Recht & Regelungen

06.03.2020

Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von kleinen Versicherungsunternehmen nach § 211 VAG (MaGo für kleine VU)

Inhalt

Rundschreiben 01/2020 (VA)

1 Ziel des Rundschreibens

1 Dieses Rundschreiben gibt Hinweise zur Auslegung der Vorschriften über die Geschäftsorganisation im Versicherungsaufsichtsgesetz (VAG). Es legt diese Vorschriften für die BaFin verbindlich aus und gewährleistet hierdurch eine konsistente Anwendung gegenüber allen kleinen Versicherungsunternehmen.

2 Das Rundschreiben basiert auf dem Ansatz, dass die Geschäftsleiter (siehe Anmerkungen) eines kleinen Versicherungsunternehmens die Gesamtverantwortung für eine ordnungsgemäße und wirksame Geschäftsorganisation des Unternehmens tragen.

2 Anwendungsbereich und Begriffsdefinitionen

3 In den Anwendungsbereich dieses Rundschreibens fallen alle von der BaFin beaufsichtigten Erstversicherungsunternehmen, die die in § 211 VAG genannten Voraussetzungen erfüllen (im Folgenden: Unternehmen).

4 Im Rahmen dieses Rundschreibens wird einheitlich der Begriff Geschäftsorganisation verwendet. Der Begriff Geschäftsorganisation ist synonym zum Begriff Governance-System.

5 Der Begriff Geschäftsleitung bezieht sich auf den Vorstand eines Unternehmens. Soweit Unternehmen, die in den Anwendungsbereich dieses Rundschreibens fallen, kein Organ mit dieser Bezeichnung besitzen, tritt an die Stelle des Vorstandes das entsprechende Geschäftsführungsorgan. An die Stelle des Aufsichtsrates tritt unter denselben Voraussetzungen das entsprechende Überwachungsorgan.

3 Verhältnis des Rundschreibens zu anderen BaFin-Veröffentlichungen / Inkrafttreten

6 Bezüglich der Anforderungen an die fachliche Eignung und Zuverlässigkeit von Geschäftsleitern und Aufsichtsräten, wird auf das Merkblatt zur fachlichen Eignung und Zuverlässigkeit von Geschäftsleitern gemäß VAG und das Merkblatt zur fachlichen Eignung und Zuverlässigkeit von Mitgliedern von Verwaltungs- und Aufsichtsorganen gemäß VAG verwiesen.

7 Spezielle Anforderungen, die die BaFin im Rahmen anderer Veröffentlichungen an die Geschäftsorganisation von Unternehmen stellt, bleiben von den Anforderungen dieses Rundschreibens unberührt.
Dies gilt insbesondere für die Anforderungen an die Geschäftsorganisation gemäß:

- Rundschreiben 11/2018 (VA) – Zusammenarbeit mit Versicherungsvermittlern sowie zum Risikomanagement im Vertrieb,
- Rundschreiben 10/2018 (VA) – Versicherungsaufsichtliche Anforderungen an die IT (VAIT),
- Rundschreiben 11/2017 (VA) – Anlage des Sicherungsvermögens,
- Rundschreiben 8/2017 (VA) – Derivative Finanzinstrumente und strukturierte Produkte,
- Rundschreiben 7/2016 (VA) – Aufstellung und Führung des Vermögensverzeichnisses, Vorlage des Ausdrucks und Aufbewahrung des Sicherungsvermögens sowie
- Rundschreiben 3/2016 (VA) – Treuhänder zur Überwachung des Sicherungsvermögens.

8 Dieses Rundschreiben tritt am 01.04.2020 in Kraft.

4 Proportionalitätsprinzip

9 Bei der Umsetzung der Anforderungen an die Geschäftsorganisation spielt das Proportionalitätsprinzip eine erhebliche Rolle. Die Anforderungen sind auf eine Weise zu erfüllen, die der Wesensart, dem Umfang und der Komplexität der mit der Tätigkeit des Unternehmens einhergehenden Risiken gerecht wird (§ 296 Abs. 1 VAG). Das Proportionalitätsprinzip knüpft also an das individuelle Risikoprofil eines jeden Unternehmens an. Geringe Größe kann ein Indikator für ein schwächer ausgeprägtes Risikoprofil sein. Soweit die Mitarbeiterzahl

bei der Bestimmung der Größe eine Rolle spielen kann, ist nicht auf die vorhandenen Mitarbeiter abzustellen, sondern auf den tatsächlichen Mitarbeiterbedarf. Demnach sind auch externe Mitarbeiter, die für das Unternehmen im Wege der Ausgliederung Aufgaben übernehmen, in die Betrachtung einzubeziehen.

10 Proportionalität wirkt sich darauf aus, wie Anforderungen erfüllt werden können. So können bei Unternehmen mit schwächer ausgeprägtem Risikoprofil einfachere Strukturen und Prozesse ausreichend sein. Für die vom Anwendungsbereich dieses Rundschreibens erfassten Unternehmen ist die Umsetzung der festgelegten Mindestanforderungen regelmäßig ausreichend. Gehen jedoch einzelne Bereiche mit überdurchschnittlich hohen Risiken einher, erfordert das Proportionalitätsprinzip auch von diesen Unternehmen insoweit aufwändigere Strukturen und Prozesse.

11 Die Fragen, welche konkreten Strukturen und Prozesse einem bestimmten Risikoprofil angemessen sind sowie ob und gegebenenfalls welche begleitenden Maßnahmen erforderlich sind, können nur im jeweiligen Kontext beantwortet werden.

12 Die Einschätzung, welche Gestaltung als proportional anzusehen ist, ist in Bezug auf das einzelne Unternehmen nicht statisch, sondern passt sich im Zeitablauf den sich verändernden Gegebenheiten an. In diesem Sinne haben die Unternehmen bei veränderten Gegebenheiten zu prüfen, ob und wie die vorhandenen Strukturen und Prozesse weiterentwickelt werden können und gegebenenfalls müssen.

13 Haben Unternehmen das individuelle Risikoprofil bestimmt, bedarf es erst wieder einer erneuten Feststellung, wenn sich Veränderungen ergeben haben. Bis dahin wirkt die getroffene Feststellung fort.

5 Gesamtverantwortung der Geschäftsleitung

14 Alle Geschäftsleiter sind für eine ordnungsgemäße und wirksame Geschäftsorganisation verantwortlich. Die gesamte Geschäftsleitung ist damit auch dafür verantwortlich, dass das Unternehmen über ein dem Risikoprofil angemessenes und wirksames Risikomanagement- und internes Kontrollsystem verfügt. Beziehen sich Anforderungen dieses Rundschreibens ausdrücklich auf die gesamte Geschäftsleitung, kann diese ihre Verantwortung nicht delegieren, auch nicht auf einen oder mehrere Geschäftsleiter.

