Bundesanstalt für
Finanzdienstleistungsaufsicht

BaFin

Rundschreiben 3/2009

Aufsichtsrechtliche Mindestanforderungen an das Risikomanagement (MaRisk VA)

1. Zielsetzung des Rundschreibens ... 3
2. Anwendungsbereich ... 5
3. Verhältnis des Rundschreibens zu sonstigen Regelungen ... 6
4. Grundsatz der Proportionalität ... 7
5. Risiken ... 7
6. Gesamtverantwortung der Geschäftsleitung ... 10
7. Elemente eines angemessenen Risikomanagements ... 10
7.1 Risikostrategie ... 10
7.2 Organisatorische Rahmenbedingungen ... 13
7.2.1 Aufbauorganisation ... 14
7.2.2 Ablauforganisation ... 17
7.2.2.1 Neue Geschäftsfelder sowie Kapitalmarkt-, Versicherungs- und Rückversicherungsprodukte ... 20
7.2.2.2 Betriebliche Anreizsysteme und Ressourcen ... 20
7.2.2.3 Organisationsentwicklung ... 22
7.3 Internes Steuerungs- und Kontrollsystem ... 23
7.3.1 Risikotragfähigkeitskonzept und Limitierung ... 23
7.3.2 Risikokontrollprozess ... 26
7.3.2.1 Risikoidentifikation ... 26
7.3.2.2 Risikoanalyse und –bewertung ... 28
7.3.2.3 Risikosteuerung ... 31
7.3.2.4 Risikoüberwachung ... 33
7.3.3 Unternehmensinterne Kommunikation und Risikokultur ... 33
7.3.4 Risikoberichterstattung ... 34
7.3.5 Qualitätssicherung Internes Steuerungs- und Kontrollsystem ... 36
7.4 Interne Revision ... 37
7.5 Interne Kontrollen ... 41
8. Funktionsausgliederungen und Dienstleistungen im Sinne des § 64 a Abs. 4 VAG ... 41
9. Notfallplanung ... 43
10. Information und Dokumentation ... 44

Rundschreiben zu aufsichtsrechtlichen Mindestanforderungen an das Risikomanagement (MaRisk VA)	Erläuterungen der Anforderungen
1. Zielsetzung des Rundschreibens	
1 Dieses Rundschreiben konkretisiert die Regelungen des § 64a und des § 104s VAG i.V.m. Artikel 9 der Richtlinie 2002/87/EG (sog. Finanzkonglomerate-Richtlinie) und gibt einen flexiblen und praxisnahen Rahmen für die Ausgestaltung des Risikomanagements der beaufsichtigten Unternehmen, Gruppen und Finanzkonglomerate vor. Es legt damit für die Aufsichtsbehörde verbindlich den § 64a und § 104s VAG aus und gewährt hierdurch eine konsistente Anwendung gegenüber allen Unternehmen/Gruppen. Das Rundschreiben basiert auf dem Ansatz, dass die Geschäftsleiter eines Versicherungsunternehmens ein Risikobewusstsein entwickeln müssen, das stetig gelebt wird. Um das risikoorientierte Verhalten der Unternehmen beaufsichtigen zu können, werden unter Berücksichtigung der Branchenvielfalt sowie unternehmensindividueller Gegebenheiten Mindestanforderungen aufgestellt, die es der Aufsichtsbehörde bzw. dem Unternehmen selbst ermöglichen, das Risikomanagement quantifizierbarer, qualifizierbarer und administrierbarer zu beurteilen bzw. auszugestalten. Das Rundschreiben setzt sich aus den prinzipienbasierten Mindestanforderungen und Erläuterungen zusammen. Der Übersichtlichkeit halber und um ein zielgerichtetes Lesen zu ermöglichen, wurden die wichtigsten Verwaltungsinterpretationen, die die Aufsicht zugrunde legt, in die linke Spalte aufgenommen.	Der Erläuterungsteil dieses Rundschreibens enthält neben Ausführungen allgemeiner Art, Erläuterungen zu den Anforderungen sowie Beispiele zum Umgang mit den Anforderungen in der Praxis. Diese unverbindlichen Beispiele sollen gerade für kleine Unternehmen eine Hilfestellung, zum Aufbau und Betreiben eines prinzipienkonformen Risikomanagements darstellen. Die Aufsicht sieht ein funktionierendes Risikomanagementsystem zur Verbesserung des Schutzes der Versicherungsnehmer als wesentlich an. Bei Mindestanforderungen, die auf eine Bewertung nach ökonomischen Maßstäben zielen (hauptsächlich 7.3.1 (2) Risikotragfähigkeit und 7.2.2 (2) Reservierung) ist das Rundschreiben so zu verstehen, dass die Unternehmen verpflichtet werden, zu prüfen, ob entsprechende Funktionen und Prozesse ihr gegenwärtiges Risikomanagement wesentlich verbessern. Es ist davon auszugehen, dass bei Einführung eines neuen risikoorientierten europäischen oder nationalen Solvenzsystems dies zukünftig umzusetzen ist. Für Einrichtungen der betrieblichen Altersversorgung (EbAV) gilt dies erst, wenn fest steht, dass auch hier neue Solvenzregeln eingeführt werden. Einrichtungen der betrieblichen Altersvorsorgung brauchen so lange, insbesondere bei der Umsetzung der im weiteren Rundschreiben folgenden Regelungen zu Limiten, zum Solvenzkapital und anderer quantitativer Größen, nicht auf eine Zeitwertbilanzierung abzustellen.
2 Mit dem Rundschreiben legt die Aufsichtsbehörde aufsichtsrechtliche Mindestanforderungen für das Risikomanagement der genannten Unternehmen bzw. Unternehmensgruppen und Konzerne	

	fest. Risikomanagement im Sinne dieses Rundschreibens umfasst die Festlegung einer angemessenen Risikostrategie, die konsistent zu der gewählten Geschäftsstrategie ist, adäquate aufbau- und ablauforganisatorische Regelungen, die Einrichtung eines angemessenen internen Steuerungs- und Kontrollsystems, die Etablierung einer internen Revision und die Einrichtung von internen Kontrollen. Die Geschäftsleitung hat das gesellschaftsrechtliche Aufsichtsorgan - soweit dieses rechtlich notwendig ist oder freiwillig gebildet wurde - adäquat und regelmäßig über die Risikosituation zu informieren. Die in diesem Rundschreiben festgelegten Mindestanforderungen hindern Versicherungsunternehmen nicht, höhere Standards festzulegen. Das Rundschreiben ist prinzipienorientiert konzipiert, d.h. es ist den Unternehmen bzw. den Gruppen überlassen, im Rahmen der einzuhaltenden Mindestanforderungen zu entscheiden, welche konkrete Ausgestaltung des Risikomanagements für sie unter Berücksichtigung der unternehmensindividuellen Risiken, der Art und des Umfangs des Geschäftsbetriebes sowie des gewählten Geschäftsmodells für sie angemessen ist. Die Aufsichtsbehörde überprüft und beurteilt die Angemessenheit des Risikomanagements unter dem Gesichtspunkt der Proportionalität (vgl. 4 (1)).	
3	Wenn auf der Ebene des einzelnen Unternehmens, der Versicherungsgruppe oder des Finanzkonglomerats die Mindestanforderungen nicht erfüllt sind, kann die Aufsichtsbehörde nach § 81 Abs. 2 Satz 1, Abs. 1 Satz 2 i.V.m. § 64a bzw. nach § 104s VAG gegenüber den jeweiligen verantwortlichen Unternehmen und Personen die geeigneten und erforderlichen Anordnungen erlassen, um eine ordnungsgemäße Geschäftsorganisation zu erreichen.	Auch Verstöße gegen andere, auf die Geschäftsorganisation bezogene Vorschriften können zu aufsichtsrechtlichen Maßnahmen führen. Dies gilt beispielsweise für § 91 Abs. 2 des Aktiengesetzes und für §§ 104d, 104e Abs. 4 VAG.

2. Anwendungsbereich	
1 In den Anwendungsbereich dieses Rundschreibens fallen die folgenden der Aufsicht unterliegenden Unternehmen: • Erst- und Rückversicherungsunternehmen mit Sitz in Deutschland einschließlich ihrer in- und ausländischen Niederlassungen im EU/EWR-Raum. • Pensionsfonds. • Versicherungsunternehmen im Sinne des § 105 VAG. • Rückversicherungsunternehmen im Sinne des § 121i VAG. • Versicherungsunternehmen im Sinne des § 110d VAG. • Versicherungs-Holdinggesellschaften gem. § 1b Abs. 1 VAG, die übergeordnete Unternehmen einer Versicherungsgruppe sind. • Gemischte Finanzholding-Gesellschaften, die nach § 104q Abs. 3 Satz 8 VAG als übergeordnetes Finanzkonglomeratsunternehmen eines Finanzkonglomerats bestimmt wurden, in dem die Versicherungsbranche am stärksten vertreten ist. Es muss sichergestellt sein, dass auch auf Gruppen- bzw. Konglomeratsebene im Rahmen einer ordnungsgemäßen Geschäftsorganisation ein angemessenes Risikomanagement vorhanden ist.	Um eine gleichartige Behandlung zwischen Einzelunternehmen, Versicherungsgruppen und Finanzkonglomeraten zu erzielen, werden die Anforderungen an eine ordnungsgemäße Geschäftsorganisation, insbesondere an das Risikomanagement, einheitlich interpretiert. Jedoch ist zu beachten, dass auf Gruppenebene eine sinngemäße Umsetzung ausreichend ist, z.B. bezogen auf die aufbau- und ablauforganisatorischen Regelungen.
2 Aus Gründen der sprachlichen Vereinfachung benutzt dieses Rundschreiben fortan den Begriff „Unternehmen" als Synonym für alle in 2 (1) aufgeführten Unternehmungen.	

3. Verhältnis des Rundschreibens zu sonstigen Regelungen	
1 Die auf Grund anderer Rundschreiben geltenden speziellen Regelungen zur Aufbau- und Ablauforganisation, insbesondere im Bereich der Kapitalanlagen und der Rückversicherung, bleiben von diesem Rundschreiben unberührt. Dies gilt - auch im Falle ihrer Überarbeitung und Ersetzung durch Nachfolgerundschreiben - für • das Rundschreiben über derivative Finanzinstrumente vom 19.10.2000 (R 3/2000 Teil A III), • das Rundschreiben R 3/99 Teil A II 2 und 3 über Strukturierte Produkte, dem Rundschreiben R 1/2002 Teil B vom 12.04.2002 für Asset-Backed-Securities und Credit-Linked Notes, • das Rundschreiben R 7/2004 (VA) Teil B vom 20.08.2004, • das Rundschreiben R 15/2005 (VA) Teil IX vom 20.08.2005 über die Anlage des gebundenen Vermögens, • die Verlautbarung vom 14.09.2005 über den Einsatz der dort genannten Finanzinstrumente (VerBaFin 11/2005), • die Hinweise zur Solvabilität von Versicherungsunternehmen R 4/2005 (VA) vom 01.03.2005, • die Hinweise zur Aufsicht über Rückversicherungsunternehmen R 6/2005 (VA) vom 02.06.2005, • das Rundschreiben R 9/2007 (VA) Teil A zu Hinweisen zum Risikomanagement im Vermittlerbereich, • das Rundschreiben R 1/1997 Hinweise zur Prüfung der Leistungsfähigkeit und Leistungsbereitschaft von Rückversicherungsunternehmen durch Zedenten.	
2 Unberührt bleiben auch die zum Zwecke der Verhinderung der Geldwäsche erlassenen Rundschreiben, soweit sie auf Versicherungsunternehmen Anwendung finden.	

