Anlage: Zweiter Entwurf vom 13.8.2007

Änderungen gegenüber dem ersten Entwurf vom 5.4.2007 sind im relevanten Auszug des Regelungstextes der MaRisk farblich gekennzeichnet (Beschränkung auf die Module AT und BT 2).

AT 1 Vorbemerkung

1	Dieses Rundschreiben gibt auf der Grundlage des § 25a Abs. 1 des Kreditwesengesetzes (KWG) einen flexiblen und praxisnahen Rahmen für die Ausgestaltung des Risikomanagements der Institute vor. Ferner ~~ergänzt und~~ präzisiert es die Anforderungen an eine ordnungsgemäße Geschäftsorganisation für die ausgelagerten Aktivitäten und Prozesse nach § 25a Abs. 2 KWG. Das Risikomanagement im Sinne dieses Rundschreibens umfasst unter Berücksichtigung der Risikotragfähigkeit die Festlegung angemessener Strategien sowie die Einrichtung angemessener interner Kontrollverfahren. Die internen Kontrollverfahren bestehen aus dem internen Kontrollsystem und der Internen Revision. Das interne Kontrollsystem umfasst insbesondere - Regelungen zur Aufbau- und Ablauforganisation und - Prozesse zur Identifizierung, Beurteilung, Steuerung, Überwachung sowie Kommunikation der Risiken (Risikosteuerungs--controllingprozesse). und Das Rundschreiben zielt insofern vor allem auf die Einrichtung angemessener institutsinterner Leitungs-, Steuerungs- und Kontrollprozesse ab. Als Grundlage für die sachgerechte Wahrnehmung der Überwachungsfunktionen des Aufsichtsorgans beinhaltet dies auch dessen angemessene Einbindung.	**Zweigstellen gemäß § 53 KWG** Da bei Zweigstellen von Unternehmen mit Sitz im Ausland gemäß § 53 KWG kein Aufsichtsorgan vorhanden ist, haben diese -Institute stattdessen in angemessener Form ihre Unternehmenszentralen einzubeziehen.
2	Das Rundschreiben soll zudem einen qualitativen Rahmen für die Umsetzung der Art. 22 und 123 der ~~Capital Requirements Directive (CRD)~~Richtlinie 2006/48/EG (Bankenrichtlinie) vorgeben. Danach sind von den Instituten angemessene Leitungs-, Steuerungs- und Kontrollprozesse („Robust Governance Arrangements“) sowie Strategien und Prozesse einzurichten, die gewährleisten, dass genügend internes Kapital zur Abdeckung aller wesentlichen Risiken vorhanden ist („Internal Capital Adequacy Assessment Process“). Die Qualität dieser Prozesse soll von der Aufsicht gemäß Art. 124 der ~~CRD~~ Bankenrichtlinie regelmäßig beurteilt werden („Supervisory Review and Evaluation Process“). Das Rundschreiben soll daher unter Berücksichtigung des Prinzips der doppelten Proportionalität der Regelungsrahmen für die neue qualitative Aufsicht in Deutschland sein („Supervisory Review Process“). Im Hinblick auf die geplanten Methoden zur Berechnung der aufsichtsrechtlich erforderlichen Eigenmittel der ~~CRD~~ Bankenrichtlinie sind die Anforderungen des Rundschreibens insofern neut-	

