MaRisk-Rechtsmonitoring

Sonderausgabe

Stand 03. November 2017

GenoTec GmbH | beraten optimieren schützen

GenoTec GmbH

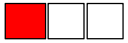
MaRisk-Rechtsmonitoring

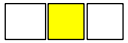
Das MaRisk-Rechtsmonitoring berücksichtigt alle rechtlich-regulatorische Anforderungen, die wesentliche Änderungen aus MaRisk-Compliance-Gesichtspunkten haben können. Die Regelungen, das heißt mögliche Handlungen sind Anhaltspunkte in Abhängigkeit zum institutsspezifischen Geschäftsmodell, der Geschäftsstrategie, den implementierten Prozessen, Verfahren und Grundsätzen. Sie erheben keinen Anspruch auf Vollständigkeit.

Hinweis

Das MaRisk-Rechtsmonitoring ist in absteigender chronologischer Reihenfolge dargestellt. Die im jeweiligen Monat neu hinzugefügten Regelungen werden zu Beginn aufgeführt und sind blau gekennzeichnet. Besonders hervorzuhebende Inhalte werden **orange** dargestellt. Verlinkungen sind durch Unterstreichungen gekennzeichnet. Geänderte Inhalte werden ebenfalls blau gekennzeichnet. Bei einem Verweis auf eine ältere Lfd. Nr. wird der Inhalt nochmals in der neuen Lfd. Nr. in einer separaten Spalte aufgeführt.


nicht Terminrelevant


Umsetzung sofort bis max. 3 Monate


Umsetzung in 3 – 6 Monaten


Umsetzung in > 6 Monaten

Für Rückfragen und auch Anregungen stehen wir Ihnen gerne jederzeit zur Verfügung!

Michael Maier
Wirtschaftsjurist LL.M.
Beauftragter MaRisk-Compliance
Tel.: 069 6978-3147
E-Mail: michael.maier@geno-tec.de

Peter Uherr
Bankbetriebswirt Management
Leiter MaRisk-Compliance
Tel.: 069 6978-3055
E-Mail: peter.uherr@geno-tec.de

Abkürzungsverzeichnis

ABB	Allgemeine Bedingungen für Bausparverträge
Az.	Aktenzeichen
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMF	Bundesfinanzministerium
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMWi	Bundesministerium für Wirtschaft und Energie
BVR	Bundesverband der Volks- und Raiffeisenbanken
BWGV	Baden-Württembergischer Genossenschaftsverband e.V.
DK	Deutsche Kreditwirtschaft
DRV	Deutscher Raiffeisenverband e.V.
e.V.	eingetragener Verein
EU	Europäische Union
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GV	Genossenschaftsverband – Verband der Regionen e.V.
GVB	Genossenschaftsverband Bayern e.V.
GVWE	Genossenschaftsverband Weser-Ems e.V.
GwG	Geldwäschegesetz
i.H.v.	in Höhe von
i.S.d.	im Sinne des
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
KAGB	Kapitalanlagegesetzbuch
KWG	Gesetz über das Kreditwesen
Lfd. – Nr.	Laufende Nummer
LG	Landgericht
MaRisk	Mindestanforderungen an das Risikomanagement
MaSI	Mindestanforderungen an die Sicherheit von Internet-zahlungen
OLG	Oberlandesgericht
PRIIP	Packaged Retail and Insurance-based Investment Products
RS	Rundschreiben
RWGV	Rheinisch-Westfälischer Genossenschaftsverband e.V.
Sog.	So genannte
VSBG	Verbraucherstreitbeilegungsgesetz
VVI	Vorvertragliche Informationen