4. Grundsatz der Proportionalität	
1 Die Anforderungen des § 64a und des § 104s VAG sowie die Mindestanforderungen dieses Rundschreibens sind unter Berücksichtigung des Grundsatzes der Proportionalität zu erfüllen. Dieser besagt, dass Anforderungen konkret immer unter Berücksichtigung der unternehmensindividuellen Risiken, der Art und des Umfangs des Geschäftsbetriebes sowie der Komplexität des gewählten Geschäftsmodells des Unternehmens zu erfüllen sind. Die Aufsichtsbehörde geht deshalb davon aus, dass die Anforderungen dieses Rundschreibens von allen Unternehmen erfüllt werden können.	Bei Anwendung des Grundsatzes der Proportionalität ist der Grundsatz der Materialität zu berücksichtigen. Der Grundsatz der Materialität bedeutet hier, dass nur wesentliche Risiken in die Betrachtung einzustellen sind. Zur Definition der Wesentlichkeit siehe 5.1. Die Anforderungen dieses Rundschreibens sind von allen Unternehmen zu erfüllen, auch von denjenigen, die nach den EU-Richtlinien unter die „Bagatellgrenze" fallen. Die Mittel und Wege können aus Gründen der Proportionalität unternehmensindividuell verschieden sein. Abweichungen z.B. von einem Konzern- bzw. Gruppenstandard muss ein Unternehmen rechtfertigen (Darlegungslast).
2 Die Besonderheiten von Einrichtungen der betrieblichen Altersversorgung sind bei der Beurteilung des Risikomanagements zu berücksichtigen.	Einrichtungen der betrieblichen Altersversorgung haben in der Regel einen eingeschränkten Geschäftsbetrieb und ein weniger komplexes Geschäftsmodell.
5. Risiken	
1 Die Anforderungen des Rundschreibens beziehen sich auf das Risikomanagement von im folgenden Absatz beschriebenen wesentlichen Risiken. Als **Risiko** wird die Möglichkeit des Nichterreichens eines explizit formulierten oder sich implizit ergebenden Zieles verstanden. Alle von der Geschäftsleitung identifizierten Risiken, die sich nachhaltig negativ auf die Wirtschafts-, Finanz- oder Ertragslage des Unternehmens auswirken können, werden als **wesentlich** erachtet. Zur Beurteilung der Wesentlichkeit hat sich die Geschäftsleitung einen Überblick über das Gesamtrisikoprofil des Unternehmens zu verschaffen. Die Bestimmung der wesentlichen Risiken ist das Ergebnis der unternehmensindividuellen Risikoidentifikation (7.3.2.1) sowie Risikoanalyse und	Der Begriff Risiko wird hier wirkungsbezogen definiert. Der Risikobegriff ist im Zusammenhang mit den Zielsetzungen zu interpretieren. Es sind sowohl negative als auch positive Zielabweichungen möglich. Negative Zielabweichungen realisieren sich zumeist als Verluste. Dennoch ist es Aufgabe eines guten Risikomanagementsystems, unternehmerische Chancen und Risiken zu handhaben. Dieses Rundschreiben fokussiert auf die negativen Zielabweichungen. Risikobewertung sollte in einem ersten Schritt immer qualitativ erfolgen. Hierbei hat das Unternehmen sowohl die bilanziellen als auch außerbilanziellen Auswirkungen von Risiken zu berücksichtigen. Letztere resultieren häufig aus schwer zuzuordnenden Risken, die

-bewertung (7.3.2.2) und der unternehmensindividuellen Skalierung der Wesentlichkeit. Durch die Implementierung von wirksamen Kontroll- und Überwachungsmaßnahmen muss sichergestellt werden, dass keine wesentlichen Fehler auftreten, die zur Akzeptanz eines untragbaren Risikos durch das Unternehmen führen. Für Risiken, die als nicht wesentlich eingestuft werden, sind angemessene Vorkehrungen zu treffen.	gleichwohl erfasst werden müssen, wie z.B. Risiken in Zweckgesellschaften, für die das Unternehmen haftet oder die sich negativ auf seine Wirtschafts-, Finanz- oder Ertragslage auswirken können. Erst nach Einschätzung auf einer Referenzskala des Unternehmens als wesentliches Risiko sollte eine Quantifizierung erfolgen.
2 Aufsichtsrechtlich zur Erfüllung des Risikomanagements mindestens vom Unternehmen zu berücksichtigende Risikokategorien sind:	Eine Risikokategorisierung stellt eine Komplexitätsreduktion dar. Die Aufsicht erwartet, dass Unternehmen sich in den nach § 55c VAG einzureichenden Risikoberichten inhaltlich zumindest mit den hier aufgelisteten Risiken auseinandersetzen. Unternehmen können auch eine andere Risikokategorisierung als die im Rundschreiben vorgeschlagene verwenden, soweit alle in dem Erläuterungsteil beschriebenen Risiken abgedeckt werden.
• Versicherungstechnisches Risiko	Das versicherungstechnische Risiko bezeichnet das Risiko, dass bedingt durch Zufall, Irrtum oder Änderung der tatsächliche Aufwand für Schäden und Leistungen vom erwarteten Aufwand abweicht.
• Marktrisiko	Das Marktrisiko bezeichnet das Risiko, das sich direkt oder indirekt aus Schwankungen in der Höhe bzw. in der Volatilität der Marktpreise für die Vermögenswerte, Verbindlichkeiten und Finanzinstrumente ergibt. Das Marktrisiko schließt das Währungskursrisiko und Zinsänderungsrisiko ein.
• Kreditrisiko (einschließlich Länderrisiko)	Das Kreditrisiko bezeichnet das Risiko, das sich aufgrund eines Ausfalls oder aufgrund einer Veränderung der Bonität oder der Bewertung von Bonität (Credit-Spread) von Wertpapieremittenten, Gegenparteien und anderen Schuldnern ergibt, gegenüber denen das Unternehmen Forderungen hat.

• Operationelles Risiko	Das operationelle Risiko bezeichnet das Risiko von Verlusten aufgrund von unzulänglichen oder fehlgeschlagenen internen Prozessen oder aus mitarbeiter- und systembedingten oder aber externen Vorfällen. Das operationelle Risiko umfasst auch Rechtsrisiken, jedoch nicht strategische Risiken und Reputationsrisiken.
• Liquiditätsrisiko	Das Liquiditätsrisiko bezeichnet das Risiko, dass ein Unternehmen auf Grund mangelnder Fungibilität nicht in der Lage ist, seinen finanziellen Verpflichtungen bei Fälligkeit nachzukommen.
• Konzentrationsrisiko	Das Konzentrationsrisiko bezeichnet das Risiko, das sich dadurch ergibt, dass das Unternehmen einzelne Risiken oder stark korrelierte Risiken eingeht, die ein bedeutendes Schaden- oder Ausfallpotenzial haben.
• Strategisches Risiko	Das strategische Risiko ist das Risiko, das sich aus strategischen Geschäftsentscheidungen ergibt. Zu dem strategischen Risiko zählt auch das Risiko, das sich daraus ergibt, dass Geschäftsentscheidungen nicht einem geänderten Wirtschaftsumfeld angepasst werden. Strategisches Risiko ist in der Regel ein Risiko, das im Zusammenhang mit anderen Risiken auftritt. Es kann aber auch als Einzelrisiko auftreten.
• Reputationsrisiko	Das Reputationsrisiko ist das Risiko, das sich aus einer möglichen Beschädigung des Rufes des Unternehmens infolge einer negativen Wahrnehmung in der Öffentlichkeit (z.B. bei Kunden, Geschäftspartnern, Aktionären, Behörden) ergibt. Ebenso wie das strategische Risiko ist das Reputationsrisiko in der Regel ein Risiko, das im Zusammenhang mit anderen Risiken auftritt. Es kann aber auch als Einzelrisiko auftreten.

6. Gesamtverantwortung der Geschäftsleitung	
1 Alle Geschäftsleiter sind - unabhängig von der internen Zuständigkeitsregelung - für die ordnungsgemäße Geschäftsorganisation des Unternehmens verantwortlich (§ 64a Abs. 1 Satz 2, § 104s Satz 3 VAG).	Die Gesamtverantwortung der Geschäftsleitung besagt, dass alle Geschäftsleiter über die Risiken, denen das Unternehmen ausgesetzt ist, informiert sind, ihre wesentlichen Auswirkungen auf das Unternehmen beurteilen können und die erforderlichen Maßnahmen zur Begrenzung treffen müssen, d.h. alle Geschäftsleiter sind für die Implementierung eines funktionierenden Risikomanagements und dessen Weiterentwicklung verantwortlich. Risikomanagemententscheidungen (Entscheidungen über den Eingang und die Handhabung wesentlicher Risiken) liegen in der Verantwortung der Geschäftsleitung und sind nicht delegierbar. Unberührt bleibt die Möglichkeit, die Verantwortung für die laufende Durchführung einzelner Elemente der Geschäftsorganisation auf ein oder mehrere Mitglieder der Geschäftsleitung zu übertragen, sofern nicht andere gesetzliche Regelungen entgegenstehen.
7. Elemente eines angemessenen Risikomanagements	
1 Unternehmen müssen ein Risikomanagement einrichten, welches die in § 64a Abs. 1 Satz 4 VAG genannten Elemente enthält. Die notwendigen Elemente des Risikomanagements stehen nicht unabhängig nebeneinander, sondern sind miteinander zu einem konsistenten und ineinander greifenden Ganzen zu verzahnen (ganzheitlicher Ansatz), so dass ein effektiver Umgang mit den unternehmensindividuellen Risiken möglich ist.	Der ganzheitliche Ansatz verlangt, dass die dem Gesamtrisikoprofil angemessene Risikostrategie von oben nach unten in notwendigem Umfang in das operative Tagesgeschäft umgesetzt wird und Risiken des operativen Tagesgeschäfts wiederum von unten nach oben berichtet werden (Gegenstromplanung), so dass ein Gesamtrisikoprofil erstellt werden kann.
7.1 Risikostrategie	
1 Die Festlegung der Geschäftsstrategie und der daraus abgeleiteten adäquaten Risikostrategie liegt in der nicht delegierbaren	Unter Geschäftsstrategie versteht die Aufsicht die geschäftspolitische Ausrichtung, die Zielsetzungen und Planungen des Unternehmens

Gesamtverantwortung der Geschäftsleitung und ist von dieser zu dokumentieren.	über einen angemessenen Zeithorizont, unter Risikostrategie hingegen die Beschreibung des Umgangs mit den sich aus der Geschäftsstrategie ergebenden Risiken. Die Geschäftstrategie ist nicht Gegenstand von Prüfungshandlungen von Aufsicht oder interner Revision. Die Risikostrategie hingegen unterliegt der Prüfung durch die Aufsicht. Die Aufsicht zieht bei Überprüfung der Risikostrategie die Geschäftsstrategie unter dem Aspekt der Folgerichtigkeit heran, um die Konsistenz beider Strategien nachvollziehen zu können. Insbesondere schildert die Risikostrategie die Auswirkungen der Geschäftsstrategie auf die Risikosituation des Unternehmens und beschreibt den Umgang mit den vorhandenen Risiken und die Fähigkeit des Unternehmens, neu hinzugekommene Risiken zu tragen. Die Art und Weise der Dokumentation der Risikostrategie durch den Vorstand liegt im Ermessen des Unternehmens. Neben einer zusammenfassenden Darstellung in einem Dokument (z.B. für eine Gruppe) ist auch eine Darstellung über mehrere Dokumente möglich, soweit zwischen diesen Dokumenten ein konsistenter Zusammenhang besteht.
2 Die Risikostrategie soll die sich aus der Geschäftsstrategie ergebenden Risiken darstellen und so gestaltet sein, dass sich die operative Steuerung der Risiken an diese anknüpfen kann. Die Risikostrategie muss auf • die Art (welche Risiken sollen überhaupt eingegangen werden?), • die Risikotoleranz (welche Höhe des Risikos wird gewählt?), • die Herkunft (woher stammt das Risiko?), • den Zeithorizont der Risiken (welche Risiken in welcher Zeitperiode sollen mit der vorhandenen Risikodeckung bewältigt werden?) und • die Risikotragfähigkeit eingehen.	In der Geschäftsstrategie sind die nachhaltigen Geschäftserwartungen zu erfassen (z.B. Art des Geschäftes, anvisiertes Volumen, Gewinnerwartung, Kosten). In der Risikostrategie werden die sich daraus ergebenden Risiken bezüglich ihres Einflusses auf die Wirtschafts-, Finanz- oder Ertragslage des Unternehmens dargestellt sowie daraus resultierende Leitlinien für den Umgang mit den Risiken. Dabei ist es existenziell, dass auf operativer Ebene daraus die Erwartungen/Risiken definiert werden, so dass Handlungsvorgaben für die Mitarbeiter im Tagesgeschäft entstehen. Herkunft ist nicht zwingend geografisch zu verstehen, beispielsweise können auch Sparten oder Versicherungszweige gemeint sein.

3	Bei Aufnahme neuer Geschäftsfelder oder der Einführung neuer Kapitalmarkt-, Versicherungs- oder Rückversicherungsprodukte ist deren Auswirkung auf das Gesamtrisikoprofil zu bewerten. Das gleiche gilt für signifikante Veränderungen von Marktparametern und Risikoeinschätzungen. Änderungen der Risikostrategie können erforderlich werden, wenn sich das Gesamtrisikoprofil substantiell verändert. Dies ist fortlaufend durch die Geschäftsleitung des Unternehmens zu prüfen. Die Einbindung des Verantwortlichen Aktuars gemäß seiner aufsichtsrechtlichen Funktion ist ggf. zu prüfen.	Veränderungen im Gesamtrisikoprofil sollten nicht nur auf Kapitalanlageparameter beschränkt bleiben, sondern auch die Auswirkungen von Veränderungen in der Risikoeinschätzung insgesamt und speziell bezogen auf neue Risikoarten (vgl. z.B. Terrorismus, Pandemie, Asbest) berücksichtigen.
4	Die Geschäftsleitung hat sowohl die Geschäftsstrategie als auch die Risikostrategie mindestens einmal im Geschäftsjahr zu überprüfen und ggf. anzupassen. Die Strategien sind an das Aufsichtsorgan des Unternehmens - soweit vorhanden - zu berichten und mit diesem zu erörtern.	Grundsätzlich sollte die Risikostrategie an jedes Mitglied des Aufsichtsorgans berichtet werden. Soweit das Aufsichtsorgan einen dafür zuständigen Ausschuss gebildet hat, kann die Risikostrategie auch an diesen berichtet und mit ihm erörtert werden. Voraussetzung dafür ist, dass ein entsprechender Beschluss über die Einrichtung des Ausschusses besteht und der Vorsitzende des Ausschusses regelmäßig das gesamte Aufsichtsorgan informiert. Zusätzlich ist jedem Mitglied des Aufsichtsorgans das Recht einzuräumen, die Risikostrategie jederzeit einsehen zu können. Insbesondere um strategischen Risiken vorzubeugen, empfiehlt die Aufsicht der Geschäftsleitung, die von ihnen vorgegebene Risikostrategie regelmäßig einer kritischen Qualitätsanalyse (sog. „Strategieaudit“) zu unterziehen oder schriftlich darzulegen, warum sie dies für entbehrlich hält. Das Strategieaudit könnte zum Beispiel in Zusammenarbeit mit der internen Revision oder dem Aufsichtsorgan durchgeführt werden.