	ral konzipiert, als sie unabhängig von der gewählten Methode eingehalten werden können.	
3	Das Rundschreiben setzt zudem über § 33 Abs. 1 WpHG in Verbindung mit § 25a Abs. 1 KWG Art. 13 der Richtlinie ~~über Märkte für Finanzinstrumente (MiFID)~~2004/39/EG (Finanzmarktrichtlinie) um, soweit diese auf Kreditinstitute und Finanzdienstleistungsinstitute gleichermaßen Anwendung findet. Dies betrifft die allgemeinen organisatorischen Anforderungen gemäß Art. 5, die Anforderungen an das Risikomanagement und die Interne Revision gemäß Art. 7 und 8, Anforderungen zur Geschäftsleiterverantwortung gemäß Art. 9 sowie an Auslagerungen gemäß Art. 13 und 14 der Richtlinie 2006/73/EG (Durchführungsrichtlinie zur ~~MiFID~~ Finanzmarktrichtlinie). Diese Anforderungen dienen der Verwirklichung des Ziels der Finanzmarktrichtlinie, die Finanzmärkte in der Europäischen Union im Interesse des grenzüberschreitenden Finanzdienstleistungsverkehrs und einheitlicher Grundlagen für den Anlegerschutz zu harmonisieren.	
4	Das Rundschreiben trägt der heterogenen Institutsstruktur und der Vielfalt der Geschäftsaktivitäten Rechnung. Es enthält zahlreiche Öffnungsklauseln, die abhängig von der Größe der Institute, den Geschäftsschwerpunkten und der Risikosituation eine vereinfachte Umsetzung ermöglichen. Insoweit kann es vor allem auch von kleineren Instituten flexibel umgesetzt werden. Das Rundschreiben ist gegenüber der laufenden Fortentwicklung der Prozesse und Verfahren im Risikomanagement offen, soweit diese im Einklang mit den Zielen des Rundschreibens stehen. Für diese Zwecke wird die Bundesanstalt für Finanzdienstleistungsaufsicht einen fortlaufenden Dialog mit der Praxis führen.	
5	Die Bundesanstalt für Finanzdienstleistungsaufsicht erwartet, dass der flexiblen Grundausrichtung des Rundschreibens im Rahmen von Prüfungshandlungen Rechnung getragen wird. Prüfungen sind daher auf der Basis eines risikoorientierten Prüfungsansatzes durchzuführen.	
6	Das Rundschreiben ist modular strukturiert, so dass notwendige Anpassungen in bestimmten Regelungsfeldern auf die zeitnahe Überarbeitung einzelner Module beschränkt werden können. In einem allgemeinen Teil (Modul AT) befinden sich grundsätzliche Prinzipien für die Ausgestaltung des Risikomanagements; spezifische Anforderungen an die Organisation des Kredit- und Handelsgeschäfts beziehungsweise die Identifizierung, Beurteilung, Steuerung sowie die Überwachung und Kommunikation von Adressenausfallrisiken, Marktpreisrisiken, Liquiditätsrisiken sowie operationellen Risiken sind in einem besonderen Teil niedergelegt (Modul BT). Darüber	

hinaus wird in diesem Modul ein Rahmen für die Ausgestaltung der Internen Revision in den Instituten vorgegeben.	

AT 2 Anwendungsbereich

1. Die Beachtung der Anforderungen des Rundschreibens durch die Institute soll dazu beitragen, Missständen im Kredit- und Finanzdienstleistungswesen entgegenzuwirken, welche die Sicherheit der den Instituten anvertrauten Vermögenswerte gefährden, die ordnungsgemäße Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen oder erhebliche Nachteile für die Gesamtwirtschaft herbeiführen können. Bei der Erbringung von Wertpapierdienstleistungen und Wertpapiernebendienstleistungen müssen die Institute die Anforderungen darüber hinaus mit der Maßgabe einhalten, die Interessen der Wertpapierdienstleistungskunden zu schützen.	

AT 2.1 Anwenderkreis

1	Die Anforderungen des Rundschreibens sind von allen Instituten im Sinne von § 1 Abs. 1b KWG beziehungsweise im Sinne von § 53 Abs. 1 KWG zu beachten. Sie gelten auch für die Zweigniederlassungen deutscher Institute im Ausland. Auf Zweigniederlassungen von Unternehmen mit Sitz in einem anderen Staat des Europäischen Wirtschaftsraums nach § 53b KWG finden sie keine Anwendung. Das übergeordnete Unternehmen beziehungsweise übergeordnete Finanzkonglomeratsunternehmen einer Institutsgruppe, einer Finanzholdinggruppe oder eines Finanzkonglomerats hat ein Verfahren einzurichten, das eine angemessene Steuerung und Überwachung der wesentlichen Risiken auf Gruppenebene im Rahmen der gesellschaftsrechtlichen Möglichkeiten sicherstellt.	**Anforderungen auf Gruppenebene** Die Anforderung in Satz 4 ist an die übergeordneten Unternehmen von Institutsgruppen gemäß § 10a Abs. 2 KWG und Finanzholding-Gruppen gemäß § 10a Abs. 3 KWG sowie an übergeordnete Finanzkonglomeratsunternehmen gemäß § 10b Abs. 3 KWG adressiert. Die konkrete Ausgestaltung des Verfahrens liegt dabei im Ermessen der übergeordneten Unternehmen. Soweit die Risiken eines nachgeordneten Unternehmens vom übergeordneten Unternehmen als nicht wesentlich eingestuft werden, kann dieses von der Anwendung des Verfahrens auf Gruppenebene ausgenommen werden. Die Anforderung in Satz 4 bezieht sich nicht auf die Umsetzung der organisatorischen Anforderungen des Rundschreibens (z. B. der aufbau- und ablauforganisatorischen Regelungen in Modul BTO). Dem Verfahren muss keine einheitliche Methodik zu Grunde liegen.
2	Finanzdienstleistungsinstitute und Wertpapierhandelsbanken haben die Anforderungen des Rundschreibens ~~nach den Modulen AT 3, AT 4, AT 5, AT 7 und AT 9 grundsätzlich und die übrigen Module~~ insoweit zu beachten, wie dies vor dem Hintergrund der Institutsgröße sowie von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten zur Einhaltung der gesetzlichen Pflichten aus § 25a KWG geboten erscheint; dies gilt insbesondere für die Module AT 3, AT 5, AT 7 und AT 9.	
3	Die Anforderungen des Rundschreibens gelten für Kapitalanlagegesellschaf-	

