BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
GLAUCHAU
UNIVERSITY OF COOPERATIVE EDUCATION

Severn
make change work

Neuentwurf der MaRisk

Im Spannungsfeld von Risikokultur und „RegulierungsGAU“ für mittelständische Banken

Norman Nehls

Dipl.-Betriebswirt | Partner

Severn Consultancy GmbH | Frankfurt am Main

Glauchau, 13. Juni 2016

_Agenda

_Ausgestaltung der 5. MaRisk Novelle als Rechtsverordnung würde Handlungsspielräume für Banken einschränken

Severn
make change work

_ **Internationale Umsetzungs- und Regulierungsstandards,** u. a. durch die European Banking Authority (EBA), erforderten eine erneute Überarbeitung der MaRisk:

- *Anforderungen des Basler Ausschuss zur Aggregation von Risikodaten und zur Risikoberichterstattung (BCBS 239)*
- *Internationale Diskussionen zur Unternehmens- und Risikokultur (durch* Financial Stability Board)
- *Veröffentlichung des "Single Resolution Mechanism – Anpassungsgesetzes" ("SRM-AnpG") durch das BFM im März 2015*

_ Mit dem ersten Entwurf der BaFin vom 18.02.2015 werden bereits **gravierende neue Anforderungen an interne Risikosteuerungs- und -controllingprozesse** deutlich.

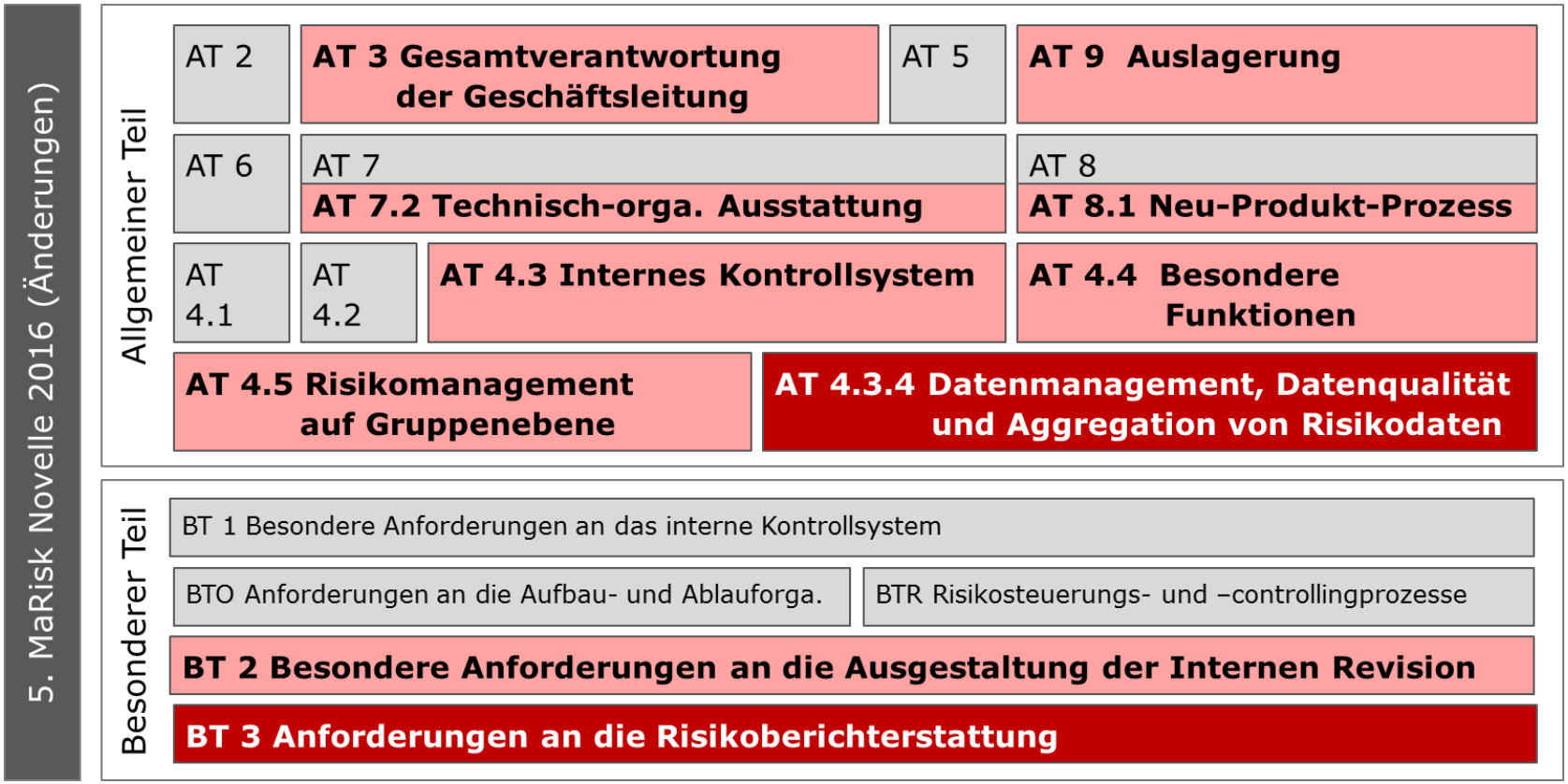
_ Im Zuge der Harmonisierung der Aufsichtspraxis wird gleichzeitig eine **Aufwertung der MaRisk** und Veröffentlichung als **Rechtsverordnung** diskutiert.