7.2 Organisatorische Rahmenbedingungen	
1 Das Unternehmen hat zur Umsetzung des § 64a VAG bzw. des § 104s VAG sicherzustellen, dass die mit wesentlichen Risiken behafteten Geschäftsaktivitäten auf der Grundlage von innerbetrieblichen Leitlinien betrieben werden. Die innerbetrieblichen Leitlinien haben die rechtlich, satzungsmäßig und strategisch definierten Grenzen der Geschäftstätigkeit zu berücksichtigen und die organisatorischen Rahmenbedingungen festzulegen, innerhalb derer das Unternehmen tätig wird, insbesondere • die Aufbauorganisation • die Ablauforganisation, mit a) der organisatorischen Einbindung von neuen Geschäftsfeldern und neuen Kapitalmarkt-, Versicherungs- oder Rückversicherungsprodukten, b) betrieblichen Anreizsystemen und Ressourcen, c) der Organisationsentwicklung, • die Einrichtung eines geeigneten internen Steuerungs- und Kontrollsystems mit a) einem Risikotragfähigkeitskonzept, b) einer Risikoidentifikation, Risikoanalyse, -bewertung, -steuerung und -überwachung, c) einer unternehmensinternen Kommunikation, d) einer aussagefähigen Berichterstattung. • Aufgaben und Funktion der internen Revision • interne Kontrollen • Entscheidungen über Funktionsausgliederungen im Sinne von	

§ 5 Abs. 3 Nr. 4 VAG • Notfallplanung • angemessene Information und Dokumentation	
2 Materiell bedeutsame Einzelentscheidungen und Anweisungen von Führungsebenen unterhalb der Geschäftsleitung, die gegen die innerbetrieblichen Leitlinien verstoßen, sind schriftlich zu begründen, zu dokumentieren und der Geschäftsleitung zur Kenntnis vorzulegen.	Damit sind nicht die Einzelentscheidungen des operativen Tagesgeschäftes gemeint, sondern Entscheidungen von Vorgängen, die für das Unternehmen von wesentlicher Bedeutung sind und die von den in der Aufbauorganisation festgelegten Führungsebenen getroffen wurden.
7.2.1 Aufbauorganisation	
1 Die Aufbauorganisation ist auf die Unterstützung der wichtigsten Strategieziele des Unternehmens auszurichten. Grundsätzlich hat eine klare Funktionstrennung bis einschließlich der Ebene der Geschäftsleitung zwischen unvereinbaren Funktionen zu erfolgen. Wer für den Aufbau von Risikopositionen verantwortlich ist, darf nicht gleichzeitig und auch nicht mittelbar mit deren Überwachung und Kontrolle betraut sein.	Eine Funktion ist die administrative Kapazität zur Übernahme bestimmter Aufgaben. Sofern nichts anderes bestimmt ist, hindert die Festlegung einer bestimmten Funktion das Unternehmen nicht daran, frei darüber zu entscheiden, wie diese Funktion in der Praxis organisiert wird.
2 Soweit es aufgrund der Größe eines Unternehmens nicht zumutbar ist, unvereinbare Funktionen vollständig voneinander zu trennen, muss die Vermeidung von Interessenkonflikten auf andere Weise angemessen gewährleistet sein. Die Konsistenz zur gewählten Risikostrategie muss dabei sichergestellt sein.	Grundsätzlich ist das beschriebene Prinzip der Funktionstrennung z.B. zwischen operativer Risikosteuerung und Risikocontrollingfunktion bis einschließlich der Ebene der Geschäftsleitung notwendig. Das Prinzip der Funktionstrennung muss hierarchisch abgesichert sein, damit es funktioniert. Bei Unternehmen, bei denen auf Grund der geringen Anzahl von Mitarbeitern eine personelle Funktionstrennung nicht möglich ist, darf ausnahmsweise die gemeinsame Wahrnehmung unterschiedlicher unvereinbarer Funktionen erfolgen, wenn durch flankierende Maßnahmen (Transparenz durch aussagekräftige Dokumentation, separate Berichtslinie außerhalb der fachlichen Weisungsbefugnis, Vier-Augen-Prinzip) sichergestellt ist, dass Interessenkonflikte vermieden werden.

3 Aufgaben und Verantwortlichkeiten innerhalb der Aufbauorganisation sind klar zu definieren und aufeinander abzustimmen. Hinsichtlich der Festlegung der Verantwortlichkeiten sind die folgenden Vorgaben für nachfolgende Funktionsträger zu beachten:	Die für die Funktionen verwendeten Begriffe sind nicht zwingend. Eine unternehmensindividuelle Gestaltung ist möglich. Insbesondere sind abweichende Bezeichnungen für die geforderten Funktionen innerhalb des Risikomanagements zulässig, entscheidend ist die inhaltliche Ausgestaltung. Alle geforderten Funktionen sind nicht mit den zuständigen Geschäftsbereichen gleichzusetzen.
a) Die **Geschäftsleitung** ist verantwortlich für • die Festlegung einheitlicher Leitlinien für das Risikomanagement unter Berücksichtigung der internen und externen Anforderungen, • die Festlegung der Geschäfts- und Risikostrategie, • die Festlegung der Risikotoleranz und die Einhaltung der Risikotragfähigkeit, • das Treffen wesentlicher risikostrategischer Vorgaben, • die laufende Überwachung des Risikoprofils und die Einrichtung eines Frühwarnsystems sowie die Lösung wesentlicher risikorelevanter Ad-hoc-Probleme.	Die Risikotoleranz ist abhängig von der individuellen Risikobereitschaft der Geschäftsleitung, diese spiegelt sich auch in der Risikostrategie wider. Die Risikotragfähigkeit ist hingegen objektiv bestimmbar und bildet die Obergrenze. Risikostrategische Vorgaben können z.B. bezüglich des Risikoprofils, des Risikokapitals und der Festlegung der Risikolimite bestimmt werden. Wesentliche risikorelevante Ad-hoc-Probleme können z.B. Limitüberschreitungen sein.
b) Die **unabhängige Risikocontrollingfunktion** koordiniert und ist verantwortlich für • die Identifikation, Bewertung und Analyse von Risiken mindestens auf aggregierter Ebene, • die Entwicklung von Methoden und Prozessen zur Risikobewertung und –überwachung, • die Risikoberichterstattung über die identifizierten und analysierten Risiken und die Feststellung von Risikokonzentrationen, • den Vorschlag von Limiten,	Die Risikocontrollingfunktion ist dann unabhängig, wenn sie nicht für das Eingehen von Risiken oder die Steuerung von Risiken auf operativer Ebene verantwortlich zeichnet (siehe auch 7.3.2.4 (3)). Durch eine abgestimmte Verfahrensweise im Sinne einer Gesamtkoordination gegenüber der Geschäftsleitung hat die unabhängige Risikocontrollingfunktion auch für eine unternehmensweite, einheitliche Aggregation und Plausibilisierung der Risiken, deren Berichterstattung sowie die Unterbreitung von Vorschlägen zur Risikobegrenzung gegenüber der Geschäftsleitung zu sorgen. Unter abgestimmter Verfahrensweise ist z.B. die Hoheit über die Festlegung von Formaten, Inhalten, Schnittstellen, Methoden, Software-Nutzung etc. zu verste-

• die Überwachung von Limiten sowie von Risiken auf aggregierter Ebene, die Überwachung von Maßnahmen zur Risikobegrenzung, • die Beurteilung geplanter Strategien unter Risikoaspekten, • die Bewertung von neuen Produkten als auch des aktuellen Produktportfolios aus Risikosicht, • die Validierung der ggf. von den Geschäftsbereichen vorgenommenen Risikobewertungen. Personen oder Geschäftsbereiche, die diese Funktion ausüben, müssen ihre Aufgaben objektiv und unabhängig erfüllen können. Sie muss nicht zwingend auf Ebene der Geschäftsleitung angesiedelt sein. Zur Wahrnehmung ihrer Aufgaben ist der Risikocontrollingfunktion ein vollständiges und uneingeschränktes Informationsrecht einzuräumen. Die unverzügliche Berichterstattung gegenüber der unabhängigen Risikocontrollingfunktion ist notwendig, wenn wesentliche Mängel zu erkennen oder wesentliche finanzielle Schäden aufgetreten sind oder ein konkreter Verdacht auf Unregelmäßigkeiten besteht. Das Aufsichtsorgan - soweit vorhanden - hat die Möglichkeit, sich direkt an die unabhängige Risikocontrollingfunktion zu wenden, um weitere Informationen einzuholen. Diese Möglichkeit findet ihre Grenzen in den für das Aufsichtsorgan bestehenden gesetzlich oder vertraglich vereinbarten Informationsrechten und –pflichten.	hen. Die unabhängige Risikocontrollingfunktion muss gegenüber der gesamten Geschäftsleitung berichtspflichtig sein. Dies ist insbesondere sicherzustellen, falls ein Mitglied der Geschäftsleitung unmittelbar die unabhängige Risikocontrollingfunktion innehat. Spezielle für die Kapitalanlage geltende Berichtspflichten, z.B. von dem Kapitalanlagerisikomanagement gegenüber der Risikocontrollingfunktion, bleiben unberührt. Falls das Aufsichtsorgan von seinem direkten Informationsrecht Gebrauch machen möchte, empfiehlt es sich, dies in einer allgemeingültigen Informationsordnung losgelöst vom Einzelfall detailliert festzulegen. Dies zeigt, dass dieser Zugriff keine Misstrauensbekundung gegenüber der Geschäftsleitung ist.
c) Die operativen **Geschäftsbereiche** sind für die Umsetzung der Identifikation, die Analyse und insbesondere Steuerung aller wesentlichen Risiken ihres Bereiches zuständig. Die Geschäftsbereiche haben die Möglichkeit, die von der Geschäfts-	

leitung vorgegebenen Limite für ihren Geschäftsbereich detaillierter aufzuteilen. Die Aufgaben, Verantwortlichkeiten, Vertretungsregelungen und Kompetenzen für den Geschäftsbereich im Umgang mit Risiken sind zu definieren und zu dokumentieren.	
d) Die interne **Revision** prüft selbständig, (prozess-) unabhängig und objektiv risikoorientiert alle Geschäftsbereiche, Abläufe, Verfahren und Systeme. Dadurch kann sie frühzeitig Risiken, Gefahren und Mängel erkennen und diese an die Geschäftsleitung berichten.	Die konkreten Aufgaben der internen Revision sind in 7.4 Interne Revision, Seite 37, dargelegt.
7.2.2 Ablauforganisation	
1 Die Ablauforganisation hat im Einklang mit der Risikostrategie die wesentlichen Funktionen der Aufbauorganisation zu unterstützen. Die Ablauforganisation ermöglicht es, alle mit wesentlichen Risiken behafteten Geschäftsabläufe sowie die Verantwortlichkeiten festzulegen. Die Ablauforganisation ist klar zu definieren. Für jeden mit wesentlichen Risiken behafteten Geschäftsablauf einschließlich der Übergabe von Daten und Ergebnissen sind entsprechende Verantwortlichkeiten zu definieren. Die Ablauforganisation setzt eine adäquate Personalausstattung voraus. Die Personalausstattung hat sich u.a. an den betriebsinternen Erfordernissen, den Geschäftsaktivitäten und der Risikosituation zu orientieren. Mitarbeiter sind so zu schulen, dass sie Risiken identifizieren und angemessen auf diese reagieren können.	Alle mit wesentlichen Risiken behafteten Geschäftsabläufe und deren Schnittstellen sind so zu steuern, dass sie die Geschäftsziele unterstützen und Abweichungen hiervon gering halten.
2 Alle mit wesentlichen Risiken behaftete Geschäftsabläufe sind adäquat zu steuern und zu überwachen. Zu diesen Geschäftsabläufen zählen zumindest das versicherungstechnische Geschäft, die Reservierung, das Kapitalanlagemanagement (einschließlich	

