BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Mindestanforderungen an das Risikomanagement von ZAG-Instituten – ZAG-MaRisk

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

Inhalt

AT 1 Vorbemerkung

1 Dieses Rundschreiben gibt auf der Grundlage des § 27 Abs. 1 des Zahlungsdiensteaufsichtsgesetzes (ZAG) einen flexiblen und praxisnahen Rahmen für die Ausgestaltung einer ordnungsgemäßen Geschäftsorganisation der Institute vor. Es präzisiert ferner die Anforderungen der §§ 17 und 18 ZAG (Sicherungsanforderungen) sowie des § 26 ZAG (Auslagerung). Eine ordnungsgemäße Geschäftsorganisation umfasst insbesondere angemessene Maßnahmen der Unternehmenssteuerung sowie Kontrollmechanismen und Verfahren, die gewährleisten, dass das Institut seine Verpflichtungen erfüllt.

Die internen Kontrollmechanismen bestehen aus dem internen Kontrollsystem und der Internen Revision und umfassen insbesondere

- Regelungen zur Aufbau- und Ablauforganisation und
- Prozesse zur Identifizierung, Beurteilung, Steuerung, Überwachung sowie Kommunikation der Risiken (Risikosteuerungs- und -controllingprozesse).

Das interne Kontrollsystem impliziert ebenfalls die Einrichtung einer Risikocontrolling-Funktion und einer Compliance-Funktion.

Ein wirksames Risikomanagement ist ein Verfahren, das sicherstellt, dass ein Institut seine Verpflichtungen gemäß §27 Abs. 1 ZAG erfüllen kann.

Soweit ein Aufsichtsorgan besteht, schafft das Risikomanagement auch eine Grundlage für die sachgerechte Wahrnehmung der Überwachungsfunktionen des Aufsichtsorgans und beinhaltet deshalb auch dessen angemessene Einbindung.

2 Das Rundschreiben bildet einen Regelungsrahmen für die qualitative Aufsicht von Instituten unter Berücksichtigung des Prinzips der doppelten Proportionalität. Der sachgerechte Umgang mit dem Proportionalitätsprinzip seitens der Institute beinhaltet in dem prinzipienorientierten Aufbau der ZAG-MaRisk auch, dass Institute im Einzelfall über bestimmte, in den ZAG-MaRisk explizit formulierte Anforderungen hinaus weitergehende Vorkehrungen treffen, soweit dies zur Sicherstellung der Angemessenheit und Wirksamkeit des Risikomanagements erforderlich sein sollte. Insofern haben Institute, deren Geschäftsaktivitäten durch besondere Komplexität, Internationalität, als kritische Infrastruktur oder eine besondere Risikoexponierung gekennzeichnet sind, weitergehende Vorkehrungen im Bereich des Risikomanagements zu treffen als Institute mit weniger komplex strukturierten Geschäftsaktivitäten, die keine außergewöhnliche Risikoexponierung aufweisen.

3	Das Rundschreiben trägt der heterogenen Institutsstruktur und der Vielfalt der Geschäftsaktivitäten Rechnung. Es enthält zahlreiche Öffnungsklauseln, die abhängig von Komplexität der Geschäftsaktivitäten und der Risikosituation eine vereinfachte Umsetzung ermöglichen. Insoweit kann es vor allem auch von Instituten mit wenig komplexen Geschäftsaktivitäten 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.	Wenig komplexe Geschäftsaktivitäten Ob Geschäftsaktivitäten im Sinne der Proportionalität als wenig komplex gelten, ist in Abhängigkeit von Art, Umfang, der Komplexität und dem Risikogehalt der betriebenen Geschäfte im Rahmen der Risikoinventur zu beurteilen.
4	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	
5	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 der Zahlungsdienste und des Betreibens des E-Geld-Geschäfts sind in einem besonderen Teil niedergelegt (Modul BTO). Unter Berücksichtigung von Risikokonzentrationen werden in diesem Modul auch Anforderungen an die Identifizierung, Beurteilung, Steuerung sowie die Überwachung und Kommunikation von Risiken gestellt (Modul BTR). Darüber hinaus wird in Modul BT ein Rahmen für die Ausgestaltung der Internen Revision in den Instituten sowie für die Ausgestaltung der Risikoberichterstattung vorgegeben.	

AT 2 Anwendungsbereich

1 Die Beachtung der Anforderungen des Rundschreibens durch die Institute soll dazu beitragen, Missständen entgegenzuwirken, welche die Sicherheit der den Instituten anvertrauten Vermögenswerte gefährden können, die ordnungsgemäße Durchführung der Zahlungsdienste oder E-Geld-Geschäfte beeinträchtigen oder erhebliche Nachteile für die Gesamtwirtschaft herbeiführen können.

AT 2.1 Anwenderkreis

1 Die Anforderungen des Rundschreibens sind von allen Instituten im Sinne von § 1 Abs. 3 bzw. § 42 Abs. 1 ZAG 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 § 39 ZAG finden sie keine Anwendung.

AT 2.2 Risiken

1 Die Anforderungen des Rundschreibens beziehen sich auf das Management der für das Institut wesentlichen Risiken. Zur Beurteilung der Wesentlichkeit hat sich die Geschäftsleitung regelmäßig und anlassbezogen im Rahmen einer Risikoinventur einen Überblick über die Risiken des Instituts zu verschaffen, wobei die Auswirkungen von ESG-Risiken angemessen und explizit einzubeziehen sind (Gesamtrisikoprofil). Die Risiken sind auf der Ebene des gesamten Instituts zu erfassen, unabhängig davon, in welcher Organisationseinheit die Risiken verursacht wurden.

Grundsätzlich sind operationelle Risiken (einschließlich IT-Risiken) als wesentlich einzustufen. In Abhängigkeit vom Geschäftsmodell kann es erforderlich werden, u. a. die nachfolgenden Risiken als wesentlich einzustufen:

- Adressenausfallrisiken (einschließlich Erfüllungsrisiken und Charge-Back-Risiken),
- Marktpreisrisiken (einschließlich FX-Risiken und Risiken im Hinblick auf die Anlagen zur Liquiditätssicherung und Einhaltung der gesetzlichen Sicherungsanforderungen)
- Geschäftsmodellrisiken
- Liquiditätsrisiken

Mit wesentlichen Risiken verbundene Risikokonzentrationen sind zu berücksichtigen. Für Risiken, die als nicht wesentlich eingestuft werden, sind angemessene Vorkehrungen zu treffen.

Risikokonzentrationen
Neben solchen Risikopositionen gegenüber Einzeladressen, die allein aufgrund ihrer Größe eine Risikokonzentration darstellen, können Risikokonzentrationen sowohl durch den Gleichlauf von Risikopositionen innerhalb einer Risikoart („Intra-Risikokonzentrationen“) als auch durch den Gleichlauf von Risikopositionen über verschiedene Risikoarten hinweg (durch gemeinsame Risikofaktoren oder durch Interaktionen verschiedener Risikofaktoren unterschiedlicher Risikoarten - „Inter-Risikokonzentrationen“) entstehen.

Berücksichtigung von ESG-Risiken
Als ESG-Risiken im Sinne dieses Rundschreibens sind Ereignisse oder Bedingungen aus den Bereichen Umwelt, Soziales oder Unternehmensführung zu verstehen, deren Eintreten potenziell negative Auswirkungen auf die Vermögens-, Finanz- oder Ertragslage eines beaufsichtigten Unternehmens haben kann. ESG-Risiken wirken insofern als Risikotreiber und können sich auf die in Tz. 1 Satz 3 aufgeführten sowie weitere wesentliche Risikoarten auswirken.

2 Das Institut hat im Rahmen der Risikoinventur zu prüfen, welche Risiken die Vermögenslage (inklusive Kapitalausstattung), die Ertragslage oder die Liquiditätslage wesentlich beeinträchtigen können. Die Risikoinventur darf sich dabei nicht ausschließlich an den Auswirkungen in der Rechnungslegung sowie an formalrechtlichen Ausgestaltungen orientieren.

Ganzheitliche Risikoinventur
Abhängig vom konkreten Gesamtrisikoprofil des Instituts sind ggf. auch sonstige Risiken, wie etwa Reputationsrisiken, als wesentlich einzustufen.

AT 2.3 Geschäfte

1 Zahlungsdienste und E-Geld-Geschäfte und alle zugelassenen Nebentätigkeiten im Sinne dieses Rundschreibens werden in dem Merkblatt – Hinweise zum Zahlungsdiensteaufsichtsgesetz (ZAG) konkretisiert und können unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html diesem entnommen werden.

AT 3 Gesamtverantwortung der Geschäftsleitung

1	Alle Geschäftsleiter (§ 1 Abs. 8 ZAG) sind, unabhängig von der internen Zuständigkeitsregelung, für die ordnungsgemäße Geschäftsorganisation und deren Weiterentwicklung verantwortlich. Diese Verantwortung bezieht sich unter Berücksichtigung ausgelagerter Aktivitäten und Prozesse auf alle wesentlichen Elemente des Risikomanagements. Die Geschäftsleiter werden dieser Verantwortung nur gerecht, wenn sie die Risiken, einschließlich ESG-Risiken, beurteilen können und die erforderlichen Maßnahmen zu ihrer Begrenzung treffen. Hierzu zählen auch die Entwicklung, Förderung, Integration und Überwachung einer angemessenen Risikokultur auf allen Ebenen innerhalb des Instituts.	Risikokultur Die Risikokultur beschreibt allgemein die Art und Weise, wie die Beschäftigten des Instituts im Rahmen ihrer Tätigkeit mit Risiken umgehen (sollen). Die Risikokultur soll die Identifizierung und den bewussten Umgang mit Risiken fördern und sicherstellen, dass Entscheidungsprozesse zu Ergebnissen führen, die auch unter Risikogesichtspunkten ausgewogen sind. Kennzeichnend für eine angemessene Risikokultur ist vor allem das klare Bekenntnis der Geschäftsleitung zu risikoangemessenem Verhalten die strikte Beachtung des durch die Geschäftsleitung kommunizierten Risikoappetits durch alle Mitarbeiter, die Rechenschaftspflicht der Mitarbeiter für ihr Risikoverhalten und die Ermöglichung und Förderung eines transparenten und offenen Dialogs innerhalb des Instituts zu risikorelevanten Fragen. Die Institute müssen Verfahren einrichten, mit denen sie überwachen, ob die Mitarbeiter die Risikokultur einhalten. Wenn bei dieser Überwachung Mängel der Risikokultur festgestellt werden, sollte das Institut diese durch durchdachte, ergebnisorientierte und frühzeitige Maßnahmen beenden.
2	Ungeachtet der Gesamtverantwortung der Geschäftsleitung für die ordnungsgemäße Geschäftsorganisation und insbesondere für ein angemessenes und wirksames Risikomanagement ist jeder Geschäftsleiter für die Einrichtung angemessener Kontroll- und Überwachungsprozesse in seinem jeweiligen Zuständigkeitsbereich verantwortlich.	

AT 4 Allgemeine Anforderungen an das Risikomanagement

AT 4.1 Abschirmung von Risiken

1	Auf der Grundlage des Gesamtrisikoprofils ist sicherzustellen, dass die wesentlichen Risiken des Instituts durch Risikodeckungspotenzial, unter Berücksichtigung von Risikokonzentrationen, ausreichend abgeschirmt sind. Die Auswirkungen von ESG-Risiken i.S. von AT 2.2 Tz. 1 sind angemessen und explizit zu berücksichtigen.	Begrenzung und Überwachung von Risiken und damit verbundenen Risikokonzentrationen Geeignete Maßnahmen zur Begrenzung von Risiken und damit verbundenen Risikokonzentrationen können qualitative Instrumente (z. B. regelmäßige Risikoanalysen und Vorkehrungen zur Risikomitigation) bzw. quantitative Instrumente (z. B. Szenarioansätze, Ampelsysteme oder – soweit sinnvoll – Limitsysteme,) umfassen.
2	Die Angemessenheit der Methoden und Verfahren ist zumindest jährlich durch die fachlich zuständigen Mitarbeiter zu überprüfen.	

AT 4.2 Strategien

1 Die Geschäftsleitung hat eine ökonomisch nachhaltige Geschäftsstrategie festzulegen, in der die Ziele des Instituts für jede wesentliche Geschäftsaktivität sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden. Diese Strategieentwicklung setzt daher eine eingehende, zukunftsgerichtete Analyse des Geschäftsmodells voraus. Bei der Festlegung und Anpassung der Geschäftsstrategie sind sowohl externe Einflussfaktoren (z. B. Marktentwicklung, Wettbewerbssituation, regulatorisches Umfeld, veränderte Umweltbedingungen und Transition zu einer nachhaltigen Wirtschaft unter Berücksichtigung möglicher Entwicklungen über einen angemessen langen Zeitraum) als auch interne Einflussfaktoren (z. B. Liquidität, Ertragslage, personelle und technisch-organisatorische Ressourcen) zu berücksichtigen. Im Hinblick auf die zukünftige Entwicklung der relevanten Einflussfaktoren sind Annahmen zu treffen. Die Annahmen sind einer mindestens jährlichen und anlassbezogenen Überprüfung zu unterziehen; erforderlichenfalls ist die Geschäftsstrategie anzupassen.