Quelle/ Herausgeber	Inhalt und möglicher Handlungsbedarf	Ihre Anmerkungen
BaFin Anschreiben Erläuterungen zu den MaRisk Endfassung im Überarbeitungs-modus	Nach zahlreichen intensiven Diskussionen mit Praxis- und Verbandsvertretern hat die BaFin nunmehr die **finale Fassung** der seit Februar 2016 in Konsultation befindlichen MaRisk veröffentlicht. Durch diesen engen Austausch haben sich gegenüber der Konsultation einige Änderungen ergeben. Ziel der Änderungen waren dabei insbesondere die Berücksichtigung der berechtigten Interessen auch kleinerer Institute sowie die stärkere Herausstellung der Zielrichtung der Aufsicht. Die Überarbeitung der MaRisk war primär aufgrund zahlreicher Änderungen im Aufsichtsrecht notwendig geworden. So wurden beispielsweise die „Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung“ (BCBS 239) in die MaRisk eingearbeitet. Ebenfalls wurden Erfahrungen aus der Aufsichtspraxis aufgenommen, die überwiegend in den Regelungen zu den Auslagerungen Einzug erhalten haben. Die MaRisk-Novelle ist **mit Veröffentlichung in Kraft** getreten. Es ergeben sich jedoch folgende **Übergangsfristen**: · Änderungen, die lediglich klarstellender Natur sind, müssen **unmittelbar** von den Instituten umgesetzt werden · neue Anforderungen (die nicht lediglich eine Klarstellung vorhandener Regelungen sind) müssen bis zum **31.10.2018** umgesetzt werden · für Institute, die die Anforderungen des AT 4.3.4 (Datenmanagement, Datenqualität und Aggregation von Risikodaten) erfüllen müssen, wird eine Umsetzungsfrist von **drei Jahren** gewährt. Diese gilt grundsätzlich ab dem Zeitpunkt der Einstufung als systemrelevantes Institut. Global systemrelevante Institute haben diese Regelungen jedoch bereits seit Januar 2016 zu erfüllen und können sich folglich nicht auf die Übergangsfrist berufen. Die Einstufung als „neue Anforderung“ oder „klarstellend“ ist dabei zum Teil sehr fließend. Es ist davon auszugehen, dass die Verbände hierzu sehr zeitnah eine Unterstützungsleistung anbieten werden. Nachfolgend soll auf die wesentlichsten Änderungen und Aspekte in den neuen MaRisk eingegangen werden:	

Quelle/ Herausgeber	Inhalt und möglicher Handlungsbedarf	Ihre Anmerkungen
	1) AT 4.3.4 Risikodatenaggregation Die Vorschriften zur Risikodatenaggregation richten sich ausschließlich an global und anderweitig **systemrelevante Institute**. Inhalte des Baseler Papiers BCBS 239 werden in die Aufsichtspraxis aufgenommen und in einem neuen Modul AT 4.3.4 gebündelt. Intention ist es, die IT-Infrastruktur der systemrelevanten Institute zu verbessern, sodass eine umfassende, genaue und zeitnahe Aggregation der Risikopositionen des Instituts ermöglicht wird und dem Berichtswesen der Bank zur Verfügung steht. Institute, die nicht in der Lage sind, Informationen zu Gesamtexposures gegenüber bestimmter Adressen und in bestimmten Produkten innerhalb eines kurzen Zeitraums zu generieren, können nicht schnell genug auf kritische Entwicklungen reagieren. Um jedoch in Krisensituationen auf fundierte Daten zurückgreifen zu können und zur Überlebensfähigkeit der Institute beizutragen, wurden die Regelungen zum Datenmanagement, Datenqualität und Aggregation von Risikodaten eingeführt. Dabei hat das Institut insbesondere zu gewährleisten, dass **Risikodaten genau und vollständig** sind. Weiter müssen die Daten nach **unterschiedlichen Kategorien auswertbar** sein und sollten (sofern möglich und sinnvoll) automatisch aggregiert werden können. Falls manuelle Prozesse und Eingriffe erforderlich sind, sind diese zu dokumentieren, zu begründen sowie auf das notwendige Maß zu beschränken. **Datenqualität und –vollständigkeit** sind vom Institut anhand geeigneter Kriterien zu überwachen. Aggregierte Risikodaten sind mit anderen vorhandenen Informationen abzugleichen und zu **plausibilisieren**. Entsprechende Prozesse und Verfahren zum Abgleich der Risikodaten sind einzurichten, um Datenfehler und Schwachstellen in der Datenqualität identifiziert werden können. Die Datenaggregationskapazitäten müssen so ausgestaltet sein, dass auch in Stressphasen die aggregierten Risikodaten zeitnah zur Verfügung stehen. Für alle Prozessschritte müssen Verantwortlichkeiten festgelegt werden und entsprechende prozessabhängige Kontrollen eingerichtet werden. Die Einhaltung der institutsinternen Regelungen, Verfahren und Methoden ist von einer von den geschäftsinitiierenden bzw. geschäftsabschließenden Organisationseinheiten unabhängigen Stelle zu überprüfen. ð **Handlungsempfehlung:** Das Modul AT 4.3.4 richtet sich zwar ausschließlich an global und anderweitig systemrelevante Institute, die BaFin empfiehlt jedoch auch den übrigen Instituten, im Eigeninteresse zu prüfen, ob hinsichtlich der Risikodatenaggregationskapazitäten Optimierungsbedarf besteht. Dies stellt jedoch lediglich eine Empfehlung dar und hat keinen verpflichtenden Charakter für nicht systemrelevante Banken	