ten im Sinne von § 2 Abs. 6 InvG mit der Maßgabe, dass a) BTO 1 für Kapitalanlagegesellschaften keine Geltung beansprucht, b) BTO 2 und BTR für Aktivitäten und Prozesse im Rahmen der Verwaltung von Sondervermögen und der individuellen Vermögensverwaltung nicht zur Anwendung kommen; für Aktivitäten und Prozesse im Rahmen des Eigengeschäfts der Kapitalanlagegesellschaften gelten die Anforderungen dieser Module lediglich sinngemäß, c) die Anforderungen des AT nur insoweit anzuwenden sind, wie sie nicht explizit in speziellen Regelwerken für Kapitalanlagegesellschaften festgelegt sind.	

AT 2.2 Risiken

1	Die Anforderungen des Rundschreibens beziehen sich auf das Management der für das Institut wesentlichen Risiken sowie damit verbundener Risikokonzentrationen. ~~Dabei sind auch Risiken im Zusammenhang mit dem Anlegerschutz zu berücksichtigen.~~ Zur Beurteilung der Wesentlichkeit hat sich die Geschäftsleitung einen Überblick über das Gesamtrisikoprofil des Instituts zu verschaffen. Zu den dabei zu berücksichtigenden Risikoarten zählen in der Regel: a) Adressenausfallrisiken (einschließlich Länderrisiken), b) Marktpreisrisiken, c) Liquiditätsrisiken und d) operationelle Risiken.	

AT 2.3 Geschäfte

1	Kreditgeschäfte im Sinne des Rundschreibens sind grundsätzlich Geschäfte nach Maßgabe des § 19 Abs. 1 KWG (Bilanzaktiva und außerbilanzielle Geschäfte mit Adressenausfallrisiken).	