Prüfungshandlungen durch Jahresabschlussprüfer oder die Interne Revision

Der Inhalt der Geschäftsstrategie liegt allein in der Verantwortung der Geschäftsleitung und ist nicht Gegenstand von Prüfungshandlungen durch Jahresabschlussprüfer oder die Interne Revision. Bei der Überprüfung der Risikostrategie ist die Geschäftsstrategie heranzuziehen, um die Konsistenz zwischen beiden Strategien nachvollziehen zu können. Gegenstand der Prüfung ist außerdem der Strategieprozess nach AT 4.2 Tz. 5.

Strategische Ziele sowie Maßnahmen zu deren Erreichung

Die Darstellung der strategischen Ziele sowie der Maßnahmen zur Erreichung dieser Ziele stecken die Eckpunkte für die operative Planung ab und müssen daher hinreichend konkret formuliert sein, um plausibel in die operative Unternehmensplanung überführt werden zu können.

Analyse des Geschäftsmodells

Mithilfe der Geschäftsmodellanalyse soll das Institut beurteilen, ob sich das eigene Geschäftsmodell über einen angemessen langen, mehrjährigen Zeitraum aufrechterhalten lässt. Dazu ist es erforderlich, dass die für den betreffenden Zeitraum getroffenen strategischen Vorgaben und die daraus abgeleiteten Geschäftsplanungen das angestrebte Geschäftsmodell umsetzen. Das Institut soll dadurch in die Lage versetzt werden, Anpassungsbedarf am Geschäftsmodell frühzeitig zu erkennen und erforderliche strategische Steuerungsmaßnahmen zu ergreifen.

Besondere strategische Aspekte

Aufgrund der Bedeutung für das Funktionieren der Prozesse im Institut hat das Institut in Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten auch Aussagen zur zukünftig geplanten Ausgestaltung der IT-Systeme zu treffen. Im Falle umfangreicher Auslagerungen sind auch entsprechende Ausführungen hierzu erforderlich.

2	Die Geschäftsleitung hat eine mit der Geschäftsstrategie und den daraus resultierenden Risiken konsistente Risikostrategie festzulegen. Die Risikostrategie hat, ggf. unterteilt in Teilstrategien für die wesentlichen Risiken, unter expliziter Berücksichtigung der Auswirkungen von ESG-Risiken, die Ziele der Risikosteuerung der wesentlichen Geschäftsaktivitäten sowie die Maßnahmen zur Erreichung dieser Ziele zu umfassen. Risikokonzentrationen sind dabei auch mit Blick auf die Ertragssituation des Instituts (Ertragskonzentrationen) zu berücksichtigen. Dies setzt voraus, dass das Institut seine Erfolgsquellen voneinander abgrenzen und diese quantifizieren kann.	Risikoappetit Mit der Festlegung des Risikoappetits trifft die Geschäftsleitung eine bewusste Entscheidung darüber, in welchem Umfang sie bereit ist, Risiken einzugehen. Der Risikoappetit kann in vielfacher Weise zum Ausdruck gebracht werden. Neben rein quantitativen Vorgaben kann der Risikoappetit auch in der Festlegung von qualitativen Vorgaben zur Geltung kommen. Basierend auf geeigneten Risikoindikatoren sind bei der Festlegung des Risikoappetits ebenfalls die Auswirkungen von ESG-Risiken explizit zu berücksichtigen.
3	Nutzt das Institut die Möglichkeit der Anlage in sichere, liquide Aktiva mit niedrigem Risiko nach § 17 Abs. 1 S. 2 Nr. 1. b) ZAG, hat die Geschäftsleitung zudem eine nachhaltige Investitionsstrategie und Anlagepolitik festzulegen, in der die Ziele der Investitionsstrategie sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden.	
4	Die Geschäftsleitung ist verantwortlich für die Festlegung und Anpassung der Strategien; diese Verantwortung 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. Es bleibt dem Institut überlassen, die Risikostrategie in die Geschäftsstrategie zu integrieren.	
5	Die Geschäftsleitung hat einen Strategieprozess einzurichten, der sich insbesondere auf die Prozessschritte Planung, Umsetzung, Beurteilung und Anpassung der Strategien erstreckt. Für die Zwecke der Beurteilung sind die in den Strategien niedergelegten Ziele so zu formulieren, dass eine sinnvolle Überprüfung der Zielerreichung möglich ist. Die Ursachen für etwaige Abweichungen sind zu analysieren.	
6	Die Strategien sowie ggf. erforderliche Anpassungen der Strategien sind dem Aufsichtsorgan des Instituts zur Kenntnis zu geben und mit diesem zu erörtern. Die Erörterung erstreckt sich auch auf die Ursachenanalyse nach AT 4.2 Tz. 5 im Falle von Zielabweichungen.	Ausschüsse des Aufsichtsorgans Soweit ein Aufsichtsorgan besteht, sollte Adressat der Strategien 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.
7	Die Inhalte sowie Änderungen der Strategien sind 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,
b) Risikosteuerungs- und -controllingprozesse einzurichten und
c) eine Risikocontrolling-Funktion und eine Compliance-Funktion zu implementieren.

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 und auch bei Arbeitsplatzwechseln Interessenkonflikte vermieden werden.

2 Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen sowie Kommunikationswege sind klar zu definieren und aufeinander abzustimmen. Berechtigungen und Kompetenzen sind nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) zu vergeben und bei Bedarf zeitnah anzupassen. Dies beinhaltet auch die regelmäßige und anlassbezogene Überprüfung von IT-Berechtigungen, Zeichnungsberechtigungen und sonstigen eingeräumten Kompetenzen innerhalb angemessener Fristen. Die Fristen orientieren sich dabei an der Bedeutung der Prozesse und, bei IT-Berechtigungen, dem Schutzbedarf verarbeiteter Informationen. Das gilt auch bezüglich der Schnittstellen zu wesentlichen Auslagerungen.

Überprüfung von Berechtigungen und Kompetenzen
Zeichnungsberechtigungen in Verbindung mit Zahlungsverkehrskonten und wesentliche IT-Berechtigungen sind mindestens jährlich zu überprüfen, alle anderen mindestens alle drei Jahre. Besonders kritische IT-Berechtigungen, wie sie bspw. Administratoren aufweisen, sind mindestens halbjährlich zu überprüfen.

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

Intragruppenforderungen
Intragruppenforderungen sind in den Risikosteuerungs- und –controllingprozessen angemessen abzubilden.

Berücksichtigung von ESG-Risiken
Das Institut untersucht und dokumentiert vor dem Hintergrund der Besonderheiten seiner Risikopositionen umfassend und, soweit sinnvoll und möglich, auch quantitativ die Auswirkungen wesentlicher

	der wesentlichen Risiken und explizit der Auswirkungen von ESG-Risiken und damit verbundener Risikokonzentrationen gewährleisten. Diese Prozesse sind in eine gemeinsame Ertrags- und Risikosteuerung („Gesamtinstitutsteuerung“) einzubinden.	ESG-Risiken auf die in AT 2.2 Tz. 1 a)-d) aufgeführten sowie weitere wesentliche Risikoarten.
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. Hierzu hat das Institut geeignete Indikatoren für die frühzeitige Identifizierung von Risiken sowie von risikoartenübergreifenden Effekten abzuleiten, die je nach Risikoart auf quantitativen und/oder qualitativen Risikomerkmalen basieren.	
3	Die Geschäftsleitung hat sich in angemessenen Abständen über die Geschäftslage und die Risikosituation einschließlich vorhandener Risikokonzentrationen berichten zu lassen. Zudem hat die Geschäftsleitung das Aufsichtsorgan mindestens jährlich über die Geschäftslage und Risikosituation einschließlich vorhandener Risikokonzentrationen in angemessener Weise schriftlich zu informieren. Einzelheiten zur Geschäfts- und Risikoberichterstattung an die Geschäftsleitung und an das Aufsichtsorgan sind in BT 3 geregelt.	
4	Unter Risikogesichtspunkten wesentliche Informationen sind unverzüglich an die Geschäftsleitung, die jeweiligen Verantwortlichen und ggf. die Interne Revision weiterzuleiten, so dass geeignete Maßnahmen bzw. Prüfungshandlungen frühzeitig eingeleitet werden können. Hierfür ist ein geeignetes Verfahren festzulegen.	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.
5	Die Risikosteuerungs- und -controllingprozesse sowie die zur Risikoabschirmung eingesetzten Methoden und Verfahren sind regelmäßig sowie bei sich ändernden Bedingungen auf ihre Angemessenheit zu überprüfen und ggf. anzupassen. Dies betrifft insbesondere auch die Plausibilisierung der ermittelten Ergebnisse und der zugrundeliegenden Daten.	

AT 4.3.3 Stresstests

1	Es sind regelmäßig sowie anlassbezogen angemessene Stresstests für die wesentlichen Risiken durchzuführen, die Art, Umfang, Komplexität und den Risikogehalt der Geschäftsaktivitäten widerspiegeln. Hierfür sind die für die jeweiligen Risiken wesentlichen Risikofaktoren zu identifizieren und gegebenenfalls die Auswirkungen von ESG-Risiken zu berücksichtigen. Die Stresstests haben	

	auch außergewöhnliche, aber plausibel mögliche Ereignisse abzubilden. Bei der Festlegung der Szenarien sind die strategische Ausrichtung des Instituts und sein wirtschaftliches Umfeld zu berücksichtigen. Die Stresstests haben sich auch auf die angenommenen Risikokonzentrationen zu erstrecken.
2	Die Angemessenheit der Stresstests sowie deren zugrunde liegende Annahmen sind in regelmäßigen Abständen, mindestens aber jährlich, zu überprüfen.
3	Die Ergebnisse der Stresstests sind kritisch zu reflektieren. Dabei ist zu ergründen, inwieweit und, wenn ja, welcher Handlungsbedarf besteht.

AT 4.4 Besondere Funktionen

AT 4.4.1 Risikocontrolling-Funktion

1 Jedes Institut muss über eine unabhängige Risikocontrolling-Funktion verfügen, die für die angemessene Überwachung und Kommunikation der wesentlichen Risiken unter Berücksichtigung der Auswirkungen von ESG-Risiken zuständig ist. Die Risikocontrolling-Funktion ist aufbauorganisatorisch bis einschließlich der Ebene der Geschäftsleitung von den operativen Geschäftsbereichen zu trennen.

2 Die Risikocontrolling-Funktion hat insbesondere die folgenden Aufgaben:

- Unterstützung der Geschäftsleitung in allen risikopolitischen Fragen, insbesondere bei der Entwicklung und Umsetzung der Risikostrategie sowie bei der Ausgestaltung eines Systems zur Begrenzung der Risiken,
- Durchführung der Risikoinventur und Erstellung des Gesamtrisikoprofils,
- Unterstützung der Geschäftsleitung bei der Einrichtung und Weiterentwicklung der Risikosteuerungs- und -controllingprozesse,
- Einrichtung und Weiterentwicklung eines Systems von Risikokennzahlen und eines Risikofrüherkennungsverfahrens,
- Laufende Überwachung der Risikosituation des Instituts und der Risikoabschirmung
- Regelmäßige Erstellung der Risikoberichte für die Geschäftsleitung,
- Verantwortung für die Prozesse zur unverzüglichen Weitergabe von unter Risikogesichtspunkten wesentlichen Informationen an die Geschäftsleitung, die jeweiligen Verantwortlichen und ggf. die Interne Revision.

3 Den Mitarbeitern der Risikocontrolling-Funktion sind alle notwendigen Befugnisse und ein uneingeschränkter Zugang zu allen Informationen einzuräumen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Hierzu gehört insbesondere auch ein uneingeschränkter und jederzeitiger Zugang zu den Risikodaten des Instituts

4	Die Leitung der Risikocontrolling-Funktion ist einer Person auf einer ausreichend hohen Führungsebene zu übertragen.	
5	Wechselt die Leitung der Risikocontrolling-Funktion, ist das Aufsichtsorgan rechtzeitig vorab unter Angabe der Gründe für den Wechsel zu informieren.	

