Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Stellungnahme

Konsultation des Rundschreibens „Bankaufsichtliche Anforderungen an die IT" (BAIT) vom 22.03.2017

Kontakt:
Berit Schimm
Telefon: +49 30 2021- 2111
Telefax: +49 30 2021-19 - 2100
E-Mail: b.schimm@bvr.de

Berlin, 04.05.2017

Federführer:
Bundesverband der Deutschen Volksbanken
und Raiffeisenbanken e. V.
Schellingstraße 4 | 10785 Berlin
Telefon: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

Allgemeine Anmerkungen/ Anmerkungen zu I. Vorbemerkung

Die BAIT konkretisieren laut Vorbemerkungen die **MaRisk** und sollten somit keine über die Vorgaben der MaRisk hinausgehenden Anforderungen enthalten. Im vorgelegten Entwurf wird dem durch die Referenzierung auf die MaRisk in der ersten Tz. jedes Moduls grundsätzlich Rechnung getragen. Damit sind für die maßgeblichen Regelungen zur IT beide Rundschreiben heranzuziehen. Da die 5. MaRisk-Novelle noch nicht veröffentlicht wurde, ist die Prüfung der Konsistenz zwischen BAIT und MaRisk im Rahmen der BAIT-Konsultation nur eingeschränkt auf Basis des Zwischenentwurfs der MaRisk vom 23.6.2016 möglich. Im Einzelnen sind Unklarheiten in der Interpretation der BAIT i.V.m. den MaRisk und Widersprüche in den Begrifflichkeiten zu erkennen (vgl. Kommentare zum Informationsrisiko-management, Berechtigungsmanagement, IT-Auslagerungen und sonstigem Fremdbezug). Deshalb sollte auf Basis des finalen MaRisk-Textes eine inhaltliche und formale Konsistenzprüfung erfolgen.

Die BAIT nutzen an unterschiedlichen Stellen Begriffe, die in den MaRisk nicht enthalten sind und teilweise aus unterschiedlichen IT-Standards entlehnt sind. Wir bitten um Erläuterung dieser Begriffe in einem Glossar oder in den jeweiligen Modulen, um Missverständnissen bzw. unterschiedlichen Auslegungen vorzubeugen.

In der Vorbemerkung des aktuellen Entwurfs der BAIT (Tz. 1) sowie dem Anschreiben zur Konsultation wird ausgeführt, dass das Rundschreiben auch die Anforderungen an das Risikomanagement auf Gruppenebene konkretisieren soll. Dies kann u.E. dahingehend missverstanden werden, dass die einzelnen auf die Institutsebene bezogenen Anforderungen vollständig und in gleicher Weise auch auf Gruppenebene umzusetzen sind. Eine solche Anforderung würde zu einer unverhältnismäßigen Verschärfung des Regulierungsrahmens für Gruppen führen. Wir plädieren daher für eine Streichung des Bezugs auf § 25a Abs. 3 KWG (Risikomanagement auf Gruppenebene) auch mit Blick darauf, dass eine Umsetzung der BAIT auf Ebene der Institute bereits eine ausreichende Grundlage für eine ordnungsgemäße Geschäftsorganisation in der Gruppe bezogen auf die IT darstellt.

In den Vorbemerkungen der BAIT wird dargelegt, dass mit den prinzipienorientierten Anforderungen dem **Proportionalitätsprinzip** Rechnung getragen werden soll. Durch die Verknüpfung mit den Hinweisen auf die Erfüllung möglicherweise weitergehender Anforderungen aufgrund von Größe, Komplexität und besonderer Risikoexponiertheit in derselben Textziffer, wird die Proportionalität nach „oben" interpretiert. Wir bitten zusätzlich um eine klare Bezugnahme auf MaRisk AT 1 Tz. 5 (Zwischenentwurf[1]) in den Vorbemerkungen, um dem Proportionalitätsprinzip in den BAIT analog zu den MaRisk Rechnung zu tragen und darzulegen, dass kleineren Instituten eine flexible Umsetzung ermöglicht wird.

Weitere Öffnungsklauseln, die die Anforderungen in Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der IT-gestützten Geschäftsaktivitäten bzw. der Ausgestaltung des IT-Betriebs differenzieren, sollten in den BAIT ergänzt werden. Die entsprechenden Vorschläge sind in unsere speziellen Anmerkungen eingearbeitet.

[1] „Das Rundschreiben trägt der heterogenen Institutsstruktur und der Vielfalt der Geschäftsaktivitäten Rechnung. Es enthält zahlreiche Öffnungsklauseln, die abhängig von der Größe der Institute, den Geschäftsschwerpunkten und der Risikosituation eine vereinfachte Umsetzung ermöglichen. Insoweit kann es vor allem auch von kleineren Instituten flexibel umgesetzt werden."

Für Institute, die die IT weitestgehend auf nach deutschem Recht organisierte IT-Dienstleister ausgelagert haben (insbesondere solche, die von Instituten eines Finanzverbundes oder eines Konzerns getragen werden und deren Geschäftstätigkeit im Wesentlichen darin besteht, standardisierte IT für die angeschlossenen Institute zu erbringen), ergeben sich im Hinblick auf diese besondere Konstellation und die Arbeitsteilung bei den beschriebenen Anforderungen unter Berücksichtigung der Risiken besondere Ansätze für die Proportionalität. Wir interpretieren die BAIT-Anforderungen so, dass diese Institute zumindest in Teilen auf die beim IT-Dienstleister geltenden Richtlinien, Verfahren, Dokumentationen und Prozesse für die Erfüllung der Anforderungen abstellen können.

Wir bitten, für die BAIT ausreichende Übergangsfristen vorzusehen. Durch die Konkretisierung der MaRisk über die BAIT werden einige Vorgaben der Aufsicht für den Einsatz von Informationstechnik erstmalig transparent. Die konkrete Umsetzung der MaRisk in den Instituten kann sich heute im Detail von diesen Vorgaben unterscheiden, da z.B. andere Modelle oder Vorgehensweisen gewählt wurden oder die aufsichtlichen Erwartungen anders interpretiert wurden. Des Weiteren beziehen sich die BAIT bereits auf Regelungen der MaRisk, die erst mit der neuen MaRisk-Novelle veröffentlicht werden und folglich heute noch nicht vollständig bekannt und umgesetzt sind. Wir bitten deshalb um eine angemessene Übergangsfrist von einem Jahr für die Umsetzung der BAIT.