Quelle/ Herausgeber	Inhalt und möglicher Handlungsbedarf	Ihre Anmerkungen
	2) BT 3 Risikoberichterstattung Gemäß Anschreiben der BaFin können die Institute, die nicht systemrelevant sind, auch weiterhin die Ausgestaltung ihrer Risikoberichterstattung nach ihren individuellen Bedürfnissen zuschneiden, sofern dadurch die aussagekräftige und **nachvollziehbare Berichterstattung** nicht negativ beeinträchtigt wird. Wichtig ist der BaFin insbesondere eine inhaltlich aussagekräftige Aufbereitung der Informationen auf der Grundlage eines ausgewogenen Verhältnisses zwischen **quantitativen und qualitativen Informationen**. Die Geschäftsleitung muss sich auf der Grundlage **vollständiger, genauer und aktueller Daten** über die Risikosituation in regelmäßigen Abständen berichten lassen. Die Risikoberichte müssen ebenfalls eine zukunftsorientierte Risikoeinschätzung enthalten und dürfen sich nicht ausschließlich auf historische und aktuelle Daten stützen. Ebenfalls sind die Ergebnisse der Stresstests und deren potenzielle Auswirkungen auf die Risikosituation und das Risikodeckungspotenzial sowie die zugrunde liegenden wesentlichen Annahmen darzustellen. Das Institut muss in der Lage sein, neben der turnusmäßigen Erstellung von Risikoberichten auch ad hoc Risikoinformationen zu generieren, sofern die aktuelle Marktsituation eine ad hoc Generierung erforderlich macht. Die Risikoberichte müssen in einem **zeitlich angemessenen Rahmen erstellt** werden, sodass eine aktive und zeitnahe Steuerung der Risiken ermöglicht wird. Die Geschäftsleitung muss das Aufsichtsorgan mindestens vierteljährlich schriftlich über die Risikosituation informieren. Dabei hat sie auf besondere Risiken für die Geschäftsentwicklung und geplante Maßnahmen zur Begrenzung der Risiken gesondert einzugehen. Wesentliche Informationen hinsichtlich der Risikosituation sind dem Aufsichtsorgan, sofern für dieses erforderlich, unverzüglich durch die Geschäftsleitung weiterzuleiten. Um eine unverzügliche Weiterleitung zu gewährleisten, sind von der Geschäftsleitung und dem Aufsichtsorgan geeignete Verfahren festzulegen. ð **Handlungsempfehlung**: Prüfung und Ergänzung der bisherigen Vorschriften, sowie Anpassung der relevanten Prozesse und Organisationsdokumente	