_ Dies würde für Banken eine **Einschränkung der bisherigen Prinzipienorientierung und Methodenfreiheit** bedeuten. Ferner sind mit einer erhöhten Rechtsverbindlichkeit **erweiterte Eingriffsrechte der Aufsicht** und Sanktionsmöglichkeiten verbunden.

_ Das Konsultationsverfahren wurde im April 2016 abgeschlossen. Anhand der Stellungnahmen der Verbände bleiben zahlreiche Fragen offen. Eine **zeitnahes in Kraft treten** wird allerdings erwartet.

MaRisk sollen Risikokultur stärken und bringen neue Vorgaben an Risikodatenaggregation und Risikoberichterstattung mit sich

- Erklärtes Ziel der Aufsicht ist die fortlaufende Verbesserung des internen Risikomanagements sowie die Etablierung einer **nachhaltigen Risikokultur** in Banken
- Die geplanten Neuregelungen lassen auf umfassenden Handlungsbedarf schließen

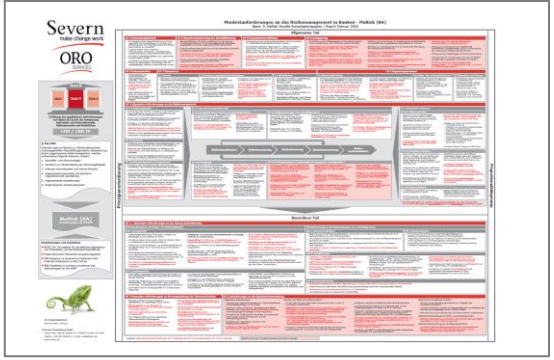


Geplante **Änderungen / Neureglungen in Modulen** gemäß Konsultationspapier der MaRisk vom 18.02.2016

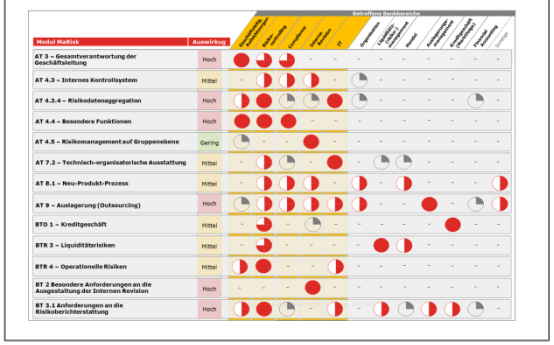
_Zahlreiche Bankbereiche sind von den erwarteten Änderungen der 5. MaRisk Novelle betroffen