6 Wesentliche Risiken

15 Einzelne Anforderungen beziehen sich nicht auf sämtliche, sondern nur auf wesentliche Risiken. Die gesamte Geschäftsleitung beschließt zur Bestimmung der entsprechenden wesentlichen Risiken anhand geeigneter und nachvollziehbarer Kriterien dem Risikoprofil angemessene unternehmensindividuelle Wesentlichkeitsgrenzen. Die Angemessenheit der Wesentlichkeitsgrenzen ist fortlaufend sicherzustellen. Hierfür verschafft sich die gesamte Geschäftsleitung sowohl regelmäßig als auch anlassbezogen einen Überblick über alle Risiken, denen das Unternehmen tatsächlich oder möglicherweise ausgesetzt ist.

16 Separate Wesentlichkeitsgrenzen sind mindestens auf Ebene der folgenden Risikokategorien erforderlich: versicherungstechnisches Risiko und Marktrisiko.

17 Die Wesentlichkeitsgrenzen dürfen sich nicht ausschließlich an den Auswirkungen im Rahmen der Rechnungslegung oder den Auswirkungen von Rechtsverstößen orientieren.

18 Die Geschäftsleitung stellt sicher, dass die Wesentlichkeitsgrenzen einheitlich angewandt werden.

7 Risikokultur

19 Eine im Unternehmen gelebte Risikokultur bildet die Grundlage für ein dem Risikoprofil angemessenes und wirksames Risikomanagementsystem. Sie umfasst insbesondere:

- das Herstellen eines einheitlichen Verständnisses über die eigenen Risiken sowie den Umgang mit diesen, welches auf allen Hierarchieebenen sicherzustellen ist und sich in einer gemeinsamen Risikosprache äußert;
- das Festlegen der Verantwortlichkeiten beim Umgang mit Risiken zumindest für die Personen, die mit dem Aufbau sowie der Identifikation, Bewertung, Überwachung und Steuerung der wesentlichen Risiken betraut sind;
- das Prüfen, ob und welche Anreizstrukturen zum Umgang mit Risiken im Unternehmen geeignet sind und eingeführt werden;
- das Fördern eines offenen Dialoges aller betroffenen Personen im Unternehmen zum Umgang mit Risiken, so dass alle Personen die für sie relevanten Informationen rechtzeitig erhalten.

20 Die Risikokultur muss dem Risikoprofil angemessen sein. Sie schlägt sich nieder in den Normen des Unternehmens sowie den Einstellungen und Verhaltensweisen der Mitarbeiter. Sie wirkt sich auf das Risikobewusstsein, den Risikoappetit, die Risikosteuerung sowie die Risikokontrollen des Unternehmens aus und spiegelt sich in dessen Dokumentationen und schriftlichen Leitlinien wider.

21 Die gesamte Geschäftsleitung fördert die Risikokultur. Dabei kommt ihr eine Vorbildfunktion zu („Tone at the Top“). Sie sorgt dafür, dass die Risikokultur innerhalb des Unternehmens kommuniziert, beim Aufbau von Risiken beachtet und mit dem Risikomanagement und den internen Kontrollen verknüpft wird.

8 Allgemeine Anforderungen an die Geschäftsorganisation

8.1 Aufbau- und Ablauforganisation

8.1.1 Allgemeines

22 Die Unternehmen entscheiden unter Berücksichtigung ihres Risikoprofils und im Rahmen der einzuhaltenden Anforderungen, welche konkrete Organisationsstruktur für sie angemessen ist.

8.1.2 Festlegung von Aufgaben, Verantwortlichkeiten und Berichtslinien

23 Eine dem Risikoprofil des Unternehmens angemessene transparente Aufbauorganisation erfordert eine klare Definition und Abgrenzung von Aufgaben und Verantwortlichkeiten. Es ist eindeutig zu regeln, wer im Unternehmen für die Aufgaben zuständig ist und für Entscheidungen verantwortlich zeichnet.

24 Neben den Aufgaben und Verantwortlichkeiten sind auch Vertretungsregelungen und Berichtslinien klar festzulegen. Es ist sicherzustellen, dass alle Personen im Unternehmen die sie betreffenden Informationen unverzüglich erhalten und ihre Bedeutung erkennen können und eine Wahrnehmung der jeweiligen Aufgabe bzw. Verantwortlichkeit stets gewährleistet ist.

8.1.3 Angemessene Trennung der Zuständigkeiten

25 Die Organisationsstruktur eines Unternehmens muss eine dem Risikoprofil angemessene Trennung der Zuständigkeiten vorsehen, und zwar bis auf Ebene der Geschäftsleitung. Der Trennungsgrundsatz besagt unter anderem, dass der Aufbau wesentlicher Risiken einerseits und deren Überwachung und Kontrolle andererseits angemessen zu trennen sind. Wesentliche Risiken werden entsprechend dem Geschäftsmodell der von diesem Rundschreiben erfassten Unternehmen zumindest in den Bereichen Risikozeichnung und Kapitalanlage aufgebaut.

26 Unternehmen, die in den Anwendungsbereich dieses Rundschreibens fallen, weisen in der Regel eine angemessene Trennung der Zuständigkeiten auf, es sei denn, Interessenkonflikten wird nicht begegnet oder Aufgaben werden nicht objektiv oder nicht unabhängig wahrgenommen. Beispiel: Unter den genannten Voraussetzungen kann bei schwächer ausgeprägtem Risikoprofil ein Geschäftsleiter sowohl für die

Risikozeichnung als auch – allein oder mit den anderen Geschäftsleitern zusammen – für das Risikomanagement zuständig sein. Bisherige Erfahrungen zeigen, dass unternehmensindividuell sachgerechte Lösungen im Dialog mit der BaFin gefunden wurden.

8.1.4 Festlegung ablauforganisatorischer Regelungen

27 Die Ablauforganisation hat sicherzustellen, dass mit Risiken einhergehende Prozesse und deren Schnittstellen angemessen gesteuert und überwacht werden. Dies setzt zunächst voraus, dass alle Prozesse aus Risikosicht beurteilt werden.