Spezielle Anmerkungen zu den einzelnen Textziffern

1. IT-Strategie

Tz. 1

Hinsichtlich der beschriebenen Aufgabe der Geschäftsleitung, eine IT-Strategie festzulegen, sollte der Zusatz „nachhaltige" gestrichen werden. Gemäß AT 4.2 Tz. 1 MaRisk soll die Geschäftsstrategie nachhaltig sein, alle ergänzenden Strategien müssen konsistent dazu formuliert sein.

Tz. 2

Wir gehen davon aus, dass wie im Fachgremium IT mündlich erörtert, die IT-Strategie nicht zwingend in einem separaten Strategiedokument neben der Geschäftsstrategie darzustellen ist. Das Modul erläutert vielmehr die Mindestinhalte, zu denen strategische Aussagen zur IT getroffen werden sollen.

Formulierungsvorschlag zu Tz. 2, Satz 1, linke Spalte: „Die Geschäftsleitung hat ~~eine~~ mit der Geschäftsstrategie konsistente strategische Aussagen zur IT zu treffen ~~IT-Strategie festzulegen~~. „

Ergänzung eines einleitenden Satzes zu Tz. 2, rechte Spalte: „In der IT-Strategie müssen grundsätzliche strategische Aussagen zur IT enthalten sein. Zur Detaillierung fachlicher Inhalte kann auf weitere Dokumente auf operationeller Ebene verwiesen werden."

Zu a) In den Erläuterungen wird der Begriff Dienstleistungsportfolio mit IT-Bezug aufgeführt. Wir bitten um Erläuterung des Begriffs. Weiterhin sind IT-Prozesse Bestandteil der IT-Ablauforganisation, daher ist die Bezugnahme auf IT-Prozesse redundant und kann hier entfallen.

Zu b) Wir bitten um Erläuterung, was in Bezug auf die Zuordnung gängiger Standards mit „Zielbild im Hinblick auf den Erfüllungsgrad" gemeint ist.

Zu c) In der Aufzählung der Mindestinhalte zur IT-Strategie sollte „Eckpunkte der Informationssicherheitsorganisation" ersetzt werden durch „Zuständigkeiten und Einbindung der

Informationssicherheit in die Organisation", da diese Formulierung das in den Erläuterungen unter c) gewollte passender umschreibt.

Zu e) Es sollte über die Erläuterungsspalte klargestellt werden, dass es um Aussagen zum Notfallmanagement mit Bezug auf IT-Belange geht.

Zu f) Wir schlagen vor, den Klammerzusatz „Hardware- und Softwarekomponenten" auf der linken Seite zu streichen. In die Erläuterungsspalte sollten weiterführende Hinweise / Beispiele aufgenommen werden.

2. IT-Governance

Tz. 3

Der Begriff "IT-Risikosteuerungsprozesse" steht im Widerspruch zum Modul 3 Informationsrisikomanagement und sollte ersetzt werden durch „Steuerungsprozesse für Informationsrisiken".

Tz. 5

Der Begriff „Informationsrisikomanagement" sollte in der Aufzählung zur angemessenen Personalausstattung gestrichen werden, da das Informationsrisikomanagement im Sinne des 3. Moduls der BAIT keine personell vorzuhaltende Funktion sondern Methoden und Verfahren beschreibt.

Tz. 6

Bei Anwendung des Proportionalitätsprinzips werden kleinere Institute Interessenkonflikte grundsätzlich zu vermeiden versuchen, aber diese aufgrund Größe, Art und Umfang des Geschäftsbetriebs nicht vollständig vermeiden können und daher diesen über institutsinterne Grundsätze Rechnung tragen. Beispielsweise kommen in anderen Vorschriften wie den MaComp auch vergleichbare organisatorische Maßnahmen in Betracht, um Interessenkonflikte möglichst gering zu halten. Es führt auch nicht jede Tätigkeit in Anwendungsentwicklung und IT-Betrieb zwangsläufig zu Interessenkonflikten. In der Entwurfsfassung aus dem Januar 2017 war die Rollendefinition im zweiten Satz in den Erläuterungen noch explizit als eine sachgerechtere Kann-Bestimmung definiert.

Formulierungsvorschlag zur linken Spalte: „~~Interessenkonflikte und~~ ~~u~~Unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation (z.B. aufgrund wesentlicher Interessenkonflikte) sind zu vermeiden."

Formulierungsvorschlag zur rechten Spalte: "Zum Beispiel kann Interessenkonflikten zwischen Tätigkeiten, die gegebenenfalls im Zusammenhang mit der Anwendungsentwicklung und den Aufgaben des IT-Betriebs entstehen, durch aufbau- oder ablauforganisatorische Maßnahmen begegnet werden. Dies ~~schließt~~ kann beispielsweise adäquate Rollendefinitionen einschließen."

3. Informationsrisikomanagement

Der Anspruch dieses Moduls ist bzw. sollte es sein, dass Risiken mit Bezug zur Informationstechnologie (IT) ebenfalls im Risikomanagement der Institute zu berücksichtigen sind und Bestandteile zum Management dieser Risiken aufgezeigt werden. Einzelne Risiken der Informationstechnologie können in Zusammenhang mit Risiken anderer Bereiche stehen, z.B. Personal-, Prozess-, Rechtsrisiken. IT-Risiken fließen als Teil des operationellen Risikos und nicht als eigenständige Kategorie in die Risikosteuerungs- und -controllingprozesse des Instituts insgesamt ein. Durch den Begriff „Informationsrisikomanagement" kann die Fehlinterpretation entstehen, dass hier eine separate Risikodisziplin etabliert werden solle.

Tz. 8

Es wird auf den allgemeinen Passus zum Risikocontrolling unter AT 4.3.1 MaRisk referenziert und nicht auf den Passus zu den IT-Risiken unter AT 7.2 Tz. 4 MaRisk (lt. Zwischenentwurf vom 23.6.2016). Sofern die finalen MaRisk den Passus zu den IT-Risiken[2] unter AT 7.2 Tz. 4 enthalten werden, bitten wir um Referenzierung und regen eine konsistente Verwendung der Begriffe in den MaRisk und BAIT an. Redundante Regelungen sollten dessen ungeachtet vermieden werden. Berichtspflichten zu wesentlichen operationellen Risiken, unter denen Informationsrisiken eine Teilmenge bilden, sind in BT 3.2 Tz. 6 MaRisk (Zwischenentwurf) anstelle BT 3.2 Tz. 7 geregelt. Wir bitten um Richtigstellung. Zudem ist der BTR 4 für das Management der operationellen Risiken zu beachten und dort abschließend behandelt.