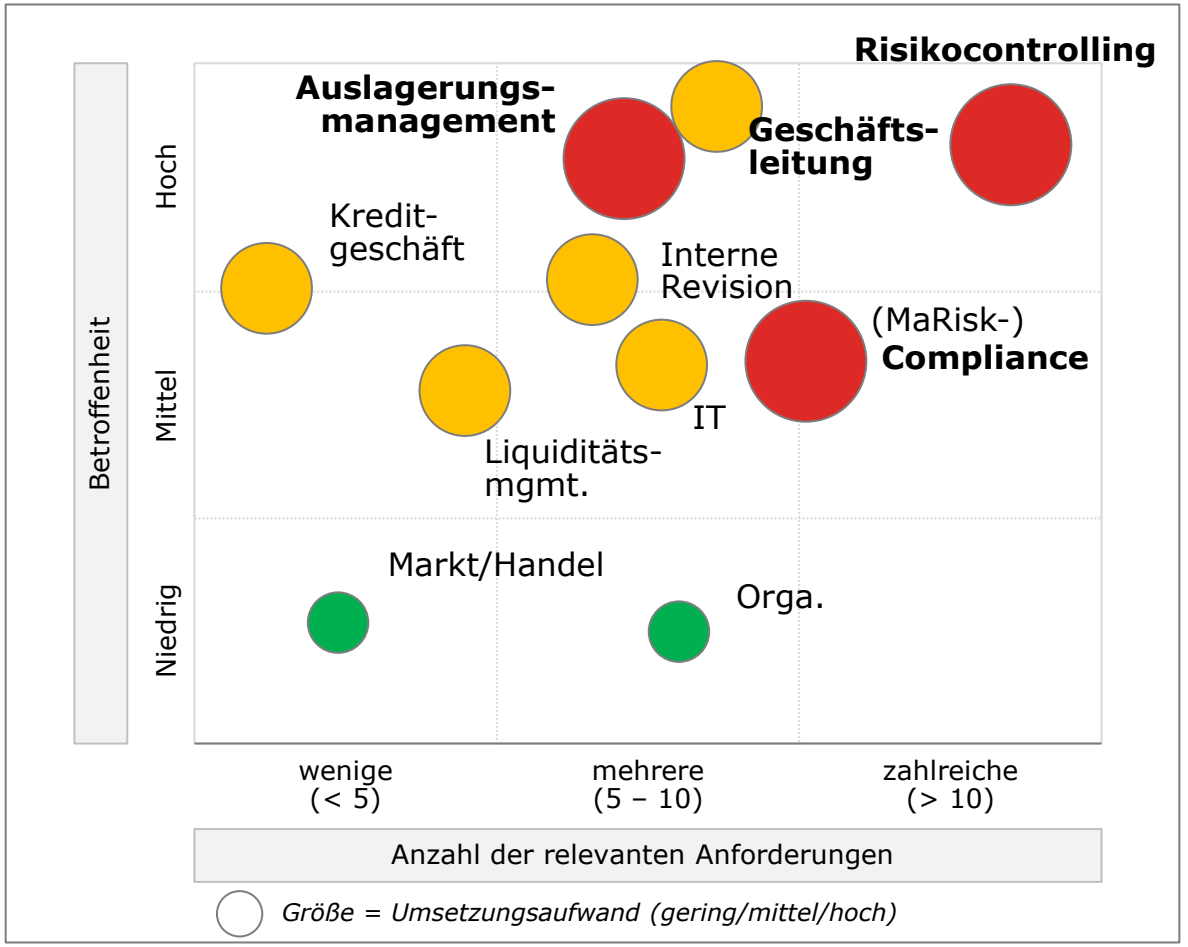
_ Durch die Novellierung sind nahezu **alle wesentlichen Kernfunktionen der Bank** – u.a. Risikocontrolling, Compliance, Auslagerungsmanagement bis hin zur Geschäftsleitung – betroffen.

5. MaRisk-Novelle



Auswirkungsanalyse





_Agenda

AT 3 und AT 4 Anforderungen an die Geschäftsleitung

Anforderungen an die Geschäftsleitung

AT 3	Entwicklung, Förderung und Integration einer **angemessenen institutsinternen und gruppenübergreifenden Risikokultur**
	Einrichtung angemessener Kontroll- und Überwachungsprozesse durch die Geschäftsleitung (GL) **im jeweiligen Zuständigkeitsbereich**
AT 5	Erweiterung der Organisationsrichtlinien um einen **Verhaltenskodex** für Mitarbeiter
AT 4.3.4	Genehmigung **instituts- und gruppenweiter Grundsätze** für das Datenmanagement, die Datenqualität und die Aggregation von Risikodatenaggregation durch die GL
AT 4.4.1	**Leitung der Risikocontrolling-Funktion** ausschließlich durch einen Geschäftsleiter (CRO). Der CRO darf keine Verantwortung für die Bereiche Finanzen/ Rechnungswesen (CFO) oder Organisation/IT (COO) inne haben. *[gilt für große und komplexe Institute]*
AT 4.4.2	Die **Compliance-Funktion** ist unmittelbar der Geschäftsleitung zu unterstellen. Einrichtung einer eigenständigen Compliance-Einheit unmittelbar unterhalb der Ebene der GL *[zwingend für große Institute]*