Asset-Liability-Management) und das passive Rückversicherungsmanagement.	
• **Versicherungstechnisches Geschäft** Die Steuerung des versicherungstechnischen Geschäfts umfasst - sofern im Geschäftsbetrieb vorhanden - mindestens das Produktdesign, die Tarifierung, die Vertriebs- und Zeichnungspolitik, die Risikoprüfung und das Schadenmanagement sowie Markt- und Wettbewerbsrisiken.	Mit Annahme- und Zeichnungsrichtlinien wird das versicherungstechnische Geschäft zumeist gesteuert. Diese enthalten sowohl sachliche Regeln (Art und geografische Herkunft des Geschäfts), als auch personenbezogene, quantitative Zeichnungsgrenzen. Ausschlüsse sollten klar festgelegt werden. Für die Tarifberechnung sollten ausreichende Informationen über alle Risiken verwandt werden. Die Tarifierung ist ausreichend zu dokumentieren. Sind in einem Zweig deutliche Abwicklungsverluste zu verzeichnen, muss das Unternehmen die vorgenommene Tarifierung begründen können. Zur Steuerung einzelner Arbeitsschritte erwartet die Aufsicht, dass risikorelevante Kennzahlen eingesetzt werden (z.B. Stornoquote, Anzahl der Zeichnungsrichtlinienüberschreitungen).
• **Reservierung** Die Bewertung der versicherungstechnischen Rückstellungen erfolgt für Zwecke der Rechnungslegung nach §§ 341e-h HGB. Sie dient derzeit auch als Grundlage für Solvenzzwecke. Eine marktnahe aktuarielle Berechnung der versicherungstechnischen Rückstellungen für Solvenzzwecke ist derzeit gesetzlich nicht zwingend vorgeschrieben. Die Aufsicht erwartet von allen Unternehmen mit Ausnahme von Einrichtungen der betrieblichen Altersversorgung bereits zum gegenwärtigen Zeitpunkt, dass sie prüfen, ob die Einrichtung risikoadäquater Prozesse für den Aufbau einer statistischen Datenbasis und für die Bestimmung und IT-technische Implementierung angemessener Bewertungsverfahren ihr gegenwärtiges Risikomanagement wesentlich verbessert. In diesem Fall sollte die Umstellung auf eine marktnahe aktuarielle Bewertung der versicherungstechnischen Rückstellungen als integrierter Be-	

standteil des Risikomanagements eingeleitet werden. Diese Prozesse müssen auch die Verantwortlichkeiten im Unternehmen festlegen und eine ausreichende Qualitätssicherung vorsehen.	
• **Kapitalanlagemanagement (einschließlich Asset-Liability-Management)** Es gelten die speziellen Regelungen und Meldepflichten der in 3 (1) genannten Rundschreiben.	
• **Passives Rückversicherungsmanagement** Es gelten die speziellen Regelungen und Meldepflichten der in 3 (1) genannten Rundschreiben. Sowohl Erst- als auch Rückversicherer haben zudem die Anforderungen der Finanzrückversicherungsverordnung zu berücksichtigen.	Zur Steuerung des passiven Rückversicherungsmanagements sollte das Unternehmen sich insbesondere mit folgenden Fragen auseinandersetzen: • Was ist der akzeptable Selbstbehalt je Geschäftsart und wie wurde er bestimmt (soweit möglich auf Basis des Einzelrisikos oder aggregierter Risiken)? • Berücksichtigt der Rückversicherungsvertrag die Möglichkeit mehrerer Ereignisse innerhalb einer Deckungsperiode, soweit erforderlich? • Welche Ausschlüsse sind in den Rückversicherungsverträgen enthalten? Decken sich diese mit den Ausschlüssen der Erstversicherungsverträge? Wie werden evtl. verbleibende Risiken abgedeckt? • Wie werden Instrumente des Alternativen Risikotransfers sowohl im Bereich der Rückversicherungsmarktprodukte (z.B. Finite Re), als auch auf dem Gebiet der Kapitalmarktprodukte (z.B. Securitisation, Derivate, Hedging) eingesetzt? • In welchen zeitlichen Abständen erfolgt eine Kontrolle der vollständigen Ausfinanzierung der Verpflichtungen von Versicherungs-Zweckgesellschaften (SPV)?

7.2.2.1 Neue Geschäftsfelder sowie Kapitalmarkt-, Versicherungs- und Rückversicherungsprodukte	
1 Die Risiken neuer Geschäftsfelder oder neuer Kapitalmarkt-, Versicherungs- und Rückversicherungsprodukte sind vorab auf ihre Auswirkung auf das Gesamtrisikoprofil zu untersuchen. Die Einschätzung der Risiken auf das Gesamtrisikoprofil ist ausreichend zu dokumentieren. Vor Anwendung oder Verkauf der neuen Produkte hat durch die Geschäftsleitung eine offizielle Freigabe zu erfolgen.	Am Ende eines „Produktentwicklungsprozesses" könnte beispielsweise ein Abschlussbericht stehen, der die allgemeinen Eigenschaften, die Preisfindung und das Produktdesign, die erwarteten Profitabilitätsergebnisse sowie deren Sensitivität bei Abweichungen in den Annahmen beinhaltet. Dabei sind Optionen und Garantien in den Produkten von besonderem Interesse. In allen Fällen sind die Entscheidungsfindung und das Ergebnis des Abschlussberichts hinreichend zu dokumentieren.
2 Neue Geschäftsfelder sind ihrem Risikogehalt entsprechend in das bestehende Risikomanagement des Unternehmens zu integrieren. Eine geeignete Anpassung der Organisation sowie der Steuerungs- und Kontrollprozesse ist zu gewährleisten.	Die Anpassung der Organisation sowie der Steuerungs- und Kontrollprozesse sollte so erfolgen, dass die Veränderungen in der Risikolage durch das neue Geschäftsfeld hinreichend transparent werden. Dies ist hinreichend zu dokumentieren und der unabhängigen Risikocontrollingfunktion zur Kenntnis zu geben.
7.2.2.2 Betriebliche Anreizsysteme und Ressourcen	
1 ~~Die Ausgestaltung der Anreizsysteme, insbesondere der Vergütungssysteme sowie die Zuteilung von finanziellen, personellen, sachlichen und technischen Ressourcen muss mit den in den Strategien niedergelegten Zielen in Einklang stehen; Änderungen der Strategien sind zu berücksichtigen. Anreizsysteme dürfen nicht manipulierbar sein. Sie müssen so ausgestaltet sein, dass negative Anreize vermieden werden (z.B. Interessenkonflikte oder das Eingehen unverhältnismäßig hoher Risikopositionen). Die Vergütungssysteme müssen sicherstellen, dass sich der variable Teil der Vergütung an dem langfristigen Erfolg des Unternehmens orientiert. Zusätzlich sind die wesentlichen Risiken und deren Zeithorizont angemessen zu berücksichtigen. Bei~~	Der Punkt 7.2.2.2 Unternummer 1 ist durch Rundschreiben 23/2009 vom 21.12.2009 aufgehoben.

	~~der Ausgestaltung der Vergütungssysteme einzelner Organisationseinheiten ist auch der gesamte Erfolg des Unternehmens angemessen zu berücksichtigen.~~	
2	Die Angemessenheit der den Geschäftsbereichen zur Verfügung gestellten Mittel ist in Bezug auf die eingegangenen und zu steuernden Risiken von deren Verantwortlichen im Hinblick auf vorgegebene Risikostrategien und innerbetriebliche Leitlinien zu bewerten und angemessen zu dokumentieren.	Als zur Verfügung gestellte Mittel kommen u.a. Budgets, qualifiziertes Personal und die technische Ausstattung in Betracht. Der jeweilige Verantwortliche ist z.B. der Leiter der Organisationseinheit. Beispiel: Wenn in den innerbetrieblichen Leitlinien eine wöchentliche Berichterstattung aller Geschäftsbereiche verankert wird, aber das IT-System nur eine monatliche Berichterstattung technisch zulässt, sollte dies der Geschäftsleitung berichtet werden.
3	Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Ihre Eignung ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.	Standards zur Ausgestaltung der IT-Systeme: Zu solchen Standards zählen z.B. das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der internationale Sicherheitsstandard ISO/IEC 27002 der International Standards Organization. Das Abstellen auf gängige Standards zielt nicht auf die Verwendung von Standardhardware beziehungsweise -software ab. Eigenentwicklungen sind grundsätzlich ebenso möglich.
4	Die IT-Systeme sind vor ihrem erstmaligen Einsatz und nach wesentlichen Veränderungen zu testen und von den fachlich sowie auch von den technisch zuständigen Mitarbeitern abzunehmen. Produktions- und Testumgebung sind dabei grundsätzlich voneinander zu trennen.	Veränderungen an IT-Systemen: Bei der Beurteilung der Wesentlichkeit von Veränderungen ist nicht auf den Umfang der Veränderungen, sondern auf die Auswirkungen, die eine Veränderung auf die Funktionsfähigkeit des betroffenen IT-Systems haben kann, abzustellen. Abnahme durch die technisch und fachlich zuständigen Mitarbeiter: Bei der Abnahme durch die fachlich und die technisch zuständigen Mitarbeiter steht die Eignung und Angemessenheit der IT-Systeme für die spezifische Situation des jeweiligen Unternehmens im Mittelpunkt. Ggfs. vorliegende Testate Dritter können bei der Abnahme berücksichtigt werden, sie können die Abnahme jedoch nicht vollständig

	ersetzen.
5 Die Entwicklung und Änderung programmtechnischer Vorgaben (z.B. Parameteranpassungen) sind unter Beteiligung der fachlich und technisch zuständigen Mitarbeiter durchzuführen. Die programmtechnische Freigabe hat grundsätzlich unabhängig vom Anwender zu erfolgen.	
6 Die vom Unternehmen eingesetzte Software - sowohl selbst erstellte als auch extern eingekaufte - hat den Anforderungen dieses Rundschreibens zu genügen.	
7.2.2.3 Organisationsentwicklung	
1 Der organisatorische Rahmen und das interne Steuerungs- und Kontrollsystem müssen in angemessener Zeit an die Änderungen des Umfelds angepasst werden. Hierfür sind Leitlinien zur Organisationsentwicklung aufzustellen.	

7.3 Internes Steuerungs- und Kontrollsystem	
7.3.1 Risikotragfähigkeitskonzept und Limitierung	
1 Auf Basis des unternehmensindividuellen Gesamtrisikos ist ein Risikotragfähigkeitskonzept zu erstellen, welches darlegt, wie viel Risikodeckungspotenzial insgesamt zur Verfügung steht und wie viel davon zur Abdeckung aller wesentlichen Risiken verwendet werden soll. Die Einhaltung der aufsichtsrechtlichen Kapitalausstattungsanforderungen bildet dabei die Untergrenze für die notwendige Risikotragfähigkeit. Unternehmen haben des Weiteren zu prüfen, ob die aufsichtsrechtlich geforderte Kapitalausstattung ausreichend ist, um ihrem aktuellen Gesamtrisiko und ihren strategischen Zielen gerecht zu werden.	Eine ausreichende Risikotragfähigkeit beschreibt im engeren Sinne somit die Fähigkeit des Unternehmens, Verluste aus identifizierten Risiken zu absorbieren, ohne dass daraus eine Gefahr für die Existenz des Unternehmens resultiert. Das Risikotragfähigkeitskonzept sollte daher immer verschiedene Anforderungsdimensionen des Risikomanagements berücksichtigen. Dazu gehören mindestens: 1) die Einhaltung aufsichtsrechtlicher Kapitalausstattungsanforderungen als Minimalanforderung, 2) die Bewertung durch Dritte, z.B. Ratingagenturen, 3) unternehmensinterne Ziele, 4) Rechnungslegungszwecke. Die Aufsicht wird für die von ihr vorzunehmende Beurteilung auch die Bewertung durch Dritte berücksichtigen, um Rückschlüsse auf mögliche Einflüsse auf das Risikomanagement des Unternehmens zu den Punkten 1 und 3 erkennen zu können. Dies jedoch nur dann, wenn diese auf umfassenden Informationen beruht.
2 Im Rahmen der strategischen Überlegungen hat die Geschäftsleitung die angestrebten Ertrags- bzw. Kapitalziele zu bestimmen und sich einen Überblick über das Gesamtrisikoprofil des Unternehmens auf Basis einer - soweit technisch möglich - ökonomischen Bewertung zu verschaffen. Entsprechend der Risikoneigung der Geschäftsleitung ist darauf aufbauend dann der Anteil an Risikodeckungspotenzial im Risikotragfähigkeitskonzept festzulegen, der tatsächlich zur Abdeckung der Risiken eingesetzt werden soll.	Sofern es um die Bestimmung aufsichtsrechtlicher Eigenmittel geht, sind vom Unternehmen die geltenden aufsichtsrechtlichen Anforderungen einzuhalten. Möchte das Unternehmen über das vorhandene hinaus weiteres Risikodeckungspotenzial darstellen, können für diesen Teil andere als die aufsichtsrechtlichen Maßstäbe herangezogen werden.