Tz. 9

In den Erläuterungen zu Tz. 9 wird der Begriff "verantwortliche Stellen" verwendet. Dieser Begriff ist jedoch nicht Bestandteil der Regelung in Tz. 9 (dort: "maßgebliche Stellen und Funktionen"). Wir bitten um einheitliche Begriffsverwendung.

Tz. 10

Wir bitten um eine Konkretisierung des Begriffes "Informationsverbund", da dieser Begriff z.B. gemäß der BSI-Definition[3] die Ausweitung der bisherigen MaRisk-Anforderungen bedeuten würde.

Nach unserem Verständnis sollen hier ausschließlich die wesentlichen Geschäftsprozesse, die mittels IT-Systemen unterstützt werden, sowie die schutzwürdigen Räume (z.B. Rechenzentrum, Treasury Büros) adressiert werden. Dies sollte klargestellt werden. Nach der derzeitigen Formulierung von „räumliche Gegebenheiten" könnte jeder Raum (z.B. auch eine Kantine) gemeint sein.

Wir verstehen die Übersicht zum Informationsverbund so, dass die Einbeziehung der Informationen von der durch Dienstleister betriebenen IT nur bis zu einer Granularität darzustellen ist, die für die Risikosteuerung erforderlich ist. Wir bitten um Konkretisierung der Inhalte und der Granularität der zum Informationsverbund mindestens vorzuhaltenden Informationen.

Wir bitten um eine Erläuterung des Begriffes „Risikosituation" zur Orientierung bei der Erhebung eines Informationsverbundes, da sich die Risikosituation aus der Schutzbedarfsfeststellung ergibt. Wir verstehen den Begriff in der Aufzählung dahingehend, dass kleinere Institute ohne wesentliche eigenbetriebene IT vereinfachte Verfahren zur Erhebung des Informationsverbundes anwenden können.

Formulierungsvorschlag zur rechten Spalte:
„Zu einem Informationsverbund gehören neben den Informationen bspw. wesentliche IT-gestützte Geschäftsprozesse, IT-Systeme und ~~räumliche Begebenheiten~~ schutzwürdige IT-Räume (z.B. Rechenzentrum)."

---

[2] „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"

[3] BSI Definition: „Unter einem Informationsverbund (oder auch IT-Verbund) ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen."

Tzn. 12 und 13

Laut Tz. 12 sind sachgerecht die Soll-Anforderungen zur Umsetzung der Schutzziele des Instituts festzulegen. Das Ergebnis dieses Arbeitsschrittes sollte als „Sollmaßnahmenkatalog" bezeichnet werden, um eine Verwechslung mit Referenzmaßnahmen etwa nach BSI-Grundschutz auszuschließen. Ein Abstellen auf Referenzmaßnahmen wäre u.U. nicht sachgerecht, da bei entsprechendem Schutzbedarf die Referenzmaßnahmen nicht ausreichen oder bezogen auf das Schutzobjekt nicht relevant sein können.
In Tz. 13 sollte ebenfalls durchgängig der Begriff „Sollmaßnahmen" anstelle von „Referenzmaßnahmen" verwendet werden.

Tzn. 14 und 15

Die Ergebnisse der in den bis Tz. 13 dargestellten Schritten fließen in das Risikomanagement des Instituts ein. Eine einheitliche Behandlung aller operationellen Risiken auch mit Blick auf übergreifende Risikosteuerungsmaßnahmen ist sinnvoll. Der Begriff „Restrisiken" ist jedoch missverständlich und sollte gestrichen werden. Er impliziert, dass jegliche Risiken – also auch sehr unwahrscheinliche oder solche mit geringem Schadenspotenzial – aktiv gesteuert werden müssten. Dies widerspricht dem Grundgedanken der MaRisk.
Wir schlagen deshalb vor, Tz. 14 und Tz. 15 zusammenzufassen und dort lediglich auszuführen, dass die Ergebnisse der Risikoanalyse in Bezug auf Risiken mit Bezug zur Informationstechnologie im Rahmen der operationellen Risiken im Prozess des Risikomanagements des Instituts zu berücksichtigen sind.

4. Informationssicherheitsmanagement

Im Rahmen der BAIT wird durchgängig der Begriff „Informationssicherheit" verwendet. Im Hinblick auf die Sicherheit der Informationstechnik wird in den Häusern häufig der Begriff „IT-Sicherheit" genutzt. Unter die Informationssicherheit können grundsätzlich auch Aspekte ohne IT-Bezug (z. B. Aktenaufbewahrung) gefasst werden. Wir bitten um Definition des Begriffes „Informationssicherheit", um Missverständnisse im Sinne der BAIT zu vermeiden.

Tz. 16

Wir bitten um Erläuterung, ob die hier genannten „Soll-Anforderungen" identisch sind zu den in Tz. 12 (Informationsrisikomanagement) festzulegenden Soll-Anforderungen und folglich eine Verknüpfung zwischen beiden Modulen besteht. Zutreffender ist, dass der Informationssicherheitsbeauftragte deren Umsetzung steuert (statt für Umsetzung sorgt). Die Anforderung einer angemessenen Personalausstattung wird bereits in Tz. 5 (IT-Governance) genannt und könnte hier gestrichen werden.

Lt. Tz. 16 sind die „nicht umgesetzten Soll-Maßnahmen zur adäquaten Steuerung der hieraus entstehenden Risiken an das Informationsrisikomanagement zu berichten". Wie bereits in der Stellungnahme zum Modul 3 erläutert, handelt es sich beim Informationsrisikomanagement nicht zwingend um eine eigene Funktion, an die eine Berichterstattung erfolgt.

Formulierungsvorschlag:
„Nicht umgesetzte Soll-Maßnahmen sind zur adäquaten Steuerung der hieraus entstehenden Risiken im Rahmen des ~~an das~~ Informationsrisikomanagements zu ~~berichten~~ bewerten und im operationellen Risiko zu berücksichtigen."

Bzgl. Berichtspflichten ist auch hier die Referenz auf BT 3.2 Tz. 6 MaRisk anstelle BT 3.2 Tz. 7 zutreffend, wo u.a. die Berichterstattung zu bedeutenden Schadensfällen geregelt wird.