AT 4.3 Internes Kontrollsystem

IT (Risiko)Management

AT 4.3.2 Risikosteuerungs- und Controllingprozesse

Einrichtung angemessener Risikosteuerungs- und –controllingprozesse für **IT-Risiken** welche insbesondere umfassen:

1. Feststellung des Schutzbedarfs,
2. Ableitung von Sicherheitsanforderungen,
3. Festlegung von Sicherheitsmaßnahmen.

AT 4.3.4 Risikodatenaggregation

Datenaggregationskapazitäten müssen **flexibel** und **leistungsfähig** sein
Automatisierte Aggregation der Daten und Beschränkung manueller Prozesse

AT 7.2 Technisch-organisatorische Ausstattung

Die Vorgaben aus AT 7.2 an IT-Banksysteme sind auch **für selbst entwickelte IT-Anwendungen (IDV)** anzuwenden. Maßnahmen zur **Sicherstellung der Datensicherheit** haben sich am Schutzbedarf der verarbeiteten Daten zu orientieren

Auslagerungsmanagement – 1/2

AT 9 **Definition Auslagerung**

Eine Auslagerung stellt auch **bezogene Software** für Risikomanagement und Kernbanksysteme dar - keinen Fremdbezug

Eine Auslagerung von Kontroll- oder Kernbankbereichen ist nur zulässig, wenn **weiterhin fundierte Kenntnisse** erhalten bleiben und auch nach Beendigung der Auslagerung der **ordnungsgemäße Betrieb** fortgesetzt werden kann

Risikoanalyse

Die Risikoanalyse von Auslagerungen ist **regelmäßig** sowie **anlassbezogen** nach **instituts- bzw. gruppenweit einheitlichen Kriterien** durchzuführen Risikokonzentrationen und **Risiken aus Weiterverlagerung** sind zu berücksichtigen

Ausstiegsstrategien

Festlegung von Ausstiegsstrategien und **regelmäßige Prüfung der Handlungs-optionen** zur Sicherstellung der Kontinuität der (ausgelagerten) Prozesse

Auslagerungsmanagement – 2/2

AT 9 **Auslagerungsvertrag**

Bei Weiterverlagerungen sind **Zustimmungsvorbehalte** oder konkrete Voraussetzungen sowie **Informationspflichten** des weiterverlagerten Instituts bereits im Auslagerungsvertrag zu definieren

Der **Grad der akzeptierten Schlechtleistung** ist zu definieren und Kündigungsrechte sind zu vereinbaren

Vereinbarung von sonstigen **Sicherheitsanforderungen** (Zugangsbestimmungen und Zugriffsberechtigungen) im Auslagerungsvertrag

Auslagerungsmanagement

Festlegung **klarer Verantwortlichkeiten** für die Steuerung und Überwachung

Einrichtung eines **zentralen Auslagerungsmanagements** (Implementierung zentraler Kontroll- und Überwachungsprozesse, Vollständigkeit der Dokumentation, Überwachung der Einhaltung interner und gesetzl. Anforderungen, Koordination der Risikoanalyse)

Neu-Produkt-Prozess (NPP)

AT 8.2 Produktkatalog

Vorhalten eines **Katalogs für Produkte und Märkte**, die Gegenstand der Geschäftsaktivität sind

Prüfung in einem angemessenen Turnus, ob **Produkte noch verwendet werden**, ggf. Streichung von Produkten

Nachbetrachtung

Mindestens jährliche **Überprüfung des sachgerechten Umgangs** mit neuen Produkten oder Märkten, umfasst:

1. Überprüfung der vormals getroffenen Annahmen zum Risikogehalt,
2. Validierung der Testergebnisse,
3. Einschätzung der **sachgerechten Handhabung** und Prüfung auf Mängel in der Organisation und Durchführung des NPP