3	Die Methoden und Annahmen bei der Erstellung des Risikotragfähigkeitskonzeptes sind zu dokumentieren und nachvollziehbar zu begründen.	Zu den Annahmen zählen z.B. der Planungshorizont der Risikomessung, die Berücksichtigung von Konjunkturzyklen und zu den Methoden etwa die Behandlung von Diversifikationseffekten.
4	Die Annahmen zur Ermittlung des für die Abdeckung der Risiken notwendigen Risikodeckungspotenzials sind von der Geschäftsleitung zu dokumentieren und zu begründen. Die Höhe des ermittelten erforderlichen Betrags ist im Rahmen der Geschäftsstrategie, die die Geschäftsleitung zur Erreichung ihrer Ertrags- und Kapitalziele verfolgt, zu berücksichtigen und bei der Risikolimitierung darzulegen.	
5	Auf Basis der Risikotragfähigkeit ist ein konsistentes System von Limiten zur Risikobegrenzung zu installieren, welches die von der Geschäftsleitung im Einklang mit der Risikostrategie gesetzten Begrenzungen der Risiken auf die wichtigsten steuernden Organisationsbereiche des Unternehmens herunter bricht. Die Limitauslastung ist in Form von Risikokennzahlen darzustellen. Diese können sowohl quantitativer als auch qualitativer Natur sein. Die Risikokennzahlen sind auf Gesamtunternehmensebene zu aggregieren und mit dem Anteil an Risikodeckungspotenzial zu vergleichen, der zur Abdeckung der Risiken eingesetzt werden soll. Während des Geschäftsjahres ist die tatsächliche Risikobedeckung anhand von Risikokennzahlen regelmäßig zu kontrollieren und das Kontrollergebnis periodisch an die Geschäftsleitung zu berichten. Die Berichterstattung muss unabhängig erfolgen, d.h. sie darf nicht durch Personen vorgenommen werden, die selbst mittels dieser Risikokennzahlen operativ steuern. Die gewählten Limite müssen mit der von der Geschäftsleitung festgelegten Risikostrategie und dem Anteil an Risikodeckungspotenzial, der zur Abdeckung der Risiken eingesetzt werden soll, konsistent sein.	Limite sind Instrumente, um die gewählte Strategie unter Berücksichtigung der Risikotragfähigkeit umzusetzen. Sie ermöglichen dem jeweiligen Entscheidungsträger der steuernden Organisationsbereiche bewusst nur solche Risiken einzugehen, die im Einklang mit der Risikotragfähigkeit stehen. Die Limitierung kann auf Ebene von Organisationsbereichen, Produkten, Tarifen und Risikoarten erfolgen. Die Geschäftsleitung muss darlegen, inwieweit eine Steuerung auf der jeweiligen Ebene erfolgen kann und aus welchem Grund die angewandten Allokationsmethoden am besten zur Erfüllung der von ihr festgelegten Risikostrategie geeignet sind. Periodisch ist in diesem Zusammenhang als individuell abhängig vom Risiko zu interpretieren. Es liegt in der Entscheidung des Unternehmens festzulegen, wer die unabhängige Berichterstattung an die Geschäftsleitung durchführt.

6	Grundsätzlich müssen Limite auf allen relevanten Steuerungsebenen und für alle in 5 genannten Risiken - soweit diese das Unternehmen betreffen - existieren. Limite sind adressatenadäquat und - soweit möglich - spartenspezifisch auszuwählen und können deshalb auf den verschiedenen Steuerungsebenen unterschiedlich sein. Die Verantwortung für die adäquate Bestimmung und Vorgabe von wesentlichen Limiten für das Unternehmen liegt bei der Geschäftsleitung.	Limite sollten - soweit technisch möglich - quantitativer Natur sein. Eine quantitative Limitierung aller im Geschäftsbetrieb auftretenden Risiken (z.B. operationeller) ist insbesondere für kleine und mittlere Unternehmen nicht immer möglich. Hier lassen sich Verfahren und qualitative Regelungen zur Organisation der Risikobegrenzung einführen. Dies können z.B. Anweisungen, Notfallpläne, Schulungen sein.
7	Es ist sicherzustellen, dass alle mit Risiken behafteten Geschäfte auf die einschlägigen Limite angerechnet werden und der jeweilige Geschäftsbereich über die für ihn relevanten Limite und ihre Auslastung laufend und umfassend informiert ist.	Um die Risikotragfähigkeit jederzeit sicherzustellen, sollten die quantitativen Limite soweit als möglich „selbst verzehrend" sein, d.h. Verluste müssen neben den Risiken aus bereits bestehenden Geschäften auf das jeweilige Limit angerechnet werden. Dies hat zur Folge, dass das Limit nur einmal eingesetzt und ggf. verbraucht werden kann. Sollte im Ausnahmefall ein Limit durch Verluste vollständig aufgezehrt sein, können keine weiteren Geschäfte mehr auf dieses Limit abgeschlossen werden. Vielmehr hat die Geschäftsleitung in diesem Fall neu zu entscheiden, ob ein weiteres Limit erteilt werden kann oder ob die diesbezügliche Geschäftsaktivität auf das Limit eingestellt wird.
8	Die Einhaltung der Limite ist zu überwachen. Über Limitüberschreitungen und die deswegen ggf. getroffenen Maßnahmen ist Bericht zu erstatten. In dem Bericht sind Begründungen für die Limitüberschreitung und daraus abgeleitete Maßnahmen anzugeben. In innerbetrieblichen Leitlinien ist festzulegen, wer im Falle von Limitverletzungen wann und in welcher Form informiert werden muss, und welche Konsequenzen die Limitüberschreitung auslöst (Eskalationsverfahren).	Limite werden aus der Risikotragfähigkeit abgeleitet, ihre Auslastung ist anhand von geeigneten Risikokennzahlen laufend durch die unabhängige Risikocontrollingfunktion zu kontrollieren und das Ergebnis der Kontrolle ist periodisch an die Geschäftsleitung zu berichten. Sollten ausnahmsweise die vorgegebenen Limite überschritten werden, sind die in diesem Bereich eingegangenen Risiken im Rahmen eines durch die Geschäftsleitung festgelegten Verfahrens im Regelfall zurückzuführen. Dauer und Überschreitung der vorab definierten Schwellenwerte (z.B. Größenordnung, Dauer der Überschreitung) sind der Geschäftsleitung zu berichten. Beispiele für mögliche Limitierungen:

	• **Versicherungstechnische Risiken:** Begrenzungen z.B. durch VaR-Limite, Selbstbehalte, Zeichnungslimite, Kumulbudgets/ Kumullimite (besonders bei Naturgefahren oder in der Kreditversicherung), Rückversicherungslimite, • **Marktrisiken:** Begrenzungen z.B. durch VaR-Limite, Limite, die sich aus dem ALM-Prozess ergeben, Limite des Kursrisikos der Aktien, • **Kreditrisiken:** Begrenzungen z.B. durch VaR-Limite, Kontrahenten-, Emittenten-/Spread-Limite, Liquiditätsplanung/-limite, • **Operationelle Risiken:** Begrenzung z.B durch Versicherungen.
7.3.2 Risikokontrollprozess	
7.3.2.1 Risikoidentifikation	
1 Alle Risiken sind im Unternehmen konsistent zu definieren sowie strukturiert und systematisch unternehmensweit (in allen betrieblichen Prozessen, Funktionsbereichen und auf allen Hierarchieebenen) zeitnah aufzunehmen und zu klassifizieren. Interne wie externe Faktoren, die das Risiko beeinflussen (sog. **Risikotreiber**) sowie Bezugsgrößen, die von der Risikowirkung betroffen sind (sog. **Risikobezugsgröße**), sind zu definieren. Des Weiteren sind die konkreten Risikoursachen zu benennen. Darüber hinaus sind Wesentlichkeitsgrenzen für die Risikobeurteilung festzulegen. Zur Identifizierung der Risiken sind daher alle wesentlichen Risikotreiber, die die Risikolage des Unternehmens beeinflussen können, und - soweit für das Unternehmen relevant und mathematisch-technisch möglich - auch alle Abhängigkeiten zwischen den Risikotreibern regelmäßig zu erfassen. Die Risiken sind möglichst überschneidungsfrei zu definieren.	Dieser neue Risikoidentifizierungsprozess geht tiefer als der bisher nach KonTraG verlangte. Es geht hier nicht mehr nur um bestandsgefährdende Risiken, sondern um die Erstellung einer umfänglichen Grundlage für die Messung aller Risiken. Wichtig dabei ist, sämtliche Risiken zu erfassen, denn nicht erkannte Risiken entziehen sich der Einflussnahme durch das Risikomanagement. Risikotreiber sollten sowohl interne Faktoren, wie z.B. • die interne Struktur (Aufbau- und Ablauforganisation) und • unterschiedliche Geschäftsaktivitäten und Komplexität des Unternehmens als auch externe Faktoren, wie z.B. • branchenspezifische Veränderungen, • Veränderungen an den Kapitalmärkten, • neue bzw. veränderte rechtliche und regulatorische Anforderungen, • technische Weiterentwicklung

	berücksichtigen. Als Risikobezugsgrößen kommen beispielsweise Eigenmittel, Prämieneinnahmen oder verschiedene Ertragsgrößen in Betracht. Bezugsgrößen sollten so gewählt werden, dass sie die Wirkung der Risiken auf die Wirtschafts-, Finanz- oder Ertragslage des Unternehmens widerspiegeln. Beispiele für Methoden zur Risikoidentifikation sind u.a.: • strukturierte Assessments (z.B. Business-Plan-Risk-Assessment), • Szenariotechnik (definierte Szenarien unter exemplarischer Vorgabe von Störgrößen), • Checklisten, • standardisierte Fragebögen, • Trendanalysen, • Expertenschätzungen/Workshops, • Interviews, • Delphi Methode. Um eine möglichst vollständige Risikoidentifikation durchzuführen, bietet sich eine Kombination der vor genannten Methoden und Verfahren, abgestimmt auf das spezifische Risikoprofil des Unternehmens an.
2 Die Risikoidentifikation hat bereits im strategischen Planungsprozess zu beginnen und ist auf das Gesamtrisikoprofil des Unternehmens abzustimmen und in regelmäßigen Intervallen, mindestens jedoch einmal jährlich, zu wiederholen. Ändert das Unternehmen seine Strategien oder Ziele, so sind die Ergebnisse des Risikoidentifikationsprozesses hinsichtlich der geänderten Rahmenbedingungen zeitnah zu überprüfen und ggf. anzupassen.	Das Ergebnis des Risikoidentifikationsprozesses sollte systematisch in einer Risikobeschreibung, einem Risikokatalog oder einer Risikoinventarliste erfasst werden. Die Berichte sollten sich inhaltlich, formal und zeitlich nach den Anforderungen der Adressaten richten. Diese sollten mindestens detailliert Auskunft geben über: • Risikoart, • den/die verantwortlichen Geschäftsbereich/e, • die Risikotreiber (z.B. Aktienkurse),

	• die Risikobezugsgrößen, • mögliche Wechselwirkungen und Zusammenhänge mit anderen Risiken, • bereits eingeleitete bzw. laufende Maßnahmen, • derzeit bereits absehbare zukünftige Risikopotenziale. Der Mindeststandard ist eine einmalige jährliche Erfassung mit anschließender halbjährlicher Überprüfung. Zudem können je nach Gegebenheit und Bedarf zusätzlich Abweichungs- und Bedarfsberichte existieren.
3 Die Risikoidentifikation hat in allen Geschäftsbereichen des Unternehmens zu erfolgen.	
7.3.2.2 Risikoanalyse und –bewertung	
1 Aufbauend auf den Ergebnissen der Risikoidentifikation erfolgt die Analyse und Bewertung der Risiken. In Betracht gezogen werden nur Risiken, die bei der Risikoidentifikation erfasst wurden, unerkannte Risiken bleiben unberücksichtigt. Die Risikoanalyse und -bewertung hat grundsätzlich zu einer qualitativen und quantitativen Einschätzung potenzieller und realisierter Zielabweichungen sowohl durch die einzelnen Risiken, als auch durch das Gesamtrisiko zu führen. Zusätzlich ist die potenzielle Zielabweichung grundsätzlich in Abhängigkeit ihrer Risikotreiber zu bewerten.	
2 Die Risikoanalyse soll die identifizierten Risiken ihrer Wesentlichkeit nach und in die vom Unternehmen vorgegebenen Risikokategorien einordnen. Weiterhin sollte die Risikoanalyse aufzeigen, welche Bezugsgrößen betroffen sind sowie welche Korrelationen zwischen den identifizierten Risiken bestehen. Zur Analyse und Bewertung eines Risikos sind, soweit es die Art des Risi-	Aufbauend auf der Priorisierung nach Wesentlichkeit sowie der Einteilung der Risiken nach Risikokategorien und Bezugsgrößen kann das Unternehmen entscheiden, mit welcher Methodik die Risiken bewertet werden. Grundsätzlich sind geeignete Zufallsvariable und die entsprechenden Wahrscheinlichkeitsverteilungen zu bestimmen. Zur Ermittlung der