AT 4.4.2 Compliance-Funktion

1	Jedes Institut muss über eine Compliance-Funktion verfügen, um den Risiken, die sich aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben ergeben können, entgegenzuwirken. Die Compliance-Funktion hat auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben und entsprechender Kontrollen hinzuwirken. Ferner hat die Compliance-Funktion die Geschäftsleitung hinsichtlich der Einhaltung dieser rechtlichen Regelungen und Vorgaben zu unterstützen und zu beraten.	Verantwortung der Geschäftsleiter und der Geschäftsbereiche Unbeschadet der Aufgaben der Compliance-Funktion bleiben die Geschäftsleiter und die Geschäftsbereiche für die Einhaltung rechtlicher Regelungen und Vorgaben uneingeschränkt verantwortlich. Verhältnis zu anderen aufsichtlichen Vorgaben Alle sonstigen Vorgaben zur Compliance-Funktion, die sich aus anderen Aufsichtsgesetzen ergeben , bleiben unberührt.
2	Die Identifizierung der wesentlichen rechtlichen Regelungen und Vorgaben, deren Nichteinhaltung zu einer Gefährdung des Vermögens des Instituts führen kann, erfolgt unter Berücksichtigung von Risikogesichtspunkten in regelmäßigen Abständen durch die Compliance-Funktion.	
3	Grundsätzlich ist die Compliance-Funktion unmittelbar der Geschäftsleitung unterstellt und berichtspflichtig. Sie kann auch an andere Kontrolleinheiten angebunden werden, sofern eine direkte Berichtslinie zur Geschäftsleitung existiert. Zur Erfüllung ihrer Aufgaben kann die Compliance-Funktion auch auf andere Funktionen und Stellen zurückgreifen. Die Compliance-Funktion ist abhängig von der Art, dem Umfang, der Komplexität und dem Risikogehalt der Geschäftsaktivitäten in einem von den operativen Geschäftsbereichen unabhängigen Bereich anzusiedeln.	Anbindung an andere Kontrolleinheiten Andere Kontrolleinheiten können z. B. das Risikocontrolling oder der Geldwäschebeauftragte, nicht jedoch die Interne Revision sein.

4	Das Institut hat einen Compliance-Beauftragten zu benennen, der für die Erfüllung der Aufgaben der Compliance-Funktion verantwortlich ist. Abhängig von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten des Instituts kann im Ausnahmefall die Funktion des Compliance-Beauftragten auch einem Geschäftsleiter übertragen werden.	
5	Den Mitarbeitern der Compliance-Funktion sind ausreichende Befugnisse und ein uneingeschränkter Zugang zu allen Informationen einzuräumen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Weisungen und Beschlüsse der Geschäftsleitung, die für die Compliance-Funktion wesentlich sind, sind ihr bekanntzugeben. Über wesentliche Änderungen der Regelungen, die die Einhaltung der wesentlichen rechtlichen Regelungen und Vorgaben gewährleisten sollen, sind die Mitarbeiter der Compliance-Funktion rechtzeitig zu informieren.	
6	Die Compliance-Funktion hat mindestens jährlich sowie anlassbezogen der Geschäftsleitung über ihre Tätigkeit Bericht zu erstatten. Darin ist auf die Angemessenheit und Wirksamkeit der Regelungen zur Einhaltung der wesentlichen rechtlichen Regelungen und Vorgaben einzugehen. Ferner hat der Bericht auch Angaben zu möglichen Defiziten sowie zu Maßnahmen zu deren Behebung zu enthalten. Die Berichte sind auch an das Aufsichtsorgan und die Interne Revision weiterzuleiten.	Ausschüsse des Aufsichtsorgans Adressat der Berichterstattung 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	Wechselt die Position des Compliance-Beauftragten, ist das Aufsichtsorgan rechtzeitig vorab unter Angabe der Gründe für den Wechsel zu informieren.	

AT 4.4.3 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. Unbeschadet dessen ist sicherzustellen, dass der Vorsitzende des Aufsichtsorgans unter Einbeziehung der Geschäftsleitung direkt bei dem Leiter der Internen Revision Auskünfte einholen kann.	Einholung von Auskünften durch den Vorsitzenden des Aufsichtsorgans Wenn das Institut einen Prüfungsausschuss eingerichtet hat, kann alternativ sichergestellt werden, dass der Vorsitzende des Prüfungsausschusses Auskünfte beim Leiter der Internen Revision einholen kann.
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.	
6	Wechselt die Leitung der Internen Revision, ist das Aufsichtsorgan rechtzeitig vorab unter Angabe der Gründe für den Wechsel 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 bekanntgemacht 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 zu den Verantwortlichkeiten, b) Regelungen hinsichtlich der Ausgestaltung der Risikosteuerungs- und -controllingprozesse, c) Regelungen zur Internen Revision, d) Regelungen, die die Einhaltung rechtlicher Regelungen und Vorgaben (z. B. Datenschutz, Compliance) gewährleisten, e) Regelungen zu Verfahrensweisen bei Auslagerungen, f) abhängig von der Größe des Instituts sowie der Art, dem Umfang, der Komplexität und dem Risikogehalt der Geschäftsaktivitäten, einen Verhaltenskodex für die Mitarbeiter. g) Verfahren für den Zugang zu und Umgang mit sensiblen Zahlungsdaten Die Organisationsrichtlinien haben auch Regelungen zur Berücksichtigung der Auswirkungen von ESG-Risiken zu beinhalten.	Regelungen zu Verfahrensweisen bei Auslagerungen Die Regelungen zu Verfahrensweisen bei Auslagerungen haben die zentralen Phasen des Lebenszyklus von Auslagerungsvereinbarungen zu umfassen und Definitionen der Grundsätze, Zuständigkeiten und Prozesse zu enthalten. Die Regelungen zu Verfahrensweisen in Bezug auf Auslagerungen sollen sicherstellen, dass das Auslagerungsunternehmen in einer mit den Werten und dem Verhaltenskodex des auslagernden Instituts im Einklang stehenden Weise handelt.
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 grundsätzlich fünf 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 der Inanspruchnahme wesentlicher Öffnungsklauseln, die ggf. zu begründen ist.	

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. Dies gilt auch beim Rückgriff auf Leiharbeitnehmer.	
2	Die Mitarbeiter sowie deren Vertreter müssen abhängig von ihren Aufgaben, Kompetenzen und Verantwortlichkeiten über die erforderlichen Kenntnisse und Erfahrungen verfügen sowie mit den Werten und Risikoerwartungen des Instituts vertraut sein. Durch geeignete Maßnahmen ist zu gewährleisten, dass das Qualifikationsniveau der Mitarbeiter angemessen ist.	Anforderungen an die Qualifikation bei besonderen Funktionen Die mit der Leitung der Risikocontrolling-Funktion und der Leitung der Internen Revision betrauten Personen sowie der Compliance-Beauftragte haben besonderen qualitativen Anforderungen entsprechend ihres Aufgabengebietes zu genügen.
3	Die Abwesenheit oder das Ausscheiden von Mitarbeitern sollte nicht zu nachhaltigen Störungen der Betriebsabläufe führen.	

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), die zugehörigen IT-Prozesse und sonstige Bestandteile des Informationsverbundes 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, insbesondere sind Prozesse für eine angemessene IT-Berechtigungsvergabe einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt; die Zusammenfassung von Berechtigungen in einem Rollenmodell ist möglich. Die Eignung der IT-Systeme und der zugehörigen Prozesse ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.	Informationsverbund Zu einem Informationsverbund gehören bspw. geschäftsrelevante Informationen, Geschäfts- und Unterstützungsprozesse, IT-Systeme und die zugehörigen IT-Prozesse sowie Netz- und Gebäudeinfrastrukturen. Standards zur Ausgestaltung der IT-Systeme Zu solchen Standards zählen z. B. der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und die internationalen Sicherheitsstandards ISO/IEC 270XX der International Organization for Standardization. Das Abstellen auf gängige Standards zielt nicht auf die Verwendung von Standardhardware bzw. -software ab. Eigenentwicklungen sind grundsätzlich ebenso möglich. Zugriffsrechte Die eingerichteten Berechtigungen dürfen nicht im Widerspruch zur organisatorischen Zuordnung von Mitarbeitern stehen. Insbesondere bei Berechtigungsvergaben im Rahmen von Rollenmodellen ist darauf zu achten, dass Funktionstrennungen beibehalten bzw. Interessenkonflikte vermieden werden.
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. Hierfür ist ein Regelprozess der Entwicklung, des Testens, der Freigabe und der Implementierung in die Produktionsprozesse zu etablieren. 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	Für IT-Risiken sind angemessene Überwachungs- und Steuerungsprozesse einzurichten, die insbesondere die Festlegung von IT-Risikokriterien, die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie die Festlegung entsprechender Maßnahmen zur Risikobehandlung und –minderung umfassen. Beim Bezug von Software sind die damit verbundenen Risiken angemessen zu bewerten.	
5	Die Anforderungen aus AT 7.2 sind auch beim Einsatz von durch Mitarbeiter des Fachbereichs entwickelten oder betriebenen Anwendungen (Individuelle Datenverarbeitung - „IDV“) entsprechend der Kritikalität der unterstützten Geschäftsprozesse und der Bedeutung der Anwendungen für diese Prozesse zu beachten. Die Festlegung von Maßnahmen zur Sicherstellung der Datensicherheit hat sich am Schutzbedarf der verarbeiteten Daten zu orientieren.	

AT 7.3 Notfallmanagement

1	Das Institut hat Ziele zum Notfallmanagement zu definieren und hieraus abgeleitet einen Notfallmanagementprozess festzulegen. 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. Das Notfallkonzept ist anlassbezogen zu aktualisieren, jährlich auf Aktualität zu überprüfen und angemessen zu kommunizieren. Die Geschäftsleitung hat sich mindestens quartalsweise und anlassbezogen über den Zustand des Notfallmanagements schriftlich berichten zu lassen.	Zeitkritische Aktivitäten und Prozesse Zeitkritisch sind grundsätzlich jene Aktivitäten und Prozesse, bei deren Beeinträchtigung für definierte Zeiträume ein nicht mehr akzeptabler Schaden für das Institut zu erwarten ist. Zur Identifikation von zeitkritischen Aktivitäten und Prozessen sowie von unterstützenden Aktivitäten und Prozessen, hierfür notwendigen IT-Systemen und sonstigen notwendigen Ressourcen sowie der potentiellen Gefährdungen führt das Institut Auswirkungsanalysen und Risikoanalysen durch. Als Basis hierfür dient eine Übersicht über alle Aktivitäten und Prozesse (z. B. in Form einer Prozesslandkarte). Auswirkungsanalysen In Auswirkungsanalysen (Business Impact Analysen) wird über abgestufte Zeiträumebetrachtet, welche Folgen eine Beeinträchtigung von Aktivitäten und Prozessen für den Geschäftsbetrieb haben kann. Die Auswirkungsanalysen sollten u. a. folgende Aspekte berücksichtigen: - Art und Umfang des (im-)materiellen Schadens, - Zeitpunkt des Ausfalls. Risikoanalysen In Risikoanalysen (Risk Impact Analysen) für die identifizierten zeitkritischen Aktivitäten und Prozesse werden potentielle Gefährdungen identifiziert und bewertet, welche eine Beeinträchtigung der zeitkritischen Geschäftsprozesse verursachen könnte.
2	Das Notfallkonzept muss Geschäftsfortführungs- sowie Wiederherstellungspläne umfassen. Geschäftsfortführungspläne müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen. Wiederherstellungspläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen. Bei Notfällen ist eine angemessene interne und externe	Notfallkonzept Im Notfallkonzept werden Verantwortlichkeiten, Ziele und Maßnahmen zur Fortführung bzw. Wiederherstellung von zeitkritischen Aktivitäten und Prozessen bestimmt und Kriterien für die Einstufung sowie für das Auslösen der Pläne definiert.

	Kommunikation sicherzustellen. Im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen haben das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte zu verfügen.	Notfallszenarien Hierbei werden mindestens folgende Szenarien berücksichtigt: - (Teil-)Ausfall eines Standortes (z. B. durch Hochwasser, Großbrand, Gebietssperrung, Ausfall der Zutrittskontrolle) - Erheblicher Ausfall von IT-Systemen oder Kommunikationsinfrastruktur (z. B. aufgrund von Fehlern oder Angriffen) - Ausfall einer kritischen Anzahl von Mitarbeitern (z. B. bei Pandemie, Lebensmittelvergiftung, Streik) - Ausfall von Dienstleistern (z. B. Zulieferer, Stromversorger).
3	Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig zu überprüfen. Für zeitkritische Aktivitäten und Prozesse ist sie für alle relevanten Szenarien mindestens jährlich und anlassbezogen nachzuweisen. Überprüfungen des Notfallkonzeptes sind zu protokollieren. Ergebnisse sind hinsichtlich notwendiger Verbesserungen zu analysieren. Risiken sind angemessen zu steuern. Die Ergebnisse sind den jeweiligen Verantwortlichen schriftlich mitzuteilen.	Überprüfungen des Notfallkonzeptes Die Häufigkeit und der Umfang der Überprüfungen soll sich grundsätzlich an der Gefährdungslage orientieren. Dienstleister sind angemessen einzubinden. Überprüfungen beinhalten u. a.: - Test der technischen Vorsorgemaßnahmen - Kommunikations-, Krisenstabs- und Alarmierungsübungen - Ernstfall- oder Vollübungen.