AT 4 Allgemeine Vorgaben an das Risikomanagement

Personal

AT 4.3.1 Aufbau- und Ablauforganisation

Übergangsfristen bei **Wechsel von Mitarbeitern** der Handels- und Vertriebsbereiche **in Kontrollbereiche**, innerhalb derer sie keine Tätigkeiten ausüben oder verantworten dürfe, die gegen das Verbot der Selbstprüfung und –überprüfung verstoßen („**Cooling-Off**“)

Kontrollbereiche sind: Risikocontrolling-Funktion, Compliance-Funktion, Marktfolge, Abwicklung und Kontrolle.

BT 2.2 Grundsätze der Internen Revision

Übergangsfristen von mindestens einem Jahr, beim Wechsel von Mitarbeitern anderer Organisationseinheiten **zur Internen Revision**, innerhalb derer diese keine Tätigkeiten prüfen dürfen, die gegen das Verbot der Selbstprüfung und –überprüfung verstoßen („Cooling-Off“).

NEU AT 4.3.4 Datenmanagement und Aggregation von Risikodaten

Risikocontrolling - 1/2

AT 4.3.4 Grundsätze, Analyse und Überprüfung der Datenaggregation

Festlegung **instituts- und gruppenweiter Grundsätze** für das Datenmanagement, die Datenqualität und die Risikodatenaggregation

Flexible und **leistungsfähige** Datenaggregationskapazitäten zur Verarbeitung von Ad-hoc-Informationen

Möglichkeit der Analyse von Risikopositionen auf den unterschiedlichsten Ebenen

Festlegung von Verantwortlichkeiten und **Einrichtung prozessabhängiger Kontrollen**

Überprüfung der Einhaltung institutsinterner Regelungen, Verfahren, Methoden und Prozesse von einer **unabhängigen Stelle**

NEU AT 4.3.4 Datenmanagement und Aggregation von Risikodaten

Risikocontrolling - 2/2

AT 4.3.4 Verfügbarkeit und Integrität der Risikodaten

Zweifelsfreie **Identifizierung**, **Zusammenführbarkeit** und **Auswertbarkeit** der Risikodaten

Einheitliche Namenskonventionen und Kennzeichnungen von Daten

Zeitnahe Verfügbarkeit der aggregierten Risikodaten auch in Stressphasen

Auswertbarkeit und Plausibilisierung der Risikodaten

Sicherstellung genauer und vollständiger Risikodaten; Überwachung der Datenqualität und -vollständigkeit anhand geeigneter Kriterien

Beschränkung und Dokumentation **manueller Prozesse** und Eingriffe

Plausibilisierung der Risikodaten mit anderen Daten (z.B. Rechnungslegung)

Abgleich der Risikodaten und Risikoberichte, um **Datenfehler** und **Schwachstellen** in der Datenqualität zu identifizieren

BT 2 Anforderungen an die Interne Revision

Interne Revision

BT 2 **Besondere Anforderungen an die Interne Revision**

Risikobewertungsverfahren beinhalten eine Analyse des **aktuellen und zukünftigen Risikopotenzials** der Aktivitäten und Prozesse

Berücksichtigung des Verlustpotenzials durch u.a. die **Manipulationsfähigkeit** der Prozesse durch Mitarbeiter

Überprüfung der **Wesentlichkeitseinstufung** der Aktivitäten und Prozesse

Vierteljährliche Erstellung eines **Gesamtberichtes** der Internen Revision an Geschäftsleitung und Aufsichtsorgan

Erstellung eines **Jahresberichtes** über festgestellte schwerwiegende Mängel sowie über noch nicht behobene **wesentliche Mängel, einschl. Maßnahmen** zu deren Behebung

Unverzügliche Berichterstattung über besonders schwerwiegende Mängel

NEU BT 3 Anforderungen an die Risikoberichterstattung

Risikoberichterstattung - 1/2

BT 3.1 Allgemeine Anforderungen

Berichte müssen zukunftsorientierte Risikoeinschätzungen beinhalten

Erstellung von Ad-hoc-Risikoberichten, sofern aufgrund der Risikosituation erforderlich

