergriffenen Maßnahmen und Sanktionen unterliegen im Regelfall strengster Vertraulichkeit. Die Ablage der Unterlagen erfolgt verschlusssicher innerhalb des Compliance-Bereichs, im Personalbereich oder beim Vorstand.

4.2.2 Lenkung von Vorgabedokumenten

Die dem Compliance-Management-System zugrundeliegenden Vorgabedokumente unterliegen einem vorgegebenen, unter anderem aus den Mindestanforderungen an das Risikomanagement resultierenden, Freigabeprozess. Alle Vorgabedokumente werden nach Durchlaufen des jeweils erforderlichen Prozesses abschließend von einem Mitglied der Geschäftsführung genehmigt und somit für alle Mitarbeitenden verbindlich in Kraft gesetzt. Die vorherige Version des Vorgabedokuments wird archiviert und steht den Usern nicht mehr zur Verfügung. Die Führungskräfte des Hauses haben insbesondere die Aktualität der in ihrem Verantwortungsbereich liegenden Vorgabedokumente fortlaufend zu überwachen und zu bewerten. Im Bedarfsfall ist die erforderliche Aktualisierung unter Einbindung des Bereichs Organisation einzuleiten. Die vorgenommenen Anpassungen von Vorgabedokumenten werden entsprechend gekennzeichnet. Über eine Änderungshistorie sind sämtliche vorgenommene Änderungen revisionstechnisch nachvollziehbar.

4.2.3 Lenkung von Nachweisdokumenten

Der Vorstand hat entschieden, unabhängig von im Einzelfall möglicherweise kürzeren, gesetzlich geregelten Aufbewahrungsfristen, alle Unterlagen, so auch die Vorgabedokumente, für einen 10-jährigen Zeitraum zu archivieren.

5. Verantwortung der Leitung

5.1 Verpflichtung der Leitung

Um die Entwicklung und Verwirklichung des Compliance-Management-Systems sowie die ständige Verbesserung und dessen Wirksamkeit innerhalb der Organisation nachzuweisen, hat der Vorstand eine für alle Mitarbeitende verbindliche Organisation, die sich auch auf die compliance-relevanten Belange erstreckt, in Kraft gesetzt. Diese zeigt sich insbesondere durch die im Corporate Governance Kodex und in der Teilstrategie Compliance-Management sowie sonstigen Organisationsunterlagen fixierten Inhalte.

Der Vorstand unterstützt und fordert das compliance-relevante Verhalten aller Mitarbeitenden. Die Führungskräfte werden durch den Vorstand anhand von Führungsgrundsätzen dazu angehalten, für ein compliance-konformes Verhalten aller Mitarbeitenden und die Einhaltung rechtlicher Regelungen und Vorgaben zu sorgen. Die Führungskräfte haben, gemäß Entscheidung des Vorstands, die Compliance-Thematik in die regelmäßig stattfindenden Mitarbeitenden-Entwicklungsdialoge einzubinden und hierzu entsprechende Aussagen aufzunehmen. Der Vorstand erhält regelmäßig, unter anderem über die monatlich stattfindende Runde der leitenden Mitarbeitenden sowie über Compliance-Quartalsberichte, Informationen zum aktuellen Compliance-Sachstand und kann somit die Angemessenheit und Funktionsfähigkeit des Compliance-Management-Systems überwachen und im Bedarfsfall entsprechende Gegensteuerungsmaßnahmen einleiten.

5.2 Verantwortung, Befugnis und Kommunikation

5.2.1 Verantwortung und Befugnis

Der Vorstand hat die Verantwortungen und Befugnisse eines jeden einzelnen Mitarbeitenden über Stellenbeschreibungen und Kompetenzprofile geregelt. Die Regelungen sind für alle Mitarbeitenden über GenoHR einsehbar. Erforderlich gewordene Änderungen werden bekanntgemacht.

5.2.2 Compliance-Beauftragter MaRsik und WpHG

Zur Compliance-Kultur gehören auch der Compliance-Beauftragte MaRisk sowie der Compliance-Beauftragte WpHG. Der Vorstand hat nach sorgfältiger Auswahl einen Compliance-Beauftragten MaRisk aus der Unternehmensorganisation benannt, der selbständig oder in Zusammenarbeit mit anderen die Verantwortung und Befugnis hat:

a) Darauf hinzuwirken, dass die für das CMS erforderlichen Prozesse eingeführt, verwirklicht und aufrechterhalten werden,

b) der obersten Leitung über die Leistung und Wirksamkeit des CMS und jegliche Notwendigkeit für Verbesserungen zu berichten,

c) das Bewusstsein und die Kommunikation über die Compliance-Anforderungen in der gesamten Organisation sicherzustellen und

d) auf Eigeninitiative compliance-relevante Vorgänge aufzugreifen, zu dokumentieren und an die oberste Leitung zu berichten.

Der Vorstand ermöglicht den Compliance-Beauftragten MaRisk und WpHG eine unabhängige Wahrnehmung der Compliance-Aufgaben. Er weist den Compliance-Beauftragten MaRisk und WpHG keine weiteren Aufgaben zu, die Zielkonflikte mit der Erfüllung der Compliance-Aufgaben mit sich bringen.

5.2.3 Interne Kommunikation

Die jeweils betroffenen Mitarbeitenden und ggf. Dritte werden über das Compliance-Programm sowie die festgelegten Rollen und Verantwortlichkeiten informiert, damit diese ihre Aufgaben im CMS ausreichend verstehen und sachgerecht erfüllen können. Im Unternehmen wird festgelegt, wie Compliance-Risiken sowie Hinweise auf mögliche und festgestellte Regelverstöße an die zuständigen Stellen im Unternehmen (z.B. den Compliance-Beauftragten MaRisk, die gesetzlichen Vertreter und erforderlichenfalls das Aufsichtsorgan) berichtet werden. Um eine erfolgreiche Implementierung des CMS sicherzustellen, ist eine sachgerechte Kommunikation innerhalb der Organisation aber auch außerhalb der Bank für Kirche und Diakonie erforderlich.