AT 8 Anpassungsprozesse

AT 8.1 Neu-Produkt-Prozess

1	Jedes Institut muss die von ihm betriebenen Geschäftsaktivitäten verstehen. Für die Aufnahme von Geschäftsaktivitäten in neuen Produkten oder auf neuen Märkten (einschließlich neuer Vertriebswege) ist vorab ein Konzept auszuarbeiten. Grundlage des Konzeptes müssen das Ergebnis der Analyse des Risikogehalts dieser neuen Geschäftsaktivitäten sowie deren Auswirkungen auf das Gesamtrisikoprofil 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, der Methoden zur Beurteilung damit verbundener Risiken sowie rechtliche Konsequenzen (Bilanz- und Steuerrecht etc.), soweit sie von wesentlicher Bedeutung sind.
2	Das Institut hat einen Katalog jener Produkte und Märkte vorzuhalten, die Gegenstand der Geschäftsaktivitäten sein sollen. In einem angemessenen Turnus ist zu überprüfen, ob die Produkte noch verwendet werden. Produkte, die über einen längeren Zeitraum nicht mehr Gegenstand der Geschäftstätigkeit waren, sind zu kennzeichnen.	
3	Bei der Entscheidung, ob es sich um Geschäftsaktivitäten in neuen Produkten oder auf neuen Märkten handelt, ist ein vom operativem Geschäftsbereich unabhängiger Bereich einzubinden.	
4	In die Erstellung des Konzeptes sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzuschalten. Im Rahmen ihrer Aufgaben sind auch die Risikocontrolling-Funktion, die Compliance-Funktion und die Interne Revision zu beteiligen.	
5	Das Konzept und die Aufnahme der laufenden Geschäftstätigkeit sind von den zuständigen Geschäftsleitern unter Einbeziehung der für die Überwachung der Geschäfte verantwortlichen Geschäftsleiter zu genehmigen. Diese Genehmigungen können delegiert werden, sofern dafür klare Vorgaben erlassen wurden und die Geschäftsleitung zeitnah über die Entscheidungen informiert wird.	
6	Soweit nach Einschätzung der in die Arbeitsabläufe eingebundenen Organisationseinheiten Aktivitäten in einem neuen Produkt oder auf einem neuen Markt sachgerecht gehandhabt werden können, ist die Ausarbeitung eines Konzeptes nach Tz. 1 nicht erforderlich.	

AT 8.2 Änderungen betrieblicher Prozesse oder Strukturen

1 Vor wesentlichen Veränderungen in der Aufbau- und Ablauforganisation sowie in den IT-Systemen hat das Institut die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren. In diese Analysen sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzuschalten. Im Rahmen ihrer Aufgaben sind auch die Risikocontrolling-Funktion, die Compliance-Funktion und die Interne Revision zu beteiligen.

AT 8.3 Übernahmen und Fusionen

1 Vor der Übernahme anderer Unternehmen oder Fusionen mit anderen Unternehmen hat das Institut ein Konzept zu erarbeiten, in dem die wesentlichen strategischen Ziele, die voraussichtlichen wesentlichen Konsequenzen für das Management der Risiken und die wesentlichen Auswirkungen auf das Gesamtrisikoprofil des Instituts bzw. der Gruppe gemäß § 1 Abs. 6 ZAG dargestellt werden. Dies umfasst auch die mittelfristig geplante Entwicklung der Vermögens-, Finanz- und Ertragslage, die voraussichtliche Höhe der Risikopositionen, die notwendigen Anpassungen der Risikosteuerungs- und –controllingprozesse und der IT-Systeme sowie die Darstellung wesentlicher rechtlicher Konsequenzen (Bilanzrecht, Steuerrecht etc.).

AT 9 Auslagerung

1 Eine Auslagerung liegt vor, wenn ein anderes Unternehmen mit der Wahrnehmung solcher Aktivitäten und Prozesse im Zusammenhang mit dem Betrieb von E-Geld-Geschäften, Zahlungsdiensten oder sonstigen institutstypischen Dienstleistungen beauftragt wird, die ansonsten vom Institut selbst erbracht würden. Zivilrechtliche Gestaltungen und Vereinbarungen können dabei das Vorliegen einer Auslagerung nicht von vornherein ausschließen.

Sonstiger Fremdbezug von Leistungen

Der sonstige Fremdbezug von Leistungen ist nicht als Auslagerung im Sinne dieses Rundschreibens zu qualifizieren. Hierzu zählt zunächst der einmalige oder gelegentliche Fremdbezug von Gütern und Dienstleistungen. Ebenso erfasst werden Leistungen, die typischerweise von einem beaufsichtigten Unternehmen bezogen und aufgrund tatsächlicher Gegebenheiten oder rechtlicher Vorgaben regelmäßig weder zum Zeitpunkt des Fremdbezugs noch in der Zukunft vom Institut selbst erbracht werden können. Dazu zählen z. B.

- die Nutzung von Zentralbankfunktionen (innerhalb von Finanzverbünden) bzw. Clearingstellen im Rahmen des Zahlungsverkehrs und der Wertpapierabwicklung,
  die Inanspruchnahme von Liquiditätslinien,
- die Nutzung der Verwahrung von Vermögensgegenständen nach dem Depotgesetz,
- die Nutzung öffentlich zugänglicher (auch kostenpflichtiger) Daten von Marktinformationsdienstleistern (z. B. öffentliche Daten von Ratingfirmen, die nicht zielgerichtet für das Institut generiert / bearbeitet worden sind),
- die Verwendung von globalen Zahlungsverkehrsinfrastrukturen (z. B. Kartenzahlverfahren),
- die Nutzung von globalen Nachrichteninfrastrukturen zur Übermittlung von Zahlungsverkehrsdaten, die der Aufsicht durch zuständige Behörden unterliegen, sowie
- der Erwerb von Dienstleistungen wie die Bereitstellung eines Rechtsgutachtens, die Vertretung vor Gericht und Verwaltungsbehörden als auch Versorgungsleistungen.

Die Anwendung der einschlägigen Regelungen zu § 26 ZAG ist angesichts der besonderen, mit solchen Konstellationen einhergehenden Risiken regelmäßig nicht angemessen. Dessen ungeachtet hat das Institut auch beim sonstigen Fremdbezug von Leistungen die

		allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 27 ZAG zu beachten. Der isolierte Bezug von Software ist in der Regel als sonstiger Fremdbezug einzustufen. Hierzu gehören u. a. auch die folgenden Unterstützungsleistungen: - die Anpassung der Software an die Erfordernisse des Instituts, - die entwicklungstechnische Umsetzung von Änderungswünschen (Programmierung), - das Testen, die Freigabe und die Implementierung der Software in die Produktionsprozesse beim erstmaligen Einsatz und bei wesentlichen Veränderungen insbesondere von programmtechnischen Vorgaben, - Fehlerbehebungen (Wartung) gemäß der Anforderungs-/Fehlerbeschreibung des Auftraggebers oder Herstellers, - sonstige Unterstützungsleistungen, die über die reine Beratung hinausgehen. Dies gilt nicht für Software, die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt wird oder die für die Durchführung des E-Geld-Geschäfts oder Zahlungsdiensten von wesentlicher Bedeutung ist; bei dieser Software sind Unterstützungsleistungen als Auslagerung einzustufen. Die gleichen Maßstäbe gelten für den Betrieb der Software durch einen externen Dritten.
2	Das Institut muss anhand einer Risikoanalyse bewerten, welche Risiken mit einer Auslagerung verbunden sind. Ausgehend von dieser Risikoanalyse ist eigenverantwortlich festzulegen, welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind (wesentliche Auslagerungen). Diese ist auf der Grundlage von institutsweit bzw. gruppenweit einheitlichen Rahmenvorgaben sowohl regelmäßig als auch anlassbezogen durchzuführen. Die Ergebnisse der Risikoanalyse sind in der Auslagerungs- und Risikosteuerung zu beachten. Die maßgeblichen Organisationseinheiten sind bei der Erstellung der Risikoanalyse einzubeziehen. Im Rahmen ihrer Aufgaben ist auch die Interne Revision zu beteiligen.	Risikoanalyse Bei der Risikoanalyse sind alle für das Institut relevanten Aspekte im Zusammenhang mit der Auslagerung zu berücksichtigen (z. B. die wesentlichen Risiken der Auslagerung einschließlich möglicher Risikokonzentrationen (u. a. mehrere Auslagerungsvereinbarungen bzw. Auslagerungsverträge mit demselben Auslagerungsunternehmen), Risiken aus Weiterverlagerungen, politische Risiken, ESG-Risiken, Maßnahmen zur Steuerung und Minderung der Risiken, Eig-

		nung des Auslagerungsunternehmens, mögliche Interessenkonflikte, Schutzbedarf der an das Auslagerungsunternehmen übermittelten Daten, Kosten), wobei die Intensität der Analyse von Art, Umfang, Komplexität und Risikogehalt der ausgelagerten Aktivitäten und Prozesse abhängt. Insbesondere ist in der Risikoanalyse zu berücksichtigen, inwiefern eine auszulagernde Aktivität oder ein auszulagernder Prozess innerhalb der Prozesslandschaft des Instituts als von wesentlicher Bedeutung einzustufen ist. Bei Auslagerungen von erheblicher Tragweite, wie z. B. der vollständigen oder teilweisen Auslagerung der besonderen Funktionen Risikocontrolling-Funktion, Compliance-Funktion, Interne Revision oder von Kerninstitutsbereichen, ist entsprechend intensiv zu prüfen, ob und wie eine Einbeziehung der ausgelagerten Aktivitäten und Prozesse in das Risikomanagement sichergestellt werden kann. Die Risikoanalyse ist durch eine Szenarioanalyse, soweit sinnvoll und verhältnismäßig, zu ergänzen. Für die Szenarioanalyse sind, sofern verfügbar, interne und externe Verlustdaten zu verwenden. Kleinere, weniger komplexe Institute können qualitative Ansätze für die Risikoanalyse heranziehen.
3	Bei unter Risikogesichtspunkten nicht wesentlichen Auslagerungen sind die allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 27 ZAG zu beachten.	
4	Grundsätzlich sind Aktivitäten und Prozesse auslagerbar, solange dadurch die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 27 ZAG nicht beeinträchtigt wird. Die Auslagerung darf nicht zu einer Delegation der Verantwortung der Geschäftsleitung an das Auslagerungsunternehmen führen. Die Leitungsaufgaben der Geschäftsleitung sind nicht auslagerbar. Besondere Maßstäbe für Auslagerungsmaßnahmen ergeben sich bei der vollständigen oder teilweisen Auslagerung der besonderen Funktionen Risikocontrolling-Funktion und Compliance-Funktion. Auslagerungen dürfen nicht dazu führen, dass das Institut nur noch als leere Hülle (empty shell) existiert.	Leitungsaufgaben der Geschäftsleitung Zu den nicht auslagerbaren Leitungsaufgaben der Geschäftsleitung zählen die Unternehmensplanung, -koordination, -kontrolle und die Besetzung der Führungskräfte. Hierzu gehören auch Aufgaben, die der Geschäftsleitung durch den Gesetzgeber oder durch sonstige Regelungen explizit zugewiesen sind (z. B. die Festlegung der Strategien). Von den Leitungsaufgaben abzugrenzen sind Funktionen oder Organisationseinheiten, deren sich die Geschäftsleitung bei der Ausübung ihrer Leitungsaufgaben bedient (insbesondere Risikocontrolling-Funktion, Compliance-Funktion, Interne Revision).

		Diese können sowohl nach innen als auch – unter den Voraussetzungen der Tz. 5 - durch Auslagerung nach außen delegiert werden. Befugnis der Leistungserbringung des Auslagerungsunternehmens Durch das Institut ist sicherzustellen, dass das Auslagerungsunternehmen nach dem Recht seines Sitzlandes zur Ausübung der ausgelagerten Aktivitäten und Prozesse befugt ist und über dazu ggf. erforderliche Erlaubnisse und Registrierungen verfügt. Bei Auslagerungen an Unternehmen mit Sitz außerhalb des Europäischen Wirtschaftsraums (EWR) hat das Institut, sofern es sich um ausgelagerte Aktivitäten oder Prozesse i. V. m. dem Erbringen von Zahlungsdiensten und E-Geld-Geschäften in einem Umfang handelt, der im Inland eine Zulassung oder Registrierung durch die zuständigen Aufsichtsbehörden erfordern würde, ferner sicherzustellen, dass das Auslagerungsunternehmen von den zuständigen Aufsichtsbehörden in dem Drittstaat beaufsichtigt wird und eine entsprechende Kooperationsvereinbarung, z. B. in Form einer Absichtserklärung (Memorandum of Understanding) oder Collegevereinbarung zwischen den für die Beaufsichtigung des Instituts zuständigen Aufsichtsbehörden und den für die Beaufsichtigung des Auslagerungsunternehmens zuständigen Aufsichtsbehörden, besteht.
5	Eine Auslagerung von Aktivitäten und Prozessen in Kontrollbereichen und Kerninstitutsbereichen der Institute kann unter Beachtung der in Tz. 4 genannten Anforderungen in einem Umfang vorgenommen werden, der gewährleistet, dass hierdurch das Institut weiterhin über Kenntnisse und Erfahrungen verfügt, die eine wirksame Überwachung der vom Auslagerungsunternehmen erbrachten Dienstleistungen gewährleistet. Es ist sicherzustellen, dass bei Bedarf - im Falle der Beendigung des Auslagerungsverhältnisses oder der Änderung der Gruppenstruktur - der ordnungsmäßige Betrieb in diesen Bereichen fortgesetzt werden kann. Eine vollständige Auslagerung der besonderen Funktionen Risikocontrolling-Funktion oder Compliance-Funktion ist lediglich für Tochterinstitute innerhalb einer Gruppe gemäß § 1 Abs. 6 ZAG zulässig, sofern das auslagernde Institut sowohl hinsichtlich seiner Größe, Komplexität und dem Risikogehalt der Geschäftsaktivitäten für den nationalen Finanzsektor als auch hinsichtlich seiner Bedeutung innerhalb der Gruppe als nicht wesentlich	

einzustufen ist. Gleiches gilt für Gruppen, wenn das Mutterunternehmen kein Institut und im Inland ansässig ist. Eine vollständige Auslagerung der Compliance-Funktion ist ferner nur bei wenig komplexen Geschäftsaktivitäten möglich.