Risikoberichte sind in einem zeitlich angemessenen Rahmen zu erstellen

BT 3.2 Berichte der Risikocontrolling-Funktion

Erstellung eines mindestens **vierteljährlichen Gesamtrisikoberichts** über die wesentlichen Risikoarten und Vorlage bei der Geschäftsleitung

Monatliche, **wöchentliche** oder gar **tägliche** Berichte zu einzelnen Risikoarten

Zusätzliche Angaben zu: Angemessenheit der Kapitalausstattung und zu Liquiditätskennzahlen und Refinanzierungspositionen sowie diesbezügliche Prognosen

Mindestens vierteljährliche Berichte zu **sonstigen wesentlichen Risiken** (Risiken, Ursachen, mögliche Implikationen sowie getroffene Gegenmaßnahmen)

NEU BT 3 Anforderungen an die Risikoberichterstattung

Risikoberichterstattung – 2/2

BT 3.3 Berichte der Compliance-Funktion (unverändert, bisher AT 4.4.2)

BT 3.4 Berichte der Markt- und Handelsbereiche

Erstellung **regelmäßiger Berichte** der Markt- und Handelsbereiche zur Geschäftssituation im jeweiligen Bereich, u.a. zu Kreditgeschäft, Handel, Liquiditätsrisikomanagement und Treasury

Monatliche Berichte des **Kreditgeschäfts** für einen umfassenden Überblick

Risikoberichterstattung des **Handelsbereiches** an Geschäftsleitung

Monatliche, wöchentliche oder ggf. tägliche Berichte des **Aktiv-/ Passivmanagements**

BT 3.5 Risikoberichterstattung der Auslagerungsfunktion

Mindestens jährliche Berichterstattung über die **wesentlichen** Auslagerungen

Analyse der von den Auslagerungsunternehmen **eingereichten Berichte**

Aussage, ob erbrachte Leistungen den **vertraglichen Vereinbarungen** entsprechen

_Agenda

_Neue MaRisk Vorgaben schränken Handlungsspielräume, insbesondere für mittelständische Banken, drastisch ein …

Severn
make change work

_ Neue MaRisk Vorgaben gehen häufig über die Vorgaben internationaler Regulierungsstandards (Basel Standards, EBA) hinaus (**„Gold plating"**).

_ Eine Definition für „große und komplexe" Institute (> 30 Mrd. EUR Bilanzsumme) ersetzt die bislang akzeptierte Bewertung des Risikogehalts der Geschäftstätigkeit (**Abkehr vom Proportionalitätsprinzip**).

_ Anhand detaillierter Regelungen und verbindlicher Vorgaben werden die bewährten Grundsätze der **Prinzipienorientierung** und **Methodenfreiheit** für Institute aufgeweicht.

_ Anforderungen der MaRisk sind nicht in allen Fällen deckungsgleich mit Vorgaben an die von der EZB beaufsichtigten Institute in Europa. Dies erschwert die Umsetzung **einheitlicher gruppenweiter Standards** in Institutsgruppen und deren angehörigen Unternehmen.

… und verursachen erheblichen Mehraufwand für Institute ohne gleichwertig erkennbaren Zusatznutzen