	kos (insbesondere seine Quantifizierbarkeit) und die vorhandene Datenbasis erlauben, Risikohöhen und zugehörige Eintrittswahrscheinlichkeiten sowie die Korrelation der wesentlichen Risiken zueinander in einem definierten Zeithorizont zu schätzen. Falls die Datenbasis für diese Schätzungen nicht vorhanden ist, ist sie aufzubauen.	Wahrscheinlichkeitsfunktion ist die Verteilung der Zufallsvariablen aus Vergangenheitsdaten zu bestimmen. Die Hintergründe für die Einschätzung sind auf Nachfrage zu erläutern. Es stehen hierfür sowohl empirische als auch analytische Methoden zur Verfügung. Sollte auf Grund der Datenbasis, der Art des Risikos oder anderer Faktoren eine Ermittlung nicht anhand mathematisch statistischer Methoden erfolgen, ist die Eintrittwahrscheinlichkeit wenigstens in Prozent durch Expertenschätzung vorzunehmen. Im Anschluss erfolgt die Risikobewertung. Anzuwendende Methoden sind beispielsweise die Fehlerbaumanalyse, die Sensitivitätsanalyse und die ABC-Analyse.
3	Die Risikobewertungsmethodik und die Bewertungshäufigkeit müssen dem Risiko angemessen sein und eine Aggregation der Ergebnisse ermöglichen. Das Unternehmen muss eine konsistente Datenanforderung für wesentliche Risiken erarbeiten. Die verwendeten Daten sind den Bedürfnissen der Risikosteuerung folgend adäquat zu der bestehenden Geschäfts- und Risikostruktur zu erheben. Die verwendeten Methoden und Verfahren zur Risikoanalyse und –bewertung sind spezifisch für die jeweiligen Risiken (vgl. 5) zu definieren.	Die Risikoanalyse und -bewertung kann anhand qualitativer und quantitativer Methoden erfolgen, beispielsweise anhand von Befragungstechniken, Stresstests und Sensitivitätsanalysen. Bei der Bewertung kann es erforderlich sein, zwischen Brutto- und Nettobewertung zu unterscheiden. Die Bruttobewertung ist eine Einschätzung der Risikosituation vor risikomindernden Maßnahmen. Die Nettobewertung berücksichtigt bestehende risikomindernde Maßnahmen.
4	Der Zeithorizont der Bewertung der Risiken hat im Einklang mit dem vom Unternehmen festgelegten Planungshorizont zu stehen, um eine konsistente Steuerung der zu ergreifenden Maßnahmen zu ermöglichen. Dennoch ist sicher zu stellen, dass er unter besonderen Umständen auf neue Gegebenheiten angepasst werden kann.	Aus Gründen der Vergleichbarkeit wird aus Sicht der Aufsicht als Mindeststandard eine Einjahresbetrachtung als Zeithorizont befürwortet. Der Zeithorizont für die Berechnung der aufsichtsrechtlich geforderten Solvabilitätsspanne kann vom Zeithorizont des intern zur Risikosteuerung genutzten Risikokapitals abweichen.
5	Es sind sinnvolle und widerspruchsfreie Kennzahlen zur Messung des Risikos zu verwenden.	Unter Kennzahlen sind nicht nur Verhältniszahlen zu verstehen, sondern auch absolute Größen. Widerspruchsfreie Kennzahlen basieren auf einer einheitlichen Grundlage und konsistenten Logik, da ansonsten eine aussagekräftige Aggregation nicht möglich ist.

6	Auf Basis der Bewertung ist eine Priorisierung und Kategorisierung der Risiken vorzunehmen, um für die Risiken angemessene Steuerungsmaßnahmen/-strategien abzuleiten.	Grundsätzlich sind alle wesentlichen Risiken mit entsprechenden Steuerungsmaßnahmen zu versehen. Die Reihenfolge der Bearbeitung kann jedoch z.B. anhand eines Rankings (A-, B-, C-, D-Risiken), das sich nach den Auswirkungen der Risiken auf das Unternehmen richtet, erfolgen. Eine Visualisierung kann beispielsweise in Form einer Risikolandkarte vorgenommen werden.
7	Basierend auf der Bewertung der Einzelrisiken ist eine Gesamtrisikobewertung für das Unternehmen zu definieren. Dabei sind Kumulationen/Konzentrationen und Interdependenzen sowohl innerhalb von Risiken als auch zwischen diesen zu berücksichtigen.	Risiken können zu einem festgelegten Zeitpunkt nach Unternehmensbereichen und/oder nach Risikoarten aggregiert werden. Eine vollständige Wahrscheinlichkeitsverteilung des Gesamtrisikos kann als Ziel zwar grundsätzlich vom Unternehmen angestrebt werden, muss aber für Risikosteuerungszwecke nicht notwendigerweise vorliegen.
8	Risikobewertung sollte in einem ersten Schritt immer qualitativ erfolgen. Erst nach Einschätzung auf einer Referenzskala des Unternehmens als wesentliches Risiko sollte eine Quantifizierung erfolgen. Nur für Risikoarten, für die eine quantitative Risikomessung ökonomisch nicht sinnvoll oder möglich ist, ist ausschließlich eine qualitative Einschätzung vorzunehmen. Im Falle einer nur qualitativen Einschätzung, ist dies ausführlich zu begründen.	
9	Das Ergebnis der Risikoanalyse und –bewertung ist der Ausweis aller für das Unternehmen bestehender Risiken und des dafür vorzuhaltenden Risikokapitals. Es ist sicherzustellen, dass die Geschäftsleitung über das aktuelle Gesamtrisikoprofil bzw. mögliche Verluste aus den für sie relevanten einzelnen Risiken informiert ist und mit Steuerungsmaßnahmen und Änderungen reagieren kann. Die Einschätzungen bzw. Handlungsempfehlungen der Geschäftsleitung sind den Geschäftsbereichen zeitnah mitzuteilen.	Im Ergebnis der Risikoanalyse und –bewertung werden (Netto-)Risikopositionen ermittelt, die im Rahmen der Risikosteuerung aktiv beeinflusst werden sollen. Die Steuerungsmaßnahmen zielen auf die Verringerung der Eintrittswahrscheinlichkeiten, z.B. durch Kontrollen oder die Begrenzung der Schadenhöhe, z.B. durch Risikotransfer, ab.

7.3.2.3 Risikosteuerung	
1 Die Risikosteuerung ist ein Teil des Risikomanagementprozesses. Unter Risikosteuerung wird das Treffen von Maßnahmen zur Risikohandhabung verstanden. Die Risikosteuerung umfasst demzufolge den Entwicklungs- und Umsetzungsprozess von Strategien und Konzepten, die darauf ausgerichtet sind, identifizierte und analysierte Risiken entweder bewusst zu akzeptieren, zu vermeiden oder zu reduzieren.	Unter Risikohandhabung werden konkrete Maßnahmen zur Risikovermeidung, -verminderung, -überwälzung und –übernahmen verstanden. Beispiele für konkrete Maßnahmen können z.B. verstärkte Kontrollen sein, die die Eintrittwahrscheinlichkeit des Risikos mindern oder aber eine Erhöhung des Rückversicherungsschutzes zur Begrenzung der Schadenhöhe. Mit Hilfe von Daten, Methoden und Verfahren können z.B. in der Risikosteuerung auch dynamische, pfadabhängige Managementregeln abgebildet werden. Darunter werden Steuerungsregeln verstanden, die auf Wechselwirkungen der Teilprozesse untereinander und mit dem Gesamtprozess reagieren. Managementregeln sollen eine Analysemöglichkeit darstellen und Handlungsalternativen aufzeigen; sie ersetzen aber nicht die Entscheidung der Geschäftsleitung. Grundsätzlich sind eingeführte Managementregeln von der Geschäftsleitung zu erläutern und zu dokumentieren.
2 Die auf der Risikostrategie basierende Risikosteuerung wird durch die Geschäftsbereiche wahrgenommen, die die Ergebnisverantwortung innehaben.	Die Verantwortung für den Aufbau von Risikopositionen kann prinzipiell an der mittelbaren und unmittelbaren Verantwortung für die Erzielung von Gewinnen gemessen werden.
3 Die strategischen Risikoziele sind für alle relevanten Geschäftsbereiche im Rahmen des Risikomanagements in operativ messbare Teilziele zu zerlegen. Die Teilziele sind hierbei konsistent zur Aufbau- und Ablauforganisation des Unternehmens festzulegen. Zur Überprüfung des Zielerreichungsgrades sind Risikokennzahlen einzusetzen. Es ist sicherzustellen, dass entsprechende Steuerungskennzahlen für alle Steuerungsebenen existieren und auf jeder Aggregationsstufe in sich und zu den erstellten Risikogrößen konsistent sind. Bei mehreren Steuerungsebenen sind die Steuerungskennzahlen sinnvoll zu aggregieren.	Gemeint sind in diesem Zusammenhang Risikoziele, die mit den angestrebten Geschäftszielen konsistent sind.

4	Die eingesetzten Steuerungskennzahlen müssen zu der jeweiligen Organisationseinheit passen, die die betrachteten Risiken abschätzt, aber auch innerhalb des Unternehmens vergleichbar sein. Die Steuerungskennzahlen müssen sich im Risikobericht wieder finden. Die Wirkungsweise dieser Kennzahlen sowie die Hintergründe für deren Einsatz müssen angemessen erläutert werden können.	Die Strukturierung z.B. des Kapitalanlagen- bzw. des (Rück-)Versicherungsgeschäfts mit Hilfe von Steuerungskennzahlen hängt stark von der Aufbau- und Ablauforganisation des Unternehmens ab. Die „Objekte" der Steuerung müssen perspektivisch festgelegt werden. Jede ermittelte Zahl ergibt nur Sinn, wenn sie einer klaren Verantwortlichkeit aus der operativen Steuerung zugeordnet werden kann. Es ist beispielsweise irrelevant, eine Analyse spartenbezogen separat nach Allgemeine Unfall, Hausrat, Feuer usw. durchzuführen, wenn jeder Kundengruppenverantwortliche eine Tarifhoheit für seinen Betreuungsbereich besitzt. Die Aufsicht wird beispielsweise auch Steuerungskennzahlen aus dem Controllingbericht und der Personalabteilung mit dem Risikobericht abgleichen, um zu prüfen, inwieweit die Steuerungskennzahlen sowie die Aufbau- und Ablauforganisation die Erreichung der gesetzten Ziele unterstützen.
5	Zur Risikosteuerung ist die Nettobewertung heranzuziehen. Mittels einer Gegenüberstellung der vorhandenen Nettorisikoposition (IST) mit der gewünschten Nettorisikoposition (SOLL) ist der Handlungsbedarf zur Verbesserung bestehender bzw. zusätzlicher Steuerungsmaßnahmen abzuleiten. Die Handlungsempfehlungen sind im Einklang mit der Risikostrategie zu treffen.	Stattfinden soll ein Abgleich zwischen der Risikoposition, die das Unternehmen gemäß Beschluss/Vorgabe der Geschäftsleitung eingehen soll (ggf. in Form eines Limits) und der aktuell tatsächlich bestehenden Risikoposition. Eingetretene Risiken sind ex-post auszuwerten und mit den Ergebnissen der ex-ante vorgenommenen Risikoanalysen und -bewertungen in regelmäßigen Abständen, mindestens jedoch einmal jährlich, zu vergleichen. Überschreitungen (auch kurzfristige) sind umgehend an die Geschäftsbereiche zu melden.
6	Sofern eine wesentliche Veränderung des Gesamtrisikoprofils oder eine aus Sicht des Unternehmens wesentliche Konzentration einzelner Risiken erkennbar wird, sind durch die verantwortlichen Geschäftsbereiche die Risikotreiber zu identifizieren und Risikokennzahlen nach ergriffenen Maßnahmen neu zu berechnen. Bei der Verwendung von Risikokennzahlen sind kritische Grenzen als Schwellenwerte zu benennen. Bei deren Überschreitung oder auch bei ungünstigen Trendentwicklungen sind ein-	Eine Ursachenanalyse dient als Voraussetzung der adäquaten Definition von Risikokennzahlen. Die Effektivität der Risikokennzahl wird wiederum beeinflusst durch die Messfrequenz. Die ständig aktualisierte Kenntnis der maximal vertretbaren (abgewickelten) Schadenquoten und Combined Ratios je Versicherungszweig wäre beispielsweise eine Risikokennzahl, mit der festegestellt werden kann, ob gerade noch eine Wertschöpfung erzielt wurde, d.h. die Kapitalkosten gedeckt sind.

deutige Meldewege zu definieren und zu dokumentieren oder die Geschäftsleitung damit zu befassen. In einem weiteren Schritt ist bei bestimmten Kriterienkombinationen oder Risikokennzahlen auf mögliche Gegen-/Steuerungsmaßnahmen bis hin zu Notfallplanungen zu verweisen.	Zur Visualisierung von Risikokennzahlen können Ampelsysteme dienen.
7.3.2.4 Risikoüberwachung	
1 Zur Überwachung aller identifizierten und analysierten Risiken gehört die Kontrolle von • Risikoprofil • Limiten • Umsetzung der Risikostrategie • Risikotragfähigkeit • risikorelevanten Methoden und Prozessen • Risikohandhabung.	Die regelmäßige Überwachung der identifizierten, analysierten und bewerteten Risiken bildet eine wesentliche Voraussetzung dafür, dass Mängel bei der Umsetzung der Risikostrategie sowie in den risikorelevanten Methoden und Prozessen aufgedeckt und korrigiert werden können. Dazu gehört ein angemessener Dokumentationsprozess.
2 Die Risikoüberwachung hat regelmäßig zu erfolgen und sollte sich am bestehenden unternehmensindividuellen Gesamtrisikoprofil orientieren sowie an der Häufigkeit und Art von Veränderungen des Geschäftsumfeldes.	
3 Die Risikoüberwachung ist durch die unabhängige Risikocontrollingfunktion durchzuführen und beinhaltet keine Steuerungsfunktion.	
7.3.3 Unternehmensinterne Kommunikation und Risikokultur	
1 Unternehmen müssen eine ausreichende unternehmensinterne Kommunikation über alle wesentlichen Risiken sicherstellen.	Unter Risikokultur versteht die Aufsicht den Umgang mit den unternehmensindividuellen Risiken. Die Risikokultur ist dabei entscheidend