6	Das Institut hat bei wesentlichen Auslagerungen im Fall der beabsichtigten oder erwarteten Beendigung der Auslagerungsvereinbarung Vorkehrungen zu treffen, um die Kontinuität und Qualität der ausgelagerten Aktivitäten und Prozesse auch nach Beendigung zu gewährleisten. Für Fälle unbeabsichtigter oder unerwarteter Beendigung dieser Auslagerungen, die mit einer erheblichen Beeinträchtigung der Geschäftstätigkeit verbunden sein können, hat das Institut etwaige Handlungsoptionen auf ihre Durchführbarkeit zu prüfen und zu verabschieden. Dies beinhaltet auch, soweit sinnvoll und möglich, die Festlegung entsprechender Ausstiegsprozesse. Die Handlungsoptionen sind regelmäßig und anlassbezogen zu überprüfen.	Handlungsoptionen und Ausstiegsprozesse Ausstiegsprozesse sind mit dem Ziel festzulegen, die notwendige Kontinuität und Qualität der ausgelagerten Aktivitäten und Prozesse aufrechtzuerhalten bzw. in angemessener Zeit wieder herstellen zu können. Existieren keine Handlungsoptionen, ist zumindest eine angemessene Berücksichtigung in der Notfallplanung erforderlich.
7	Bei wesentlichen Auslagerungen ist im in Textform dokumentierten Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: a) Spezifizierung und ggf. Abgrenzung der vom Auslagerungsunternehmen zu erbringenden Leistung, b) Datum des Beginns und ggf. des Endes der Auslagerungsvereinbarung, c) sofern von deutschem Recht abweichend, das geltende Recht für die Auslagerungsvereinbarung, d) Standorte (d.h. Regionen oder Länder), in denen die Durchführung der Dienstleistung erfolgt und / oder maßgebliche Daten gespeichert und verarbeitet werden, sowie die Regelung, dass das Institut benachrichtigt wird, wenn das Auslagerungsunternehmen den Standort wechselt, e) vereinbarte Dienstleistungsgüte mit eindeutig festgelegten Leistungszielen, f) soweit zutreffend, dass das Auslagerungsunternehmen für bestimmte Risiken einen Versicherungsnachweis vorzulegen hat. g) Anforderungen für die Umsetzung und Überprüfung von Notfallkonzepten, h) Festlegung angemessener Informations- und Prüfungsrechte der Internen Revision sowie externer Prüfer, i) Sicherstellung der uneingeschränkten Informations- und Prüfungsrechte sowie der Kontrollmöglichkeiten der gemäß § 26 ZAG zuständigen Behörden bezüglich der ausgelagerten Aktivitäten und Prozesse, j) soweit erforderlich Weisungsrechte,	Weisungsrechte des Instituts/Prüfungen der Internen Revision Auf eine explizite Vereinbarung von Weisungsrechten zugunsten des Instituts kann verzichtet werden, wenn die vom Auslagerungsunternehmen zu erbringende Leistung hinreichend klar im Auslagerungsvertrag spezifiziert ist. Ferner kann die Interne Revision des auslagernden Instituts unter den Voraussetzungen von BT 2.1 Tz. 3 auf eigene Prüfungshandlungen verzichten. Diese Erleichterungen können auch bei Auslagerungen auf so genannte Mehrmandantendienstleister in Anspruch genommen werden. Informations- und Prüfungsrechte Informations- und Prüfungsrechte gem. Tz. 7 h) und i) sollten möglichst auch für nicht wesentliche Auslagerungen vereinbart werden, sofern abzusehen ist, dass diese Auslagerungen in naher oder mittlerer Zukunft wesentlich im Sinne der Tz. 2 werden könnten. Informations- und Prüfungsrechte gem. Tz. 7 h) und i) umfassen auch die für den Zutritt, Zugang oder Zugriff erforderlichen Rechte. Eskalation bei Schlechtleistung Bereits bei der Vertragsanbahnung hat das Institut intern festzulegen, welchen Grad einer Schlechtleistung es akzeptieren möchte. Kündigungsrechte

	k) Regelungen, die sicherstellen, dass datenschutzrechtliche Bestimmungen und sonstige Sicherheitsanforderungen beachtet werden, l) Kündigungsrechte und angemessene Kündigungsfristen, m) Regelungen über die Möglichkeit und über die Modalitäten einer Weiterverlagerung, die sicherstellen, dass das Institut die aufsichtsrechtlichen Anforderungen weiterhin einhält, n) Verpflichtung des Auslagerungsunternehmens, das Institut über Entwicklungen zu informieren, die die ordnungsgemäße Erledigung der ausgelagerten Aktivitäten und Prozesse beeinträchtigen können,	Die Auslagerungsvereinbarung sollte das Auslagerungsunternehmen für den Fall einer Kündigung verpflichten, das Institut bei der Übertragung der ausgelagerten Aktivität bzw. des ausgelagerten Prozesses an ein anderes Auslagerungsunternehmen oder ihre bzw. seine Reintegration in das Institut zu unterstützen. Sonstige Sicherheitsanforderungen Regelungen zu sonstigen Sicherheitsanforderungen sollten für alle, also auch nicht wesentliche Auslagerungen, vertraglich vereinbart werden. Zu den sonstigen Sicherheitsanforderungen zählen vor allem Zugangsbestimmungen zu Räumen und Gebäuden (z. B. bei Rechenzentren) sowie Zugriffsberechtigungen auf Softwarelösungen zum Schutz wesentlicher Daten und Informationen. Die Einhaltung dieser Anforderungen ist fortlaufend zu überwachen. Institute sollten einen risikobasierten Ansatz betreffend den Standort der Datenspeicherung und Datenverarbeitung sowie hinsichtlich der Informationssicherheit wählen. Es ist sicherzustellen, dass auf die sich im Eigentum des Instituts befindlichen Daten im Fall einer Insolvenz, Abwicklung oder der Einstellung der Geschäftstätigkeit des Auslagerungsunternehmens zugegriffen werden kann. Ort der Durchführung der Dienstleistung Zusätzlich zu Tz. 7 d) muss der Ort der Leistungserbringung (z. B. Stadt oder, sofern notwendig, genaue Anschrift) dem Institut jederzeit bekannt sein.
8	Mit Blick auf Weiterverlagerungen sind möglichst Zustimmungsvorbehalte des auslagernden Instituts oder konkrete Voraussetzungen, wann Weiterverlagerungen einzelner Arbeits- und Prozessschritte möglich sind, im Auslagerungsvertrag zu vereinbaren. Zumindest ist vertraglich sicherzustellen, dass die Vereinbarungen des Auslagerungsunternehmens mit Subunternehmen im Einklang mit den vertraglichen Vereinbarungen des originären Auslagerungsvertrags stehen. Ferner haben die vertraglichen Anforderungen bei Weiterverlagerungen auch eine Informationspflicht des Auslagerungsunternehmens an das auslagernde Institut zu umfassen. Es muss sichergestellt sein,	

	dass das Auslagerungsunternehmen im Falle einer Weiterverlagerung auf ein Subunternehmen weiterhin gegenüber dem auslagernden Institut berichtspflichtig bleibt.	
9	Das Institut hat die mit Auslagerungen verbundenen Risiken angemessen zu steuern und die Ausführung der ausgelagerten Aktivitäten und Prozesse ordnungsgemäß zu überwachen. Dies umfasst bei wesentlichen Auslagerungen auch die laufende Überwachung der Leistung des Auslagerungsunternehmens anhand vorzuhaltender Kriterien (z. B. Key Performance Indicators, Key Risk Indicators) und vertraglich vereinbarter Informationen des Auslagerungsunternehmens; die Qualität der erbrachten Leistungen ist regelmäßig zu beurteilen.	
10	Für die Dokumentation, Steuerung und Überwachung wesentlicher Auslagerungen hat das Institut klare Verantwortlichkeiten festzulegen. Soweit besondere Funktionen nach Maßgabe von Tz. 5 vollständig ausgelagert werden, hat die Geschäftsleitung jeweils einen Beauftragten zu benennen, der eine ordnungsgemäße Durchführung der jeweiligen Aufgaben gewährleisten muss. Die Anforderungen des AT 4.4.3 und BT 2 sind entsprechend zu beachten.	Besondere Aufgaben des Revisionsbeauftragten Der Revisionsbeauftragte hat den Prüfungsplan gemeinsam mit dem beauftragten Dritten zu erstellen. Er hat, gegebenenfalls gemeinsam mit dem beauftragten Dritten, zudem den Gesamtbericht nach BT 2.4 Tz. 4 zu verfassen und nach Maßgabe von BT 2.5 zu prüfen, ob die festgestellten Mängel beseitigt wurden. Der Revisionsbeauftragte ist der Geschäftsleitung unmittelbar zu unterstellen. Die Aufgaben des Revisionsbeauftragten können in Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten des Instituts von einer Organisationseinheit, einem Mitarbeiter oder einem Geschäftsleiter wahrgenommen werden. Ausreichende Kenntnisse und die erforderliche Unabhängigkeit sind jeweils sicherzustellen.
11	Die Anforderungen an die Auslagerung von Aktivitäten und Prozessen sind auch bei der Weiterverlagerung ausgelagerter Aktivitäten und Prozesse zu beachten.	Risikoanalyse gem. AT 9 Tz. 2 Die mit der Weiterverlagerung verbundenen Risiken werden im Rahmen der Risikoanalyse bewertet. Hierzu zählt auch die Bewertung der Wesentlichkeit von Weiterverlagerungen. Die erweiterten Anforderungen für wesentliche Auslagerungen finden nur für die unter Risikogesichtspunkten wesentlichen Weiterverlagerungen Anwendung. Zudem sollte das Risiko berücksichtigt werden, dass durch lange und komplexe Auslagerungsketten die Fähigkeit der Institute zur

		Überwachung der ausgelagerten Aktivitäten und Prozesse eingeschränkt sein kann.
12	Jedes Institut, das Auslagerungen vornimmt, hat einen zentralen Auslagerungsbeauftragten im Institut selbst einzurichten. Zusätzlich hat das Institut abhängig von der Art, dem Umfang und der Komplexität der Auslagerungsaktivitäten ein zentrales Auslagerungsmanagement zur Unterstützung des zentralen Auslagerungsbeauftragten einzurichten. Zu den Aufgaben zählen insbesondere: a) Implementierung und Weiterentwicklung eines angemessenen Auslagerungsmanagements und entsprechender Kontroll- und Überwachungsprozesse, b) Erstellung und Pflege einer vollständigen Dokumentation der Auslagerungen (einschließlich Weiterverlagerungen), c) Unterstützung der Fachbereiche bezüglich der institutsinternen und gesetzlichen Anforderungen bei Auslagerungen, d) Koordination und Überprüfung der durch die zuständigen Bereiche durchgeführten Risikoanalyse gemäß Tz. 2.	Zentraler Auslagerungsbeauftragter Der zentrale Auslagerungsbeauftragte hat einer Organisationseinheit anzugehören, die der Geschäftsleitung unmittelbar unterstellt ist. Er kann auch bei anderen Einheiten angesiedelt werden, sofern eine direkte Berichtslinie zur Geschäftsleitung sichergestellt ist. Weniger komplexe Institute können diese Funktion auch einem Mitglied der Geschäftsleitung übertragen. Als Auslagerungsbeauftragter kann auch der Leiter des zentralen Auslagerungsmanagements benannt werden.
13	Der Auslagerungsbeauftragte bzw. das zentrale Auslagerungsmanagement haben mindestens jährlich einen Bericht über die wesentlichen Auslagerungen zu erstellen und der Geschäftsleitung zur Verfügung zu stellen. Zudem ist anlassbezogen zu berichten. Der Bericht hat unter Berücksichtigung der dem Institut vorliegenden Informationen bzw. der institutsinternen Bewertung der Dienstleistungsqualität der Auslagerungsunternehmen eine Aussage darüber zu treffen, ob die erbrachten Dienstleistungen der Auslagerungsunternehmen den vertraglichen Vereinbarungen entsprechen, die ausgelagerten Aktivitäten und Prozesse angemessen gesteuert und überwacht werden können und ob weitere risikomindernde Maßnahmen ergriffen werden sollen.	Berichterstattung bei weniger komplexen Geschäftsaktivitäten Bei, weniger komplexen Geschäftsaktivitäten ist eine Berichterstattung im Rahmen einer Geschäftsleitersitzung ausreichend.
14	Grundsätzlich hat das Institut ein aktuelles Auslagerungsregister mit Informationen über alle Auslagerungsvereinbarungen vorzuhalten. Die inhaltlichen Mindestanforderungen an das Auslagerungsregister finden sich für alle Auslagerungen in Tz. 54 und für wesentliche Auslagerungen in Tz. 55 der EBA Leitlinien zu Auslagerungen (EBA/GL/2019/02). Das Auslagerungsregister umfasst alle Auslagerungsvereinbarungen, einschließlich der Auslagerungsvereinbarungen mit Auslagerungsunternehmen innerhalb einer Gruppe oder eines Finanzverbundes. Ferner ist bei der Weiterverlagerung von wesentlichen Auslagerungen von dem auslagernden Institut festzulegen, ob der weiter zu verlagernde Teil wesentlich und dieser wesentliche Teil im Auslagerungsregister zu erfassen ist.	