Tzn. 17 bis 19

Einschlägige Standards benutzen verschiedene Begriffe für die Dokumente zur Informationssicherheit, z.B. Informationssicherheitsrichtlinie, Informationssicherheitsleitlinie, Informationssicherheitskonzepte. Die Verwendung erfolgt nicht konsistent zu den BAIT. Um Fehlinterpretationen vorzubeugen, schlagen wir vor, auf die Einführung von fest vorgegebenen Begriffen für die Dokumente in den BAIT zu verzichten und stattdessen Informationssicherheitsrichtlinie bzw. Informationssicherheitskonzepte durch „allgemeine Regelungen zur Informationssicherheit" bzw. „konkretisierende Regelungen" zu ersetzen.

Tz. 18

Wir bitten um Klarstellung, ob der Zusatz „hinsichtlich der Dimensionen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren" sich auf die Informationssicherheitsprozesse oder auch auf die Informationssicherheitskonzepte bezieht und was mit diesen Dimensionen konkret gemeint ist. In den Erläuterungen schlagen wir vor, den Begriff „ihrer Materialisierung" zu ersetzen durch „ihres Eintretens".

Tz. 19

Die Verantwortung des Informationssicherheitsbeauftragten umfasst nicht das transparent machen der Ziele und Maßnahmen der IT-Strategie, sondern nur der hieraus abgeleiteten Regelungen zur Informationssicherheit. Daher sollte der Begriff „IT-Strategie" in der Aufzählung gestrichen werden.

Wir schlagen vor, in der Erläuterung in der rechten Spalte das Wort „insbesondere" durch „beispielsweise" zu ersetzen. Je nach Größe des Instituts und Aufgabenteilung kann sich ein unterschiedliches Aufgabenprofil für den Informationssicherheitsbeauftragten ergeben.

Zu den einzelnen Unterpunkten:
- Die Erstellung und Fortschreibung der Informationssicherheitskonzepte erfolgt ggf. nicht durch den Informationssicherheitsbeauftragten selbst, dieser hat eine verantwortliche Koordinationsrolle.
- Die Beteiligung bei der Erstellung und Fortschreibung des IT-Notfallkonzepts sollte durch „Notfallkonzept in Bereichen mit IT-Bezug" ersetzt werden, um klarer zu fassen, dass nicht die Erstellung eines separaten IT-Notfallkonzepts notwendig ist.
- Der Informationssicherheitsbeauftragte ist nur bei solchen Projekten zu beteiligen, die auch Informationssicherheitsrelevanz haben.

Tz. 20

Im Modul 4 ist durchgängig von der Funktion des Informationssicherheitsbeauftragten die Rede. Dem sollte auch in den Erläuterungen in Tz. 20 im ersten Unterpunkt Rechnung getragen werden und nicht auf eine Stelle abgestellt werden.

Formulierungsvorschlag zur rechten Spalte: „• Funktions~~- und Stellen~~beschreibung für den Informationssicherheitsbeauftragten ~~und seinen Vertreter~~, jederzeitige Sicherstellung der Funktion (Vertretungsregelung)"

Wir bitten um Klarstellung der aufbauorganisatorischen Trennung von den für Betrieb und Weiterentwicklung der IT-Systeme zuständigen Bereichen. Nach unserem Verständnis ist eine funktionale Trennung gemeint, z.B. durch eine Trennung der Organisationseinheiten. Die Funktion sollte uneingeschränkt durch die Geschäftsleitung wahrgenommen werden können. Bei kleinen Instituten, die keine wesentliche eigenbetriebene IT haben und folglich nur wenige Aufgaben im Zusammenhang mit dem Betrieb und der Weiterentwicklung der IT im Institut verbleiben, sollte Interessenskonflikten auch

anderweitig durch risikomindernde organisatorische Maßnahmen, z.B. die Einrichtung eines Informationssicherheitsteams vorgebeugt werden können. Soweit die anderen genannten Anforderungen zur Gewährleistung der Unabhängigkeit und zur Vermeidung möglicher Interessenkonflikte sichergestellt sind, kann unter Berücksichtigung von Proportionalitätsgesichtspunkten u. E. auch eine Ansiedlung der Funktion innerhalb einer Organisationsabteilung mit IT-Aufgaben erfolgen. Eine solche Lösung bietet im Hinblick auf die fachliche Qualifikation und informatorische Einbindung des Informationssicherheits-beauftragten sogar Vorteile im Vergleich zu einer abgekoppelten Stabsstelle.

Tz. 21

Wir begrüßen die Öffnungsklausel zur Möglichkeit der Auslagerung des Informationssicherheits-beauftragten. Die Formulierung „gemeinsamer Informationssicherheitsbeauftragter" hat jedoch zu zahlreichen Nachfragen seitens unserer Institute geführt.

Formulierungsvorschlag zur rechten Spalte: „Im Hinblick auf regional tätige (insbesondere verbundangehörige) Institute sowie kleine (insbesondere) gruppenangehörige Institute ohne wesentliche eigenbetriebene IT mit einem gleichgerichteten Geschäftsmodell und gemeinsamen IT-Dienstleistern für die Abwicklung von bankfachlichen Prozessen, ist es im Hinblick auf die regelmäßig (verbund- oder gruppenseitig) vorhandenen Kontrollmechanismen zulässig, ~~wenn mehrere Institute einen gemeinsamen~~ dass ein externer Informationssicherheitsbeauftragter von Instituten beauftragt werden kann ~~bestellen~~, wobei vertraglich sicherzustellen ist, dass dieser ~~gemeinsame~~ Informationssicherheitsbeauftragte die Wahrnehmung der einschlägigen Aufgaben der Funktion in allen betreffenden Instituten jederzeit gewährleisten kann. …"

Eine Beschränkung der Möglichkeit, die Funktion mit anderen Funktionen im Institut kombinieren zu dürfen, auf kleine Institute, halten wir für nicht sachgerecht. Der Aufgabenumfang hängt weniger von der Größe eines Instituts ab, sondern maßgeblich von den Geschäftsaktivitäten und davon, wie komplex die IT ist und in welchem Umfang dieses eigenentwickelte und –betriebene IT-Systeme einsetzt. Ein zutreffenderes Kriterium bezogen auf die Funktion wäre, ob der Aufgabenumfang der Funktion eine Vollzeitstelle auslastet. Ferner sind heute auch Ausgestaltungen der Funktion geübte Praxis, bei denen mehrere Mitarbeiter an den Aufgaben der Funktion mitwirken, so dass auch bei mittleren bis größeren Instituten die Funktion des Informationssicherheitsbeauftragen mit anderen Funktionen kombiniert werden kann, ohne dass es zu einem Qualitätsverlust bei der Erfüllung der Aufgaben kommt. Die MaRisk enthalten zudem keine ressourcenbezogenen Vorgaben. Wir bitten deshalb um Streichung des vorletzten Satzes in der rechten Spalte.