Quelle/ Herausgeber	Inhalt und möglicher Handlungsbedarf	Ihre Anmerkungen
	3) AT 3 Risikokultur & AT 5 Verhaltenskodex Im Rahmen ihrer Gesamtverantwortung für eine ordnungsgemäße Geschäftsführung haben gemäß AT 3 Tz. 1 Geschäftsleiter zukünftig eine **angemessene Risikokultur** zu entwickeln, zu integrieren und zu fördern. Herkunft dieser Anforderung ist der Erwägungsgrund 54 der Bankenrichtlinie CRD IV. Als Bestandteil eines wirkungsvollen Risikomanagements betont diese Regelung, dass es neben dem Vorhandensein angemessener Kontroll- und Überwachungshandlungen auch auf den Umgang und das operative Verhalten der Mitarbeiter ankommt. Das Bekenntnis der Geschäftsleitung zu einem klar definierten und eindeutig kommunizierten Risikoappetits soll die Umsetzung dieses Vorhabens gewährleisten. Dazu sind gem. AT 5 Tz. 3 in Abhängigkeit von Größe des Instituts, der Art, Umfang, der Komplexität sowie dem Risikogehalt der Geschäftsaktivitäten die Organisationsrichtlinien um einen **Verhaltenskodex für Mitarbeiter** zu erweitern. Nach Ansicht der BaFin erscheint ein Verhaltenskodex in kleineren Instituten mit weniger komplexen Aktivitäten verzichtbar, da die persönliche Ansprache der Mitarbeiter durch die Führungskräfte das effektivere Instrument sein können, um die Mitarbeiter auf die gemeinsamen Ziele und Werte einzuschwören. Die BaFin kündigt unterdessen an, dass sich die Aufsicht im Laufe der Zeit ein Bild über die gelebte Risikokultur der Institute machen wird und ggf. Nachholbedarf adressieren wird. Sie appelliert daher dazu, die Anforderungen an die Risikokultur als wesentliches Werkzeug für ein angemessenes Risikomanagement anzusehen und entsprechend zu nutzen. ð **Handlungsempfehlung:** Integration einer angemessenen Risikokultur, Prüfung der Notwendigkeit eines Verhaltenskodizes sowie ggf. Implementierung eines entsprechenden Verhaltenskodizes	

Quelle/ Herausgeber	Inhalt und möglicher Handlungsbedarf	Ihre Anmerkungen
	4) AT 9 Auslagerungen In der Neufassung des AT 9 hat die Aufsicht insbesondere ihre Sichtweise zu den Grenzen der Auslagerbarkeit deutlicher herausgearbeitet und neu definiert. Die Institute haben daher zukünftig die mit einer Auslagerung verbundenen Risiken (noch) effektiver zu managen, um einen möglichen Kontrollverlust zu verhindern. Zukünftig ist der Ausschluss durch eine zivilrechtliche Gestaltung und Vereinbarung nicht mehr von vornherein möglich. Geklärt wurde überdies, wie der **Bezug von Software** zu bewerten ist. Demnach handelt es sich beim isolierten Bezug der Software in der Regel um einen sonstigen Fremdbezug. Dies gilt ebenfalls für die Anpassung der Software an die Erfordernisse des Instituts, entwicklungstechnische Umsetzung von Änderungswünschen, Fehlerbehebungen, Wartung etc. Dies gilt jedoch ausdrücklich nicht für Software, die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt wird oder für die für die Durchführung bankgeschäftlicher Aufgaben von wesentlicher Bedeutung ist. In diesen Fällen sind Unterstützungsleistungen als Auslagerung einzustufen. Weiterhin gilt der Betrieb der Software durch einen externen Dritten als Auslagerung. Die regelmäßige Beurteilung der Auslagerungen hat nach institutsweiten bzw. gruppenweiten Rahmenvorgaben stattzufinden. Die Risikoanalyse hat dabei neben den wesentlichen Risiken der Auslagerung auch Risikokonzentrationen und Risiken aus der Weiterverlagerung zu berücksichtigen. Die Auslagerung von Aktivitäten und Prozessen in den Kontrollbereichen und Kernbankenbereichen ist nur in einem Umfang möglich, der gewährleistet, dass das Institut auch weiterhin über Kenntnisse und Erfahrungen verfügt, die eine wirksame Überwachung der vom Auslagerungsunternehmen erbrachten Dienstleistung ermöglichen. Es ist sicherzustellen, dass bei Bedarf, wie z.B. Beendigung der Auslagerung, der ordnungsmäßige Betrieb fortgesetzt werden kann. Erstmals wird die **Auslagerbarkeit der Compliance-Funktion** unter Berücksichtigung von Institutsgröße, Art, Umfang, Komplexität sowie dem Risikogehalt der betriebenen Geschäftsaktivitäten **ausdrücklich erlaubt**. Lediglich bei großen Instituten mit komplexen Geschäftsmodellen wird die Auslagerung auf Teilauslagerungen begrenzt. Für alle wesentlichen Auslagerungen sind Ausstiegsprozesse festzulegen, sodass eine ausreichende Qualität und Kontinuität aufrechterhalten bzw. zeitnah wiederhergestellt werden kann. Innerhalb von Gruppen oder einem Verbund kann auf die Erstellung eines Ausstiegsprozesses verzichtet werden. Bestehen keine Handlungsoptionen, ist eine angemessene Berücksichtigung in der Notfallplanung zu gewährleisten. Weiterhin werden die bei wesentlichen Auslagerungen zu vereinbarenden Inhalte um die Verpflichtung des Auslagerungsunternehmens zur Information des Instituts über Entwicklungen, die die Erledigung der ausgelagerten Aktivitäten und Prozesse beeinträchtigen können, ergänzt. Ebenfalls muss bereits mit Vertragsanbahnung intern festgelegt werden, welchen Grad einer Schlechtleistung seitens des Instituts akzeptiert werden kann. Überdies ist hinsichtlich von Weiterverlagerungen zu vereinbaren, dass ein Zustimmungsvorbehalt des auslagernden Instituts erforderlich sind. Alternativ können konkrete Voraussetzungen für eine Weiterverlagerung vereinbart werden. Für die Steuerung und Überwachung wesentlicher Auslagerungen muss das Institut klare Verantwortlichkeiten festlegen. Sofern besondere Funktionen, wie z.B. Compliance oder die Interne Revision vollständig ausgelagert wurden, hat die Geschäftsleitung einen Beauftragten zu benennen, der die ordnungsgemäße Erbringung der ausgelagerten Dienstleistungen gewährleisten muss. Zu den Hauptänderungen im Bereich der Auslagerungen gehört die Pflicht, in Abhängigkeit von Art, Umfang und Komplexität der Auslagerungsaktivitäten ein zentrales **Auslagerungsmanagement** zu installieren. Zu dessen Aufgaben zählen insbesondere die Überwachung und Weiterentwicklung eines angemessenen Auslagerungsmanagements inklusive Kontroll- und	