2 Im Sinne dieses Rundschreibens gilt als Kreditentscheidung jede Entscheidung über Neukredite, Krediterhöhungen, Beteiligungen, Limitüberschreitungen, die Festlegung von kreditnehmerbezogenen Limiten sowie von Kontrahenten- und Emittentenlimiten, Prolongationen und Änderungen risikorelevanter Sachverhalte, die dem Kreditbeschluss zu Grunde lagen (z. B. Sicherheiten, Verwendungszweck). Dabei ist es unerheblich, ob diese Entscheidung ausschließlich vom Institut selbst oder gemeinsam mit anderen Instituten getroffen wird (so genanntes Konsortialgeschäft)	**Prolongationen** Hinsichtlich des Begriffes „Prolongationen“ wird nicht zwischen externen und internen Prolongationen (z. B. interne Verlängerung von extern b. a. w. zugesagten Krediten) unterschieden. Interne „Überwachungsvorlagen“, die lediglich der Kreditüberwachung während der Laufzeit dienen, gelten hingegen nicht als Prolongationen und damit nicht als Kreditentscheidungen im Sinne des Rundschreibens. **Zinsanpassungen** Nach Ablauf von Zinsbindungsfristen (die nicht mit der Gesamtlaufzeit übereinstimmen) erfolgende Zinsanpassungen können als Bestandteil des Gesamtkreditvertrages angesehen werden, die vor Kreditvergabe (mit)geprüft werden. Es handelt sich daher grundsätzlich nicht um eine gesonderte Kreditentscheidung im Sinne des Rundschreibens. **Stundungen** Stundungen stellen keine von vornherein geplanten Änderungen des Kreditverhältnisses dar. Sie dienen z. B. der kurzzeitigen Überbrückung der Zeit bis zu einer Sanierung und sind somit als Kreditentscheidung im Sinne des Rundschreibens zu qualifizieren.
3 Handelsgeschäfte sind grundsätzlich alle Abschlüsse, die ein a) Geldmarktgeschäft, b) Wertpapiergeschäft, c) Devisengeschäft, d) Geschäft in handelbaren Forderungen (z. B. Handel in Schuldscheinen), e) Geschäft in Waren oder f) Geschäft in Derivaten zur Grundlage haben und die im eigenen Namen und für eigene Rechnung abgeschlossen werden. Als Wertpapiergeschäfte gelten auch Geschäfte mit Namensschuldverschreibungen sowie die Wertpapierleihe, nicht aber die Erstausgabe von Wertpapieren. Handelsgeschäfte sind auch, ungeachtet des Geschäftsgegenstandes, Vereinbarungen von Rückgabe- oder Rücknahmeverpflichtungen sowie Pensionsgeschäfte.	**Emissionsgeschäft** Die Erstausgabe von Wertpapieren ist grundsätzlich kein Handelsgeschäft im Sinne des Rundschreibens. Hingegen stellt der Ersterwerb aus einer Emission ein Handelsgeschäft im Sinne des Rundschreibens dar. Beim Ersterwerb sind Erleichterungen im Hinblick auf die Marktgerechtigkeitskontrolle möglich (Erläuterungen zu BTO 2.2.2 Tz. 5). **Einordnung von Forderungen als Handelsgeschäfte** Zu d): Forderungen sind dann als Handelsgeschäfte zu qualifizieren, wenn von Seiten des Instituts eine Handelsabsicht besteht. Hierzu hat das Institut geeignete Kriterien festzulegen. **Warengeschäfte** Zu e): Zu den Geschäften in Waren zählen insbesondere der Handel mit Edelmetallen und Rohwaren sowie der CO2-Handel und der Stromhandel. Geschäfte in Waren im Sinne des Rundschreibens umfassen in Analogie zu § 16 Grundsatz I nicht die Warengeschäfte, die infolge fest getroffener Vereinbarungen über die Abnahme beziehungsweise Lieferung der jeweiligen Ware zum

	Zeitpunkt der Erfüllung geschlossene Positionen während der gesamten Geschäftsdauer begründen.
4 Zu den Geschäften in Derivaten gehören Termingeschäfte, deren Preis sich von einem zu Grunde liegenden Aktivum, von einem Referenzpreis, Referenzzins, Referenzindex oder einem im Voraus definierten Ereignis ableitet.	**Garantien / Avale** Garantien/Avale und Ähnliches fallen nicht unter die Derivate-Definition des Rundschreibens.

AT 3 Gesamtverantwortung der Geschäftsleitung

1	Alle Geschäftsleiter (§ 1 Abs. 2 KWG) sind, unabhängig von der internen Zuständigkeitsregelung, für die ordnungsgemäße Geschäftsorganisation und deren Weiterentwicklung verantwortlich. Diese Verantwortung bezieht sich auch auf ausgelagerte Aktivitäten und Prozesse. Sie umfasst für die Zwecke des Rundschreibens die Festlegung angemessener Strategien und die Einrichtung angemessener interner Kontrollverfahren und somit die Verantwortung für alle wesentlichen Elemente des Risikomanagements. Sie werden dieser Verantwortung nur gerecht, wenn das Risikomanagement ihnen ermöglicht, die Risiken zu beurteilen und die erforderlichen Maßnahmen zu ihrer Begrenzung zu treffen.	**Risikobeurteilung durch die Geschäftsleiter** Vgl. Protokoll zur 2. Sitzung des Fachgremiums MaRisk am 17.08.2006.

AT 4 Allgemeine Anforderungen an das Risikomanagement

AT 4.1 Risikotragfähigkeit

1	Auf der Grundlage des Gesamtrisikoprofils ist sicherzustellen, dass die wesentlichen Risiken des Instituts durch das Risikodeckungspotenzial, gegebenenfalls unter Berücksichtigung von Wechselwirkungen, laufend abgedeckt sind und damit die Risikotragfähigkeit gegeben ist.	
2	Die Risikotragfähigkeit ist im Rahmen der Festlegung der Strategien (AT 4.2) sowie bei deren Anpassung zu berücksichtigen. Zur Umsetzung der Strategien beziehungsweise zur Gewährleistung der Risikotragfähigkeit sind geeignete Risikosteuerungs- und -controllingprozesse (AT 4.3.2) einzurichten.	
3	Wesentliche Risiken, die nicht in das Risikotragfähigkeitskonzept einbezogen werden, sind festzulegen (z. B. Liquiditätsrisiken); ihre Nichtberücksichtigung ist nachvollziehbar zu begründen. Es ist sicherzustellen, dass solche Risiken angemessen in den Risikosteuerungs- und -controllingprozessen berücksichtigt werden.	