28 Prozesse, die mit Risiken einhergehen, bestehen zumindest in den zuvor genannten Bereichen, die wesentliche Risiken aufbauen (siehe Rn. 25), sowie im Vertrieb, in der Reservierung (nach Handelsgesetzbuch – HGB), im Aktiv-Passiv-Management („Asset-Liability-Management" – ALM) und im passiven Rückversicherungsmanagement. Um eine angemessene Steuerung und Überwachung der identifizierten, mit Risiken einhergehenden Prozesse zu gewährleisten, sind vor allem die einzelnen Prozessschritte, einschließlich der erforderlichen Kontrollaktivitäten im Sinne des internen Kontrollsystems, und gegebenenfalls die Eskalationsschritte, die prozessspezifischen Zuständigkeiten und Verantwortlichkeiten sowie die Informationsflüsse klar festzulegen.

29 Im Hinblick auf die Kontrollaktivitäten ist es in der Regel nicht erforderlich, nach jedem einzelnen Prozessschritt umfangreiche Kontrollen durchzuführen. In jedem Fall sind jedoch besonders risikobehaftete Prozessschritte zu identifizieren und regelmäßig zu kontrollieren.

8.1.5 Umsetzung ablauforganisatorischer Regelungen

30 Für die ordnungsgemäße Erfüllung ihrer Aufgaben ist es wichtig, dass alle relevanten Mitarbeiter die sie betreffenden Arbeitsabläufe kennen, das heißt, diesbezüglich informiert und mit diesen inhaltlich vertraut sind.

8.1.6 Dokumentation der Aufbau- und Ablauforganisation

31 Die Dokumentation der Aufbau- und Ablauforganisation ist stets auf aktuellem Stand vorzuhalten. Vorgängerversionen sind mindestens sechs Jahre aufzubewahren.

8.2 Geschäftsleitung und Aufsichtsrat

32 Die Geschäftsorganisation umfasst Prozesse zur regelmäßigen und Ad-hoc-Übermittlung von Informationen und Berichten der Organisationseinheiten und Funktionen an die Geschäftsleitung. Auf dieser Basis sowie aufgrund entsprechender Beratung nimmt die Geschäftsleitung ihre Leitungsaufgaben wahr und trifft Entscheidungen. Ebenso wichtig wie Prozesse zur Übermittlung von Informationen und Berichten an die Geschäftsleitung sind Prozesse, die sicherstellen, dass die bearbeitenden Stellen über die getroffenen Entscheidungen so informiert werden, dass diese vollständig umgesetzt werden können.

33 Der Aufsichtsrat nimmt die ihm zur Erfüllung seiner Aufgaben eingeräumten Informations-, Einsichts- und Prüfungsrechte aktiv wahr und berät die Geschäftsleitung unter anderem in strategischen Fragen. § 210 VAG bleibt unberührt.

8.2.1 Vier-Augen-Prinzip

34 Die Unternehmen haben dafür Sorge zu tragen, dass die tatsächliche Leitung des Unternehmens durch mindestens zwei Personen erfolgt. Dies impliziert, dass an jeder wesentlichen Entscheidung des Unternehmens mindestens zwei Personen, die das Unternehmen tatsächlich leiten, beteiligt sind, bevor die betreffende Entscheidung umgesetzt wird.

35 Das Unternehmen legt eigenverantwortlich fest, welche Entscheidungen mit Blick auf das Geschäftsmodell und das individuelle Risikoprofil als wesentlich einzustufen sind. Als wesentliche Entscheidungen können solche gewertet werden, die erhebliche Auswirkungen auf das Unternehmen haben beziehungsweise haben können oder gemessen am regulären Geschäftsbetrieb außergewöhnlich sind.

8.2.2 Dokumentation

36 Die Geschäftsleitung hat die von ihr getroffenen Entscheidungen sowie die Art und Weise, wie Informationen aus dem Risikomanagement berücksichtigt werden (siehe hierzu unter 9.1), zu dokumentieren.

37 Ein Mindestniveau der Ausgestaltung der Dokumentation kann nicht pauschal vorgegeben werden. Umfang und Detailtiefe der Dokumentation von Entscheidungen der Geschäftsleitung sind vom Zweck der Dokumentation und von den mit der jeweiligen Entscheidung verbundenen Risiken abhängig. Daher ist die Ausgestaltung der Dokumentation im Einzelfall aufgrund einer ganzheitlichen Betrachtung unter den Gesichtspunkten Selbstkontrolle und Nutzen festzulegen. Ein vollständiger Verzicht auf die Dokumentation kommt jedoch nicht in Betracht.

38 Die Dokumentation ist ausreichend, wenn sie so vollständig und exakt und mit den wesentlichen Hintergrundinformationen (z. B. Formeln, Parameter, Entscheidungen unterhalb der Geschäftsleitung, deren wesentlichen Begründungen) angereichert ist, dass eine fachkundige Person die Entscheidung der Geschäftsleitung inhaltlich nachvollziehen und überprüfen kann.

39 Es ist nicht zwangsläufig erforderlich, insgesamt neue Unterlagen zu schaffen. Verweisungen auf vorhandene Unterlagen und deren Beifügung können genügen, solange und soweit diese nachvollziehbar und verständlich sind.

8.3 Interne Überprüfung der Geschäftsorganisation

40 Die gesamte Geschäftsleitung bewertet die Geschäftsorganisation regelmäßig (§ 23 Abs. 2 VAG), wobei der Turnus der Bewertung entsprechend dem Risikoprofil festzulegen ist, und sorgt für eine kurzfristige Umsetzung der erforderlichen Änderungen. Die Bewertung einzelner Bereiche der Geschäftsorganisation kann durch das hierfür zuständige Mitglied der Geschäftsleitung erfolgen. Die gesamte Geschäftsleitung muss jedoch im Rahmen der Gesamtverantwortung das Ergebnis dieser Bewertung kennen und die resultierende Umsetzung steuern. Daher muss jeder Geschäftsleiter zumindest die wesentlichen Risiken verstehen, denen das Unternehmen ausgesetzt ist. Das Ergebnis der Bewertung sowie die Umsetzung notwendiger Änderungen sind zu dokumentieren.

41 Die Bewertung bezieht sich gesamthaft auf die Geschäftsorganisation. Die Bewertung baut auf bereits vorhandenen Erkenntnissen auf, die etwa bei der Überprüfung der Leitlinien gewonnen wurden. Die Geschäftsleitung bewertet insbesondere vorausschauend, ob die Geschäftsorganisation die Ziele der Geschäfts- und der Risikostrategie unterstützt.

42 Ein gesonderter Prozess ist nicht erforderlich.

43 Die gesamte Geschäftsleitung legt die Anlässe für außerordentliche Bewertungen der Geschäftsorganisation fest.

8.4 Schriftliche Leitlinien

44 Die schriftlichen Leitlinien sind ein Instrument der Geschäftsleitung, das unter anderem sicherstellt, dass die Organisationseinheiten entsprechend ihren Aufgaben und Pflichten sowie effektiv und zielgerichtet vorgehen. Schriftliche Leitlinien dienen auch dazu, die prinzipienorientierten gesetzlichen Vorgaben für das Unternehmen operativ umzusetzen.