15 Im Hinblick auf Gruppen gemäß § 1 Abs. 6 ZAG oder Finanzverbünde ergeben sich die folgenden Erleichterungen:

a) Bei gruppen- und verbundinternen Auslagerungen können im Rahmen der Risikoanalyse gem. Tz. 2 wirksame Vorkehrungen auf Gruppen- bzw. Verbundebene, insbesondere ein einheitliches und umfassendes Risikomanagement sowie Durchgriffsrechte, bei der Erstellung und Anpassung der Risikoanalyse risikomindernd berücksichtigt werden.

b) Für Auslagerungen mehrerer Institute einer Gruppe bzw. eines Verbundes an ein bzw. mehrere gemeinsame Auslagerungsunternehmen, besteht die Möglichkeit, ein zentrales Auslagerungsmanagement auf Gruppen- bzw. Verbundebene einzurichten, sofern das zentrale Auslagerungsmanagement den Anforderungen des Moduls AT 9 bzw. sofern nicht einschlägig, den Anforderungen der EBA/GL/2019/02 genügt.

c) Bei der Risikoberichterstattung von Auslagerungsunternehmen, die innerhalb einer Gruppe / eines Verbundes genutzt werden, besteht die Möglichkeit einer zentralen Vorauswertung, welche den auslagernden Instituten die weitere Verwendung erleichtert.

d) Bei gruppen- und verbundinternen Auslagerungen kann auf die Erstellung von Ausstiegsprozessen und Handlungsoptionen verzichtet werden.

e) Wird gruppen- oder verbundintern ein zentrales Auslagerungsregister eingerichtet und geführt, so muss sichergestellt sein, dass das einzelne Institut und die zuständige Behörde das individuelle Auslagerungsregister bei Bedarf ohne größere Verzögerung erhalten.

Auch für Auslagerungen innerhalb einer Gruppe oder eines Finanzverbundes an ein zentrales Auslagerungsunternehmen innerhalb der Gruppe bzw. des Verbundes sind die Bedingungen, einschließlich der finanziellen Bedingungen, festzulegen.

Gemeinsame Notfallkonzepte (gem. AT 7.3)
Wenn sich die Institute innerhalb einer Institutsgruppe oder eines Finanzverbundes auf ein gemeinsames Notfallkonzept für eine wesentliche Auslagerung geeinigt haben, haben die Institute den für sie relevanten Teil des Notfallkonzeptes zu erhalten.

BT 1 Besondere Anforderungen an das interne Kontrollsystem

In diesem Modul werden besondere Anforderungen an die Ausgestaltung des internen Kontrollsystems gestellt. Die Anforderungen beziehen sich vor allem auf die Ausgestaltung der Aufbau- und Ablauforganisation bei dem Erbringen von Zahlungsdiensten und Betreiben von E-Geld-Geschäften (BTO). Darüber hinaus werden unter Berücksichtigung von Risikokonzentrationen und den Auswirkungen von ESG-Risiken Anforderungen an die angemessene Ausgestaltung der Risikosteuerungs- und -controllingprozesse für operationelle Risiken, Adressenausfallrisiken, Marktpreisrisiken und Liquiditätsrisiken gestellt (BTR).

BTO Organisatorische Anforderungen an das Erbringen von Zahlungsdiensten und das Betreiben von E-Geld-Geschäften

1	In diesem Modul werden besondere Anforderungen an die Ausgestaltung der Prozesse der Institute gestellt. Die Anforderungen beziehen sich vor allem auf die Prozesse für Sicherungsanforderungen und Absicherung von Haftungsfällen, Verfahren bei Sicherheitsvorfällen und sicherheitsbezogener Kundenbeschwerden und die Inanspruchnahme von Agenten. Abhängig von der Komplexität und dem Risikogehalt der Geschäftsaktivitäten ist eine vereinfachte Umsetzung der Anforderungen des BTO möglich.	
2	Institute haben Bearbeitungsgrundsätze für die Prozesse bei Zahlungsdiensten und E-Geld-Geschäften zu formulieren, die in geeigneter Weise zu differenzieren sind (z. B. nach Art der Zahlungsdienste). Darüber hinaus sind Verfahren für die vom Institut akzeptierten Zahlungsdienstnutzer und sonstige Geschäftspartner (z. B. Kooperationspartner) sowie Geschäftsorte für das Erbringen der Zahlungsdienste und das Betreiben des E-Geld-Geschäfts festzulegen.	Geschäftliche Beziehungen Abhängig vom Risikogehalt sind sowohl Zahlungsdienstleister und sonstige Geschäftspartner als auch Geschäftsorte für das Erbringen der Zahlungsdienste und das Betreiben des E-Geld-Geschäfts regelmäßig zu analysieren und die Risiken mindestens jährlich zu bewerten. Hängt die Bewertung maßgeblich von den Verhältnissen eines Dritten ab, so ist eine Analyse und angemessene Überprüfung des Dritten ebenfalls durchzuführen.
3	Den Zahlungsdiensten und E-Geld-Geschäften sind wirksame rechtliche Vereinbarungen zu Grunde zu legen.	
4	Institute haben eine klare und geeignete Kompetenzordnung für die Entscheidungen für Zahlungsdienste und E-Geld-Geschäfte festzulegen.	

BTO 1 Anforderungen an die Prozesse und Verfahren für Sicherungsanforderungen und die Absicherung von Haftungsfällen

1 Die Nutzung von Treuhandkonten hat auf Basis festgelegter Bearbeitungsgrundsätze zu erfolgen. Bei der Einrichtung der Treuhandkonten hat das Institut standardisierte Vereinbarungen zu nutzen. Das Institut hat die Anzahl und Funktionen der Personen, die Zugang zu den Treuhandkonten haben, auf das notwendige Maß zu begrenzen. Das Institut hat Verwaltungs- und Kontenabstimmungsprozesse einzurichten, mit denen sichergestellt und jederzeit nachvollzogen werden kann, dass die Geldbeträge des Zahlungsdienstnutzers im Falle einer Zahlungsunfähigkeit gegen Ansprüche anderer Gläubiger des Instituts abgesichert sind. Die Kontenabstimmungsprozesse sind außerhalb des operativen Geschäftsbereiches anzusiedeln.

Offene Treuhandkonten
Treuhandsammelkonto: Für sämtliche Zahlungsdienstnutzer eines Instituts oder für bestimmte Zahlungsdienstnutzer reicht ein offenes Treuhandsammelkonto aus.
Im Falle der Nutzung von Treuhandkonten bei einem CRR-Institut zur Erfüllung der Sicherungsanforderung muss das Institut die Absicherung zivilrechtlich durch Abschluss einer geeigneten Treuhandvereinbarung sicherstellen. Dazu gehört die jederzeitige Separierung vom eigenen Vermögen und dem Vermögen und dem Zugriff anderer Gläubiger (sachenrechtliche Komponente) und eine Treuhandabrede (schuldrechtliche Komponente).
Erforderliche Vertragsklauseln der Treuhandabrede sind unter anderem Ausschluss des Pfandrechts, Ausschluss des Anspruchs auf Aufrechnung auch in Bezug auf Kosten des Kontos der Bank, Verpflichtung der Bank zur Drittschuldnererklärung.

Zur Sicherstellung des insolvenzrechtlichen Aussonderungsrechtes sind die Anforderungen des §17 Abs. 1 Satz 2 Nr. 1 ZAG mit dem Zeitpunkt der Entgegennahme der Geldbeträge kumulativ zu erfüllen (Vermischungsverbot, Sicherungsgebot und Trennungsgebot). Daher sind eingehende Gelder unmittelbar auf dem Treuhandkonto entgegenzunehmen. Zu keinem Zeitpunkt dürfen eigene Gelder des Institutes auf das Treuhandkonto gelangen.
Sofern das Institut vertraglich berechtigt ist, von dem Treuhandkonto eigene Gebühren zu Lasten des Zahlungsdienstnutzers zu entnehmen, sind diese taggleich bei Fälligkeit vom Treuhandkonto abzubuchen.

Rücklastschriften dürfen nur auf Treuhandeinzelkonten zugelassen werden, nicht auf Treuhandsammelkonten.

		Kontenabstimmungsprozesse Die Institute haben Kontrollen sowie Prozesse zur Klärung von Unstimmigkeiten und Auffälligkeiten einzurichten, die im Rahmen der Kontrollen auffallen. Insbesondere soll sichergestellt werden, dass es bei der Entgegennahme und Auskehrung von Geldern zu keinem Zeitpunkt zu einer Vermischung mit den Geldern anderer natürlicher oder juristischer Personen als der Zahlungsdienstnutzer oder E-Geld-Inhaber, für die sie gehalten werden, kommt, und die Trennung von den übrigen Vermögenswerten des Instituts gewährleistet ist.
2	Nutzt das Institut die Möglichkeit der Absicherung über Investition in sichere, liquide Aktiva, hat das Institut geeignete Verfahren und Kontrollmechanismen zur Sicherstellung einzurichten, dass die ausgewählten Aktiva sicher und liquide sind.	Das Trennungs- und Vermischungsverbot ist auch bei der Investition in sichere, liquide Aktive einzuhalten.
3	Außerhalb des operativen Geschäftsbereichs sind ferner anzusiedeln - im Fall der Sicherung nach §§ 17 und 18 ZAG durch eine Versicherung oder vergleichbare Garantie, geeignete Verfahren, mit denen laufend sichergestellt werden kann, dass Versicherungssumme oder Garantie ausreichen, um die Sicherungspflichten zu erfüllen, - Prozesse zur Überwachung und regelmäßigen Überprüfung der Mindestdeckungssumme der nach §§ 16 und 36 ZAG abzuschließenden Versicherung oder vergleichbaren Garantie.	Versicherung oder vergleichbare Garantie Die Institute haben ein Überwachungsverfahren über den abzusichernden Betrag einzurichten. Die Abdeckung von Spitzenbeträgen muss jederzeit sichergestellt sein, ein Durchschnittsbetrag ist nicht ausreichend. Funktionstrennung Funktionen mit Kontrollaufgaben sind außerhalb der operativen Bereiche anzusiedeln.

BTO 2 Anforderungen an die Prozesse und Verfahren für die Betrugsprävention, für die Überwachung und Bearbeitung sowie Folgemaßnahmen bei Sicherheitsvorfällen oder sicherheitsbezogenen Kundenbeschwerden

1	Das Institut hat geeignete organisatorische Maßnahmen und Verfahren für • die Betrugsprävention und • die Überwachung, Handhabung und Folgemaßnahmen bei Sicherheitsvorfällen und sicherheitsbezogenen Kundenbeschwerden einzurichten.	
2	Das Institut hat Stellen einzurichten bzw. Personen zu benennen (Kontaktstelle), an welche sich die Kunden in Betrugsfällen, im Falle von technischen Problemen oder Anliegen beim Forderungsmanagement wenden können. Namen und E-Mail-Adresse dieser Stelle sind den Kunden zugänglich zu machen.	Kontaktstelle ist eine Anlaufstelle für Kunden im Sinne eines Customer Support Chanel.
3	Die Kontaktstelle ist so auszugestalten, so, dass Kundeneingaben wirksam und angemessen zeitnah bearbeitet werden können.	
4	Das Institut hat Verfahren für die Meldung von Vorfällen gemäß § 54 ZAG, einschließlich der Übermittlung dieser Berichte an interne oder externe Stellen, unter Einschluss der zuständigen nationale Behörden, einzurichten.	
5	Die Berichtswege sind zu dokumentieren und frei von Interessenskonflikten auszugestalten.	