4	Die Wahl der Methoden zur Beurteilung der Risikotragfähigkeit liegt in der Verantwortung des Instituts. Die den Methoden zu Grunde liegenden Annahmen sind nachvollziehbar zu begründen. Die Angemessenheit der Methoden ist zumindest jährlich durch die fachlich zuständigen Mitarbeiter zu überprüfen.	

AT 4.2 Strategien

1	Die Geschäftsleitung hat eine Geschäftsstrategie und eine dazu konsistente Risikostrategie festzulegen. Bei der Ausarbeitung der Risikostrategie sind die in der Geschäftsstrategie niederzulegenden Ziele und Planungen der wesentlichen Geschäftsaktivitäten sowie die Risiken wesentlicher Auslagerungen von Aktivitäten und Prozessen zu berücksichtigen. Die Verantwortung für die Festlegung der Strategien ist nicht delegierbar. Die Geschäftsleitung muss für die Umsetzung der Strategien Sorge tragen. Der Detaillierungsgrad der Strategien ist abhängig von Umfang und Komplexität sowie dem Risikogehalt der geplanten Geschäftsaktivitäten.	**Prüfungshandlungen durch externe Prüfer oder die Interne Revision** Die Festlegung des Inhalts der Geschäftsstrategie liegt allein in der Verantwortung der Geschäftsleitung und ist nicht Gegenstand von Prüfungshandlungen durch externe Prüfer oder die Interne Revision. Bei der Überprüfung der Risikostrategie ist die Geschäftsstrategie heranzuziehen, um die Konsistenz zwischen beiden Strategien nachvollziehen zu können. Es bleibt dem Institut überlassen, die Risikostrategie in die Geschäftsstrategie zu integrieren.
2	Die Risikostrategie hat, gegebenenfalls unterteilt in Teilstrategien (z. B. eine Strategie hinsichtlich der Adressenausfallrisiken), die Ziele der Risikosteuerung der wesentlichen Geschäftsaktivitäten zu umfassen. Der Detaillierungsgrad der Teilstrategien kann unterschiedlich sein. Der Begrenzung von Risikokonzentrationen ist im Rahmen der Festlegung der Risikostrategie angemessen Rechnung zu tragen.	**Darstellung der Risikostrategie** Die Art und Weise der Darstellung der Risikostrategie liegt im Ermessen des Instituts. Neben einer zusammenfassenden Darstellung in einem Dokument, ist auch eine Darstellung über mehrere Dokumente möglich, soweit zwischen diesen Dokumenten ein konsistenter Zusammenhang besteht.
3	Die Geschäftsleitung hat die Strategien mindestens jährlich zu überprüfen und gegebenenfalls anzupassen; sie sind dem Aufsichtsorgan des Instituts zur Kenntnis zu geben und mit diesem zu erörtern.	**Ausschüsse des Aufsichtsorgans** Adressat der Strategien sollte grundsätzlich jedes Mitglied des Aufsichtsorgans sein. Soweit das Aufsichtsorgan Ausschüsse gebildet hat, können die Strategien auch an einen Ausschuss weitergeleitet und mit diesem 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. Zudem ist jedem Mitglied des Aufsichtsorgans weiterhin das Recht einzuräumen, die an den Ausschuss geleiteten Strategien einsehen zu können.
4	Die Inhalte sowie Änderungen der Risikostrategie sind, gegebenenfalls zusammen mit der Geschäftsstrategie, innerhalb des Instituts in geeigneter Weise zu kommunizieren.	

AT 4.3 Internes Kontrollsystem

1	In jedem Institut sind entsprechend Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten a) Regelungen zur Aufbau- und Ablauforganisation zu treffen sowie b) Risikosteuerungs- und -controllingprozesse einzurichten.	**Aufbau- und Ablauforganisation** Die Anforderungen zur Aufbau- und Ablauforganisation schließen auch die Risikosteuerungs- und –controllingprozesse mit ein.

AT 4.3.1 Aufbau- und Ablauforganisation

1	Bei der Ausgestaltung der Aufbau- und Ablauforganisation ist sicherzustellen, dass miteinander unvereinbare Tätigkeiten durch unterschiedliche Mitarbeiter durchgeführt werden.	
2	Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen sowie Kommunikationswege sind klar zu definieren und aufeinander abzustimmen. Das gilt auch bezüglich der Schnittstellen zu wesentlichen Auslagerungen ~~ausgelagerten Aktivitäten und Prozessen~~.	