Jahresberichte

Der Compliance-Beauftragte MaRisk berichtet dem Vorstand sowie dem Aufsichtsrat anhand strukturierter, aus der Genossenschaftsorganisation vorgegebener Musterjahresberichte unter anderem über die im vergangenen Jahr umgesetzten Tätigkeiten, aber auch noch zu erledigende Maßnahmen aus den Bereichen Compliance MaRisk. Bei gravierenden Anmerkungen besteht im Bedarfsfall die Pflicht, adhoc-Berichte an die Organe zu leiten. Bei ausgelagerten Maßnahmen, wie dem Datenschutz-, Geldwäsche/Betrugsprävention oder Compliance WpHG werden ebenfalls Jahresberichte erstellt, die dem Vorstand über den Compliance-Beauftragten MaRisk zur Verfügung gestellt werden.

Compliance-Newsletter

Alle Mitarbeitenden des Hauses werden regelmäßig durch den Compliance-Beauftragten MaRisk über einen Newsletter zu verschiedenen compliance-relevanten Themen informiert.

Mitarbeitenden-Entwicklungsdialog

Alle Führungskräfte haben in einem zweijährigen Turnus mit den Mitarbeitenden ihres Verantwortungsbereichs einen Mitarbeitenden-Entwicklungsdialog zu führen. Dieser Entwicklungsdialog enthält auch compliance-relevante Eckpunkte, die mit dem Mitarbeitenden zu besprechen sind.

Bereichs-/Mitarbeitenden-besprechungen (Jour-Fixe)

Alle Führungskräfte führen in regelmäßigen Abständen mit den in ihrem Zuständigkeitsbereich beschäftigten Mitarbeitenden Bereichs-Besprechungen, bei denen die Thematik Compliance jeweils mit besprochen wird. Im Bedarfsfall kann der Compliance-Beauftragte auf Eigeninitiative oder auf Anforderung an den Bereichsbesprechungen teilnehmen.

Compliance-Schulungen

Alle Mitarbeitenden sind in das Compliance-Schulungskonzept (webbasierte Schulungen oder Präsenzschulungen) eingebunden. Die Führungskräfte erhalten weitergehende Schulungsmaßnahmen. Ziel der Schulungen ist es, das Verständnis für Compliance-Richtlinien, das Bewusstsein für das CMS sowie die Bereitschaft zur wirksamen Umsetzung zu stärken. Die Schulungen werden regelmäßig auf ihre Wirksamkeit und Relevanz hin überprüft und bei Bedarf aktualisiert.

Bankenaufsichtsrechtsrunde

Die Mitglieder der Bankenaufsichtsrechtsrunde (Bereiche: Vorstandsmitglied, Kreditfolge, Marktfolge, Treasury, Nachhaltige Geldanlagen und Wertpapiere, Marketing, Betriebsorganisation, Innenrevision, Risikocontrolling-Funktion, Betriebswirtschaft, Compliance-Beauftragter MaRisk) treffen sich monatlich um insbesondere sämtliche bankenaufsichtsrechtliche Themen zu besprechen und deren Umsetzung zu koordinieren. In den Runden wird auch die Umsetzung einzelner Maßnahmen überwacht. Die Ergebnisse werden jeweils per Protokoll dokumentiert.

Abstimmung bzw. Koordinierung zwischen den Schnittstellen des Risikocontrollings, der Innenrevision, sowie der Compliance-Funktion

Aufgrund gesetzlicher Vorgaben ist eine Zusammenarbeit der drei Verteidigungslinien, Risikocontrolling-Funktion, Innenrevision und Compliance-Funktion erforderlich. Die Bereiche informieren sich gegenseitig regelmäßig anhand verschiedener Unterlagen, wie zum Beispiel interne und externe Revisionsprotokolle und Risikoreportings, Compliance-Berichte etc. Des Weiteren erfolgt ein bereichsübergreifender Austausch über die monatlich stattfindende Bankenaufsichtsrechtsrunde. Um Doppelarbeiten zu vermeiden erfolgt „anlassbezogen" eine Abstimmung zwischen den Beteiligten.

Compliance-Audits

Auf Initiative des Compliance-Beauftragten MaRisk werden unter anderem mit den für einzelne Rechtsbereiche verantwortlichen Führungskräften sowie weiteren Mitarbeitenden Audits geführt. Grundlage hierfür bilden unter anderem die seitens der Genossenschaftsorganisation vorgegebene und auf die Belange des Hauses abgestimmte Matrix aller wesentlichen und unwesentlichen Rechtsbereiche. Die einzelnen Audits werden protokolliert und vom Compliance-Beauftragten MaRisk archiviert.

5.3 Managementbewertung

5.3.1 Allgemeines

Der Vorstand der Bank für Kirche und Diakonie bewertet das Compliance-Management-System planmäßig in angemessenen Abständen, um die fortlaufende Eignung, Angemessenheit und Wirksamkeit sicherzustellen. Dies erstreckt sich insbesondere auch auf Möglichkeiten für Verbesserungen und Änderungsbedarf bezüglich des Compliance-Management-Systems. Hierzu berichtet der Compliance-Beauftragte MaRisk monatlich dem für den Compliance-Bereich zuständigen Vorstandsmitglied. Der Compliance-Vorstand berichtet, in Abstimmung mit dem Compliance-Beauftragten, im Bedarfsfall dem Gesamtvorstand. Die Aufzeichnungen über die Managementbewertung werden, gemäß Entscheidung des Vorstands, über einen Zeitraum von 10 Jahren archiviert.

5.3.2 Eingaben für die Bewertung

Die vom Compliance-Beauftragten MaRisk vorzubereitende Bewertung enthält folgende Informationen:

- Ergebnisse von Audits
- Hinweise zu compliance-relevanten Angelegenheiten von Mitarbeitenden, Geschäftspartnern, Kunden, Nutzern, Behörden, Verbänden etc.
- Meldungen über erkannte Verstöße gegen Compliance-Anforderungen
- Status und Wirksamkeit von Vorbeugungs- und Korrekturmaßnahmen sowie Aufwand für ergriffene Korrekturmaßnahmen
- Folgemaßnahmen vorangegangener Managementbewertungen und Ergebnisse von Folgemaßnahmen vorausgegangener Überwachungen
- Änderungen, die sich auf das Compliance-Management-System auswirken können (z.B. Gesetzesänderungen, veränderte Risikolage)
- Empfehlungen für Verbesserungen und Kennzahlen zur Messung von Compliance

5.3.3 Ergebnisse der Bewertung

Sofern aus der Berichterstattung an den Vorstand Handlungsbedarf resultiert, werden im Rahmen einer Managementbewertung entsprechende Entscheidungen und Maßnahmen eingeleitet, um eine Verbesserung der Wirksamkeit des Compliance-Management-Systems und seiner Prozesse sicherzustellen. Hierbei wird auch der Bedarf an möglichen Ressourcen und die Abdeckung des ermittelten Schulungsbedarfs zu compliance-relevanten Themen einbezogen.