8.4.1 Allgemeines

45 In der formalen Ausgestaltung der schriftlichen Leitlinien sind die Unternehmen frei. Enthalten bereits bestehende Dokumente die vorgegebenen Inhalte der Leitlinien, können sie als Leitlinien herangezogen und verwendet werden.

46 Die praktische Umsetzung der schriftlichen Leitlinien erfolgt durch entsprechende Arbeitsabläufe. Es ist festzulegen, auf welcher Ebene die Verantwortung für diese Arbeitsabläufe liegt.

8.4.2 Inhalte der schriftlichen Leitlinien

47 Die schriftlichen Leitlinien müssen die grundlegenden ablauforganisatorischen Regelungen, die Zuständigkeiten, die Befugnisse und die Berichtsverfahren klar darstellen.

48 Um Aufgabenüberschneidungen zu vermeiden, sind auch entsprechende Schnittstellen und Abgrenzungen in den jeweiligen schriftlichen Leitlinien anzugeben.

49 Die schriftlichen Leitlinien müssen aufeinander und auf die Geschäfts- und die Risikostrategie abgestimmt sein.

8.4.3 Verabschiedung und Überprüfung der schriftlichen Leitlinien

50 Die Mindestanforderungen dieses Kapitels 8.4.3 gelten für die schriftlichen Leitlinien im Sinne des § 23 Abs. 3 Satz 2 VAG zur Geschäftsorganisation. Die Mindestanforderungen gelten nicht für die die Leitlinien umsetzenden Arbeitsabläufe.

51 Zur Unterstützung der von ihr festzulegenden Geschäfts- und Risikostrategie hat die gesamte Geschäftsleitung den schriftlichen Leitlinien bei der Erstverabschiedung sowie bei wesentlichen Änderungen zuzustimmen.

52 Die in § 23 Abs. 3 Satz 2 VAG aufgeführten schriftlichen Leitlinien zum Risikomanagement, zum internen Kontrollsystem und zur Ausgliederung müssen mit dem Risikoprofil angemessenen Methoden mindestens einmal jährlich überprüft werden. Die Überprüfung kann bei schwächer ausgeprägtem Risikoprofil und stabilem Geschäftsmodell sehr einfach und unbürokratisch erfolgen. Die Anlässe für Ad-hoc-Überprüfungen der einzelnen Leitlinien legt die gesamte Geschäftsleitung fest.

53 Die für die Überprüfung der schriftlichen Leitlinien zuständigen Personen oder Organisationseinheiten sind zu benennen. Bei der Überprüfung ist zu berücksichtigen, dass Änderungen einer schriftlichen Leitlinie direkte Auswirkungen auf die anderen schriftlichen Leitlinien haben können.

54 Die Überprüfungen der schriftlichen Leitlinien müssen dokumentiert werden. Die Ergebnisse der Überprüfung und der sich daraus gegebenenfalls ergebende Änderungsbedarf werden an die Geschäftsleitung berichtet.

55 Im Falle eines festgestellten wesentlichen Änderungsbedarfs einer schriftlichen Leitlinie wird der gesamten Geschäftsleitung berichtet, die ihre entsprechende Entscheidung kurz, aber nachvollziehbar begründet. Die Entscheidung einschließlich der Begründung ist zu dokumentieren. Besteht kein oder kein wesentlicher Änderungsbedarf, reicht eine Kenntnisnahme durch den zuständigen Geschäftsleiter aus, die zu dokumentieren ist.

8.4.4 Kenntnis und Einhaltung schriftlicher Leitlinien

56 Die Mitarbeiter müssen über die sie betreffenden schriftlichen Leitlinien in der jeweils aktuellen Fassung informiert werden.

57 Die Unternehmen führen interne Kontrollen ein, die sicherstellen, dass entsprechend den schriftlichen Leitlinien gehandelt wird bzw. Verstöße zeitnah bekannt werden.

8.5 Automatisierte Geschäftsabläufe

58 Im Kontext der im Rundschreiben 10/2018 (VA) definierten aufsichtlichen Anforderungen an die IT, die unberührt bleiben, hat die Aufbau- und Ablauforganisation sicherzustellen, dass mit Risiken einhergehende automatisierte Geschäftsabläufe, zu denen auch die automatisierte Risikozeichnung, die automatisierten Einzelfallentscheidungen bei der Bearbeitung von Schadens- und Leistungsfällen sowie die automatisierte Bestandsverwaltung gehören, angemessen gesteuert und überwacht und die Anforderungen an die Geschäftsorganisation erfüllt werden. Dies setzt neben der Beurteilung der automatisierten Geschäftsabläufe aus Risikosicht insbesondere voraus, dass alle automatisierten Geschäftsabläufe identifizierbar und nachvollziehbar sind und sichergestellt wird, dass die gesamte Geschäftsleitung in Grundzügen über die Einrichtung, die Ausgestaltung und die Funktionsfähigkeit der automatisierten Geschäftsabläufe informiert ist.

9 Risikomanagementsystem

9.1 Rolle der Geschäftsleitung im Risikomanagementsystem

59 Die gesamte Geschäftsleitung ist dafür verantwortlich, dass das Risikomanagementsystem dem Risikoprofil angemessen und wirksam ausgestaltet ist.

60 Dies schließt angemessene Berichtsverfahren und Prozesse ein, die insbesondere gewährleisten, dass zumindest über alle wesentlichen Risiken informiert, die Wirksamkeit des Risikomanagementsystems aktiv überwacht und analysiert sowie gegebenenfalls verbessert wird.

61 Die Verantwortung der gesamten Geschäftsleitung entbindet den Aufsichtsrat nicht von der Pflicht zu überwachen, ob die gesamte Geschäftsleitung ein angemessenes und wirksames Risikomanagementsystem eingerichtet hat.

62 Die Verantwortung der gesamten Geschäftsleitung für das Risikomanagementsystem bezieht sich auf die Leitungsaufgaben. Die Leitungsaufgaben umfassen unter anderem die strategischen Entscheidungen und die Festlegungen zum organisatorischen Rahmen des Risikomanagements, somit insbesondere auch den Eingang und die Handhabe wesentlicher Risiken.