AT 4.3.2 Risikosteuerungs- und –controllingprozesse

1	Das Institut hat angemessene Risikosteuerungs- und -controllingprozesse einzurichten, die eine a) Identifizierung, b) Beurteilung, c) Steuerung sowie d) Überwachung und Kommunikation der wesentlichen Risiken gewährleisten. Diese Prozesse sollten in ein in-	**Einbindung in die „Gesamtbanksteuerung“** Die Einbindung der Risikosteuerungs- und -controllingprozesse in ein integriertes System zur Ertrags- und Risikosteuerung ist eine Empfehlung der BaFin, wie in der „Sollte“-Formulierung zum Ausdruck kommt.

	tegriertes System zur Ertrags- und Risikosteuerung („Gesamtbanksteuerung“) eingebunden werden.	
2	Die Risikosteuerungs- und -controllingprozesse müssen gewährleisten, dass die wesentlichen Risiken – auch aus ausgelagerten Aktivitäten und Prozessen - frühzeitig erkannt, vollständig erfasst und in angemessener Weise dargestellt werden können. Wechselwirkungen zwischen den unterschiedlichen Risikoarten sollten berücksichtigt werden.	
3	Für die im Rahmen der Risikotragfähigkeit berücksichtigten Risiken sind regelmäßig angemessene Szenariobetrachtungen anzustellen.	
4	Die Geschäftsleitung hat sich in angemessenen Abständen über die Risikosituation und die Ergebnisse der Szenariobetrachtungen berichten zu lassen. Die Risikoberichterstattung ist in nachvollziehbarer, aussagefähiger Art und Weise zu verfassen. Sie hat neben einer Darstellung auch eine Beurteilung der Risikosituation zu enthalten. In die Risikoberichterstattung sind bei Bedarf auch Handlungsvorschläge, z. B. zur Risikoreduzierung, aufzunehmen. Einzelheiten zur Risikoberichterstattung sind in BTR 1 bis BTR 4 geregelt.	**Hinweise zur Risikoberichterstattung** Die Risikoberichterstattung an die Geschäftsleitung kann – soweit dies aus Sicht des Instituts als sinnvoll erachtet wird - durch prägnante Darstellungen ergänzt werden (z. B. ein Management Summary). Soweit sich im Hinblick auf Sachverhalte in vorangegangenen Berichterstattungen keine relevanten Änderungen ergeben haben, kann im Rahmen der aktuellen Berichterstattung auf diese Informationen verwiesen werden. Da Risikoaspekte nicht isoliert von Ertrags- und Kostenaspekten diskutiert werden können, können letztere ebenfalls in die Risikoberichterstattung aufgenommen werden. Auch eine Diskussion der Handlungsvorschläge mit den jeweils verantwortlichen Bereichen ist grundsätzlich unproblematisch, solange sichergestellt ist, dass der Informationsgehalt der Risikoberichterstattung beziehungsweise der Handlungsvorschläge nicht auf eine unsachgerechte Weise verzerrt werden.
5	Unter Risikogesichtspunkten wesentliche Informationen sind unverzüglich an die Geschäftsleitung, die jeweiligen Verantwortlichen und gegebenenfalls die Interne Revision weiterzuleiten, so dass geeignete Maßnahmen beziehungsweise Prüfungshandlungen frühzeitig eingeleitet werden können.	**Informationspflicht gegenüber der Internen Revision** Eine Informationspflicht gegenüber der Internen Revision besteht dann, wenn nach Einschätzung der Fachbereiche unter Risikogesichtspunkten relevante Mängel zu erkennen oder bedeutende Schadensfälle aufgetreten sind oder ein konkreter Verdacht auf Unregelmäßigkeiten besteht.
6	Die Geschäftsleitung hat das Aufsichtsorgan vierteljährlich über die Risikosituation in angemessener Weise schriftlich zu informieren.	**Ausschüsse des Aufsichtsorgans** Adressat der Risikoberichterstattung sollte grundsätzlich jedes Mitglied des Aufsichtsorgans sein. Soweit das Aufsichtsorgan Ausschüsse gebildet hat, kann die Weiterleitung der Informationen auch auf einen Ausschuss beschränkt werden. Voraussetzung dafür ist, dass ein entsprechender Beschluss über die Einrichtung des Ausschusses besteht und der Vorsitzende des Ausschusses regelmäßig das

	gesamte Aufsichtsorgan informiert. Zudem ist jedem Mitglied des Aufsichtsorgans weiterhin das Recht einzuräumen, die an den Ausschuss geleitete Berichterstattung einsehen zu können.
7 Die Risikosteuerungs- und –controllingprozesse sind zeitnah an sich ändernde Bedingungen anzupassen.	

