IT Finanzmagazin
Das Fachmagazin für IT und Organisation bei Banken, Sparkassen und Versicherungen

STRATEGIE

3. Februar 2026

Entwurf der 9. MaRisk-Novelle: Schluss mit Checkbox-Compliance – jetzt zählt die prüfbare Begründungskette

Die MaRisk soll lesbarer werden und sich wieder stärker an Proportionalität und Prinzipien orientieren, kündigte die BaFin noch 2025 an. Weniger komplex sollen die überarbeiteten und voraussichtlich im Laufe des Jahres veröffentlichten Vorschriften zudem ausfallen. Ferner plant die Aufsicht, Inhalte aus der CRD VI, DORA und verschiedenen EBA-Leitlinien entweder zu integrieren oder klarer voneinander abzugrenzen. Worauf sich die Institute einstellen müssen.

von Thomas Maul, Senior Manager und Mario H. Sladek, Berater – beide PPI

Quelle: ChatGPT

Zwar liegt noch kein fertiger Entwurf für die 9. Novelle der MaRisk vor. Aus öffentlich zugänglichen Äußerungen der Aufsicht, Ankündigungen auf Fachtagungen sowie mehreren Verbandsbeiträgen ergibt sich jedoch ein erstes Bild,

womit die Banken rechnen dürfen, wenn die Mindestanforderungen an das Risikomanagement novelliert werden. Im Vordergrund stehen Orientierung an Prinzipien und Proportionalität. Das bedeutet für die Banken:

Mehr Gestaltungsspielräume: Die MaRisk legen die Ziele und Grundsätze fest, doch die Institute entscheiden selbst, wie sie diese umsetzen. Als maßgeblich gilt, dass die Banken erklären können, warum sie sich für welche Maßnahmen entschieden haben und dass die Aufsicht dies als angemessen anerkennt.

Mehr Öffnungsklauseln: Die MaRisk wird künftig stärker berücksichtigen, wie groß und wie komplex ein Institut ist, wodurch kleinere Institute weniger strenge Auflagen bekommen werden („doppelte Proportionalität“). Dies bedeutet keinesfalls einen Freifahrtschein, vielmehr muss die Angemessenheit sorgfältig begründet werden.

Thomas Maul, Senior Manager, PPI Quelle: PPI

Wesentlichkeit und Klarheit: Institute müssen noch so kleine Risiken nicht bis ins kleinste Detail regeln. Es soll reichen, auf die wesentlichen Risiken zu fokussieren und darauf zu achten, dass sich kumulierte Risiken nicht zu einem wesentlichen Risiko formen.

Die Aufsicht stellt sich mit diesen selbst gegebenen Zielen dem Trend entgegen, wonach seit der Finanzkrise 2008/2009 auch durch die zahlreichen internationalen Vereinbarungen immer detaillierter vorgegeben wurde, wie die Institute ihre Risiken zu managen haben. Künftig will die Aufsicht den Instituten wieder mehr Ermessensspielräume geben und damit auch mehr Verantwortung, was beispielsweise die Aufbauorganisation, Abläufe und Dokumentationen angeht. Das wird sich auch auf die Prüfungspraxis auswirken.

Neue alte Aufsichtsphilosophie

In der Branche gilt die 9. Novelle der MaRisk bereits als eine der bedeutendsten Umbauten des Regelwerks, seit es vor zwanzig Jahren eingeführt wurde. Neben schlankeren Vorgaben, die es geben soll, ist konkret geplant, auch bestehende Dopplungen zwischen MaRisk, EBA-Leitlinien und EZB-Erwartungen abzubauen. Hinzu kommen europäische Regelwerke, die weitgehend in die MaRisk integriert werden sollen, um regulatorische Vorgaben möglichst konzentriert und widerspruchsfrei zu bündeln. Dies betrifft insbesondere:

Mario H. Sladek, Berater, PPI Quelle: PPI

1. **ESG-Vorgaben:** Die Branche erwartet, dass die 9. MaRisk-Novelle einzelne ESG-Anforderungen präzisiert und überschneidungsfreie Schnittstellen schafft, um ESG-Reportings zu erstellen und offenzulegen sowie vereinheitliche Anforderungen zu Prozessen und Dokumentationspflichten formuliert. Grund dafür sind die teils sehr hohen Aufwände, die sich aus der 7. Novelle ergeben haben, was ESG-Risiken quer über Kredit-, Marktpreis-, Liquiditäts- und OpRisk-Bereiche angeht. Teilweise gab es auch Überschneidungen zum BaFin-Merkblatt und EBA-Richtlinien.
2. **IRRBB und CSRBB:** Seit der 8. MaRisk-Novelle bestehen offene Auslegungsfragen hinsichtlich bestimmter CSRBB-Vorgaben, welche dafür sorgen sollen, dass Banken durch Markt-, Kredit- und Liquiditätsspreads verursachte Risiken im Anlagebuch in bestehende Risikomess- und Steuerungssysteme integrieren. Mit der 9. Novelle hofft die Branche auf eine Feinjustierung, welche Detailfragen klarer fasst und bestehende Schnittstellen zu Risikotragfähigkeit, Stresstests und Berichterstattung harmonisiert.
3. **DORA:** In den Bereichen Auslagerung und operationelles Risikomanagement kommt es zu notwendigen Anpassungen, weil stärker unterschieden wird zwischen MaRisk-Anforderungen und DORA-Vorgaben. Die Aufsicht will verhindern, dass sie mit der 9. MaRisk-Novelle DORA einfach nachbaut. DORA soll deshalb vorrangig die IKT-Risiken, IKT-Drittparteien und digitale Resilienz regeln. In den MaRisk werden dafür die Überschneidungen reduziert und Verweisbezüge auf DORA klarer formuliert. Die

MaRisk bleibt folglich für Nicht-IKT-Themen, etwa bei sonstigen Auslagerungen, klassischen operationellen Risiken und ESG-Risiken, der zentrale nationale Rahmen, welcher gegebenenfalls um europäische Leitlinien ergänzt wird.

MaRisk und DORA

In der Praxis werden die Institute hinsichtlich DORA und MaRisk zwei wesentliche Stränge sauber voneinander trennen müssen: IKT-Drittparteien, welche künftig ausschließlich unter die DORA-Logik fallen, und sonstige Dienstleister, welche sie mit der MaRisk-/EBA-Logik steuern. Insbesondere AT 7.3 (Notfallmanagement) und AT 9 (Auslagerungen) sollen noch viel deutlicher als bisher abgrenzen, was DORA voll abdeckt und wofür weiterhin die MaRisk maßgeblich bleiben. Im Auslagerungsmanagement nach AT 9 bedeutet dies, dass durch die MaRisk nur noch übergreifende Governance- und Proportionalitätsprinzipien gesetzt werden, während DORA die konkreten Anforderungen für IKT-Auslagerungen ausdifferenziert.

Dies bedeutet, dass DORA neben der operationellen Resilienz auch die Meldepflichten für IKT-Vorfälle sowie Resilienztests eigenständig abdeckt und bei IT-Notfällen durch AT 7.3 MaRisk dafür gesorgt wird, dass möglicherweise widersprüchlich gefasste Regelungen auf nationaler Ebene aufgelöst werden. Kurzgefasst: Die MaRisk verweisen künftig stärker auf die Notwendigkeit, DORA-konforme Abläufe einzuführen, bleibt dabei aber auf Prinzipien- und Governance-Ebene. Andere EU-Regelungen, wie CRD VI oder EBA-Leitlinien, werden im Text ebenfalls aufgegriffen oder referenziert, um Widersprüche zu EU-Recht möglichst zu vermeiden oder auszuschließen.