Quelle/ Herausgeber	Inhalt und möglicher Handlungsbedarf	Ihre Anmerkungen
	Überwachungsprozessen, Erstellung und Pflege einer vollständigen Dokumentation der Auslagerungen inklusive aller Weiterverlagerungen sowie die Unterstützung der Fachbereiche bei den Anforderungen an Auslagerungen sowie der durchzuführenden Risikoanalyse. Weiter hat das Auslagerungsmanagement mindestens jährlich einen Bericht über wesentliche Auslagerungen an die Geschäftsleitung zu erstellen. In diesem Bericht ist darauf einzugehen, ob von den Auslagerungsunternehmen die vertraglichen Vereinbarungen eingehalten werden, die ausgelagerten Prozesse und Aktivitäten angemessen gesteuert und überwacht werden können und, ob ggf. risikomindernde Maßnahmen ergriffen werden müssen. Insbesondere bei größeren Instituten bzw. Instituten mit zahlreichen Auslagerungen wird ein zentrales Auslagerungsmanagement von der BaFin als erforderlich angesehen. ð **Handlungsempfehlung:** Anpassung der Organisationsdokumente, Berücksichtigung der Vertragsinhalte bei Vereinbarung von Auslagerungen, Prüfung der Notwendigkeit eines zentralen Auslagerungsmanagements und ggf. Installation desselben, Prüfung der Notwendigkeit eines Beauftragten aufgrund der Auslagerung von Compliance und/oder Interne Revision und ggf. Bestellung desselben, Überprüfung der Auslagerungen hinsichtlich der Einstufungen Darüber hinaus ergeben sich insbesondere nachfolgende Änderungen: · **AT 4.1 Risikotragfähigkeit** Bei der Implementierung eines Prozesses zur Sicherstellung der **Risikotragfähigkeit** sind zukünftig auch das Ziel der **Fortführung** des Instituts sowie der **Gläubigerschutz** (vor Verlusten) angemessen zu berücksichtigen. Die Methoden und Verfahren zur Beurteilung der Risikotragfähigkeit können vom Institut selbst gewählt werden. Die zugrunde liegenden **Annahmen** müssen jedoch **nachvollziehbar begründet** werden. Die Geschäftsleitung hat dabei die Festlegung wesentlicher Elemente der Risikotragfähigkeitssteuerung sowie wesentliche zugrunde liegende Annahmen zu genehmigen. Dabei muss das Institut jederzeit einen vollständigen und aktuellen Überblick über die verwendeten Methoden und Verfahren zur Risikoquantifizierung haben. Die Verwendung externer Daten zur Risikodeckungspotenzial- und Risikoermittlung sowie zur Aggregation von Risikodaten ist nur unter bestimmten Voraussetzungen möglich. So dürfen beispielsweise keine Parameter einfließen, die unreflektiert aus anderen Quellen übernommen wurden. Dies gilt jedoch nicht für die inhaltliche Überprüfung der Richtigkeit von öffentlich zugänglichen Marktinformationen. Werden bei der Risiko- oder Risikodeckungspotenzialermittlung auf externe Daten beruhende Annahmen getroffen, muss das Institut plausibel darlegen, dass die zugrunde liegenden Daten die tatsächlichen Verhältnisse im Institut angemessen widerspiegeln. Wird bei der Risikoermittlung auf Berechnungen Dritter zurückgegriffen, muss sich das Institut aussagekräftige Informationen zu wesentlichen Annahmen und Parametern vorlegen lassen. Sofern eine Validierung dieser Komponenten erforderlich ist, muss eine angemessene Unabhängigkeit zwischen Methodenentwicklung und Validierung gewährleistet sein. ð **Handlungsempfehlung:** Implementierung der Fortführung und Gläubigerschutz, Festlegung von Annahmen und den	