63 Zu den Leitungsaufgaben zählt ebenfalls die Entwicklung einer Risikostrategie. Diese ist mindestens einmal jährlich zu überprüfen und gegebenenfalls anzupassen. Die Risikostrategie, die Überprüfung und etwaige Änderungen sind zu dokumentieren. Die Risikostrategie stellt die sich aus der Geschäftsstrategie ergebenden Risiken dar. Sie enthält zudem eine Aussage zum Risikoappetit, den das Unternehmen sowohl auf aggregierter Ebene als auch auf Ebene der wesentlichen Risiken besitzt, um die strategischen Ziele zu erreichen. Die Risikostrategie ist so auszugestalten, dass sich die operative Steuerung der Risiken daran anknüpfen lässt.

64 Die gesamte Geschäftsleitung und gegebenenfalls der zuständige Geschäftsleiter muss bei eigenen Entscheidungen die Informationen aus dem Risikomanagementsystem gebührend berücksichtigen.

9.2 Risikomanagementleitlinien

65 Die schriftlichen Leitlinien zum Risikomanagement enthalten mindestens Vorgaben zu den in § 26 Abs. 5 Satz 1 VAG genannten Bereichen. Sie definieren und kategorisieren zumindest die wesentlichen Risiken, falls diese Festlegungen nicht in der Risikostrategie erfolgen. Auch benennen die schriftlichen Leitlinien zum Risikomanagement die Risikotoleranzschwellen zumindest für die wesentlichen Risiken.

9.2.1 Risikomanagementleitlinien für das operationelle Risiko

66 Operationelle Risiken im Rahmen des Risikomanagements umfassen unter anderem IT-Risiken, unabhängig davon, ob sie aus der IT-Aufbauorganisation, den IT-Systemen oder den IT-Prozessen resultieren.

67 Operationelle Risiken im Rahmen des Risikomanagements schließen auch die Rechtsrisiken ein.

68 Rechtsänderungsrisiken, zumindest diejenigen, die mit in der Vergangenheit abgeschlossenen Geschäften verbunden sind, müssen unter Risikogesichtspunkten adäquat berücksichtigt werden. Rechtsänderungsrisiken bezeichnen dabei Risiken, die sich aufgrund einer Änderung des Rechtsumfeldes einschließlich der aufsichtsbehördlichen Anforderungen ergeben.

69 Eine Analyse operationeller Risiken ist auch vor der Einführung oder wesentlichen Änderung von Produkten, Prozessen und Systemen durchzuführen. Die Ergebnisse dieser Analyse sind in die Entscheidungsfindung einzubeziehen.

70 Zur Identifizierung und Überwachung möglicher operationeller Risiken implementieren die Unternehmen einen geeigneten Prozess, mit dem zumindest die internen Schadenereignisse erfasst und ausgewertet werden. Hierfür sind dem Risikoprofil angemessene Schwellenwerte festzulegen. Die notwendigen Prozessschritte sind ausreichend zu dokumentieren.

71 Bei der Identifizierung möglicher operationeller Risiken berücksichtigen die Unternehmen darüber hinaus auch bekannte externe Schadenereignisse.

72 Die Unternehmen prüfen, ob sie als Teil ihres Frühwarnsystems geeignete Risikokennziffern (Key Risk Indikatoren) oder Leistungskennziffern (Key Performance Indikatoren) einführen.

73 Wesentliche Schadenereignisse, die aus operationellen Risiken resultieren, sind der gesamten Geschäftsleitung unverzüglich zu berichten und hinsichtlich ihrer Ursachen zu analysieren. Welche Schadenereignisse hierunter fallen, ist unternehmensindividuell festzulegen. Die gesamte Geschäftsleitung entscheidet bei wesentlichen Schadenereignissen, ob und welche zusätzlichen Maßnahmen zu ergreifen sind. Die Umsetzung der Maßnahmen ist zu überwachen.

9.2.2 Risikomanagementleitlinien für Rückversicherung und andere Risikominderungstechniken

74 Die Risikomanagementleitlinien für Rückversicherung und andere Risikominderungstechniken benennen den angestrebten Grad des Risikotransfers. Dieser muss sich an den festgelegten Risikotoleranzschwellen orientieren. Anzugeben ist ferner, welche Art der Rückversicherung oder anderer Risikominderungstechniken vom Unternehmen gewählt wird. Die gewählte Art muss für das eigene Risikoprofil am besten geeignet sein. Auch sind die Kriterien für die Auswahl der Rückversicherung oder anderer Risikominderungstechniken festzulegen.

75 Es sind Grundsätze für die Auswahl der Vertragspartner bei Rückversicherungsverträgen und anderen Risikominderungstechniken zu entwickeln. Diese umfassen auch Verfahren, um die Leistungsfähigkeit und Kreditwürdigkeit von Rückversicherern und anderen Risikominderungspartnern zu bewerten und zu überwachen.

76 Entscheidet sich das Unternehmen für Rückversicherung oder andere Risikominderungstechniken, berücksichtigt das Risikomanagement sämtliche damit verbundenen Risiken, insbesondere auch das mit der Risikominderungstechnik verbundene Kreditrisiko. Dies schließt eine Dokumentation zumindest der wesentlichen Risiken, der daraus resultierenden Maßnahmen sowie der potentiellen Folgen ein. Zudem ermittelt und bewertet das Unternehmen sowohl den Umfang als auch die Wirkung des Risikotransfers.

77 In Bezug auf Rückversicherung und andere Risikominderungstechniken berücksichtigt das Liquiditätsmanagement auch mögliche Liquiditätsengpässe infolge eines zeitlichen Auseinanderfallens der zu erbringenden Versicherungsleistung und dem Eingang der Zahlung der von Rückversicherern und anderen Risikominderungspartnern einforderbaren Beträge.

10 Internes Kontrollsystem

10.1 Allgemeines

78 Das interne Kontrollsystem gewährleistet insbesondere eine angemessene und wirksame Funktionsweise der Geschäftsorganisation. Des Weiteren stellt es die Verfügbarkeit und Verlässlichkeit der für den Geschäftsbetrieb notwendigen Informationen sicher.

79 Die Unternehmen gestalten das interne Kontrollsystem in Abhängigkeit von ihrem Risikoprofil aus. Das interne Kontrollsystem ist ein eigenständiges Element der Geschäftsorganisation. Es muss adäquat in die Strukturen und Prozesse der Aufbau- und Ablauforganisation eingebunden sein, damit es seinen Zweck erfüllt.

80 Das interne Kontrollsystem berücksichtigt gegebenenfalls auch ausgegliederte Bereiche und Prozesse.

10.2 Interner Kontrollrahmen und Melderegelungen

81 Die Unternehmen legen im internen Kontrollrahmen die Grundsätze, Verfahren und Maßnahmen zu den internen Kontrollen fest. Der interne Kontrollrahmen muss dem Risikoprofil angemessen sein.