Davon unabhängig bitten wir um eine Klärung mit den Datenschutzbehörden hinsichtlich der zuletzt auf der BaFin-Veranstaltung am 16.03.2017 vorgetragenen Frage, inwieweit eine Kombination der Funktion des Informationssicherheitsbeauftragten mit Datenschutzbeauftragten möglich sei. Nach Auskunft einzelner Landesdatenschutzbehörden ist dies, anders als von der BaFin vorgetragen, durchaus möglich.

Tz. 22

In den Erläuterungen sollte die Einfügung „über dem definierten Schwellenwert" gestrichen werden, da ein „Schwellenwert" nicht explizit definiert ist und auch in keinem Standard gefordert wird. Der nachfolgende Satz macht zudem hinreichend klar, dass es eine Abstufung gibt und die Abgrenzung zu definieren ist.

Tz. 23

Die nunmehr vierteljährliche Berichterstattungspflicht hat uns überrascht, da wir auf Basis der Diskussionen im Fachgremium von einer regelmäßigen Berichterstattung auf jährlicher Basis ausgegangen sind. Die MaRisk treffen selbst keine Aussage zum Turnus der Berichterstattung an die Geschäftsleitung zur Informationssicherheit. Als vergleichbare Anforderung kann jedoch der Maßstab der Berichterstattung der Compliance-Funktion, des zentralen Auslagerungsmanagements oder der Risikocontrolling-Funktion zum OpRisk-Reporting herangezogen werden, wo die MaRisk eine mindestens jährliche Berichterstattung an die Geschäftsleitung vorsehen. Ein vierteljährlicher Statusbericht erscheint folglich nicht konsistent zu den MaRisk. Wir halten eine jährliche Berichterstattungspflicht kombiniert mit einer ad-hoc-Berichterstattung (anlassbezogen gemäß "Unverzüglichkeitsregelung bei wesentlichen Informationen" in MaRisk AT 4.3.2 Tz 5) für risikoadäquat und ausreichend.

In kleinen Häusern ist der Vorstand oftmals Mitglied des Informationssicherheitsteams. Ein Protokoll der regelmäßig stattfindenden Sitzungen des Informationssicherheitsteams, in der die hier beschriebenen Punkte besprochen werden, sollte in diesem Fall ausreichend sein.

5. Benutzerberechtigungsmanagement

Zum Benutzerberichtigungsmanagement sind diverse Regelungen (wie in Tz. 24 auch referenziert) direkt in den MaRisk enthalten. Diese sind vom Institut neben den zusätzlichen Erläuterungen der BAIT heranzuziehen, bei teilweise unterschiedlichen Begriffen. Dies erschwert in der Praxis für die Institute das Verständnis und die Einhaltung der Anforderungen aus MaRisk und BAIT.

Tz. 24 und 25

Tz. 25 ist in weiten Teilen redundant zu der in Tz. 24 referenzierten Regelung in den MaRisk, jedoch wird anders als in den MaRisk die Proportionalität weniger deutlich.

Die BAIT sehen eine mindestens jährliche Überprüfung der IT-Berechtigungskonzepte vor. Nur indirekt über AT 4.3.1 Tz. 2 (Zwischenentwurf) wird klar, dass Zeichnungsberechtigungen in Verbindung mit Zahlungsverkehrskonten und wesentliche IT-Berechtigungen mindestens jährlich, alle anderen mindestens alle drei Jahre zu überprüfen sind.

Die Möglichkeit zur Zusammenfassung von Berechtigungen in einem Rollenmodell wird nur in den MaRisk AT 7.2 Tz. 2 aufgegriffen. Ein Bezug in den BAIT fehlt, hier ist stattdessen von „allen vom IT-System bereitgestellten Berechtigungen" die Rede.

Die MaRisk lassen zudem Gestaltungsfreiheit über die Formulierung „angemessene Berechtigungsvergabe". Es werden unterschiedliche Begriffe genutzt, z.B. in AT 4.3.1 Tz. 2 MaRisk „Sparsamkeitsprinzip", in den BAIT das „Prinzip der minimalen Rechtevergabe". Hinsichtlich der Textpassage "Darüber hinaus sind miteinander unvereinbare Tätigkeiten und Interessenskonflikte des Personals zu vermeiden" verweisen wir auf unsere Anmerkungen zu Tz. 6 (nur wesentliche Interessenkonflikte). Aussagen zu Funktionstrennungen sind zudem bereits in den MaRisk AT 7.2 Tz. 2 enthalten.

Wir bitten deshalb um grundlegende Überarbeitung der Tz. 25 und um Streichung redundanter, bereits in den MaRisk enthaltener Regelungen.

Im weitesten Sinne könnte die Interpretation der Begriffe „Berechtigungen" und „Zugang zum Informationsverbund" auf Zugangs-, Zugriffs-, und Zutrittsberechtigungen ausgeweitet werden, da der Informationsverbund gemäß BSI-Definition die IT-Systeme und die Räumlichkeiten inkludiert.
Die Begriffe „Berechtigungen" und „Zugang zum Informationsverbund" sollten klarer formuliert werden, um zu vermeiden, dass die Zutritte darunter interpretiert werden. Das Management von Zutritten ist die Aufgabe des Facility Managements und nicht des Benutzerberechtigungsmanagements.

Tz. 26

Wir verstehen Tz. 26 so, dass diese Anforderung für nicht personalisierte Benutzer, nicht jedoch für technische Benutzer gilt. Im Hinblick auf technische Benutzer, die zum Betrieb automatisierter Abläufe genutzt werden (beispielsweise automatisierter Start von Systemdiensten), ist eine Genehmigung nicht notwendig. Technische User werden in den Verfahrensdokumentationen beschrieben.

Auch für nicht personalisierte Benutzer sollte die Anforderung im Zusammenhang mit dem Schutzbedarf der Informationen und IT-Systeme formuliert werden. Bei niedrigem Schutzbedarf der Schutzziele Integrität, Authentizität und Vertraulichkeit ist eine Zuordnung zu einer Person nicht zwangsläufig notwendig und ein Genehmigungsprozess überflüssig.