Schon jetzt können sich die Institute auf die 9. MaRisk-Novelle vorbereiten, indem sie:

Autor Thomas Maul, Senior Manager PPI

Thomas Maul ist seit 2018 als Senior Manager bei PPI (Website (https://www.ppi-group.eu/de/)) tätig. Davor war er jahrelang unter anderem Leiter Treasury & Markets bei der Landesbank Sachsen und der LBBW. Er betreut vor allem die ökonomische Gesamtbanksteuerung (ICAAP/ILAAP), deren Governance-Aspekte sowie das ESG-Risikomanagement.

- Sämtliche IKT-Themen entlang der DORA organisieren, vom Risikomanagement über Incident-Management bis hin zu IKT-Drittparteien, und dies nachweisen können
- Qualitative und quantitative Risikobewertungen nachvollziehbar dokumentieren, um belegen zu können, dass alle Vorgaben eingehalten werden
- Sich auf Prüfungen vorbereiten, die insbesondere die Methoden betreffen, nach denen die genannten Risikobewertungen in Risikotragfähigkeitskonzepte (ICAAP) einfließen

MaRisk und Proportionalität

Logischerweise betreffen die vorgenannten Punkte Institute unterschiedlicher Größe auch unterschiedlich stark. Dies gilt umso mehr, weil die Aufsicht darauf drängen wird, dass die Banken ihre Risikoannahmen stärker plausibilisieren müssen, anstatt sich auf einen formal sehr eng gefassten Rahmen zu verlassen. Dafür sorgen neue Klassifizierungen und neue Öffnungsklauseln, auf die sich kleinere Institute berufen können. Hier zeichnet sich also ein Shift weg von einem möglichst vollständig eingehaltenen Katalog von präzise gefassten Regeln hin zu einem widerspruchsfreien Katalog von Regeln, die sich die Institute selbst geben und die sich an der „neuen alten“ Aufsichtsphilosophie orientieren.

Autor Mario H. Sladek, Berater PPI

Mario H. Sladek ist Berater bei der PPI (Website (https://www.ppi-group.eu/de/)) im Bereich Consulting Banken und verantwortet dort unter anderem aufsichtsrechtliche Themen und Gesamtbanksteuerung. Davor studierte er Notenbankwesen und arbeitete viele Jahre bei einer international tätigen Investmentbank im Audit- und Risikomanagement.

Anpassungsbedarf entsteht jedoch in jedem Fall dort, wo sich die Anforderungen an die Governance, Compliance und Revision noch nicht an die neue Prinzipienlogik der BaFin angepasst haben. Auch die erweiterten Ermessensspielräume rücken in den Blick, sofern einzelne Institute davon Gebrauch machen möchten. Konkret geht es um:

1. **Klarere Definitionen:** Bei Governance und Compliance regelt die Aufsicht etwas eindeutiger, welche Aufgaben sie der Geschäftsleitung, Aufsichtsorganen und der

Compliance-Funktion innerhalb einer Bank zuschreibt. Auch hier soll es vermehrt darum gehen, wesentliche Rechtsvorschriften effektiv zu überwachen, anstatt eine bloße Formdokumentation zu gewährleisten.

2. **Revision und Controlling:** Wie bei Governance und Compliance verändert sich auch bei bestimmten BT-Teilen der Fokus, beispielsweise bei der Internen Revision. Zwar dürften sich die konkret ausformulierten Anforderungen ebenfalls verschlanken, aber die Anforderungen, welche etwa bei der risikoorientierten Prüfungsplanung, IKS-Bewertung oder nachvollziehbaren Kontrollen gelten, werden steigen.
3. **Risikotragfähigkeit und Stresstests:** Die neue MaRisk wird Klarstellungen bringen hinsichtlich des Risikodeckungspotenzials (RDP), etwa zur Fünfprozentschwelle im ökonomischen Risikotragfähigkeitskonzept. Kleinere Institute dürfen mit kleineren Entlastungen rechnen, weil inverse Stresstests wegfallen sollen und gleichzeitig standardisierte Verbundszenarien sowie konsistente Stresstestrahmenwerke stärker berücksichtigt werden sollen