82 Insbesondere Art, Häufigkeit und Umfang der internen Kontrollen orientieren sich an den Risiken der jeweiligen Bereiche und Prozesse.

83 Die Unternehmen gewährleisten, dass die mit den internen Kontrollen beauftragten Personenüber alle notwendigen Informationen verfügen.

84 Die Eignung und Wirksamkeit der internen Kontrollen sind mit Hilfe geeigneter Verfahren fortlaufend zu überwachen.

85 Die gesamte Geschäftsleitung lässt sich regelmäßig, mindestens jährlich, über die Ergebnisse der Überwachung berichten. In besonderen Situationen, vor allem bei erheblichen Mängeln der internen Kontrollen, sind außerdem Ad-hoc-Berichte erforderlich. Die Geschäftsleitung stellt sicher, dass die notwendigen Anpassungen zeitnah umgesetzt werden.

10.3 Einhaltung der Anforderungen und externer Standards

86 Die Unternehmen haben im Rahmen ihres internen Kontrollsystems die Einhaltung der zu beachtenden Gesetze und Verordnungen, aufsichtsbehördlichen Anforderungen sowie externen Standards sicherzustellen.

87 Zu beachten im Sinne der Rn. 86 sind nur solche externen Standards, die für die Unternehmen von großer Bedeutung sind oder mit wesentlichen Risiken einhergehen und von national oder international anerkannten Akteuren stammen, die in dem Bereich, zu dem sie Standards aufstellen, über die notwendige hohe Fachkompetenz verfügen. Als nicht abschließende Beispiele für anerkannte Standardsetzer seien etwa das Bundesamt für Sicherheit in der Informationstechnik, das Deutsche Institut für Normung oder die Internationale Organisation für Normung genannt. Auf welche externen Standards diese Kriterien zutreffen, ist, auch unter Anwendung des Proportionalitätsprinzips, unternehmensindividuell festzulegen. Die identifizierten externen Standards sind den betreffenden Mitarbeitern mitzuteilen, etwa in den schriftlichen Leitlinien.

88 Die Entscheidung, welche externen Standards zu beachten sind sowie welchen Umfang die vorzunehmenden Kontrollhandlungen haben, treffen die Unternehmen eigenverantwortlich, jedoch für Dritte, zum Beispiel die Aufsichtsbehörde, nachvollziehbar.

11 Ausgliederung

11.1 Begriff der Ausgliederung

89 Der Anwendungsbereich von § 32 VAG erfasst die Ausgliederung von Funktionen und Versicherungstätigkeiten. Die Legaldefinition in § 7 Nr. 2 VAG bezieht sich nur auf das Merkmal „Ausgliederung“ und setzt unter anderem voraus, dass der betreffende Prozess, die Dienstleistung oder die Tätigkeit ansonsten vom Unternehmen selbst erbracht werden würde. Diese Voraussetzung ist in der Regel erfüllt, wenn ein Unternehmen den betreffenden Prozess, die Dienstleistung oder die Tätigkeit aufgrund gesetzlicher Vorgaben oder als für den Geschäftsbetrieb notwendig erbringen muss. Sind die Voraussetzungen des § 7 Nr. 2 VAG erfüllt, ist kumulativ zu prüfen, ob eine Funktion oder Versicherungstätigkeit im Sinne des § 32 VAG vorliegt. Damit wird die spezifische Ausgliederungskontrolle sachgerecht begrenzt. Eine Funktion oder Versicherungstätigkeit kann auch vorliegen, wenn der entsprechende Sachverhalt auch bei anderen Unternehmen als Versicherungsunternehmen auftritt (z. B. Vermögensanlage).

90 Zu beachten ist, dass die allgemeine Missstandsaufsicht eingreifen kann, obwohl keine Ausgliederung im Sinne des § 7 Nr. 2 VAG vorliegt. Denn die allgemeine Missstandsaufsicht umfasst alle Sachverhalte, welche die Belange der Versicherten gefährden können. Hierzu zählen auch Dienstleistungsbeziehungen, die nicht den Ausgliederungsanforderungen unterliegen. – Beispiel: Der Kantinenbetrieb durch einen externen Dienstleister unterfällt – weil die betreffende Tätigkeit ansonsten nicht unbedingt vom Unternehmen selbst erbracht werden würde – nicht dem Ausgliederungsbegriff und damit auch nicht der spezifischen Ausgliederungskontrolle durch die Aufsichtsbehörde. Kommt es jedoch wiederholt durch hygienische Mängel zu Ausfällen der Mitarbeiterschaft und einer Gefährdung der ordnungsgemäßen Betriebsabläufe, so kann darin ein Missstand liegen, der die Aufsichtsbehörde zum Einschreiten berechtigt.

91 Kriterien für die Abgrenzung von Ausgliederungen und sonstigen Dienstleistungsbeziehungen sind neben dem Inhalt der betroffenen Tätigkeit vor allem ihr Umfang und ihre Dauer sowie die Häufigkeit der Inanspruchnahme des Dienstleisters. Die Begriffe lassen sich nicht generell quantifizieren, sondern stehen in Abhängigkeit dazu, wie substanziell die jeweilige Tätigkeit für das konkrete Unternehmen ist.

92 Je substanzieller oder häufiger eine in Anspruch genommene Dienstleistung durch einen Dritten ist, desto wahrscheinlicher ist das Vorliegen einer Ausgliederung. Die Schwellen für die Annahme einer Dauerhaftigkeit oder Häufigkeit sind umso niedriger anzusetzen, je substanzieller der betroffene Bereich für das Unternehmen ist. Wird der Dienstleister bloß fallweise operativ oder konsultativ herangezogen, liegt in der Regel keine Ausgliederung vor. Eine wiederkehrende Betrauung desselben Dienstleisters oder eine häufige Inanspruchnahme desselben Dienstleisters mit artgleicher Tätigkeit bei Bestehen eines Rahmenvertrages mit diesem können hingegen Indizien für eine Ausgliederung sein. Umgekehrt sind, wenn auch selten, Sachverhaltskonstellationen denkbar, in denen auch die Kriterien der Dauer bzw. Häufigkeit der Inanspruchnahme eines Dienstleisters erfüllt sind, der ausgegliederte Bereich jedoch von ganz untergeordneter Bedeutung für das Unternehmen ist. Solche Umstände können im Einzelfall die Einschätzung rechtfertigen, dass keine Ausgliederung vorliegt.

93 Die für eine Ausgliederung erforderliche Vereinbarung zwischen einem ausgliedernden Unternehmen und einem Dienstleister ist zum Zweck der Qualifikation als Ausgliederungsvereinbarung weder an eine bestimmte Form noch an einen bestimmten Vertragstypus oder eine bestimmte Vertragsbezeichnung gebunden.