6. Management von Ressourcen

6.1 Bereitstellung von Ressourcen

Der Vorstand ist verantwortlich für die Ermittlung und Bereitstellung der erforderlichen Ressourcen, um das Compliance-Management-System zu verwirklichen, aufrechtzuerhalten und seine Wirksamkeit ständig zu verbessern.

6.2 Personelle Ressourcen

6.2.1 Allgemeines

Alle Mitarbeitenden, die für ihre Tätigkeit Compliance-Anforderungen zu beachten haben, müssen über die zur Erfüllung dieser Anforderungen erforderliche Ausbildung, Schulung, Fertigkeiten und Erfahrungen verfügen.

6.2.2 Kompetenz, Schulung und Bewusstsein

Der Schulungsbedarf aller Mitarbeitenden wird systematisch, insbesondere von den Bereichsleitenden in Zusammenwirken mit dem Personalbereich ermittelt und ausgewertet, um insbesondere die erforderlichen Compliance-Anforderungen sicherzustellen. Die Schulungsmaßnahmen erstrecken sich auch auf das Verständnis für die Bedeutung der Erfüllung von Compliance-Anforderungen und das Bewusstsein für mögliche Folgen von Compliance-Verstößen. Ob die eingeleiteten Schulungsmaßnahmen ausreichen, wird über die Mitarbeitenden-Entwicklungsdialoge, die jede Führungskraft regelmäßig mit seinen Mitarbeitenden umsetzt, eruiert.

Sofern dem Compliance-Beauftragten MaRisk im Rahmen seiner Überwachungstätigkeit Hinweise auf möglichen Schulungsbedarf bekannt werden, wird dies gemeinsam mit dem zuständigen Bereichsleitenden sowie dem Personalbereich besprochen. Im Bedarfsfall werden anschließend entsprechende Maßnahmen eingeleitet.

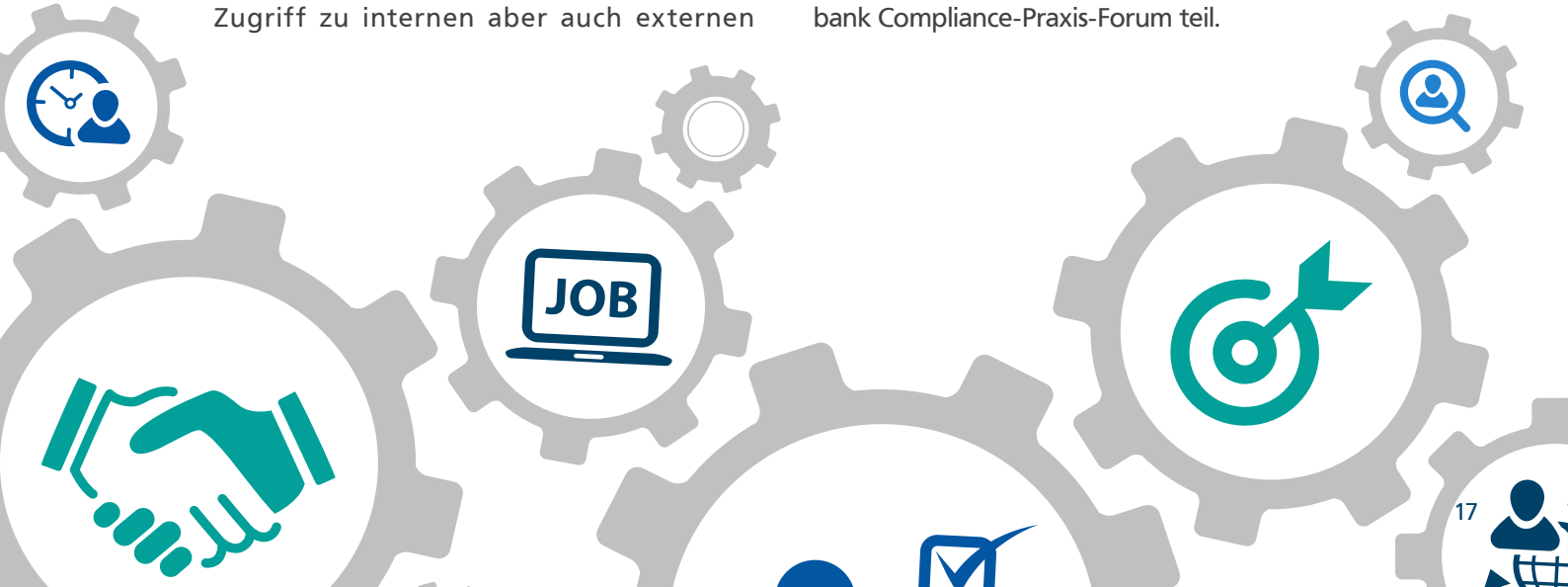
Alle mit weiteren Kontroll- oder Prüffunktion beauftragten Mitarbeitenden, wie zum Beispiel die Bereichsleitenden, die Wertpapier- und sonstigen Marktfolgemitarbeitenden und die Innenrevision, kontrollieren oder überprüfen aufgrund ihrer Funktion fortlaufend oder ge-