Proportionalität:
Small Banking Box

Das Proportionalitätsprinzip entwickelt mit der bevorstehenden 9. Novelle der MaRisk zu einem zentralen Baustein des Aufsichtsregimes. Aktuell geht es vor allem um abgestufte Anforderungen an Governance, Risikocontrolling und Berichtspflichten nach dem Muster einer „Small Banking Box“-Logik. Gemeint sind Erleichterungen und Öffnungsklauseln, auf die sich Institute berufen dürfen, die keine systemrelevante Stellung einnehmen und vergleichsweise wenig komplexe Geschäftsmodelle betreiben.

MaRisk-Akutmaßnahmen

Unabhängig von der Größte sollten sich alle Institute bereits frühzeitig auf die 9. Novelle der MaRisk vorbereiten, indem sie:

- Eine Gap-Analyse erstellen und systematisch abgleichen mit dem für Anfang des Jahres erwarteten Konsultationsentwurfs für die MaRisk
- Aktiv an den Konsultationen teilnehmen und ihre praktischen Erfahrungen aus den jüngsten Novellen der MaRisk einbringen
- Eine Dokumentation erstellen, welche im Rahmen der Proportionalität sämtliche genutzten Erleichterungen nachvollziehbar und prüfungssicher aufführt
- Systematisch sämtliche neuen und geänderten Anforderungen im institutseigenen Rechtskataster erfassen

- Neben der Geschäftsführung auch alle betroffenen Fachbereiche einbinden, um die Umsetzung der MaRisk insbesondere mit Blick auf die stärkere Eigenverantwortung vorzubereiten

Vor allem der letzte Punkt kann nicht überbetont werden, weil sich die BaFin ausdrücklich vorbehält, gewährte Erleichterungen für kleinere Institute auf den Prüfstand zu stellen, sollte sich deren Risikolage im Durchschnitt erheblich verschlechtern. Proportionalität wird also zwar gewollt, darf jedoch keinesfalls wie ein Freibrief verstanden werden. Vielmehr geht die Verantwortung dafür, wie eine Bank auf angemessenem Niveau risikoadäquat gesteuert wird, zurück in die Hände der Institute. Gefordert ist deshalb, wo nötig, ein Know-how-Aufbau, um operativ von den Erleichterungen aus der bevorstehenden MaRisk-Novelle zu profitieren, ohne Gefahr zu laufen, den Aufsichtszweck zu unterlaufen.

Je nach Größe des eigenen Instituts werden sich geplanten Änderungen an der MaRisk unterschiedlich stark auswirken. Die neue Institutsklassifizierung unterscheidet zwischen sehr kleinen Instituten mit einer Bilanzsumme bis zu einer Mrd. Euro, kleineren Instituten mit einer Bilanzsumme zwischen einer und fünf Mrd. Euro (SNCI, Small and Non-Complex Institutions, vgl. Art. 4 Abs. 1 Nr. 145 CRR) und den übrigen national beaufsichtigten Häusern. Zur Orientierung: Etwa 950 der Institute in Deutschland oder rund drei Viertel der insgesamt in Deutschland zugelassenen Banken fallen unter die SNCI-Definition.

Handlungsfelder nach Institutsgrößen

Sehr kleine Institute bis einer Mrd. Euro Bilanzsumme profitieren besonders stark von der Proportionalität, wie sie mit der 9. MaRisk-Novelle kommt. Bereits im November 2024 hat die BaFin entsprechende Erleichterungen angekündigt. Jetzt sollen sie in die Verordnung einfließen. Wenn es darum geht, die neuen Vorgaben umzusetzen, müssen diese Banken mit einem vergleichsweise geringen oder moderaten Aufwand rechnen. Dieser entsteht vor allem dabei, nachvollziehbar zu begründen, weshalb die gewählten Vereinfachungen für das eigene Risikoprofil immer noch angemessen sind, also ob die regulatorischen Mindestnormen für ihr Ambitionsniveau ausreichen.