Quelle/ Herausgeber	Inhalt und möglicher Handlungsbedarf	Ihre Anmerkungen
	dazugehörigen Begründungen, Installation eines Prozesses zur Verwendung und Plausibilisierung externer Daten · **AT 4.3.1 Aufbau- und Ablauforganisation** Wechseln Mitarbeiter der Handels- und Marktbereiche in nachgelagerte Bereiche und Kontrollbereiche, sind zukünftig zur Vermeidung der Selbstprüfung angemessene **Übergangsfristen** vorzusehen. Als nachgelagerte Bereiche und Kontrollbereiche werden dabei die Risikocontrolling-Funktion, die Compliance-Funktion, die Marktfolge sowie die Abwicklungs- und Kontrollfunktion angesehen. Für kleinere und weniger komplexe Institute ergeben sich dahingehend Erleichterungen, als dass alternative angemessene Kontrollmechanismen eingerichtet werden können, sofern eine Übergangsfrist zu unverhältnismäßigen Verzögerungen im Betriebsablauf führen würde. Darüber hinaus sind zukünftig Berechtigungen und Kompetenzen sparsam zu vergeben (**Need-to-know-Prinzip**) und gegebenenfalls zeitnah anzupassen. Zeichnungsberechtigungen in Verbindung mit Zahlungsverkehrskonten und wesentliche IT-Berechtigungen sind mindestens jährlich zu prüfen. Alle anderen Kompetenzen und Berechtigungen mindestens alle drei Jahre. Bei kritischen IT-Berechtigungen (z.B. bei Administratoren) ist eine mindestens halbjährliche Prüfung zu initiieren. ð **Handlungsempfehlung:** Berücksichtigung der Übergangsfristen (in Organisationsdokumenten), Anpassung der Prozesse zur Überprüfung der Kompetenzen und Berechtigungen sowie Berücksichtigung des Need-to-know-Prinzips · **AT 4.4.2 Compliance** Grundsätzlich ist die Compliance-Funktion unmittelbar der Geschäftsleitung zu unterstellen und dieser auch berichtspflichtig. Auch weiterhin kann eine Anbindung an andere Kontrolleinheiten stattfinden. Dies jedoch zukünftig unter der Einschränkung, dass eine direkte Berichtslinie zur Geschäftsleitung existieren muss. Weiterhin ist zukünftig in Abhängigkeit von der Größe des Instituts sowie der Art, des Umfangs, der Komplexität und dem Risikogehalt der Geschäftsaktivitäten die Compliance-Funktion in einem von den Bereichen Markt und Handel unabhängigen Bereich anzusiedeln. Systemrelevante Institute haben für die Compliance-Funktion eine eigenständige Organisationseinheit einzurichten. Sofern ein **Wechsel des Compliance-Beauftragten** stattfindet, ist das **Aufsichtsorgan zukünftig rechtzeitig vorab unter Angabe der Wechselgründe zu informieren** (analoge Anwendung der Vorschriften der Internen Revision). ð **Handlungsempfehlung:** Berücksichtigung der Vorschriften, Überprüfung und ggf. Anpassung des Organigramms, Änderung der Organisationsdokumente sowie Information des Aufsichtsorgans vorab bei Wechsel des Compliance-Beauftragten	