Dies ist Aufgabe der Geschäftsleitung sowie der Führungskräfte und setzt eine angemessene Risikokultur innerhalb des Unternehmens voraus, die das Risikobewusstsein aller mit Risiken befassten Mitarbeiter schärft, eine ausreichende Risikotransparenz herstellt und den unternehmensinternen Dialog über Risikomanagementfragen fördert.	von der jeweiligen Unternehmenskultur geprägt. Entscheidend ist, dass die unternehmensindividuelle Risikokultur von der obersten Ebene her nach unten systematisch vorgelebt wird. Ein wesentlicher Bestandteil einer gelebten Risikokultur ist die Kommunikation von Risiken. Auch die Schaffung von Anreizsystemen für die Berichterstattung von Schäden/Verlusten bzw. die Benennung einer Vertrauensperson, bei der Schäden/Verluste gemeldet werden können, ist z.B. Teil einer gelebten Risikokultur. Daneben gewährleistet eine gelebte Risikokultur eine schnelle Anpassung an veränderte Rahmenbedingungen und verhindert bzw. begrenzt so Risiken schon vor ihrer Entstehung. Alle Mitarbeiter haben bei der Erledigung ihres Tagesgeschäfts risikobewusst im Sinne des unternehmensindividuellen Risikomanagements zu agieren. Dazu ist insbesondere auch eine angemessene Information des direkten Vorgesetzten über alle wesentlichen Risiken erforderlich, so dass dieser eine erste Steuerung dieser Risiken vornehmen kann. Diesem Ansatz liegt die Vorstellung zu Grunde, dass derjenige, der dem Risiko am Nächsten ist (z.B. der Vermittler bei Vertragsabschluss bzw. der Vorgesetzte des Vermittlers), auch den ersten steuernden und kontrollierenden Einfluss auf dieses Risiko hat. Es ist zu gewährleisten, dass aus der Kommunikation von Risiken den Betroffenen keine Nachteile entstehen. Dabei bleibt es den Unternehmen belassen, ob es offene Kommunikation pflegt und diese z.B. mit arbeitsrechtlichen Maßnahmen absichert oder Anonymität beim Reporting gewährleistet und so den Schutz der Beteiligten vor Benachteiligung sicher stellt.
7.3.4 Risikoberichterstattung	
1 Mit Ausnahme der in § 64a Abs. 5 VAG genannten Unternehmen muss jedes Unternehmen über eine aussagefähige Risikoberichterstattung im Sinne des § 64a Abs. 1 Satz 4 Nr. 3d) VAG verfügen. Im Rahmen der Risikoberichterstattung hat sich die Geschäftsleitung in angemessenen Abständen über das Gesamt-	Soweit sich im Hinblick auf Sachverhalte in vorangegangenen Berichterstattungen keine relevanten Änderungen ergeben haben, können im Rahmen der aktuellen Berichterstattung diese Informationen wiederholt aufgeführt werden. Diese können mit dem Zusatz: „Keine Änderung gegenüber der vorherigen Berichterstattung" versehen wer-

	risikoprofil berichten und darstellen zu lassen, inwieweit die in der Risikostrategie festgelegten Ziele des Risikomanagements erreicht wurden (Soll-Ist-Abgleich) und inwieweit die für die Risiken gesetzten Limite ausgelastet sind. Der Risikobericht hat entsprechend den Vorgaben des § 64a Abs. 1 Nr. 3d) VAG zu erfolgen. Außerdem muss in geeigneter Weise sichergestellt werden, dass die Führungsebene unterhalb der Geschäftsleitung die für ihren jeweiligen Verantwortungsbereich erforderlichen Informationen aus dem Risikobericht erhält. Im Rahmen der Risikoberichterstattung ist auch über sämtliche Vertragsbeziehungen mit Versicherungs-Zweckgesellschaften zu berichten. In den Bericht sind mindestens der Name und das Sitzland der Versicherungs-Zweckgesellschaft, der Umfang des übertragenen Risikos sowie die Konditionen für die Risikoübernahme aufzunehmen.	den. Da Risikoaspekte nicht isoliert von Ertrags- und Aufwandsaspekten diskutiert werden können, sollten Ertrags- und Aufwandsaspekte, soweit zum Verständnis der Risikoaspekte erforderlich, ebenfalls in die Risikoberichterstattung aufgenommen werden.
2	Darüber hinaus muss die Berichterstattung auch auf eventuelle Änderungen hinsichtlich der Methoden der Risikoidentifizierung, -analyse und -bewertung eingehen, wenn diese Ergebnisauswirkungen nach sich ziehen.	Die hier angesprochenen Änderungen schließen sowohl vergangenheits- als auch zukunftsbezogene Änderungen ein.
3	In die Risikoberichterstattung sind erforderlichenfalls Hinweise auf die Folgen wesentlicher unternehmensinterner Änderungen, eingeleiteter Maßnahmen zur Risikosteuerung oder Änderungen der Geschäftspolitik aufzunehmen.	Mögliche Handlungsalternativen zur Risikosteuerung sind von den Geschäftbereichen zu erarbeiten und den für das operative Geschäft Verantwortlichen zeitnah mitzuteilen.
4	Die Risikoberichterstattung ist in nachvollziehbarer, aussagefähiger Art und Weise zu verfassen. Sie hat neben einer Darstellung auch eine Beurteilung der Risikosituation zu enthalten.	Unternehmen sollen die gegenwärtige und, soweit ihnen bekannt, die zukünftige Risikosituation einschätzen.
5	Bei überraschenden Entwicklungen und extremen Ereignissen sind deren Ursachen und Auswirkungen darzustellen.	

6 Der Turnus der Risikoberichterstattung muss der Bedeutung der Risiken angemessen sein. Hierbei ist auch die Aufbau- und Ablauforganisation zu berücksichtigen. Die regelmäßige Risikoberichterstattung hat zumindest einmal jährlich zu erfolgen. In besonderen Situationen sind Ad-hoc-Berichte erforderlich.	Ist die Umsetzung von Handlungsempfehlungen in einem Geschäftsbereich z.B. sehr zeitintensiv, ist dies durch eine entsprechende Vorlaufzeit bei der Risikoberichterstattung zu berücksichtigen.
7 Die Geschäftsleitung muss jederzeit in der Lage sein, den Risikobericht zu erläutern. Für die von ihr gewollt eingegangenen Risiken muss die Geschäftsleitung erklären können, welche Handlungsalternativen im Entscheidungszeitpunkt vorgelegen haben und aus welchem Grund die Risikoübernahme präferiert wurde. Die Handlungsalternativen und Maßnahmen sind für die Aufsichtsorgane zu dokumentieren. Für die Führungsebene unterhalb der Geschäftsleitung bezieht sich die Pflicht auf ihren jeweiligen Verantwortungsbereich.	
7.3.5 Qualitätssicherung internes Steuerungs- und Kontrollsystem	
1 Die verwendeten Daten, Methoden und Verfahren des internen Steuerungs- und Kontrollsystems und ggf. notwendige Modifizierungen sind für einen sachkundigen Dritten verständlich und nachvollziehbar zu validieren und zu dokumentieren. Der Validierungsprozess ist von den einzelnen Unternehmen individuell festzulegen und abzunehmen. Er hat insbesondere die kontinuierliche Zweckmäßigkeit, Angemessenheit, Qualität, Vollständigkeit und Wirksamkeit von Daten, Methoden und Verfahren nachzuweisen.	

7.4 Interne Revision	
1 Mit Ausnahme der in § 64a Abs. 5 VAG genannten Unternehmen muss jedes Unternehmen als notwendigen Bestandteil einer ordnungsgemäßen Geschäftsorganisation über eine funktionsfähige interne Revision verfügen.	Die Anforderungen an die interne Revision sind funktionsbezogen, d.h. die Unternehmen müssen über eine Revisionsfunktion verfügen, aber nicht über eine eigene organisatorische Revisionseinheit. Die interne Revisionsfunktion kann auch ausgelagert werden. Insbesondere bei kleinen Unternehmen muss die interne Revision nicht notwendiger Weise das ganze Jahr tätig werden. Die Aufsicht setzt voraus, dass den Mitarbeitern der internen Revision die für ihre berufliche Praxis benötigten nationalen sowie internationalen Standards (z.B. Deutsches Institut für Interne Revision [IIR], The Institute of Internal Auditors [IIA]) bekannt sind und von ihnen angewandt werden.
2 Die Prüfung der internen Revision hat sich auf alle wesentlichen Aktivitäten der gesamten Geschäftsorganisation zu beziehen, insbesondere auch das Risikomanagement. Die Tätigkeit der internen Revision muss auf einem umfassenden und von ihr jährlich fortzuschreibenden Prüfungsplan basieren. Die Prüfungsplanung hat risikoorientiert zu erfolgen. Die Prüfungsplanung, -methoden und -qualität sind laufend zu überprüfen und weiterzuentwickeln. Die Prüfungsplanung sowie wesentliche Anpassungen sind von der Geschäftsleitung zu genehmigen.	
3 Die interne Revision muss ihre Aufgaben objektiv und unabhängig erfüllen können. Sie muss außerdem über ausreichendes und angemessen qualifiziertes Personal verfügen. Zur Wahrnehmung ihrer Aufgaben ist der internen Revision jederzeit ein vollständiges und uneingeschränktes Informations- und Prüfungsrecht einzuräumen. Die interne Revision untersteht lediglich den Weisungen der Geschäftsleitung. Sofern selbständige	Die Aufsicht legt die u.g. Begriffe wie folgt aus: • **Unabhängigkeit** Die interne Revision hat ihre Aufgaben selbständig und unabhängig wahrzunehmen. Insbesondere ist zu gewährleisten, dass sie bei der Prüfungsplanung, Berichterstattung und der Wertung der Prüfungsergebnisse keinen Weisungen unterworfen ist. Das

Revisionsabteilungen bei Konzerngesellschaften bestehen, sind diese gegenüber der Konzernrevision auskunfts- und informationspflichtig. Die Bestimmungen des allgemeinen Gesellschaftsrechts werden hiervon nicht berührt. Die Konzernrevision hat im Rahmen des Risikomanagements der Gruppe ergänzend zur internen Revision der Konzerngesellschaften tätig zu werden.	Direktionsrecht der Geschäftsleitung zur Anordnung von zusätzlichen Prüfungen steht der Selbständigkeit und Unabhängigkeit der internen Revision nicht entgegen. • **Funktionstrennung** Die in der internen Revision beschäftigten Mitarbeiter dürfen grundsätzlich nicht mit revisionsfremden Aufgaben betraut werden. Auf keinen Fall dürfen sie Aufgaben wahrnehmen, die mit der Prüfungstätigkeit nicht im Einklang stehen. Die interne Revision darf im Rahmen ihrer Aufgaben für die Geschäftsleitung oder andere Geschäftsbereiche des Unternehmens beratend tätig sein unter der Maßgabe, dass die Unabhängigkeit der internen Revision gewährleistet bleibt. Mitarbeiter, die in anderen Geschäftsbereichen des Unternehmens beschäftigt sind, dürfen grundsätzlich nicht mit Aufgaben der internen Revision betraut werden. Das schließt jedoch nicht aus, dass in begründeten Einzelfällen andere Mitarbeiter aufgrund ihres Spezialwissens zeitweise für die interne Revision tätig werden. • **Informations- und Prüfungsrecht** Zur Wahrnehmung ihrer Aufgaben ist der internen Revision jederzeit ein vollständiges und uneingeschränktes Informationsrecht einzuräumen. Der internen Revision sind insoweit unverzüglich die angeforderten Informationen zu erteilen, die notwendigen Unterlagen zur Verfügung zu stellen und Einblick in die Aktivitäten und Prozesse sowie die IT-Systeme des Unternehmens zu gewähren. Die interne Revision verfügt über ein unbeschränktes Prüfungsrecht. Die interne Revision des Konzerns erstreckt sich mindestens auf alle verbundenen Unternehmen im Sinne von § 271