BTO 3 Organisatorische Anforderung bei der Inanspruchnahme von Agenten

1 Erbringt ein Institut Zahlungsdienste über einen Agenten, hat das Institut Verfahren einzurichten, die gewährleisten, dass die Anforderungen der § 25 Abs. 2 ZAG Abs. 1 eingehalten werden. Das Institut hat dauerhaft sicherzustellen

- dass der Agent zuverlässig und fachlich geeignet ist,
- bei der Erbringung der Zahlungsdienste die gesetzlichen Vorgaben erfüllt,
- seinen Informationspflichten genügt.

2 Das Institut hat die Überprüfungen des Agenten zu dokumentieren. Das Institut hat die erforderlichen Nachweise für die Erfüllung seiner Pflichten mindestens fünf Jahre nach dem Ende des Status des Agenten aufzubewahren.

3 Das Institut hat mit dem Agenten eine schriftliche Vereinbarung zu treffen, welche die Pflichten des Agenten und die Rechte des Instituts einschließlich Weisungs- und Kündigungsrechte sowie Kontrollrechte des Instituts und dessen Prüfern festschreibt.

BTR Anforderungen an die Risikosteuerungs- und -controllingprozesse

1 Dieses Modul enthält unter Berücksichtigung von Risikokonzentrationen besondere Anforderungen an die Ausgestaltung der Risikosteuerungs- und -controllingprozesse (AT 4.3.2) für

a) operationelle Risiken (BTR 1)

b) Adressenausfallrisiken (BTR 2),

c) Marktpreisrisiken (BTR 3) und

d) Liquiditätsrisiken (BTR 4)

Dabei sind die Auswirkungen von ESG-Risiken angemessen zu berücksichtigen.

BTR 1 Operationelle Risiken

1	Das Institut hat den operationellen Risiken durch ein angemessenes Risikomanagement Rechnung zu tragen. Für diese Zwecke ist eine institutsintern einheitliche Festlegung und Abgrenzung der operationellen Risiken vorzunehmen und an die Mitarbeiter zu kommunizieren.	Definition von operationellen Risiken Die Festlegung sollte auch eine möglichst klare Abgrenzung zu anderen vom Institut betrachteten Risiken enthalten. Umgang mit nicht eindeutig zuordenbaren Schadensfällen oder Beinahe-Verlusten Die Prozesse zum Management operationeller Risiken sollten auch den Umgang mit nicht eindeutig zuordenbaren Schadensfällen („boundary events“), Beinahe-Verlusten und zusammenhängenden Ereignissen umfassen. Als sog. „boundary events“ können Verluste eingestuft werden, die zwar einem anderen Risiko zugerechnet werden oder bereits wurden (z.B. Kreditverluste), die aber ihren Ursprung in Ereignissen wie z.B. mangelhaften Prozessen und Kontrollen haben oder hatten. Als „Beinahe-Verluste“ können durch Fehler oder Mängel ausgelöste Ereignisse bezeichnet werden, die zu keinem Verlust geführt haben.
2	Es muss gewährleistet sein, dass wesentliche operationelle Risiken zumindest jährlich identifiziert und beurteilt werden. Dabei sind die Auswirkungen von ESG-Risiken angemessen zu betrachten.	
3	Das Institut hat eine angemessene Erfassung von Schadensfällen sicherzustellen. Bedeutende Schadensfälle sind unverzüglich hinsichtlich ihrer Ursachen zu analysieren.	Erfassung von Schadensfällen Abhängig von der Komplexität und dem Risikogehalt der Geschäftsaktivität haben Institute hierfür eine Ereignisdatenbank für Schadensfälle einzurichten, bei welcher die vollständige Erfassung aller Schadensereignisse oberhalb angemessener Schwellenwerte sichergestellt ist. Sammelschäden Einzeln erfasste Schadensfälle, die dem gleichen Ereignis zugeordnet werden können, müssen aggregiert weiterverarbeitet werden.

4	Die Verfahren zur Beurteilung der operationellen Risiken müssen die wesentlichen Ausprägungen operationeller Risiken erfassen.	Wesentliche Ausprägungen Bei der Beurteilung der wesentlichen Ausprägungen sind historische Erkenntnisse (insbesondere Schadensfälle) und potenzielle Ereignisse zu berücksichtigen. Zur Identifikation und Beurteilung relevanter potenzieller Ereignisse sind auch Erkenntnisse zu aktuellen Schwachstellen, insbesondere aus der Internen Revision, dem Informationssicherheitsmanagement, der Compliance-Funktion, den Anpassungsprozessen sowie dem Notfall- und Auslagerungsmanagement, heranzuziehen.
5	Auf Basis der identifizierten operationellen Risiken ist zu entscheiden, ob und welche Maßnahmen zur Beseitigung der Ursachen zu treffen oder welche Risikosteuerungsmaßnahmen zu ergreifen sind. Die Umsetzung der zu treffenden Maßnahmen ist zu überwachen.	Risikosteuerungsmaßnahmen Zu den Risikosteuerungsmaßnahmen zählen z. B. Versicherungen, Ersatzverfahren, Neuausrichtung von Geschäftsaktivitäten und Maßnahmen des Notfallmanagements.

BTR 2 Adressenausfallrisiken

1	Das Institut hat durch geeignete Maßnahmen sicherzustellen, dass Adressenausfallrisiken und damit verbundene Risikokonzentrationen begrenzt werden können. Dabei sind die Auswirkungen von ESG-Risiken angemessen zu betrachten.	Risikokonzentrationen bei Adressenausfallrisiken Hierbei handelt es sich um Adressen- und Sektorkonzentrationen, regionale Konzentrationen und sonstige Konzentrationen im Kreditgeschäft, die relativ gesehen zum Risikodeckungspotenzial zu erheblichen Verlusten führen können.
2	Adressenausfallrisiken sind durch festgesetzte Limite je Einzeladresse zu begrenzen. Das Institut hat hierfür eine klare und konsistente Kompetenzordnung festzulegen.	
3	Die Geschäfte sind unverzüglich auf die Limite anzurechnen. Die Einhaltung der Limite ist zu überwachen. Limitüberschreitungen und die deswegen ggf. getroffenen Maßnahmen sind festzuhalten. Ab einer unter Risikogesichtspunkten festgelegten Höhe sind Überschreitungen von Limiten den zuständigen Geschäftsleitern täglich anzuzeigen.	
4	Risikokonzentrationen sind zu identifizieren. Gegebenenfalls vorhandene Abhängigkeiten sind dabei zu berücksichtigen. Bei der Beurteilung der Risikokonzentrationen ist auf qualitative und, soweit möglich, auf quantitative Verfahren abzustellen. Risikokonzentrationen sind mit Hilfe geeigneter Verfahren zu steuern und zu überwachen (z. B. Limite, Ampelsysteme oder auf Basis anderer Vorkehrungen).	Abhängigkeiten Vorhandene Abhängigkeiten können z. B. in Form von wirtschaftlichen Verflechtungen, juristischen Abhängigkeiten zwischen Unternehmen u. ä. vorliegen.
5	Das Institut hat sicherzustellen, dass Risiken frühzeitig erkannt werden.	
6	Abhängig vom Risikogehalt der Geschäfte sind sowohl bei Eingehen des Geschäftes als auch bei turnusmäßigen oder anlassbezogenen Beurteilungen die Risiken einer Geschäftsbeziehung zu bewerten. Eine Überprüfung der Risikobewertung ist jährlich durchzuführen.	

BTR 3 Marktpreisrisiken

1	Soweit ein Institut im Rahmen seiner Geschäftstätigkeit Marktpreisrisiken eingeht (z.B. Fremdwährungs-, Zins-, oder Kursrisiken), sind diese unter Berücksichtigung von Risikokonzentrationen zu begrenzen. Dabei sind die Auswirkungen von ESG-Risiken angemessen zu betrachten.
2	Das Institut hat eine klare und konsistente Kompetenzordnung für das Eingehen von Markpreisrisiken festzulegen
3	Geschäfte sind unverzüglich nach Geschäftsabschluss mit allen maßgeblichen Abschlussdaten zu erfassen, bei der Ermittlung der jeweiligen Position zu berücksichtigen.
4	Die Geschäfte sind einer laufenden und vom Geschäftsabschluss unabhängigen Kontrolle zu unterziehen. Dabei ist insbesondere zu kontrollieren, ob a) die Geschäftsunterlagen vollständig und zeitnah vorliegen, b) die Angaben richtig und vollständig sind und, soweit vorhanden, mit den Angaben auf Maklerbestätigungen, Ausdrucken aus Handelssystemen oder Ähnlichem übereinstimmen, c) die Abschlüsse sich hinsichtlich Art und Umfang im Rahmen der festgesetzten Limite bewegen, d) Abweichungen von vorgegebenen Standards (z. B. Stammdaten, Anschaffungswege, Zahlungswege) vereinbart sind. Änderungen und Stornierungen der Abschlussdaten oder Buchungen sind unabhängig zu kontrollieren.
5	Die Verfahren zur Beurteilung der Marktpreisrisiken sind regelmäßig zu überprüfen

BTR 4 Liquiditätsrisiken

1	Das Institut hat sicherzustellen, dass es seine Zahlungsverpflichtungen jederzeit erfüllen kann. Das Institut hat dabei, soweit erforderlich, auch Maßnahmen zur Steuerung des untertägigen Liquiditätsrisikos zu ergreifen. Konzentrationen sind wirksam zu überwachen und zu begrenzen.
2	Das Institut hat zu gewährleisten, dass ein sich abzeichnender Liquiditätsengpass frühzeitig erkannt wird. Hierfür sind Verfahren einzurichten, deren Angemessenheit regelmäßig, mindestens aber jährlich, zu überprüfen ist. Auswirkungen anderer Risiken auf die Liquidität des Instituts sind bei den Verfahren zu berücksichtigen.
3	Das Institut hat einen internen Finanzierungsplan aufzustellen, der die Strategien und das Geschäftsmodell angemessen widerspiegelt. Der Planungshorizont hat einen angemessen langen, in der Regel mehrjährigen Zeitraum zu umfassen. Dabei ist zu berücksichtigen, wie sich Veränderungen der eigenen Geschäftstätigkeit oder der strategischen Ziele sowie Veränderungen des wirtschaftlichen Umfelds auf den Finanzierungsbedarf auswirken. Möglichen adversen Entwicklungen, die von den Erwartungen abweichen, ist bei der Planung angemessen Rechnung zu tragen.

BT 2 Besondere Anforderungen an die Ausgestaltung der Internen Revision

BT 2.1 Aufgaben der Internen Revision

1	Die Prüfungstätigkeit der Internen Revision hat sich auf der Grundlage eines risikoorientierten Prüfungsansatzes grundsätzlich auf alle Aktivitäten und Prozesse des Instituts zu erstrecken.	
2	Die Interne Revision hat unter Wahrung ihrer Unabhängigkeit und unter Vermeidung von Interessenkonflikten bei wesentlichen Projekten begleitend tätig zu sein.	
3	Im Fall von Auslagerungen auf ein anderes Unternehmen kann die Interne Revision des Instituts auf eigene Prüfungshandlungen verzichten, sofern die anderweitig durchgeführte Revisionstätigkeit den Anforderungen in AT 4.4.3 und BT 2 genügt. Die Interne Revision des auslagernden Instituts hat sich von der Einhaltung dieser Voraussetzungen regelmäßig zu überzeugen. Die für das Institut relevanten Prüfungsergebnisse sind an die Interne Revision des auslagernden Instituts weiterzuleiten.	Anderweitige Durchführung der Revisionstätigkeit Die Revisionstätigkeit kann übernommen werden durch: - die Interne Revision des Auslagerungsunternehmens, - die Interne Revision eines oder mehrerer der auslagernden Institute im Auftrag der auslagernden Institute, - einen vom Auslagerungsunternehmen beauftragten Dritten oder - einen von den auslagernden Instituten beauftragten Dritten. Im Rahmen ihrer Revisionshandlungen kann die Interne Revision auch auf Nachweise/Zertifikate auf Basis gängiger Standards zurückgreifen. Hierbei sind sowohl die Detailtiefe, Aktualität und Eignung der Nachweise/Zertifikate und der zugehörigen Prüfberichte als auch die Eignung des Zertifizierers oder Prüfers zu berücksichtigen. Allerdings darf sich ein beaufsichtigtes Unternehmen bei wesentlichen Auslagerungen bei der Ausübung seiner Revisionstätigkeit nicht allein hierauf stützen.