AT 4.4 Interne Revision

1 Jedes Institut muss über eine funktionsfähige Interne Revision verfügen. Bei Instituten, bei denen aus Gründen der Betriebsgröße die Einrichtung einer Revisionseinheit unverhältnismäßig ist, können die Aufgaben der Internen Revision von einem Geschäftsleiter erfüllt werden.	
2 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.	
3 Die Interne Revision hat risikoorientiert und prozessunabhängig die Wirksamkeit und Angemessenheit des Risikomanagements im Allgemeinen und des internen Kontrollsystems im Besonderen sowie die Ordnungsmäßigkeit grundsätzlich aller Aktivitäten und Prozesse zu prüfen und zu beurteilen, unabhängig davon, ob diese ausgelagert sind oder nicht. BT 2.1 Tz. 3 bleibt hiervon unberührt.	
4 Zur Wahrnehmung ihrer Aufgaben ist der Internen Revision ein vollständiges und uneingeschränktes Informationsrecht einzuräumen. Dieses Recht ist jederzeit zu gewährleisten. Der Internen Revision sind insoweit unverzüglich die erforderlichen Informationen zu erteilen, die notwendigen Unterlagen zur Verfügung zu stellen und Einblick in die Aktivitäten und Prozesse sowie die IT-Systeme des Instituts zu gewähren.	
5 Weisungen und Beschlüsse der Geschäftsleitung, die für die Interne Revision von Bedeutung sein können, sind ihr bekannt zu geben. Über wesentliche Änderungen im Risikomanagement ist die Interne Revision rechtzeitig zu informieren.	

AT 5 Organisationsrichtlinien

1	Das Institut hat sicherzustellen, dass die Geschäftsaktivitäten auf der Grundlage von Organisationsrichtlinien betrieben werden (z. B. Handbücher, Arbeitsanweisungen oder Arbeitsablaufbeschreibungen). Der Detaillierungsgrad der Organisationsrichtlinien hängt von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten ab.	**Darstellung der Organisationsrichtlinien** Hinsichtlich der Darstellung der Organisationsrichtlinien kommt es in erster Linie darauf an, dass diese sachgerecht und für die Mitarbeiter des Instituts nachvollziehbar sind. Die konkrete Art der Darstellung bleibt dem Institut überlassen.
2	Die Organisationsrichtlinien müssen schriftlich fixiert und den betroffenen Mitarbeitern in geeigneter Weise bekannt gemacht werden. Es ist sicherzustellen, dass sie den Mitarbeitern in der jeweils aktuellen Fassung zur Verfügung stehen. Die Richtlinien sind bei Veränderungen der Aktivitäten und Prozesse zeitnah anzupassen.	
3	Die Organisationsrichtlinien haben vor allem Folgendes zu beinhalten: a) Regelungen für die Aufbau- und Ablauforganisation sowie zur Aufgabenzuweisung, Kompetenzordnung und den Verantwortlichkeiten, b) Regelungen hinsichtlich der Ausgestaltung der Risikosteuerungs- und -controllingprozesse, c) Regelungen zur Internen Revision, d) Regelungen, die die Einhaltung gesetzlicher Bestimmungen sowie sonstiger Vorgaben (z. B. Datenschutz, Compliance) gewährleisten sowie e) Regelungen zu Verfahrensweisen bei wesentlichen Auslagerungen von Aktivitäten und Prozessen.	
4	Die Ausgestaltung der Organisationsrichtlinien muss es der Internen Revision ermöglichen, in die Sachprüfung einzutreten.	

AT 6 Dokumentation

1	Geschäfts-, Kontroll- und Überwachungsunterlagen sind systematisch und für sachkundige Dritte nachvollziehbar abzufassen und, vorbehaltlich gesetzlicher Regelungen, grundsätzlich zwei Jahre aufzubewahren. Die Aktualität und Vollständigkeit der Aktenführung ist sicherzustellen.	
2	Die für die Einhaltung dieses Rundschreibens wesentlichen Handlungen und Festlegungen sind nachvollziehbar zu dokumentieren. Dies beinhaltet auch Festlegungen hinsichtlich von Inanspruchnahmen wesentlicher Öffnungsklauseln, die gegebenenfalls zu begründen sind.	