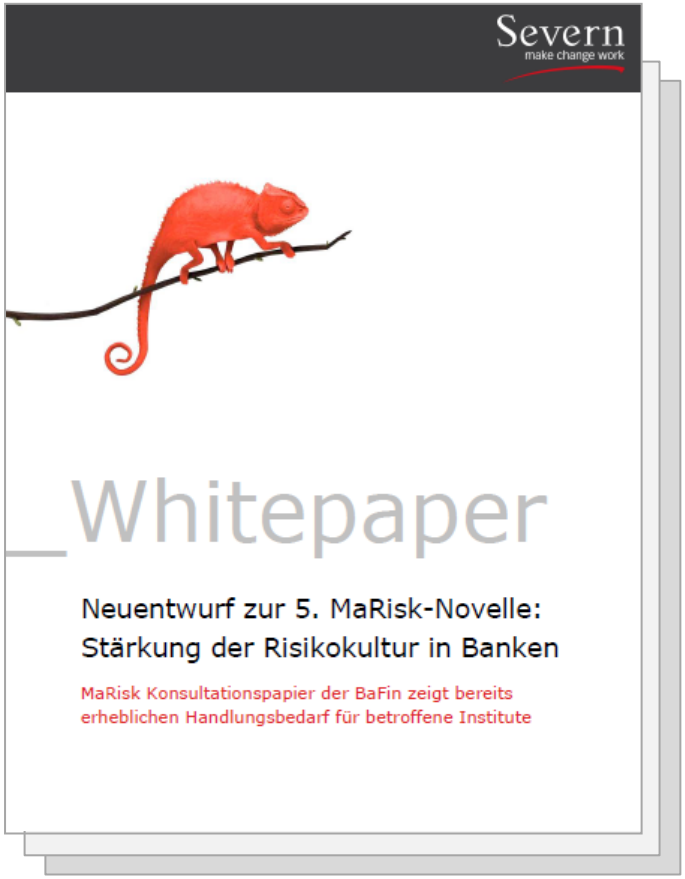
- Hohe **einmalige und auch laufende Aufwände** für die Erfüllung der MaRisk Anforderungen treffen insbesondere kleine und mittelgroße Institute (Einschränkung des Proportionalitätsprinzips).
- **Deutliche Aufwandstreiber** sind u.a. das Vorhalten von Risikodaten und deren Aggregation, zusätzliche Kontrollen und Dokumentation, Pflege eines Produktkatalogs, Anforderungen an das Auslagerungsmanagement, zusätzliche Risikoberichte, etc.
- Umsetzungsfristen für neue Anforderungen sind noch offen – insbesondere für umfassende neue Regelungsbereiche sind **ausreichende Implementierungsfristen** notwendig.
- Den vergleichsweise umfangreichen Neuregelungen stehen nur **wenig spürbare Nutzeneffekte** gegenüber. Währenddessen zeigt sich deutlich eine Entwicklung weg von Mindestanforderungen hin zu umfassenden Regelungs-standards („**Best practice**").

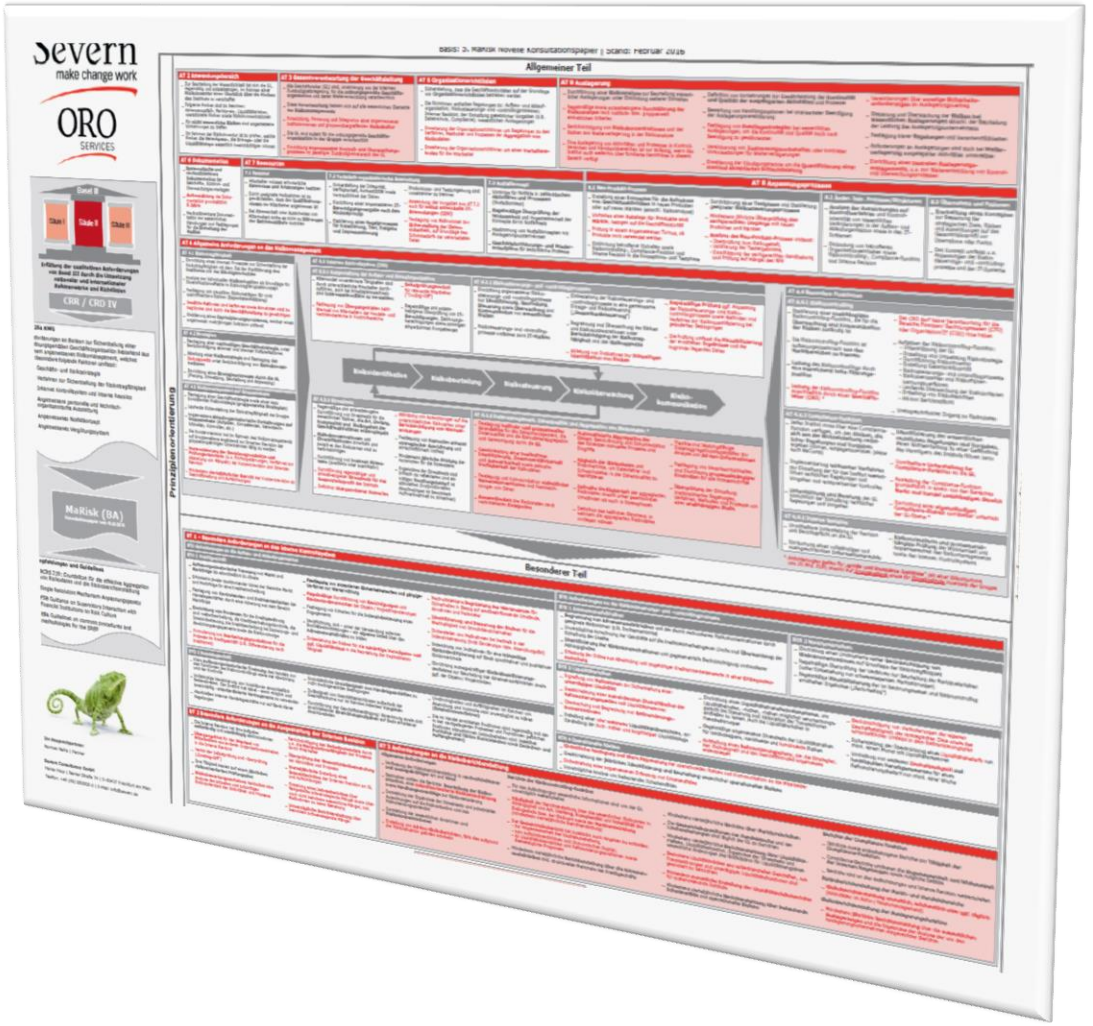
_Vielen Dank für Ihre Aufmerksamkeit.