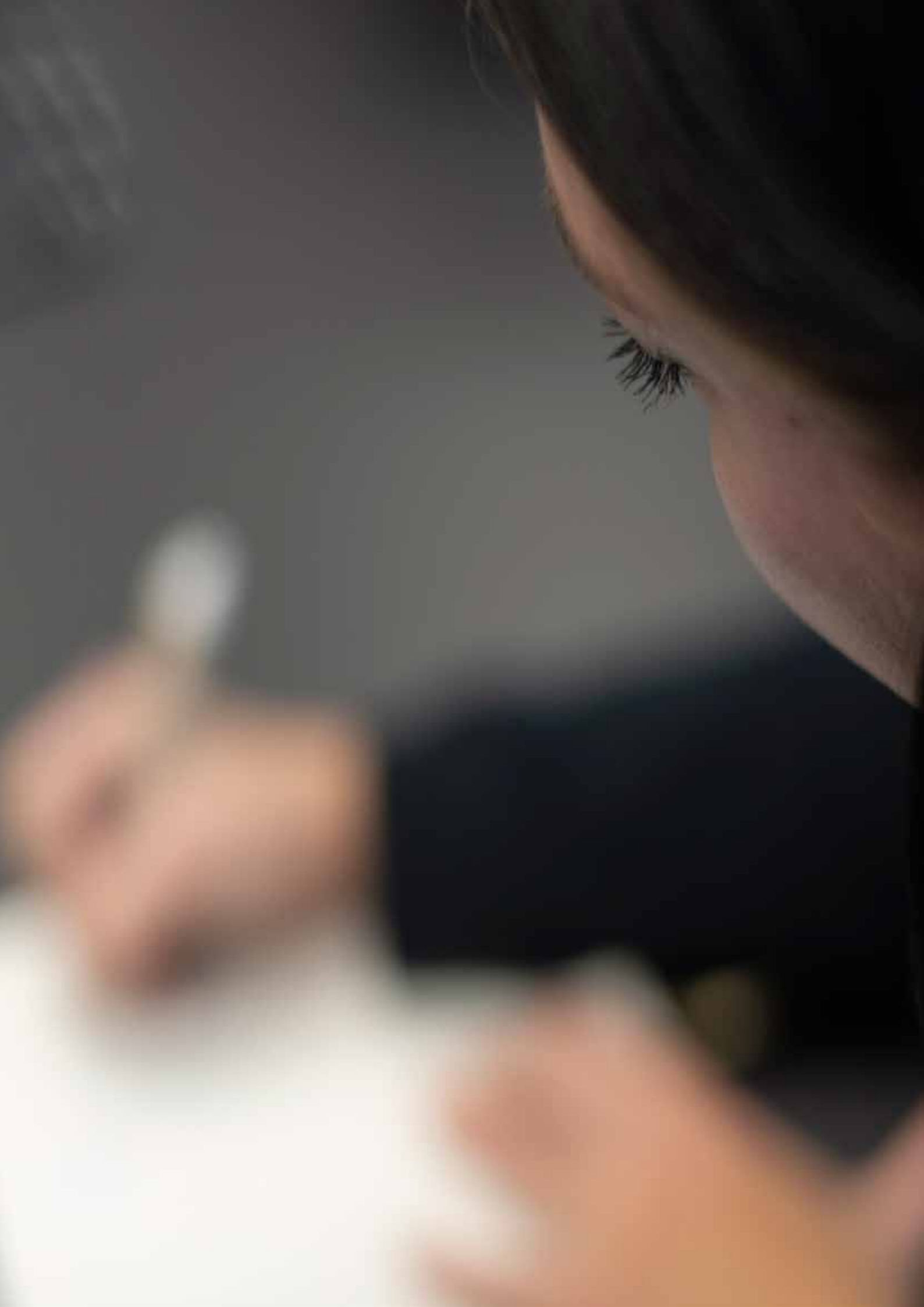
mäß Prüfungsplan die Ergebnisse bankseitig anhand festgelegter Prozesse und somit indirekt auch die Wirksamkeit der umgesetzten Schulungsmaßnahmen. Bei Fehlerhäufigkeit werden die Ursachen analysiert. Im Bedarfsfall können daraus weitere Schulungsmaßnahmen resultieren. Der Bereichsleiter Personal/Unternehmensservice führt geeignete Aufzeichnungen über Ausbildung, vorgesehene sowie umgesetzte Schulungsmaßnahmen, um die Förderung der Kompetenz eines jeden Mitarbeitenden sicherzustellen.

6.3 Infrastruktur

Der Vorstand der Bank für Kirche und Diakonie hat die für die Erfüllung der Compliance-Anforderungen erforderliche Infrastruktur ermittelt und dementsprechend bereitgestellt. Bei Bedarf besteht ein uneingeschränkter Zugriff zu internen aber auch externen Rechtsauskünften hinsichtlich des Umfangs, der Anwendbarkeit, der Geltung sowie der Reichweite von Compliance-Anforderungen. Dies wird durch die enge Zusammenarbeit mit den Rechtsbereichen der Genossenschaftsorganisation (u. a. Genossenschaftsverband – Verband der Regionen, BVR, AVR, Fiducia & GAD IT, DZ Bank), aber auch durch eigene Mitarbeitende sichergestellt.

Um des Weiteren den bankenübergreifenden Austausch (Netzwerkbildung) compliancerelevanter Themen sicherzustellen, erfolgt ein Austausch mit den Compliance-Beauftragten der übrigen Kirchenbanken. Zudem nimmt der Compliance-Beauftragte an den Arbeitsgruppen des Bundesverbandes der Compliance-Manager sowie an dem vom Genossenschaftsverband – Verband der Regionen koordinierten Gesamtbank Compliance-Praxis-Forum teil.





7. Compliance-Prozesse und Umsetzung

7.1 Spezifische Compliance-Risiken der Organisation

Um die aus der Geschäftstätigkeit der Bank für Kirche und Diakonie resultierenden Compliance-Risiken, die sich aus der Größe, Struktur sowie Geschäftsart und Regionen, in denen sie tätig ist, zu identifizieren, analysieren sowie entsprechend entgegenzuwirken, wurde entsprechend der Vorgaben der MaRisk eine Compliance-Funktion MaRisk benannt. Aufgabe der Compliance-Funktion MaRisk ist es, MaRisk-Compliance-Risiken zu identifizieren und darauf hinzuwirken, dass die einschlägigen Vorgaben und Regelungen zeitnah in den Prozessen und Verfahren der Bank berücksichtigt werden.