94 Die in § 32 VAG genannten Anforderungen setzen unter anderem voraus, die Schriftform der Ausgliederungsvereinbarung einzuhalten, die ausgegliederte Funktion oder Versicherungstätigkeit in das Risikomanagement und interne Kontrollsystem einzubeziehen, die gesetzlichen Anforderungen, insbesondere auch die Datenschutzvorschriften, zu beachten. Voraussetzung ist ebenfalls, dass die Mitarbeiter des Dienstleisters zuverlässig und fachlich geeignet sind.

11.2 Zulässiger Umfang

95 Im Falle von Ausgliederungen sowie Sub-Delegationen bleibt die Letztverantwortung der gesamten Geschäftsleitung immer bestehen. Originäre Leitungsaufgaben einschließlich der Verantwortung für die Einrichtung und die Weiterentwicklung des Risikomanagementsystems und des internen Kontrollsystems können nicht ausgegliedert werden. Dienstleister können in diesen Bereichen nur unterstützend und beratend eingebunden werden.

96 Die Ausgliederung bestimmter Teilbereiche des Risikomanagementsystems oder des internen Kontrollsystems ist unter sorgfältiger Risikoabwägung denkbar. Hiervon wiederum unberührt bleibt die Pflicht der gesamten Geschäftsleitung, die strategischen sowie die aufbau- und ablauforganisatorischen Rahmenbedingungen festzulegen.

97 Auch im Falle einer Ausgliederung ist eine angemessene Trennung der Zuständigkeiten zu wahren (§ 23 Abs. 1 Satz 3 VAG), auf Seiten des Dienstleisters ebenso wie auf Seiten des Unternehmens.

98 Befindet sich der Dienstleister außerhalb des Europäischen Wirtschaftsraums, ist durch das Unternehmen vor allem auf den Kontrollrahmen ein besonderes Augenmerk zu legen. Das Unternehmen muss auch diesen Dienstleister effektiv kontrollieren können, um bei einem Verstoß gegen die Bestimmungen der Ausgliederungs-Vereinbarung durch diesen gegebenenfalls frühzeitig reagieren zu können. Das Unternehmen achtet darauf, dass die lokale Aufsichtsbehörde des Dienstleisters oder die nationalen Regelungen insbesondere den Zugang zu Informationen über die ausgegliederten Funktionen und Versicherungstätigkeiten und zu den Geschäftsräumen des Dienstleisters nicht beschränken.

11.3 Risikoanalyse im Kontext von Ausgliederungen

99 Die mit einer Ausgliederung verbundenen Risiken sind sowohl im Vorfeld der Ausgliederung als auch im Anschluss daran zu identifizieren, zu bewerten und angemessen zu überwachen, zu steuern und zu berichten.

100 Die Unternehmen müssen zunächst eigenverantwortlich feststellen, ob die Herausgabe einer Aktivität von der Definition der Ausgliederung erfasst ist. Die weitere Bewertung, ob es sich um eine wichtige Funktion oder Versicherungstätigkeit handelt, die ausgegliedert werden soll, ist ebenfalls ein Teilbereich der Risikoanalyse, die vor jeder Ausgliederung erfolgen muss.

101 Bei der Grundentscheidung für oder gegen Ausgliederung müssen neben strategischen Motiven, ökonomischen und operativen Argumenten sowie quantitativen und qualitativen Aspekten auch Risikogesichtspunkte eine angemessene Rolle spielen. Einschlägige Risikokategorien sind regelmäßig das strategische, das operationelle und das Reputationsrisiko. Bei der Inanspruchnahme eines Mehrmandantendienstleisters ist zudem besonderes Augenmerk auf Konzentrationsrisiken zu legen.

102 Bei wesentlichen Änderungen des Risikoprofils in Bezug auf Ausgliederungssachverhalte muss erneut eine Risikoanalyse erfolgen und über die Fortführung oder Beendigung der Ausgliederung entschieden werden.

103 Die maßgeblichen Organisationseinheiten müssen bei der Erstellung der Risikoanalyse einbezogen werden. Wie intensiv die Risikoanalyse und die Einbeziehung der maßgeblichen Organisationseinheiten zu erfolgen hat, ist unter Proportionalitätsaspekten zu entscheiden. Die Ergebnisse der Risikoanalyse sind zu

dokumentieren.

11.4 Ausgliederung wichtiger Funktionen und Versicherungstätigkeiten

104 Unter den Funktionen und Versicherungstätigkeiten sind wichtige und sonstige Aktivitäten zu unterscheiden.

105 Im Fall von Teilausgliederungen wichtiger Funktionen oder Versicherungstätigkeiten ist entscheidend, ob der für die Ausgliederung vorgesehene Teilbereich auch für sich gesehen wichtig ist.

106 Die gesamte Geschäftsleitung muss alle Ausgliederungen wichtiger Funktionen oder Versicherungstätigkeiten vorab genehmigen. Die Sub-Delegation einer wichtigen Funktion oder Versicherungstätigkeit muss zumindest vom zuständigen Geschäftsleiter vorab genehmigt werden.

107 In der Regel sind folgende Bereiche wichtige Funktionen oder Versicherungstätigkeiten:

- Vertrieb,
- Bestandsverwaltung,
- Leistungsbearbeitung,
- Reservierung nach HGB,
- Rechnungswesen,
- Vermögensanlage und -verwaltung und
- elektronische Datenverarbeitung im Hinblick auf ihrerseits wichtige Funktionen oder Versicherungstätigkeiten.

Im Fall von Teilausgliederungen gilt das in Rn. 105 Gesagte.

108 Im Übrigen müssen die Unternehmen eigenverantwortlich feststellen, ob die jeweilige Funktion oder Versicherungstätigkeit wichtig ist und dies im Rahmen der Risikoanalyse (s.o. 11.3) dokumentieren. Ob eine Funktion oder Versicherungstätigkeit wichtig ist, kann nur einzelfallbezogen bewertet werden.

109 Die Bewertung, ob eine Funktion oder Versicherungstätigkeit wichtig oder nicht wichtig ist, muss wiederholt und gegebenenfalls geändert werden, wenn sich die zugrundeliegenden Umstände wesentlich geändert haben.

110 Die Kriterien und der Prozess für die Einordnung einer Funktion oder Versicherungstätigkeit als wichtig sind in der schriftlichen Leitlinie für die Ausgliederung festzulegen und ihrerseits sich ändernden Umständen anzupassen.

111 Für die Absicht, wichtige Funktionen oder Versicherungstätigkeiten auszugliedern, gilt gemäß § 47 Nr. 8 VAG eine unverzügliche Anzeigepflicht unter Vorlage des Vertragsentwurfs.