AT 7 Ressourcen

AT 7.1 Personal

1	Die quantitative und qualitative Personalausstattung des Instituts hat sich insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation zu orientieren. Die Anforderungen dieses Moduls sind auch beim Einsatz von Leiharbeitnehmern zu beachten.	
2	Die Mitarbeiter sowie deren Vertreter müssen abhängig von ihren Aufgaben, Kompetenzen und Verantwortlichkeiten über die erforderlichen Kenntnisse und Erfahrungen verfügen. Durch geeignete Maßnahmen ist zu gewährleisten, dass das Qualifikationsniveau der Mitarbeiter angemessen ist.	
3	Die Abwesenheit oder das Ausscheiden von Mitarbeitern sollte nicht zu nachhaltigen Störungen der Betriebsabläufe führen.	
4	Die Ausgestaltung der Vergütungs- und Anreizsysteme darf den in den Strategien niedergelegten Zielen nicht widersprechen.	

AT 7.2 Technisch-organisatorische Ausstattung

1	Umfang und Qualität der technisch-organisatorischen Ausstattung haben sich insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation zu orientieren.	
2	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 17799 der International Standards Organization. Das Abstellen auf gängige Standards zielt nicht auf die Verwendung von Standardhardware beziehungsweise -software ab; Eigenentwicklungen sind grundsätzlich ebenso möglich.
3	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 Instituts im Mittelpunkt. Gegebenenfalls vorliegende Testate Dritter können bei der Abnahme berücksichtigt werden, sie können die Abnahme jedoch nicht vollständig ersetzen.
4	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.	

AT 7.3 Notfallkonzept

1	Für Notfälle in zeitkritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept). Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig durch Notfalltests zu überprüfen. Die Ergebnisse der Notfalltests sind den jeweiligen Verantwortlichen mitzuteilen. Im Falle der Auslagerung von zeit-	

	kritischen Aktivitäten und Prozessen haben das auslagernde Institut und das Auslagerungsunternehmen über ~~ein~~ aufeinander abgestimmte~~s~~ Notfallkonzept<u>e</u> zu verfügen.	
2	Das Notfallkonzept muss Geschäftsfortführungs- sowie Wiederanlaufpläne umfassen. Die Geschäftsfortführungspläne müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen. Die Wiederanlaufpläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen. Die im Notfall zu verwendenden Kommunikationswege sind festzulegen. Das Notfallkonzept muss den beteiligten Mitarbeitern zur Verfügung stehen.	

AT 8 Aktivitäten in neuen Produkten oder auf neuen Märkten

1	Für die Aufnahme von Geschäftsaktivitäten in neuen Produkten oder auf neuen Märkten (einschließlich neuer Vertriebswege) ist vorab ein Konzept auszuarbeiten. Grundlage des Konzeptes muss das Ergebnis der Analyse des Risikogehalts dieser neuen Geschäftsaktivitäten sein. In dem Konzept sind die sich daraus ergebenden wesentlichen Konsequenzen für das Management der Risiken darzustellen.	**Inhalt des Konzeptes** Zu den darzustellenden Konsequenzen gehören solche bezüglich der Organisation, des Personals, der notwendigen Anpassungen der IT-Systeme sowie rechtliche Konsequenzen (Bilanz- und Steuerrecht, etc.), soweit sie von wesentlicher Bedeutung sind.
2	Bei der Entscheidung, ob es sich um Geschäftsaktivitäten in neuen Produkten oder auf neuen Märkten handelt, ist ein vom Markt beziehungsweise vom Handel unabhängiger Bereich einzubinden.	
3	Bei Handelsgeschäften ist vor dem laufenden Handel in neuen Produkten oder auf neuen Märkten grundsätzlich eine Testphase durchzuführen. Während der Testphase dürfen Handelsgeschäfte nur in überschaubarem Umfang durchgeführt werden. Es ist sicherzustellen, dass der laufende Handel erst beginnt, wenn die Testphase erfolgreich abgeschlossen ist und geeignete Risikosteuerungs- und -controllingprozesse vorhanden sind.	**Kreditgeschäfte und Testphase** Bei Kreditgeschäften kann je nach Komplexität auch eine Testphase Grundlage des Konzeptes sein. **Einmalgeschäfte** Im Rahmen von Einmalgeschäften kann auf eine Testphase verzichtet werden.
4	Sowohl in die Erstellung des Konzeptes als auch in die Testphase sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzuschalten; im Rahmen ihrer Aufgaben ist auch die Interne Revision zu beteiligen.	