7.2 Anwendbare Compliance-Anforderungen

Die unter Ziffer 7.1 aufgeführte erforderliche Organisation wurde in einer Compliance-MaRisk-Richtlinie zusammengefasst. Im Einzelnen enthält die Compliance-MaRisk-Richtlinie Vorgaben zur regelmäßigen Identifizierung wesentlicher rechtlicher Regelungen. Des Weiteren wurden Verantwortlichkeiten für einzelne Rechtsbereiche festgelegt. Alle relevanten Rechtsthemen werden in einem eigenen Rechtskataster geführt. Neben den für einzelne Rechtsbereiche verantwortlichen Mitarbeitenden überwacht der Compliance-Beauftragte MaRisk permanent, ob Handlungsbedarf aus rechtlichen Neuerungen und/oder Veränderungen resultieren. Der Compliance-Beauftragte MaRisk führt zu Dokumentationszwecken eine Matrix über die einzelnen Umsetzungsmaßnahmen sowie erledigten Teilschritte.

Die Bankenaufsichtsrechtsrunde, an der auch der Compliance-Beauftragte MaRisk teilnimmt, überwacht in Form eines Spezialisten-Arbeitskreises zusätzlich die Erfordernis zur Umsetzung rechtlicher Änderungen. Die Bankenaufsichtsrechtsrunde übernimmt eine regelmäßige Protokollierung der von ihr behandelten Rechtsthemen. Des Weiteren ist der Compliance-Beauftragte MaRisk in der Regel Mitglied der im Einzelfall hausintern zu bildenden Arbeitskreise.

Vorstand und Aufsichtsrat werden per Compliance-MaRisk-Jahresbericht über den Umsetzungsstand einzelner zu behandelnder Rechtsthemen informiert. Des Weiteren besteht die Möglichkeit und Pflicht, den Vorstand und Aufsichtsrat anlassbezogen per adhoc-Bericht zu informieren, sofern die Umsetzung einzelner Aufgaben u. a. nicht termingerecht erfolgt oder sich Tendenzen zeigen, die eine ordnungs- und fristgemäße Umsetzung in Frage stellen.

7.3 Entscheidung über die angemessenen Maßnahmen zur Erfüllung der Compliance-Anforderungen

Der Vorstand hat die Geschäftsorganisation der Bank so geregelt, dass in jedem organisatorischen Einzelfall entsprechende Maßnahmen getroffen werden, die eine Erfüllung der Compliance-Anforderungen in den jeweiligen Prozessen sicherstellt.

7.4 Integration der Compliance-Anforderungen in die Arbeitsabläufe

Alle Arbeitsabläufe sind so gestaltet, dass die Erfüllung der Compliance-Anforderungen erleichtert und ermöglicht wird. Der Compliance-Beauftragte MaRisk ist neben dem für den jeweiligen Fachbereich zuständigen Vorstandsmitglied sowie der Risikocontrolling-Funktion in das Freigabeverfahren für die nach MaRisk relevanten Organisationsanweisungen eingebunden. Im Bedarfsfall kann, sofern Compliance-Anforderungen nicht umfassend berücksichtigt wurden, eine entsprechende Anpassung eingeleitet werden.

7.5 Umgang mit compliance-relevanten Interessenskonflikten

Rechtmäßiges Handeln, Sorgfalt, Redlichkeit, Professionalität, die Einhaltung von Marktstandards sowie das Handeln im Kundeninteresse sind Verpflichtungen, von denen die Bank für Kirche und Diakonie sich in der Geschäftsbeziehung leiten lässt. Bei der Vielfalt der geschäftlichen Aktivitäten unseres Hauses können jedoch Interessenkonflikte auftreten.

Interessenkonflikte können beispielsweise bei der Erbringung von Dienstleistungen wie dem An- und Verkauf bzw. der Vermittlung von Finanzinstrumenten, der Anlageberatung, eigenen Geschäften der Bank in Finanzinstrumenten, dem Depotgeschäft, der Finanzierung von Finanzinstrumenten, Devisengeschäften im Zusammenhang mit Geschäften in Finanzinstrumenten sowie der Weitergabe von Finanzanalysen Dritter an Kunden auftreten.

Dabei können Interessenkonflikte insbesondere durch das Zusammentreffen von mehreren Kundenaufträgen, das Zusammentreffen von Kundenaufträgen mit eigenen Geschäften oder sonstigen eigenen Interessen der Bank, oder durch das Zusammentreffen von Kundenaufträgen mit Geschäften der Mitarbeitenden der Bank entstehen.

Um zu vermeiden, dass sich Interessenkonflikte zum Nachteil von Kunden auswirken können, wurden vielfältige organisatorische und arbeitsrechtliche Vorkehrungen getroffen. Wesentliche Vorkehrungen sind die Schaffung von Vertraulichkeitsbereichen, die Trennung von Verantwortlichkeiten sowie die Verpflichtung der Mitarbeitenden der Bank zur Einhaltung von Verhaltensregeln bei Geschäften mit Kunden, für die Bank oder privaten Geschäfte der Mitarbeitenden.

Die Einhaltung sämtlicher vorstehender Verpflichtungen wird von unabhängigen Stellen in unserem Haus laufend kontrolliert und regelmäßig durch die interne und externe Revision geprüft. Sämtliche Depotinhaber erhalten im Zuge einer Depoteröffnung nachweislich eine Information und eine weitergehende Information über den Umgang mit Interessenkonflikten.

7.6 System von Freigaben, Genehmigungen und Berechtigungen

Um Verstöße gegen Compliance-Anforderungen auszuschließen unterliegen alle wesentlichen Arbeitsschritte einem strengen 4-Augen-Prinzip. Dieses erstreckt sich insbesondere auch auf das Freigabe- und Genehmigungsverfahren der zur Verfügung gestellten technischen Kompetenzen. Der Bereich Organisation prüft nachweislich regelmäßig anhand eines Auswertungstools, ob die zur Verfügung gestellten Kompetenzen im Einklang mit den über Arbeitsanweisungen, Stellenbeschreibungen sowie sonstigen Organisationsunterlagen vorstandsseitig festgelegten Prozessen und Kompetenzen im Einklang stehen. Sollte sich aufgrund der Kontrollen Handlungsbedarf ergeben, wird dieser unverzüglich eingeleitet, um mögliche Compliance-Risiken auszuschließen.