112 Die Anzeige sowie alle beizufügenden Unterlagen sind in der Regel in deutscher Sprache einzureichen. Sie können nach Rücksprache mit dem zuständigen Fachreferat auch in englischer Sprache vorgelegt werden. Falls erforderlich, kann die Aufsichtsbehörde auch zu einem späteren Zeitpunkt von dem Unternehmen eine autorisierte Übersetzung anfordern.

113 Mit der unterzeichneten Anzeige ist der Vertragsentwurf vorzulegen.

114 In der Anzeige sind anzugeben:

- der Name des Dienstleisters,
- die Anschrift des Dienstleisters,
- eine Beschreibung des Umfangs der Ausgliederung,
- die Gründe für die Ausgliederung und
- eventuelle Sub-Delegationen.

11.5 Ausgliederung auf Versicherungsvermittler

115 Obwohl üblicherweise auf Dauer angelegt, unterfallen die typischen Vermittlungssachverhalte (ohne Abschluss- oder Schadenregulierungsvollmacht) nicht den Ausgliederungsanforderungen.

116 Die Übertragung des Abschlusses von Versicherungsgeschäften oder der Schadenregulierung auf Versicherungsvermittler stellen immer eine Ausgliederung wichtiger Funktionen oder Versicherungstätigkeiten dar. Die Unternehmen haben insoweit keine Einschätzungsfreiheit. Zu beachten ist, dass nach der Maßgabe der Rechtsprechung des BGH (Urteil vom 14.01.2016, I ZR 107/14) eine Schadenregulierung durch Versicherungsmakler unzulässig ist.

117 Im Falle von Teilausgliederungen gilt hinsichtlich der Frage, ob es sich um eine wichtige Ausgliederung handelt, das unter 11.4 Gesagte. Erteilt ein Unternehmen einer Vielzahl von Versicherungsvermittlern Abschluss- oder Schadenregulierungsvollmachten, so kommt es auf die Gesamtbetrachtung an.

11.6 Ausgliederungsleitlinien

118 Für den gesamten Bereich der Ausgliederung sind schriftliche Leitlinien zu erstellen. Diese haben die Auswirkungen von Ausgliederungen auf den Geschäftsbetrieb zu berücksichtigen und die bei Ausgliederungen unternehmensindividuell anzuwendenden Verfahrens- und Qualitätsstandards sowie die zu implementierenden Berichts- und Überwachungspflichten vom Beginn bis zum Ende der Ausgliederung festzulegen.

119 Die schriftlichen Leitlinien müssen konsistent in Bezug auf die Geschäftsstrategie des Unternehmens sein.

120 Die schriftlichen Leitlinien haben einen Überprüfungsprozess für den in Betracht gezogenen Dienstleister zu enthalten. Folgende Aspekte des Prozesses sind in den schriftlichen Leitlinien mindestens abzudecken:

- Finanzielle, technische und fachliche Leistungsfähigkeit des Dienstleisters,
- Kapazität des Dienstleisters, die Ausgliederungs-Leistungen erbringen zu können,
- Kontrollrahmen und
- etwaige Interessenkonflikte.

121 Die Unternehmen bestimmen darüber hinaus in den schriftlichen Leitlinien eigenständig, ob weitere Aspekte im Rahmen des Überprüfungsprozesses zu berücksichtigen sind. Diese Aspekte sind Änderungen der unternehmensinternen oder externen Umstände anzupassen.

122 Die Ausgliederungsleitlinien müssen darlegen, wie die Kontinuität und die ungeminderte Qualität der ausgegliederten Funktionen und Versicherungstätigkeiten auch im Fall der Beendigung der Vertragsbeziehung zu dem Dienstleister sichergestellt werden.

123 In die schriftlichen Leitlinien ist die Verpflichtung aufzunehmen, für ausgegliederte wichtige Funktionen und Versicherungstätigkeiten Notfallpläne zu entwickeln, die sich mit bei dem Dienstleister auftretenden Störungen befassen. Zudem haben die Leitlinien den Prozess und die Verantwortlichkeiten zur Aufstellung

dieser Notfallpläne zu beschreiben. Die Notfallpläne haben insbesondere zu berücksichtigen, wie die ausgegliederten wichtigen Funktionen und Versicherungstätigkeiten notfalls auf einen anderen Dienstleister übertragen oder in den Geschäftsbetrieb des Unternehmens wieder eingegliedert werden können.

124 Im Übrigen gelten für die schriftlichen Leitlinien zur Ausgliederung die unter 8.4 genannten Grundsätze.

12 Notfallmanagement

125 Das Notfallmanagement erhöht die Widerstandsfähigkeit von Bereichen und Prozessen im Unternehmen, um in möglichen Krisensituationen die Verfügbarkeit wesentlicher Daten und Funktionen sowie die Fortführung der Geschäftstätigkeit durch im Vorfeld definierte Verfahren zu gewährleisten.

126 Verantwortlich für das operative Notfallmanagement ist die Geschäftsleitung. Die Notfallplanung muss von der gesamten Geschäftsleitung beschlossen werden.

127 Notfallpläne sind für diejenigen Bereiche und Prozesse zu erstellen, bei denen der Eintritt einer unvorhergesehenen Störung die Fortführung der Geschäftstätigkeit gefährden kann. Die ausgegliederten Bereiche und Prozesse sind im Notfallmanagement zu berücksichtigen. Eignung und Wirksamkeit der Notfallpläne sind fortlaufend sicherzustellen. Hierzu sind den Risiken des jeweiligen Bereiches bzw. Prozesses entsprechend regelmäßig Testläufe und Übungen durchzuführen.

128 Die den Notfallplänen zugrundeliegenden Notfallszenarien haben dem individuellen Risikoprofil hinreichend Rechnung zu tragen.

129 Sowohl die Notfallplanung als auch die Bewältigung eines Notfalles müssen adäquat in die Strukturen und Prozesse der Aufbau- und Ablauforganisation eingebunden sein. Aufgaben, Verantwortlichkeiten, Informationspflichten und Eskalationsprozesse sind klar und nachvollziehbar festzulegen und zu dokumentieren.

130 Der betroffene Personenkreis muss die Notfallpläne kennen. Die Verfügbarkeit der Notfallpläne muss auch im Notfall sichergestellt sein.

Anmerkungen

Soweit aus Gründen der Lesbarkeit auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen diese sich auf alle Geschlechter.

Zusatzinformationen

Begleittext MaGo

Anlage
Begleittext MaGo (docx, 15KB, nicht barrierefrei)