Tz. 28

Sofern die vergebenen Berechtigungen den Aufgaben und Funktionen der jeweiligen Person entsprechen, stellt ein Entzug dieser Kompetenzen (vgl. Erläuterungsspalte) mit anschließender Wiedervergabe keinen Mehrwehrt an Sicherheit dar und kann massive Störungen des Betriebsablaufs verursachen. Vielmehr sind in diesem Fall die IT-Berechtigungsanträge nachträglich zu genehmigen und zu kontrollieren. Genehmigungs- und Kontrollinstanzen können sich im Laufe der Zeit zudem ändern, so dass in der linken Spalte das Wort „grundsätzlich" vor dieselben Genehmigungs- und Kontrollinstanzen eingefügt werden sollte. In der Erläuterungsspalte sollte das letzte Wort „entzogen" durch „behandelt" ersetzt werden.

Tz. 30 und 31

Grundsätzlich halten wir eine am Schutzbedarf ausgerichtete Protokollierung für sachgerecht. Die Anforderung, Prozesse zur Protokollierung einzurichten, die eine Überprüfung von IT-Berechtigungen hinsichtlich des „vorgesehenem Einsatzes" sicherstellen, ist in der Praxis nicht umsetzbar. Eine Protokollierung kann lediglich einen ggf. möglichen Missbrauch dokumentieren. Ebenso können begleitende technisch-organisatorische Maßnahmen lediglich vorbeugen, dass die Vorgaben der IT-Berechtigungskonzepte nicht umgangen werden können.

Formulierungsvorschlag zur Tz. 30 linke Spalte:
„Das Institut hat nach Maßgabe des Schutzbedarfs und der Soll-Anforderungen Prozesse zur Protokollierung einzurichten. ~~die sicherstellen, dass die IT-Berechtigungen nur wie vorgesehen eingesetzt werden.~~

Formulierungsvorschlag zur Tz. 31 linke Spalte:
Durch begleitende technisch-organisatorische Maßnahmen ist einer Umgehung ~~der sicherzustellen, dass die~~ der Vorgaben der IT-Berechtigungskonzepte vorzubeugen ~~nicht umgangen werden können~~.

6. IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen)

Klarstellend weisen wir darauf hin, dass die dargestellten Anforderungen nur für die intern in den Instituten durchgeführten IT-Projekte bzw. IT-Anwendungsentwicklungen gelten können. Bei verbund- und gruppenangehörigen Instituten mit einem gleichgerichteten Geschäftsmodell und gemeinsamen IT-Dienstleistern erfolgt die Aufstellung von Anforderungen für die Anwendungsentwicklung überwiegend gemeinsam auf zentraler Ebene und die Erfüllung dieser Anforderungen wird in wesentlichen Teilen durch die IT-Dienstleister sichergestellt. Für IT-Projekte in den Verbünden oder Gruppen werden institutsübergreifende Projektmanagementprozesse eingerichtet. Die zentral erstellten Dokumentationen sollten daher von diesen Instituten herangezogen werden können

Tz. 32

Zutreffend wird auf AT 7.2 Tz. 5 MaRisk (Zwischenentwurf) referenziert. Dort wird für die von den Fachbereichen selbst entwickelten Anwendungen auf die Beachtung der Anforderungen des AT 7.2 entsprechend der Kritikalität der unterstützten Geschäftsprozesse und der Bedeutung der Anwendungen für diese Prozesse verwiesen, die Festlegung von Maßnahmen zur Sicherstellung der Datensicherheit solle sich am Schutzbedarf der verarbeiteten Daten orientieren. Dieses proportionale Vorgehen sollte auch in den BAIT deutlich werden.

Der Verweis auf AT 4.3.2 Tz. 4 im Zusammenhang mit der Auswirkungsanalyse ist u.E. nicht konsistent und sollte gestrichen werden.

Tz. 33

Wir bitten um eine Konkretisierung des Begriffes „IT-Projekte". Es sollte klargestellt werden, ob darunter eigenständige Projekte, die nur auf IT-Anwendungsentwicklungen abzielen verstanden werden oder auch andere (bankfachliche) Projekte, die Anpassungen in der IT oder Einführungen von Software zur Folge haben, dazu zählen. Weiterhin wäre davon das Releasemanagement ausgelagerter Anwendungen abzugrenzen.

Tz. 34 ff.

Über die Beispiele in den Erläuterungen wird suggeriert, dass klassische IT-/Softwareentwicklungsprojekte grundsätzlich die von der BaFin bevorzugten Methoden sind. Wir befürworten Methodenfreiheit, bspw. für agile Software- und Prozessentwicklungen. Die in den Erläuterungsspalten als beispielsweise dargestellten Anforderungen sollten folglich um solche illustrative Beispiele agiler Methoden ergänzt werden.

Tz. 37

Es fehlt eine Definition des Begriffs Anwendungsentwicklung in den Erläuterungen zu Tz. 37. In diesem Zusammenhang erachten wir eine Differenzierung zwischen Anwendung und Arbeitshilfe für sinnvoll. Arbeitshilfen könnten bspw. definiert werden als Dateien mit einer unkritischen fachlichen und technischen Komplexität, für die keine formalen Anforderungen an die Anwendungsentwicklung zum Tragen kommen und deren Ergebnislieferung inhaltlich direkt nachvollziehbar ist und - soweit erforderlich - unter Berücksichtigung der bankinternen Richtlinien im Vier-Augen-Prinzip kontrolliert wird.

Es sollte in der linken Spalte hinsichtlich der Anforderungen an die Prozesse der Anwendungsentwicklung differenziert werden nach Art/ Einsatzzweck, Umfang, Komplexität und Risikogehalt der Anwendung. Das gilt insbesondere auch, da sich aus der Erläuterung zu Tz. 37 eine grundsätzliche Einordnung aller in den Fachbereichen selbst entwickelten Anwendungen als Anwendungsentwicklung ergibt, die eine

vollumfängliche Umsetzung der in den folgenden Textziffern genannten Anforderungen zur Folge hätte (vgl. Anmerkung zu Tz. 46).

Die Vorgaben zur Anwendungsentwicklung sollten sich vor allem am Schutzbedarf ausrichten. Bei IDV-Anwendungen sollten die Anforderungen der BAIT nur bei hohem Schutzbedarf zum Tragen kommen.