7.7 Hinweisgebersystem

Mit Hilfe unseres Hinweisgebersystems besteht die Möglichkeit, das Mitteilen von Missständen oder Unregelmäßigkeiten im Unternehmen intern zu kommunizieren, um somit Schaden zu Lasten von Kunden oder gegenüber dem Unternehmen abzuwenden. Somit stellt das Hinweisgebersystem der Bank für Kirche und Diakonie eine wichtige Präventionsmaßnahme für unser Unternehmen dar. Vorteile des elektronischen Hinweisgebersystems sind, dass der Hinweisgeber anonym Hinweise einliefern kann, da sowohl die Hinweise, als auch Nachrichten verschlüsselt gespeichert werden. Zudem können die Hinweise zeitunabhängig erfolgen und es besteht die Möglichkeit von Rückfragen mittels integrierten Postfachs.

7.8 Anti-Korruptionsrichtlinie

Die in Kraft gesetzte Anti-Korruptionsrichtlinie dokumentiert die Einstellung der Bank für Kirche und Diakonie zur Praxis des Annehmens und Gebens von Geschenken sowie sonstigen Vorteilen und Einladungen im Rahmen der beruflichen Tätigkeit für die Bank basierend auf der Informationsbroschüre zur Korruptionsprävention für Banken und Wirtschaftsunternehmen des LKA der Polizei Nordrhein-Westfalen, dem Corporate Governance Kodex für Genossenschaften, dem die Bank seit 2015 entspricht, weiteren internen Regelungen, sowie dem UN Global Compact, welcher beim Nachhaltigkeitsfilter eine wesentliche Rolle spielt.

Sie dient u.a. der operativen Umsetzung der Regelung, dass „Vorstandsmitglieder und Mitarbeitende im Zusammenhang mit ihrer Tätigkeit weder für sich noch für andere Personen von Dritten Zuwendungen oder sonstige Vorteile fordern oder annehmen oder Dritten ungerechtfertigte Vorteile gewähren dürfen". Der gute Ruf, die Glaubwürdigkeit und die ethischen Grundsätze sind dabei von besonderer Wichtigkeit. Die Organe und Mitarbeitenden der Bank haben sich zur Vermeidung und Aufdeckung aller Verstöße gegen diese Werte verpflichtet und verfolgen hinsichtlich dieser Verstöße eine Null-Toleranz-Politik.

7.9 Beratung, Unterstützung

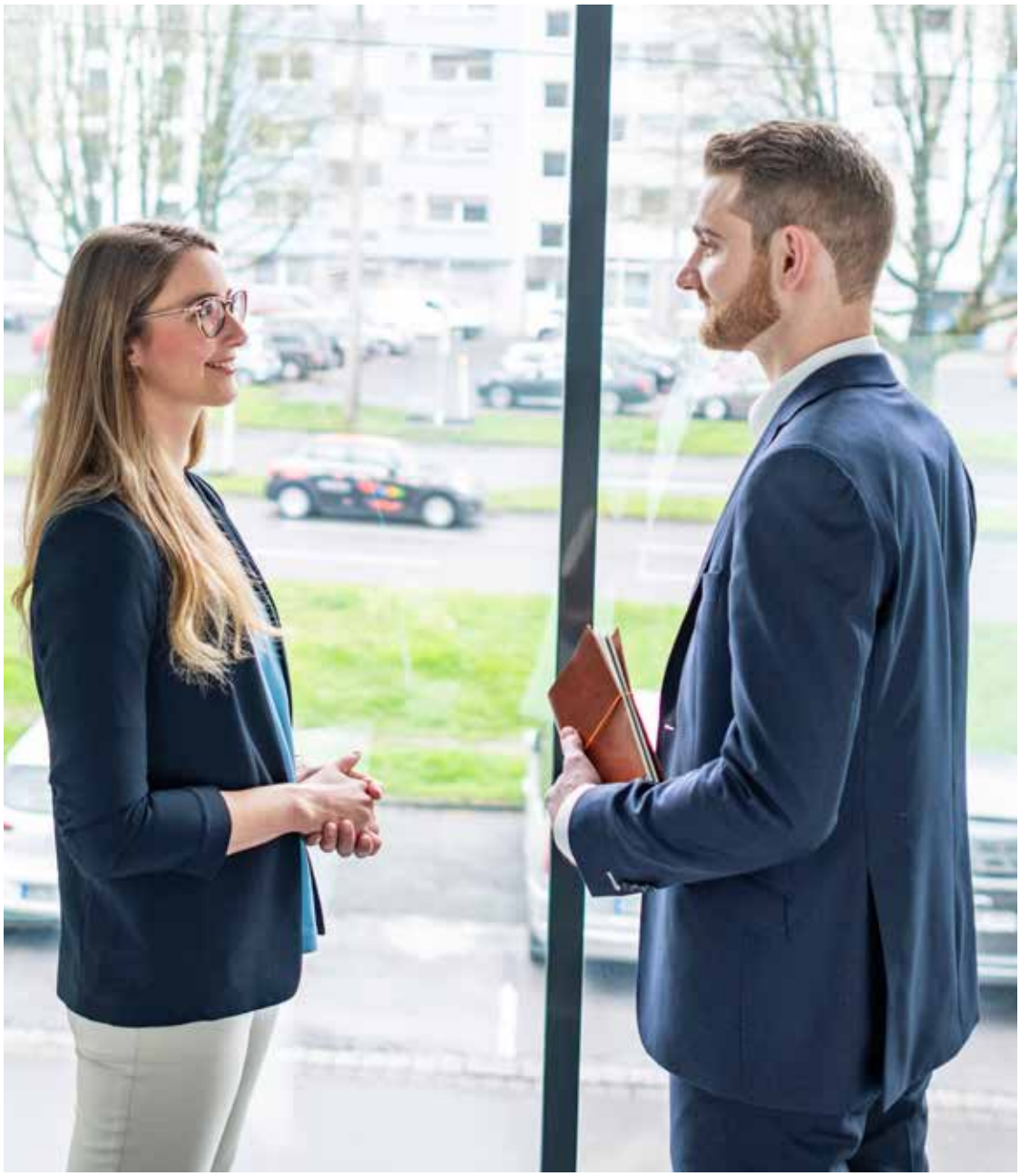
Der Compliance-Beauftragte MaRisk sowie alle mit der Compliance-Organisation beauftragten Mitarbeitenden (u. a. Geldwäsche-, Datenschutz-, und Compliance WpHG-Beauftragte, Fachkraft für Arbeitssicherheit) stehen jederzeit für die Klärung und Beantwortung compliance-relevanter Fragen sowie für den Umgang mit möglichen Interessenkonflikten zur Verfügung.