Zeit für Ihre Fragen!

_Whitepaper und MaRisk Poster erhältlich unter www.severn.de

Severn
make change work





Severn
Consultancy GmbH

Diplom-Betriebswirt
Zertifizierter Projektmanager (GPM)

Norman Nehls

Partner

Hansa Haus
Berner Straße 74
D-60437 Frankfurt am Main

Telefon +49 / (0) 69 / 950 900-18
Telefax +49 / (0) 69 / 950 900-50
Mobil +49 / (0) 175 / 27 22 62 1

Norman.Nehls@Severn.de
www.severn.de

A N H A N G

_Übersicht - geänderte Module der MaRisk und Auswirkungen auf betroffene Bankbereiche (Konsultationspapier 5. MaRisk Novelle)

Severn
make change work

Modul MaRisk	Auswirkung	Geschäftsleitg./ Aufsichtsorgan	Risiko-controlling	Compliance	Interne Revision	IT	Organisation	Liquiditäts-(risiko-)management	Handel	Auslagerungs-management	Kreditgeschäft (Marktfolge)	Financial Accounting	Sonstige
		Betroffene Bankbereiche											
AT 3 – Gesamtverantwortung der Geschäftsleitung	Hoch	●	◕	◕	-	-	-	-	-	-	-	-	-
AT 4.3 – Internes Kontrollsystem	Mittel	-	◕	◕	◕	-	◔	-	-	-	-	-	-
AT 4.3.4 – Risikodatenaggregation	Hoch	◕	●	◔	◔	●	◔	-	-	-	-	◔	-
AT 4.4 – Besondere Funktionen	Hoch	●	●	●	-	-	-	-	-	-	-	-	-
AT 4.5 – Risikomanagement auf Gruppenebene	Gering	◔	-	-	●	-	-	-	-	-	-	-	-
AT 7.2 – Technisch-organisatorische Ausstattung	Mittel	-	◕	◔	-	●	-	◔	◔	-	-	-	-
AT 8.1 – Neu-Produkt-Prozess	Mittel	-	◕	◕	◕	-	◕	-	◕	-	-	-	◕
AT 9 – Auslagerung (Outsourcing)	Hoch	◔	◕	◕	◕	◕	◕	-	-	●	-	◔	◕
BTO 1 – Kreditgeschäft	Mittel	-	◕	-	◔	-	-	-	-	-	●	-	-
BTR 3 – Liquiditätsrisiken	Mittel	-	◕	-	-	-	-	●	◕	-	-	-	-
BTR 4 – Operationelle Risiken	Mittel	◕	●	-	-	◕	-	-	-	-	-	-	-
BT 2 Besondere Anforderungen an die Ausgestaltung der Internen Revision	Hoch	-	-	-	●	-	-	-	-	-	-	-	-
BT 3.1 Anforderungen an die Risikoberichterstattung	Hoch	◕	●	◔	-	◕	-	◕	◔	◕	◕	◔	-