Tz. 38

Eine Erhebung und Bewertung von Anforderungen sollte sich auf wesentliche Anforderungen beschränken, eine vollständige Dokumentation ist nicht sinnvoll leistbar. Die Tz. sollte Öffnungsklauseln vorsehen, um agile Entwicklungsmethoden ebenso zu berücksichtigen wie klassische Entwicklungsmethoden. Es gibt auch nicht-funktionale Anforderungen, die durch den IT-Bereich zu beschreiben sind (z.B. Anforderungen des IT-Betriebs, der Wartbarkeit, der Standardisierung in der IT).

Formulierungsvorschlag zur linken Spalte:
„Wesentliche Anforderungen an die Funktionalität der Anwendung sind im Rahmen der Anwendungsentwicklung zu erheben und zu bewerten. ~~müssen ebenso erhoben, bewertet und dokumentiert werden wie nichtfunktionale Anforderungen.~~ Dabei sollten auch nichtfunktionale Anforderungen berücksichtigt werden. ~~Die Verantwortung für die vollständige Erhebung und Bewertung der Anforderungen liegt in den Fachbereichen.~~ Die Erhebung und Bewertung der nichtfunktionalen Anforderungen erfolgt gemeinsam durch IT- und Fachbereiche. Die Verantwortung für die abschließende Beurteilung liegt beim Fachbereich."

Tz. 39

In der Tz. sind drei der vier Schutzziele nach MaRisk aufgeführt. Aus welchem Grund ist hier das Schutzziel Authentizität gemäß MaRisk nicht aufgeführt?

Tz. 40

Wir bitten um Klarstellung, dass die aufgeführten Inhalte (Anwenderdokumentation, technische Systemdokumentation, Betriebsdokumentation) nicht unbedingt in drei getrennten Dokumenten vorliegen müssen.

Tz. 41

Die Formulierung ist widersprüchlich: Es "müssen" Vorkehrungen getroffen werden, aber deren Ziel wird nur "beispielsweise" angegeben.

Formulierungsvorschlag zur linken Spalte
„Im Rahmen der Anwendungsentwicklung ~~müssen~~ sollten Vorkehrungen getroffen werden, die Hinweise darauf geben ~~beispielsweise erkennen lassen~~, ob eine Anwendung versehentlich geändert oder absichtlich manipuliert wurde."

Tz. 42

Eine Konkretisierung der zu „versionierenden Dokumente / Ergebnistypen" ist notwendig. Sind unter „Dokumente / Ergebnistypen" die unter Tz. 34 benannten Ergebnistypen aus den Qualitätskriterien der Vorgehensmodelle gemeint, oder sind hier alle Dokumente gemeint, die im Rahmen einer Entwicklung entstehen können (z.B. Fachkonzepte, Programmcode, Protokolle, UseCases, Abstimmnotizen mit Fachbereich)?. Eine Konkretisierung der Auslegung „während und nach der Anwendungsentwicklung" ist notwendig. Eine Abgrenzung zu „nach der Produktivsetzung" muss klarer herausgestellt werden. Die

geforderte Versionierung kann sich nur auf die bereits produktivgenommenen Entwicklungen (Versionierung des entwickelten Programmes) beziehen. Das heißt, eine angemessene Versionierung ist zur jeder Produktivsetzung und jeder Veränderung der produktivgenommenen Entwicklung gefordert.

Formulierungsvorschlag zur linken Spalte
~~Es ist e~~Eine angemessene Versionierung ist zu jeder Produktivsetzung und jeder Veränderung der produktivgenommenen Entwicklung gefordert ~~während und nach der Anwendungsentwicklung sicherzustellen~~. ~~Auch die im Verlauf der Anwendungsentwicklung erstellten Dokumente /Ergebnistypen sind zu versionieren~~ Das Institut hat je nach Vorgehensmodell die geeigneten Ergebnistypen zu definieren und diese angemessen zu versionieren.

Tz. 43

Bei den Anforderungen an die Testverfahren ist die Proportionalität abhängig von Art/ Einsatzzweck, Komplexität und vom Schutzbedarf der Anwendung zu differenzieren. Insbesondere trifft dies auf Anwendungen zu, die auf Verbund- oder Gruppenebene von zentralen IT-Dienstleistern entwickelt wurden, für die die einzelnen Institute vereinfachte Tests sowie Programm- und Einsatzfreigabeverfahren durchführen können.

Ein Test der Systemleistung unter verschiedenen Stressbelastungsszenarien ist nicht bei jeder Anwendung (einschl. IDV) notwendig.

Tz. 44

Diese Anforderung stellt aus unserer Sicht eine Doppelung zu Tz. 52 (IT-Betrieb) dar.

Wir bitten um Klarstellung, ob mit Abweichungen vom Regelbetrieb hier ebenfalls Störungen gemeint sind und um eine Definition des Begriffs Regelbetrieb.

Tz. 45

Das angemessene Verfahren ist das im Modul 3 Tz. 11 und 12 dargestellte institutsspezifische Verfahren zur Schutzbedarfsermittlung. Die hier verwendete Formulierung kann fälschlicherweise so gedeutet werden, als wenn ein zusätzliches Verfahren/Konzept entwickelt werden muss. Die Anforderungen für die von den Endbenutzern entwickelten Anwendungen sollten sich an der Kritikalität der unterstützten Geschäftsprozesse orientieren (vgl. MaRisk-Zwischenentwurf, AT 7.2 Tz. 5) und nicht pauschal in der Erläuterung gefordert werden, dass jeder Anwendung ein Schutzbedarf zuzuordnen ist.

Zur Bestimmung von IDV-Anwendungen wäre es hilfreich, wenn klargestellt werden würde, wann Excel-Spreadsheets o.ä. Anwendungen zur einmaligen und gelegentlichen Nutzung, unter die Anforderungen der Tz. 45 und 46 fallen.

Tz. 46

Wir schlagen vor, in Tz. 46 eine Öffnungsklausel aufzunehmen, um einen angemessenen Umgang mit einfachen IDV-Anwendungen zu ermöglichen. Die Tz. nennt nicht nur vom Fachbereich entwickelte, sondern auch betriebene Anwendungen (auch wenn sie fremdentwickelt sind). Die Anforderungen im Modul 6 richten sich jedoch an die Anwendungsentwicklung und nicht den IT-Betrieb.