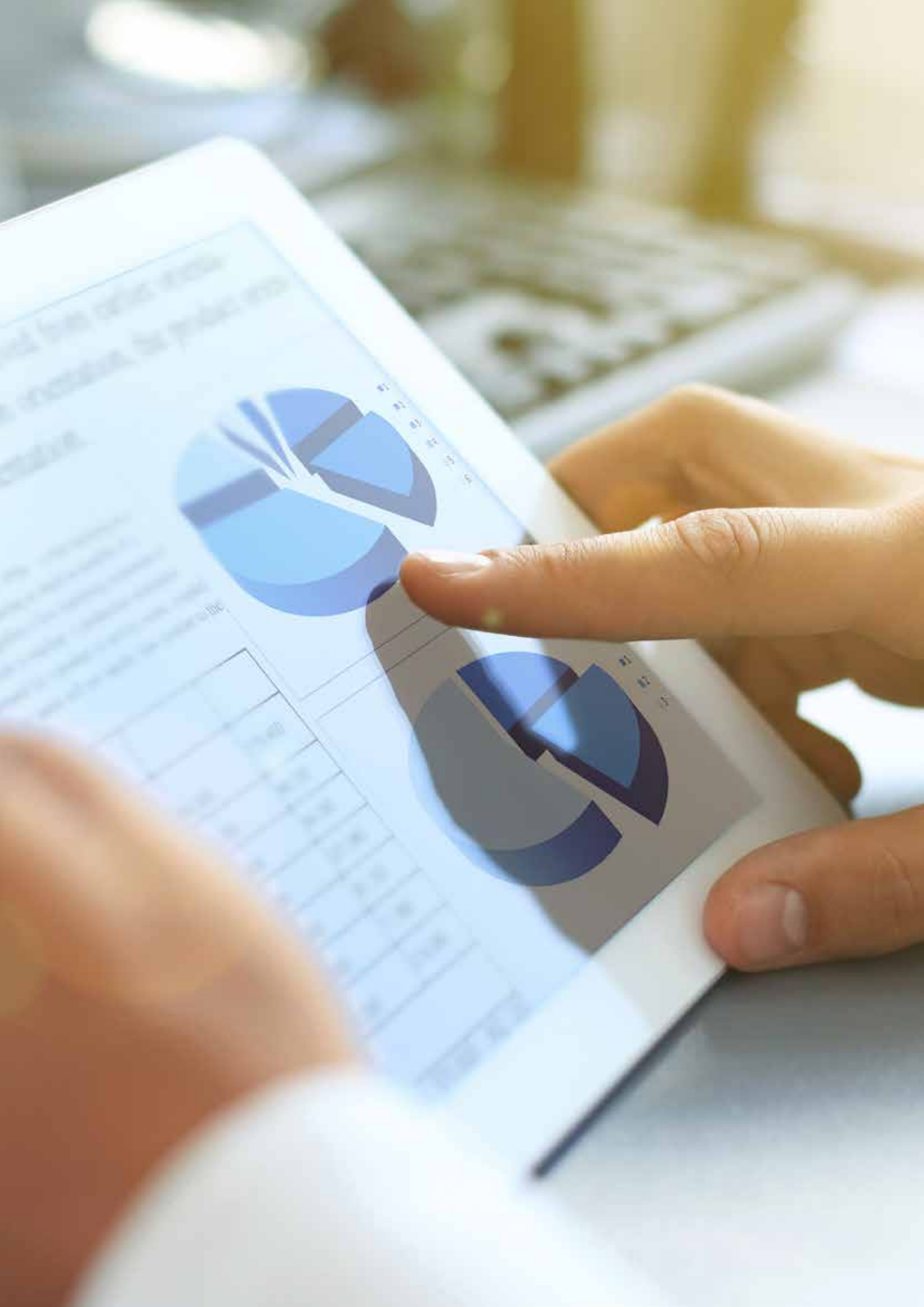
7.10 Umgang mit compliance-relevanten Vorgängen

Der Vorstand der Bank für Kirche und Diakonie hat ein über Organisationsanweisungen und Stellenbeschreibungen geregeltes Verfahren für den Umgang sowie die Zuständigkeiten und Berichtswege mit compliance-relevanten Vorgängen festgelegt. Einbezogen wurden hierbei auch die Belange für Berichts-, Melde-, Informations- und Warnpflichten u. a. gegenüber Behörden, Kapitalmarkt und Kunden. Alle Compliance-Vorgänge sowie deren Behandlung und Lösung werden revisionssicher dokumentiert und archiviert.

7.11 Externe Dienstleister

Externe Dienstleister und Auslagerungsunternehmen, die im Auftrag unseres Hauses in die Erfüllung compliance-relevanter Anforderungen eingebunden sind, wie zum Beispiel für die Bereiche Geldwäsche, Datenschutz und Arbeitssicherheit sowie Compliance WpHG, haben dieselben Compliance-Anforderungen zu beachten, die für die Bank für Kirche und Diakonie gelten. Die mit den Dienstleistern geschlossenen Verträge sind entsprechend ausgestaltet.





8. Systemüberwachung, -analyse und -verbesserung

Um die Wirksamkeit des Compliance-Management-Systems sicherzustellen hat der Vorstand der Bank für Kirche und Diakonie geeignete Überwachungs-, Analyse-, und Verbesserungsprozesse eingeführt.

8.1 Interne Audits

Um die Wirksamkeit des Compliance-Management-Systems zu überprüfen und sicherzustellen werden in regelmäßigen Abständen interne Audits durchgeführt. Insbesondere soll festgestellt werden, ob die Compliance-Anforderungen und die in der Teilstrategie, dem CMS Handbuch sowie sonstigen Organisationsunterlagen beschriebenen Anforderungen wirksam umgesetzt und erfüllt sowie aufrechterhalten werden.

Die Zuständigkeit für die Planung und Durchführung, die Erstellung von Aufzeichnungen sowie Fertigung eines Ergebnisberichts liegt beim Compliance-Beauftragten MaRisk. Dabei entscheidet der Compliance-Beauftragte MaRisk über die Auditkriterien, den Auditumfang, die Audithäufigkeit sowie die Auditmethoden. Sofern nicht dem Compliance-Bereich zugehörende Mitarbeitende in die Umsetzung der Audits eingebunden werden, ist die Objektivität und Unparteilichkeit des Auditprozesses sicherzustellen. Auditoren dürfen ihre eigene Tätigkeit nicht auditieren.