Quelle/ Herausgeber	Inhalt und möglicher Handlungsbedarf	Ihre Anmerkungen
	· **AT 4.5 Risikomanagement auf Gruppenebene** Die Vorschriften zur Implementierung angemessener ablauforganisatorischer Vorkehrungen auf Gruppenebene werden um eine **zeitnahe Berichtspflicht an die Geschäftsleiter** des übergeordneten Unternehmens ergänzt. Das übergeordnete Unternehmen hat in die regelmäßigen und anlassbezogenen Stresstests auch das **Gesamtrisikoprofil auf Gruppenebene** durchzuführen. Innerhalb einer Gruppe sind die **Revisionsgrundsätze und Prüfungsstandards zu vereinheitlichen**. Darüber hinaus müssen Prüfungsplanungen und die Überwachung der festgestellten Mängel aufeinander abgestimmt werden. Dabei hat die Konzernrevision in angemessenen Abständen (zumindest jedoch vierteljährlich) an die Geschäftsleitung und das Aufsichtsorgan des übergeordneten Unternehmens über die Tätigkeiten auf Gruppenebene zu berichten. ð **Handlungsempfehlung:** Überprüfung und ggf. Anpassung der Revisionsgrundsätze und Prüfungsstandards · **AT 7.2 Technisch-organisatorische Ausstattung** Insbesondere zur Feststellung des Schutzbedarfes, die Ableitung von Sicherheitsanforderungen sowie zur Festlegung entsprechender Sicherheitsmaßnahmen sind für IT-Risiken auch eigenentwickelter Anwendungen **angemessene Risikosteuerungs- und –überwachungsprozesse** einzurichten. Beim Bezug von Software sind die damit verbundenen Risiken ebenfalls angemessen zu bewerten. ð **Handlungsempfehlung:** Nutzung von Standardanwendungen und Prozessen so weit wie möglich, Sicherstellung entsprechender Verfahren und Methoden für den Fall des Einsatzes eigenentwickelter Anwendungen, ebenfalls ist zeitnah mit einer finalen Veröffentlichung der BAIT zu rechnen, die voraussichtlich eine weitere Konkretisierung mit sich bringen wird · **AT 8.1 Neu-Produkt-Prozess** Es ist seitens des Instituts ein **Katalog** derjenigen Produkte und Märkte vorzuhalten, die Gegenstand der Geschäftsaktivitäten sein sollen. Es muss in einem **angemessenen Turnus überprüft** werden, ob Produkte noch verwendet werden. Sofern Produkte über einen längeren Zeitraum nicht mehr Gegenstand der Geschäftsaktivität waren, sind diese zu kennzeichnen. Vor Wiederaufnahme der gekennzeichneten Produkte müssen die in die Arbeitsabläufe eingebundenen Organisationseinheiten den Fortbestand der beim letztmaligen Geschäftsabschluss vorherrschenden Geschäftsprozesse bestätigen. Bei Veränderungen muss geprüft werden, ob ein **neuer Neu-Produkt-Prozess durchlaufen** werden muss. ð **Handlungsempfehlung:** Anpassung der Organisationsdokumente und Erstellung eines Katalogs über Produkte und Märkte	