Die zentralen Handlungsfelder lauten:

- **Risikoinventur und Risikotragfähigkeit:** Konzentration auf wesentliche Risiken mit einem Schwellenwert von fünf Prozent des ökonomischen Risikodeckungspotenzials sowie Nutzung vereinfachter Verfahren, wie „Säule 1+“ barwertnahe Verfahren

Stresstests: Reduktion auf einen risikoartenübergreifenden Stresstest und je einen Test pro wesentlicher Risikoart. Einfache Sensitivitätsanalysen können ausreichend sein. Inverse Stresstests können qualitativ erfolgen oder gänzlich entfallen

Funktionenbündelung: Compliance- und Auslagerungsbeauftragte dürfen als gemeinsame Funktion kombiniert werden, sofern deren operative Tätigkeiten weiter unabhängig voneinander stattfinden können

Auslagerungsmanagement: Nutzung gruppen- oder verbundinterner Lösungen zur Bewertung von Dienstleistern

Dokumentation: Schlankere Berichterstattung und Prozessdokumentation. Keine separaten Berichte für Sanierungsindikatoren erforderlich

Kleine Institute (SNCI) mit einer Bilanzsumme zwischen einer und fünf Mrd. Euro erhalten ebenfalls deutliche Erleichterungen. Gegenüber sehr kleinen Banken steigt der Aufwand vor allem bei teils sehr differenzierten Nachweisen. Insgesamt dürfte der Aufwand immer noch moderat ausfallen und vor allem für eine Gap-Analyse anfallen, welche die heutige MaRisk-Implementation an die Proportionalitätslogik anpasst, idealerweise pro AT/BT-Modul. Dazu kommen anzupassende Dokumente sowie MaRisk-Handbücher, Prozessbeschreibungen und Richtlinien, um sie in die Proportionalitätsargumentation zu übernehmen. Anpassungen wird es auch bei den Risikoberichten geben, welche zwar gestrafft werden dürfen, jedoch dabei ihre Aussagekraft nicht verlieren. Schließlich werden Schulungen nötig, damit die von der Aufsicht gewünschte Prinzipienlogik auch innerhalb der Häuser gelebt wird.

Weitere Handlungsfelder lauten:

Risikomanagement: Wesentliche Risiken stehen künftig im Fokus, unwesentliche dürfen dagegen pauschal behandelt werden, sofern sie kumuliert kein wesentliches Risiko ergeben

Stresstests: Drei bis fünf Stresstests pro Jahr müssen die Institute einkalkulieren, inverse Stresstests dürfen auf qualitative Analysen beschränkt werden oder entfallen komplett, sofern das Stresstestprogramm eine angemessene Steuerung erlaubt

Modellvalidierung: Bei Verbundlösungen oder Branchenpools muss geprüft werden, ob und inwieweit sie sich mit dem eigenen Portfolio vergleichen lassen. Anders als bei selbst entwickelten Modellen fällt die Dokumentation deutlich schlanker aus

ESG-Integration: ESG-Risiken müssen systematisch und risikoorientiert in die Risikoinventur sowie -strategie aufgenommen werden, jedoch ohne übermäßigem Formalisierungsgrad

CRD VI/DORA-Umsetzung: MaRisk-Strukturen geben künftig den Referenzrahmen vor, während IT-Governance und Auslagerungsdokumentation an die Anforderungen der DORA anzupassen sind