Die Audits werden planmäßig einmal jährlich umgesetzt. Die einzelnen Audits werden anhand der vom Compliance-Beauftragten MaRisk vorbereiteten Checklisten geführt. Um einen reibungslosen Ablauf der einzelnen Audits sicherzustellen werden mit den in den Auditprozess eingebundenen Mitarbeitenden rechtzeitig terminliche Abstimmungen getroffen.

Die Ergebnisse der Audits werden dem für den Compliance-Bereich zuständigen Vorstandsmitglied zur Kenntnisnahme sowie im Bedarfsfall, falls hierzu weitere Maßnahmen zu treffen sind, zur Beschlussfassung vorgelegt. Die/der für den auditierten Bereich verantwortliche Bereichsleitende hat sicherzustellen, dass jegliche notwendige Korrekturen und Korrekturmaßnahmen ohne ungerechtfertigte Verzögerung zur Behebung von anerkannten Abweichungen und ihren Ursachen ergriffen werden. Folgemaßnahmen müssen die Verifizierung der ergriffenen Maßnahmen und die Berichterstattung über die Verifizierungsergebnisse enthalten. Sämtliche aus den einzelnen Audits resultierende Unterlagen sind für einen Zeitraum von 10 Jahren aufzubewahren. Hierbei besteht auch die Möglichkeit der elektronischen Archivierung mit gleichen Fristen.

8.2 Überwachung

Der Vorstand der Bank hat verschiedene Methoden zur Überwachung des Compliance-Management-Systems festgelegt. Hierzu zählen beispielsweise die Selbstkontrollen der Marktbereiche, die Kontrollen der Mitarbeitenden der Wertpapierfolge, die von der Innenrevision sowie der externen Revision vorzunehmenden Prüfungshandlungen sowie die vom Compliance-Beauftragten MaRisk umzusetzenden Audits. Im Zuge des geregelten Auslagerungsmanagements unterliegen auch die ausgelagerten Prozesse einer permanenten Qualitätskontrolle durch die jeweils zuständigen Auslagerungsverantwortlichen sowie dem zentralen Auslagerungsbeauftragten. Sofern anwendbar, werden Kennzahlen zur Messung der Ermittlung der Wirksamkeit der zugrundeliegenden Prozesse zur Erfüllung der generellen aber auch Compliance-Anforderungen verwendet.

In der Teilstrategie Compliance-Management-System ist unter Ziffer 5. und 6. aufgeführt, wie im Fall eines Compliance-Verstoßes zu verfahren ist. Die Koordination von Compliance-Vorfällen wird von einem Lenkungskreis „Compliance“ vorgenommen. Nach Abschluss der eingeleiteten Recherchen werden dem Vorstand die für die diesbezüglich zu treffende Entscheidung alle erforderlichen Eckdaten mit einer vorbereiteten Handlungsempfehlung zur Verfügung gestellt. Sofern im Einzelfall Korrekturmaßnahmen eingeleitet werden, ist der Umsetzungsstatus der Maßnahmen durch den vom Vorstand im Einzelfall bestimmten Mitarbeitenden in Zusammenwirken mit dem Compliance-Beauftragten MaRisk und der Innenrevision nachzuhalten.

8.3 Verbesserung

8.3.1 Ständige Verbesserung

Die Bank für Kirche und Diakonie bedarf zur Erfüllung ihrer vielfältigen Aufgaben einem Höchstmaß an Qualität und Effizienz. Um die Leistungs- und Wettbewerbsfähigkeit zu steigern, ist eine permanente Prozessoptimierung erforderlich. Ein Schlüssel hierzu ist die Einbindung aller Mitarbeitenden unseres Hauses. Vor diesem Hintergrund wurde das Ideenmanagement auf Basis einer mit dem Betriebsrat vereinbarten Betriebsvereinbarung eingeführt. Aufgabe aller Bereichsleitungen der unterschiedlichen Organisationseinheiten ist es, das Ideenmanagement zu fördern, die Vorschlagsberechtigten zu beraten und zu Verbesserungsvorschlägen ausdrücklich zu motivieren.

8.3.2 Korrekturmaßnahmen

In der Teilstrategie Compliance-Management-System ist aufgeführt, welche Konsequenzen bei der Nichteinhaltung von Compliance-Regelungen und somit im Falle eines möglichen Compliance-Verstoßes einzuleiten sind. Hierzu zählen insbesondere die Bewertung der Verstöße, die Ermittlung der Ursachen,

die Beurteilung des Handlungsbedarfs, die Ermittlung und Verwirklichung der erforderlichen Maßnahmen sowie die Dokumentation der Ergebnisse und Maßnahmen. Die für die Vorstandsentscheidung erforderlichen Eckdaten werden vom Lenkungskreis „Compliance“ aufbereitet und mit Vorschlägen sowie einem Votum versehen.

Sofern aus dem Compliance-Verstoß Anpassungsbedarf bestehender Organisationsunterlagen resultiert und/oder neue Arbeitsablaufbeschreibungen einzuführen sind, wird der Compliance-Beauftragte MaRisk in den hierfür erforderlichen Prozess eingebunden.

8.3.3 Vorbeugungsmaßnahmen

Der Vorstand der Bank für Kirche und Diakonie hat die Organisation des Geschäftsbetriebs insgesamt so ausgerichtet, um mögliche Verstöße gegen Compliance-Anforderungen zu verhindern. Hierzu zählen u. a. folgende Maßnahmen:

- Risikoidentifikation (durch: Bestandsaufnahme der Ist-Situation; Erfassung von Kunden-, Produkt- und transaktionsbezogenen Risiken; Risikobewertung und Festlegung einer Risikoobergrenze)
- Berichterstattungen
- Regelungen Datenschutz
- Regelungen zur Arbeitssicherheit
- Interne Kontrollen
- Verhaltensrichtlinien
- Schulungsmaßnahmen
- Kommunikation und Beratung
- Hinweisgebersystem
- Anti-Korruptionsrichtlinie
- Interne und externe Revisionsprüfungen