Quelle/ Herausgeber	Inhalt und möglicher Handlungsbedarf	Ihre Anmerkungen
	ð **BTO 1.2 Prozesse im Kreditgeschäft** Bei der Festlegung der Bearbeitungsgrundsätze für die Prozesse im Kreditgeschäft sind zukünftig auch die vom Institut akzeptierten Sicherheitenarten sowie Verfahren zur Wertermittlung, Verwaltung und Verwertung der Sicherheiten festzulegen. Bei der Festlegung der Verfahren zur **Wertermittlung** der Sicherheiten muss auf geeignete Wertermittlungsverfahren zurückgegriffen werden. Bei Objekt-/Projektfinanzierungen sind in unter Risikogesichtspunkten festzulegenden Abständen **Besichtigungen und Bautenstandskontrollen** während der Entwicklungsphase des Projekts/Objekts durchzuführen. Bei der Beurteilung der Kapitaldienstfähigkeit im Rahmen von Immobiliar-Verbraucherdarlehen sind auch zukünftige, als wahrscheinlich anzusehende, **Einkommensschwankungen** zu berücksichtigen. Die für die Kreditgewährung relevanten Informationen müssen vollständig dokumentiert werden und sind über die Laufzeit des Kredites aufzubewahren. Zur Bewertung der Werthaltigkeit einer Sicherheit ist in Abhängigkeit von der Sicherheitenart ab einem unter Risikogesichtspunkten festzulegenden Wert eine Objektbesichtigung durchzuführen. Zur Überprüfung der Werthaltigkeit von Immobiliensicherheiten ist der alleinige Einsatz von Marktschwankungskonzepten nicht geeignet. Entsprechend muss das Institut ab einer unter Risikogesichtspunkten festzulegenden Grenze eigenverantwortlich beobachten und Risiken für die Werthaltigkeit der Sicherheit identifizieren und steuern. Bei der Bewertung zur Überführung eines Kredits in die Intensivbetreuung bzw. Sanierung oder Abwicklung sind auch Zugeständnisse zugunsten des Kreditnehmers zu berücksichtigen (Forbearance). ð **Handlungsempfehlung:** Berücksichtigung der Vorschriften, Anpassung der Organisationsdokumente, Überprüfung der Kreditrisikogrundsätze, Anpassung der Prozesse zur Kreditweiterberarbeitung · **BTR Anforderungen an die Risikosteuerungs- und -controllingprozesse** Auch hinsichtlich der Anforderungen an die Risikosteuerungs- und -controllingprozesse wurden zahlreiche Änderungen vorgenommen. So müssen beispielsweise die Erkenntnisse aus der Erlösquotensammlung bei der Steuerung der Adressenausfallrisiken zukünftig angemessen berücksichtigt werden. Bezüglich der Liquiditätsrisiken ist auf eine ausreichende Diversifikation der Refinanzierungsquellen und der **Liquiditätspuffer** zu achten. Konzentrationen müssen ausreichend überwacht und begrenzt werden. Für die Bemessung des Liquiditätspuffers ist darauf zu achten, dass sowohl in normalen Marktphasen als auch in vorab definierten Stressszenarien ein auftretender Liquiditätsbedarf vollständig durch den Liquiditätspuffer überbrückt werden kann. Die Verfahren zur Steuerung und Beurteilung der Liquiditätsrisiken haben ebenfalls zu gewährleisten, dass Höhe, Art, Umfang und Entwicklung der Belastung von Vermögenswerten (Asset Encumbrance) zeitnah identifiziert und an die Geschäftsleitung berichtet werden können. Ebenfalls muss jedes Institut einen internen Refinanzierungsplan aufstellen, der Strategien, Risikoappetit und das Geschäftsmodell angemessen widerspiegelt und in der Regel einen mehrjährigen Bemessungszeitraum umfasst. Überdies hat die BaFin festgelegt, wie mit nicht eindeutig zuordenbaren **Schadensfällen** und Beinaheverlusten im Bereich der operationellen Risiken umzugehen ist. Jedes Institut hat eine einheitliche Festlegung und Abgrenzung der **operationellen Risiken** vorzunehmen und an die Mitarbeiter zu kommunizieren.	

Quelle/ Herausgeber	Inhalt und möglicher Handlungsbedarf	Ihre Anmerkungen
	Für größere Institute besteht die Pflicht zur Einrichtung einer Ereignisdatenbank für Schadensfälle, in welche sämtliche Schadensereignisse oberhalb eines angemessenen Schwellenwertes erfasst werden. ð **Handlungsempfehlung:** Überprüfung der Verfahrensgrundsätze und ggf. Anpassung vorbereiten	

Alle Angaben ohne Gewähr