BT 2.2 Grundsätze für die Interne Revision

1	Die Interne Revision hat ihre Aufgaben selbständig und unabhängig wahrzunehmen. Insbesondere ist zu gewährleisten, dass sie bei der Berichterstattung und der Wertung der Prüfungsergebnisse keinen Weisungen unterworfen ist. Das Direktionsrecht der Geschäftsleitung zur Anordnung zusätzlicher Prüfungen steht der Selbständigkeit und Unabhängigkeit der Internen Revision nicht entgegen.	
2	Die in der Internen Revision beschäftigten Mitarbeiter dürfen grundsätzlich nicht mit revisionsfremden Aufgaben betraut werden. Sie dürfen insbesondere keine Aufgaben wahrnehmen, die mit der Prüfungstätigkeit nicht im Einklang stehen. Soweit die Unabhängigkeit der Internen Revision gewährleistet ist, kann sie im Rahmen ihrer Aufgaben für die Geschäftsleitung oder andere Organisationseinheiten des Instituts beratend tätig sein.	
3	Mitarbeiter, die in anderen Organisationseinheiten des Instituts 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. Beim Wechsel von Mitarbeitern anderer Organisationseinheiten zur Internen Revision sind angemessene Übergangsfristen von in der Regel mindestens einem Jahr vorzusehen, innerhalb derer diese Mitarbeiter keine Tätigkeiten prüfen dürfen, die gegen das Verbot der Selbstprüfung und -überprüfung verstoßen. Erleichterungen hinsichtlich der Übergangsfristen sind für Institute in Abhängigkeit von der Art, dem Umfang, der Komplexität und dem Risikogehalt der betriebenen Geschäftsaktivitäten möglich.	

BT 2.3 Prüfungsplanung und -durchführung

1	Die Tätigkeit der Internen Revision muss auf einem umfassenden und jährlich fortzuschreibenden Prüfungsplan basieren. Die Prüfungsplanung hat risikoorientiert zu erfolgen. Die Aktivitäten und Prozesse des Instituts sind, auch wenn diese ausgelagert sind, in angemessenen Abständen, grundsätzlich innerhalb von drei Jahren, zu prüfen. Wenn besondere Risiken bestehen, ist jährlich zu prüfen. Bei unter Risikogesichtspunkten nicht wesentlichen Aktivitäten und Prozessen kann vom dreijährigen Turnus abgewichen werden. Die Risikoeinstufung der Aktivitäten und Prozesse ist regelmäßig zu überprüfen.	Unter Risikogesichtspunkten nicht wesentliche Aktivitäten und Prozesse Ein Abweichen vom dreijährigen Prüfungsturnus für unter Risikogesichtspunkten nicht wesentliche Aktivitäten und Prozesse ist nicht gleichbedeutend mit einem weitgehenden Verzicht von Prüfungshandlungen in diesen Bereichen. Auch diese sind in die Prüfungsplanung zu integrieren und in angemessenen Abständen zu prüfen.
2	Die Risikobewertungsverfahren der Internen Revision haben eine Analyse des Risikopotenzials der Aktivitäten und Prozesse unter Berücksichtigung absehbarer Veränderungen zu beinhalten. Dabei sind die verschiedenen Risikoquellen und die Manipulationsanfälligkeit der Prozesse durch Mitarbeiter angemessen zu berücksichtigen.	
3	Die Prüfungsplanung, -methoden und -qualität sind regelmäßig und anlassbezogen auf Angemessenheit zu überprüfen und weiterzuentwickeln.	
4	Es muss sichergestellt sein, dass kurzfristig notwendige Sonderprüfungen, z. B. anlässlich deutlich gewordener Mängel oder bestimmter Informationsbedürfnisse, jederzeit durchgeführt werden können.	
5	Die Prüfungsplanung sowie wesentliche Anpassungen sind von der Geschäftsleitung zu genehmigen.	

BT 2.4 Berichtspflicht

1	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. Wesentliche Mängel sind besonders herauszustellen. Dabei sind die Prüfungsergebnisse zu beurteilen. Bei schwerwiegenden Mängeln muss der Bericht unverzüglich der Geschäftsleitung vorgelegt werden.	Abstufung der Mängel Das Rundschreiben unterscheidet in BT 2 zwischen „wesentlichen“, „schwerwiegenden“ und „besonders schwerwiegenden“ Mängeln. Damit wird eine ordinale Abstufung hinsichtlich der (potenziellen) Bedeutung der unter Risikogesichtspunkten relevanten festgestellten Mängel erreicht. Die genaue Abgrenzung der einzelnen Stufen bleibt dem jeweiligen Institut überlassen. Es liegt im Ermessen des Instituts, für unter Risikogesichtspunkten weniger relevante festgestellte Mängel eigene Festlegungen zu treffen.
2	Die Prüfungen sind durch Arbeitsunterlagen zu dokumentieren. Aus ihnen müssen die durchgeführten Arbeiten sowie die festgestellten Mängel und Schlussfolgerungen für sachkundige Dritte nachvollziehbar hervorgehen.	
3	Besteht hinsichtlich der zur Erledigung der Feststellungen zu ergreifenden Maßnahmen keine Einigkeit zwischen geprüfter Organisationseinheit und Interner Revision, so ist von der geprüften Organisationseinheit eine Stellungnahme hierzu abzugeben.	
4	Die Interne Revision hat über die im Jahresablauf festgestellten schwerwiegenden sowie über die noch nicht behobenen wesentlichen Mängel in inhaltlich prägnanter Form an die Geschäftsleitung und das Aufsichtsorgan zu berichten (Jahresbericht). Es ist ferner darzulegen, ob und inwieweit die Vorgaben des Prüfungsplans eingehalten wurden. Die aufgedeckten schwerwiegenden Mängel, die beschlossenen Maßnahmen sowie der Status dieser Maßnahmen sind dabei besonders hervorzuheben. Über besonders schwerwiegende Mängel hat die Interne Revision unverzüglich zu berichten.	Darstellung von Feststellungen im Jahresbericht Die Darstellung kann dabei akzentuiert vorgenommen werden. Gleichartige Einzelfeststellungen sowie der Stand der beschlossenen Umsetzungsmaßnahmen können inhaltlich zusammengefasst werden. Berichterstattung an das Aufsichtsorgan Die Berichterstattung an das Aufsichtsorgan kann auch über die Geschäftsleitung erfolgen, sofern dadurch keine nennenswerte Verzögerung der Information des Aufsichtsorgans verbunden und der Inhalt der Berichterstattung an Geschäftsleitung und Aufsichtsorgan deckungsgleich ist.

5	Ergeben sich im Rahmen der Prüfungen schwerwiegende Feststellungen gegen Geschäftsleiter, so ist der Geschäftsleitung unverzüglich Bericht zu erstatten. Diese hat unverzüglich den Vorsitzenden des Aufsichtsorgans sowie die Aufsichtsinstitutionen (Bundesanstalt für Finanzdienstleistungsaufsicht, Deutsche Bundesbank) zu informieren. Kommt die Geschäftsleitung ihrer Berichtspflicht nicht nach oder beschließt sie keine sachgerechten Maßnahmen, so hat die Interne Revision den Vorsitzenden des Aufsichtsorgans zu unterrichten.
6	Revisionsberichte und Arbeitsunterlagen sind sechs Jahre aufzubewahren.

BT 2.5 Reaktion auf festgestellte Mängel

1	Die Interne Revision hat die fristgerechte Beseitigung der bei der Prüfung festgestellten Mängel in geeigneter Form zu überwachen. Gegebenenfalls ist hierzu eine Nachschauprüfung anzusetzen.
2	Werden die wesentlichen Mängel nicht in einer angemessenen Zeit beseitigt, so hat der Leiter der Internen Revision darüber zunächst den fachlich zuständigen Geschäftsleiter schriftlich zu informieren. Erfolgt die Mängelbeseitigung nicht, so ist die Geschäftsleitung spätestens im Rahmen des nächsten Gesamtberichts schriftlich über die noch nicht beseitigten Mängel zu unterrichten.

BT 3 Anforderungen an die Risikoberichterstattung

BT 3.1 Allgemeine Anforderungen an die Risikoberichte

1	Die Geschäftsleitung hat sich in angemessenen Abständen über die Geschäftslage und die Risikosituation berichten zu lassen. Die hierfür zu erstellenden Berichte sind in nachvollziehbarer, aussagefähiger Art und Weise zu verfassen. Die Berichterstattung hat neben einer Darstellung auch eine Beurteilung der Risikosituation zu enthalten. Die Berichte müssen auf vollständigen, genauen und aktuellen Daten beruhen. Die Risikoberichte müssen auch eine zukunftsorientierte Risikoeinschätzung abgeben und sich nicht ausschließlich auf aktuelle und historische Daten stützen. In die Risikoberichterstattung sind bei Bedarf auch Handlungsvorschläge, z. B. zur Risikoreduzierung, aufzunehmen.	Nachvollziehbarkeit und Aussagefähigkeit der Berichte Eine nachvollziehbare und aussagefähige Geschäfts- und Risikoberichterstattung setzt auch ein inhaltlich angemessenes Verhältnis zwischen quantitativen Informationen und qualitativer Beurteilung wesentlicher Positionen und Risiken voraus. Aktualität der Daten Daten sind grundsätzlich zum Stichtag des Risikoberichts zu erheben und zu berichten. Bei Verwendung vorläufiger Daten oder Daten aus Vorperioden ist dies gesondert zu kennzeichnen und ggf. zu begründen. Berücksichtigung von ESG-Risiken Die Risikoberichterstattung gibt der Geschäftsleitung einen aktuellen und, soweit sinnvoll und möglich, quantitativen Überblick über die Auswirkungen von ESG-Risiken.
2	Neben der turnusmäßigen Erstellung von Risikoberichten (Gesamtrisikobericht, Berichte über einzelne Risikoarten) muss das Institut in der Lage sein, ad hoc Risikoinformationen zu generieren, sofern dies aufgrund der aktuellen Risikosituation des Instituts oder der aktuellen Situation der Märkte, auf denen das Institut tätig ist, geboten erscheint.	
3	Die Risikoberichte sind in einem zeitlich angemessenen Rahmen zu erstellen, der eine aktive und zeitnahe Steuerung der Risiken auf der Basis der Berichte ermöglicht, wobei die Produktionszeit auch von der Art und der Volatilität der Risiken abhängt.	
4	Die Geschäftsleitung hat das Aufsichtsorgan mindestens jährlich über die Risikosituation einschließlich vorhandener Risikokonzentrationen in angemessener Weise schriftlich zu informieren. Die Berichterstattung ist in nachvollziehbarer, aussagefähiger Art und Weise zu verfassen und hat neben der Darstellung auch eine Beurteilung der Risikosituation zu enthalten. Auf besondere Risi-	Ausschüsse des Aufsichtsorgans Soweit ein Aufsichtsorgan besteht, sollte Adressat der Risikoberichterstattung grundsätzlich jedes Mitglied des Aufsichtsorgans sein. Soweit das Aufsichtsorgan Ausschüsse gebildet hat, kann die

	ken für die Geschäftsentwicklung und dafür geplante Maßnahmen der Geschäftsleitung ist gesondert einzugehen. Für das Aufsichtsorgan unter Risikogesichtspunkten wesentliche Informationen sind von der Geschäftsleitung unverzüglich weiterzuleiten. Hierfür hat die Geschäftsleitung gemeinsam mit dem Aufsichtsorgan ein geeignetes Verfahren festzulegen.	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.

BT 3.2 Berichte der Risikocontrolling-Funktion

1	Die Risikocontrolling-Funktion hat in angemessenen Abständen einen Gesamtrisikobericht über die als wesentlich eingestuften Risikoarten unter Berücksichtigung der Auswirkungen von ESG-Risiken zu erstellen und der Geschäftsleitung vorzulegen. Der Turnus ist in Abhängigkeit von der Risikoart, der Art, dem Umfang, der Komplexität und dem Risikogehalt festzulegen. .	Berichterstattung in Stressphasen Von den Instituten wird erwartet, dass sie in Stressphasen des eigenen Instituts den Berichtsturnus erhöhen, soweit dies für die aktive und zeitnahe Steuerung der Risiken erforderlich erscheint. Als wesentlich eingestufte Risikoarten Die als wesentlich eingestuften Risikoarten ergeben sich aus der Wesentlichkeitsbeurteilung entsprechend AT 2.2 Tz. 1.
2	Der Gesamtrisikobericht hat neben den wesentlichen Informationen zu den einzelnen als wesentlich eingestuften Risikoarten, den Stresstestergebnissen und Informationen zu den Risikokonzentrationen auch Angaben zur Angemessenheit der Risikoabschirmung und zur regulatorischen Eigenmittelausstattung aufzunehmen.	Hinweise zur Risikoberichterstattung Bei der Risikoberichterstattung zu den einzelnen als wesentlich eingestuften Risikoarten sind Risikoinformationen mit aussagekräftigen Strukturmerkmalen darzustellen (z. B. Risikokonzentrationen nach Branchen, Ländern, Risikoklassen, Größenklassen; etwaige Limite und deren Auslastung bzw. bedeutende Limitüberschreitungen; Umfang und Entwicklung des Neugeschäfts sowie von Rückbelastungen/“Chargebacks") 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 bzw. der Handlungsvorschläge nicht auf eine unsachgerechte Weise verzerrt wird.
3	Die Geschäftsleitung ist mindestens jährlich über bedeutende Schadensfälle, wesentliche Schwächen sowie über wesentliche potenzielle Ereignisse (gem. BTR 1 Tz. 5 Erläuterungen) aus operationellen Risiken zu unterrichten. Die Berichterstattung hat die Art des Schadens bzw. Risikos, die Ursachen, das Ausmaß des Schadens bzw. Risikos und initiierte sowie bereits getroffene Gegenmaßnahmen zu umfassen.	