Mittelgroße und große Institute mit einer Bilanzsumme von fünf Mrd. Euro oder mehr müssen sich auf größeren Aufwand einstellen. Bei ihnen liegt der Schwerpunkt darauf, von der detail- auf die prinzipienorientierte Steuerung umzustellen und neue Regelwerke zu integrieren. Dies zieht eine strategisch neu ausgerichtete Risikosteuerung nach sich sowie eine Governance und Risikokultur, welche die Gesamtverantwortung der Geschäftsleitung stärker als bisher in den Vordergrund rückt. Hinzu kommen Anpassungen bei CRD IV, DORA, ESG, IRRBB und CSRBB wie weiter vorne beschrieben. Darüber hinaus müssen Banken dieser Größe ihre Modelle auch unabhängig validieren sowie ein Modellinventar erstellen. DORA erfordert schließlich, dass Auslagerungsverträge und die Steuerung von Weiterverlagerungen angepasst werden müssen.

> **Besonderheit: Verbundinstitute**
>
> Zentrale fachliche und technische Verbundanbieter müssen sich weiterhin dem vollen MaRisk-Umfang unterwerfen, weil viele ihrer Mitgliedsinstitute die SNCI-Kriterien nicht erfüllen. Einzelne Verbundinstitute profitieren deshalb womöglich nur begrenzt von den in der kommenden MaRisk-Novelle vorgesehenen Erleichterungen, falls sie auf solcherlei standardisierte Verbundlösungen zurückgreifen wollen.

Weitere Handlungsfelder lauten:

Konzeptioneller Umbau: Chance Management wird erheblichen Aufwand nach sich ziehen, um die Steuerungslogiken innerhalb des Instituts von detaillierten Vorgaben auf die eigenverantwortliche Prinzipienorientierung umzustellen

Systemanpassungen: Bestehende IT-Systeme müssen um Datenfelder für ESG-Risiken ergänzt sowie DORA-Compliance und Auslagerungsmanagement ergänzt werden

Ressourcenaufbau: Fachkräfte und Schulungen werden nötig, um die eingesetzten Modelle zu validieren, ESG-Risikomanagement zu betreiben und DORA-Compliance zu gewährleisten

Dokumentation: Richtlinien, Handbücher und Arbeitsanweisungen (SfO) müssen in allen betroffenen Bereichen überarbeitet werden, auch mit besonderen Blick auf Angemessenheit und Begründungsfähigkeit der gewählten Ansätze

Vertragsmanagement: Je nach Größe und Komplexität des Instituts müssen bis zu mehrere hundert Auslagerungsverträge angepasst werden

Prüfungsvorbereitung: Externe Wirtschaftsprüfer kontrollieren und prüfen, ob die Vorgaben eingehalten werden, was eine nachweisbare Compliance unverzichtbar macht

Zusätzlicher Aufwand entsteht mit zunehmender Komplexität und einer möglicherweise internationalen Ausrichtung von großen Instituten. Einige Geschäftsaktivitäten erfordern darüber hinaus, dass die Bank einschlägige Veröffentlichungen des Baseler Ausschusses und des Financial Stability Boards im Blick behält.

Fazit

Die 9. MaRisk-Novelle markiert eine bedeutende Weiterentwicklung des Regelwerks mit Rückbesinnung auf dessen ursprüngliche Prinzipienorientierung. Während sehr kleine und kleine Institute von deutlichen Erleichterungen profitieren, steht mittelgroßen und großen Instituten ein umfassender konzeptioneller und operativer Umbau bevor. Die von der Aufsicht angekündigte Vereinfachung bedeutet jedoch keine Deregulierung, sondern eine Rückkehr zu dem bereits 2005 intendierten Ansatz: qualitativ hochwertige, risikoadäquate Steuerung auf Basis fundierter Eigenverantwortung statt formaler Regelerfüllung.

Thomas Maul und Mario H. Sladek, PPI/ aj ■

Sie finden diesen Artikel im Internet auf der Website:
https://itfm.link/239421

© 2026 IT Finanzmagazin - Das Fachmagazin für IT und Organisation bei Banken, Sparkassen und Versicherungen