	Abs. 2 HGB. • **Unterstellung der Geschäftsleitung** Die interne Revision ist ein Instrument der Geschäftsleitung, ihr unmittelbar unterstellt und berichtspflichtig. Sie kann auch einem Mitglied der Geschäftsleitung, nach Möglichkeit dem Vorsitzenden, unterstellt sein.
4 Eine Ausgliederung der Revisionsfunktion auf Externe oder ein Konzernunternehmen des Unternehmens i.S.d. § 18 des Aktiengesetzes ist vollständig oder teilweise auf Grundlage einer schriftlichen Vereinbarung zulässig (vgl. Nr. 8 dieses Rundschreibens). Bei einer Ausgliederung auf Externe hat sich das Unternehmen davon zu überzeugen, dass der Dritte über ausreichende Kenntnisse sowie über genügend Kapazitäten verfügt, um eine ordnungsgemäße Revisionstätigkeit zu gewährleisten. Die Geschäftsleitung hat im Fall einer Ausgliederung einen Revisionsbeauftragten zu benennen, der eine ordnungsgemäße Durchführung der internen Revision sicherstellen muss. Der Revisionsbeauftragte sollte entweder ein Geschäftsleiter oder ein Mitarbeiter mit ausreichenden Kenntnissen und der erforderlichen Unabhängigkeit sein. Die Aufgaben der internen Revision können vollständig durch die Konzernrevision wahrgenommen werden, sofern die erforderlichen Auskunftsrechte und Weisungsbefugnisse der Geschäftsleitung und die Berichtspflichten der Konzernrevision vertraglich gesichert sind. Der Prüfungsplan ist gemeinsam von dem Revisionsbeauftragten mit dem Externen zu erstellen. Der Revisionsbeauftragte hat ggf. gemeinsam mit dem Externen den Revisionsbericht zu verfassen und zu prüfen, ob die festgestellten Mängel zeitnah beseitigt wurden.	Die Aufgaben der internen Revision sind in der Regel von Unternehmensmitarbeitern wahrzunehmen. Eine Übertragung auf Externe kommt dann, wenn dies unter Risikoaspekten vertretbar ist, in Betracht. Im Falle einer Ausgliederung innerhalb des Konzerns erwartet die Aufsicht, dass das auslagernde Unternehmen ebenfalls einen Revisionsbeauftragten benennt.
5 Die Geschäftsleitung hat in innerbetrieblichen Leitlinien Aufgaben, Verantwortung, organisatorische Einbindung, Befugnisse	

	sowie Berichtspflichten der mit der internen Revision betrauten Personen sowie die Grundsätze der Unabhängigkeit, der Funktionstrennung und der vollständigen Informationspflicht gegenüber der internen Revision zu fixieren. Darüber hinaus haben alle Organisationseinheiten der internen Revision unverzüglich zu berichten, wenn wesentliche Mängel zu erkennen oder wesentliche finanzielle Schäden aufgetreten sind oder ein konkreter Verdacht auf Unregelmäßigkeiten besteht.	
6	Weisungen und Beschlüsse der Geschäftsleitung, die für die interne Revision von Bedeutung sein können, sind ihr unverzüglich bekannt zu geben. Über wesentliche organisatorische, prozessuale und ergebnisorientierte Änderungen ist die interne Revision rechtzeitig zu informieren.	
7	Über jede Prüfung muss von der internen Revision zeitnah ein schriftlicher Bericht angefertigt und grundsätzlich den fachlich zuständigen Mitgliedern der Geschäftsleitung vorgelegt werden. Der Bericht muss insbesondere eine Darstellung des Prüfungsgegenstandes und der Prüfungsfeststellungen, ggf. einschließlich der vorgesehenen Maßnahmen, enthalten. Dabei sind die Prüfungsergebnisse zu beurteilen; wesentliche Mängel sind besonders herauszustellen. Bei schwerwiegenden Mängeln muss der Bericht unverzüglich der Geschäftsleitung vorgelegt werden. Ergeben sich im Rahmen der Prüfungen schwerwiegende Feststellungen gegen Geschäftsleiter, so ist allen Geschäftsleitern unverzüglich Bericht zu erstatten. Das Unternehmen hat zu definieren, was wesentliche/schwerwiegende Mängel sind.	
8	Die interne Revision hat zeitnah einen Gesamtbericht über sämtliche von ihr im Laufe des Geschäftsjahres durchgeführten Prüfungen zu verfassen und allen Mitgliedern der Geschäftsleitung vorzulegen. Der Gesamtbericht muss über die festgestellten we-	Kriterien, nach denen die interne Revision ihre Feststellungen zu klassifizieren hat, sind beispielsweise die Schwere der Feststellungen, die betroffenen Geschäftsbereiche und die Art der Feststellungen.

sentlichen Mängel, deren Klassifizierung, die ergriffenen Maßnahmen sowie den Stand der Mängelbeseitigung informieren. Die interne Revision und die unabhängige Risikocontrollingfunktion haben sich regelmäßig über signifikante risikorelevante Sachverhalte und Entwicklungen auszutauschen, die wesentlichen Inhalte der Gespräche sind zu dokumentieren.	
9 Die interne Revision hat die fristgerechte Beseitigung der bei der Prüfung festgestellten Mängel in geeigneter Form zu überwachen und aktenkundig zu machen. Für den Fall der nicht termingerechten Beseitigung von Mängeln ist ein Eskalationsverfahren an die Geschäftsleitung einzurichten.	
7.5 Interne Kontrollen	
1 Zur Sicherstellung der Funktionsfähigkeit sämtlicher Bestandteile des Risikomanagementsystems sind dem Risiko entsprechende Kontrollen einzurichten. Die Funktionsfähigkeit der Kontrollen ist mindestens jährlich zu überwachen. Kontrollschwächen sind zu beurteilen und zeitnah zu beseitigen.	
8. Funktionsausgliederungen und Dienstleistungen im Sinne des § 64a Abs. 4 VAG	
1 Die teilweise oder vollständige Ausgliederung von Funktionen oder Dienstleistungen darf nur unter Maßgabe der in § 64a Abs. 4 VAG niedergelegten Grundsätze erfolgen. Ferner ist dieses Rundschreiben zu beachten.	Eine Funktionsausgliederung liegt gemäß § 5 Abs. 3 Nr. 4 VAG vor, wenn durch einen Vertrag der Vertrieb, die Bestandsverwaltung, die Leistungsbearbeitung, das Rechnungswesen, die Vermögensanlage, die Vermögensverwaltung oder die interne Revision eines Versicherungsunternehmens ganz oder zu einem wesentlichen Teil einem anderen Unternehmen auf Dauer übertragen wird. Unter Ausgliederung von Dienstleistungen ist die Ausgliederung sonstiger Funktionen, die nicht unter § 5 Abs. 3 Nr. 4 VAG fallen, zu verstehen. Grundsätzlich können damit alle Aktivitäten und Prozesse ausgegliedert werden,

	solange dadurch die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 64a VAG nicht beeinträchtigt wird. Die Ausgliederung darf nicht zu einer Delegation der Verantwortung der Geschäftsleitung an das Auslagerungsunternehmen führen. Die Leitungsaufgaben der Geschäftsleitung können nicht ausgegliedert werden.
2 Das Unternehmen muss auf der Grundlage einer Risikoanalyse eigenverantwortlich festlegen, welche Aktivitäten und Prozesse unter Risikogesichtspunkten überhaupt ausgegliedert werden können. Auf dieser Basis soll über eine Ausgliederung beschlossen werden. Die maßgeblichen Geschäftsbereiche sind bei der Erstellung der Risikoanalyse einzubeziehen. Im Rahmen ihrer Aufgaben ist auch die interne Revision zu beteiligen. Bei wesentlichen Änderungen der Risikosituation ist die Risikoanalyse anzupassen und ggf. die Ausgliederung zu beenden.	Aus Sicht der Aufsicht sind bei einer Ausgliederung nachfolgende Kriterien im Rahmen von vertraglichen Vereinbarungen zu beachten: • Spezifizierung und ggf. Abgrenzung der vom Unternehmen, auf das ausgegliedert wird, zu erbringenden Leistung, • Festlegung von Informations- und Prüfungsrechten der internen Revision sowie externer Prüfer, • Sicherstellung der Informations- und Prüfungsrechte sowie der Kontrollmöglichkeiten der Aufsicht, • Weisungsrechte, • Regelungen, die sicherstellen, dass datenschutzrechtliche Bestimmungen beachtet werden, • angemessene Kündigungsfristen, • Sicherstellung, dass das Unternehmen, auf das ausgegliedert wird, die versicherungsaufsichtsrechtlichen Anforderungen einhält, • Verpflichtung des ausgliedernden Unternehmens, das Unternehmen über Entwicklungen zu informieren, die die ordnungsgemäße Erledigung der ausgegliederten Aktivitäten und Prozesse beeinträchtigen.
3 Die mit der Ausgliederung verbundenen Risiken sind zu identifizieren, zu analysieren und zu bewerten und angemessen zu steuern und die Ausführung der ausgegliederten Aktivitäten und Prozesse ordnungsgemäß zu überwachen. Dies gilt insbesondere für operationelle Risiken. Zur Überwachung zählt auch die regelmäßige Beurteilung der Leistung des Unternehmens, auf das	Bei Beendigung ist z.B. sicher zu stellen, dass die Organisationsstruktur so vorbereitet wird, dass eine reibungslose Wiedereingliederung ohne Qualitätseinbußen erfolgen kann.

	ausgegliedert wird, anhand vorzuhaltender Kriterien. Für die Steuerung und Überwachung hat das Unternehmen klare Verantwortlichkeiten festzulegen. Das Unternehmen hat für den Fall der beabsichtigten Beendigung der Ausgliederungsvereinbarung Vorkehrungen zu treffen, um die Kontinuität und Qualität der ausgegliederten Aktivitäten und Prozesse auch nach Beendigung zu gewährleisten.	
4	Die Anforderungen an die Ausgliederung von Aktivitäten und Prozessen sind auch bei der Weiterverlagerung ausgegliederter Aktivitäten und Prozesse zu beachten.	
9. Notfallplanung		
1	Unternehmen haben Vorsorge (Notfallplanung) zu treffen für Störfälle, Notfälle und Krisen, in denen die Kontinuität der wichtigsten Unternehmensprozesse und –systeme nicht mehr gewährleistet ist und die normalen Organisations-/Entscheidungsstrukturen nicht mehr ausreichen, um sie zu beherrschen. Ziel der Notfallplanung ist die Fortführung der Geschäftstätigkeit mit Hilfe von definierten Verfahren und der Schutz von Personen und Sachen sowie Vermögen im Sinne der Wertschöpfung.	Wesentliche Elemente einer Notfallplanung sind neben dem Vorhalten eines Geschäftsfortführungs- bzw. Geschäftwiederaufnahmeplans auch die Festlegung der Kommunikationswege für Notfälle. Eine Notfallplanung muss nicht jede Aktivität im Unternehmen einbeziehen, sondern nur wesentliche Aktivitäten. Jedes Unternehmen hat individuell in innerbetrieblichen Leitlinien festzulegen, welche Störungen der Organisation, wie z.B. Versagen von IT-Systemen, unter welchen Umständen für das Unternehmen als wesentlich anzusehen sind.
2	Die Notfallplanung ist regelmäßig hinsichtlich Wirksamkeit und Angemessenheit zu überprüfen.	
3	Die Notfallplanung muss den beteiligten Geschäftsbereichen zur Verfügung gestellt werden.	Die Erstellung von geschäftsbezogenen Notfallplänen liegt jeweils in der Verantwortung des beteiligten Geschäftsbereiches. Unterstützung bei der Erstellung sollte durch eine zentrale Stelle erfolgen.

10. Information und Dokumentation	
1 Alle für die Funktionsfähigkeit des Risikomanagements wesentlichen Informationen müssen den Entscheidungsträgern exakt und vollständig zur Verfügung stehen. Wie gesteuert werden soll, ist dabei in Abstimmung mit der Strategie des Unternehmens festzulegen. Hinsichtlich der Dokumentation gelten die Anforderungen des § 64a Abs. 3 VAG. Die Dokumentation umfasst alle wesentlichen Formeln, Parameter, Methoden, Verfahren, Handlungen, Festlegungen, Entscheidungen und ggf. Begründungen sowie festgestellten Mängel und daraus gezogene Schlussfolgerungen. Wesentliche unterjährige Änderungen sind aufzuzeichnen und zeitnah innerhalb des Unternehmens zu kommunizieren. Die Dokumentation muss für sachverständige Dritte nachvollziehbar und überprüfbar sein.	Für das Risikomanagement in der Versicherungswirtschaft kommen eine Vielzahl von Daten und Informationen aus den verschiedensten betrieblichen Teilfunktionen und wissenschaftlichen Disziplinen infrage, z.B. • Vertrieb • Interne und externe Rechnungslegung • Unternehmensplanung, –entwicklung und -bewertung • Datenarchivierung und –sicherung • Asset Management, inklusive Kapitalmarktinformationen • Tarifierung, Produktentwicklung, Aktuariat • Schadenmanagement • Versicherungstechnische Bestandsführung • Mathematisch-statistische Verfahren Die Dokumentation soll einen systematischen Überblick über Risiken, Prozesse und Kontrollen geben. Die hier geschilderte Dokumentationspflicht stellt aus Sicht der Aufsicht keine abschließende Liste für den gem. § 55c VAG zu erstellenden Risikobericht dar, sondern benennt die Felder, die als Minimum dokumentiert werden müssen.