Formulierungsvorschlag zur linken Spalte:

„Für die von Endbenutzern in den Fachbereichen entwickelten Anwendungen sind abgestufte Regelungen in Abhängigkeit von der Kritikalität der unterstützten Geschäftsprozesse und der Bedeutung der Anwendungen für diese Prozesse sowie vom Schutzbedarf der verarbeitenden Daten zu treffen, die die in Tz. 38 bis 44 genannten Prinzipien grundsätzlich berücksichtigen. Die Vorgaben zur Identifizierung aller von Endbenutzern des Fachbereichs entwickelten ~~oder betriebenen~~ Anwendungen, zur Dokumentation, zu den Programmierrichtlinien und zur Methodik des Testens, zur Schutzbedarfsfeststellung und zum Rezertifizierungsprozess der Berechtigungen sind innerhalb einer Arbeitsanweisung (z.B. IDV-Richtlinie) zu regeln."

Es sollte klargestellt werden, dass ein zentrales Register nur für IDV-Anwendungen mit hohem Schutzbedarf erforderlich ist. Dies könnte dadurch umgesetzt werden, dass die Fachbereiche verpflichtet sind, diese Applikationen zentral zu registrieren. Für alle anderen zu betrachtenden IDV-Anwendungen sollte eine dezentrale Ablage mit den in der Erläuterung genannten Angaben ausreichen.

7. IT-Betrieb (inkl. Datensicherung)

Im Hinblick auf Institute mit ausgelagertem IT-Betrieb erfolgt die Erfüllung der Anforderungen an den IT-Betrieb überwiegend durch die IT-Dienstleister auf Basis von Verträgen und zugehörigen SLA. Insbesondere bei verbund-/ gruppenangehörigen Instituten mit einem gleichgerichteten Geschäftsmodell und gemeinsamen IT-Dienstleistern wird die Erfüllung dieser Anforderungen in wesentlichen Teilen durch die IT-Dienstleister zentral sichergestellt.

Tz. 48

Wir bitten um Klarstellung, dass Bestandsangaben auch in mehreren Tools verwaltet werden können und nicht ein zentrales Inventartool notwendig ist, was eine redundante Pflege erforderlich machen würde.

Tz. 50

Die Formulierung in den Erläuterungen „Umzug des Standorts der IT-Systeme" ist missverständlich und sollte geändert werden in „Umzug der IT-Systeme zu einem anderen Standort".

Tz. 51

Der Umgang mit Änderungen sollte sich am Schutzbedarf der Anwendung orientieren.

Tz. 53

Eine mindestens jährliche Überprüfungsperiode für die regelmäßige (nicht anlassbezogene) Prüfung der Lesbarkeit von Datensicherungen halten wir unter Risikogesichtspunkten für überzogen.
Es sollte zwischen den Verfahren im Eigenbetrieb und im Verbund bei zentralen IT-Dienstleistern unterschieden werden. Wiederherstellungstests für Daten bei zentralen IT-Dienstleistern erfolgen institutsübergreifend.

8. Auslagerungen und sonstiger Fremdbezug von IT-DL

Die Konsultationsfassung formuliert nach wie vor Anforderungen an den sonstigen Fremdbezug von IT-Dienstleistungen, ohne das Proportionalitätsprinzip ausreichend zu berücksichtigen. Im Unterschied zu Auslagerungen werden die Anforderungen an jeglichen sonstigen Fremdbezug von IT-Dienstleistungen gestellt, unabhängig davon, welchen Umfang dieser besitzt und welchem Einsatzzweck in der Bank dieser zugrunde liegt.

Die MaRisk AT 9 Tz. 1 (Erläuterung gemäß Zwischenentwurf) führen aus, dass die Anwendung der einschlägigen Regelungen zu § 25b KWG für den sonstigen Fremdbezug von Leistungen angesichts der mit solchen Konstellationen einhergehenden Risiken regelmäßig nicht angemessen sind, jedoch die allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 25a Abs. 1 KWG zu beachten sind.

Die Anforderungen zum Management des „sonstigen IT-Fremdbezugs" sind dies bezüglich zu weitreichend und nicht risikogerecht. Wir schlagen deshalb für das gesamte Modul eine Begrenzung auf solche IT-Dienstleistungen vor, die für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung sind (vgl. auch Tz. 54).

Tz. 54

Eine Klarstellung des Begriffs "sonstiger Fremdbezug von IT-Dienstleistungen" ist für die Umsetzung in der Praxis erforderlich. Ausgenommen vom sonstigen Fremdbezug von IT-Dienstleistungen sollten sein:

- IT-Dienstleistungen, die die Bank aufgrund tatsächlicher Gegebenheiten (WAN-Leitungen, Wartung von Standard-Software, etc.) oder rechtlicher Vorgaben (Clearing-Plattformen) nicht selbst erbringen kann
- IT-Dienstleistungen, die von Unternehmen erbracht werden, die von der Bankenaufsicht überwacht sind,
- IT-Dienstleistungen ohne bankgeschäftlichen Bezug (Bestell- /Schulungsplattformen, etc.)

Es wird in der Tz. zwischen der Auslagerung und dem sonstigen Fremdbezug von IT-Dienstleistungen unterschieden und zusätzlich auf die Regelung zum Bezug von Software in den MaRisk AT 7.2 Tz. 4 verwiesen. Auch in den MaRisk AT 9 Tz. 1 Erläuterungen wird eine Aussage zum isolierten Bezug von Software getroffen („die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt wird oder für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung ist"). Diese sei in der Regel als Fremdbezug (ohne den Zusatz „von IT-Dienstleistungen") einzustufen.

Wir bitten um klarere Abgrenzung der Begriffe sowie eindeutige Zuordnung der Anforderungen aus den MaRisk und den BAIT für die „Auslagerung von IT-Dienstleistungen", den „sonstigen Fremdbezug von IT-Dienstleistungen" und den „Bezug von Software", um Fehlinterpretationen der Banken und Prüfer zu vermeiden. In diesem Zusammenhang sollte klarer herausgestellt werden, dass der Bezug einer Software (mit oder ohne Wartungsvertrag) nicht unter dem Begriff „IT-Dienstleistung" subsumiert wird. Der ausschließliche Bezug von Standardsoftware (einschließlich der für die Lizenznehmer üblichen Standardwartungen und -weiterentwicklungen) stellt keinen Fremdbezug von IT-Dienstleistungen dar, soweit die Software auf den Systemen des Instituts betrieben wird.

Um Missverständnisse zu vermeiden, sollte der zweite Satz wie folgt ergänzt werden: "Dies gilt ~~insbesondere~~ auch für Auslagerungen …".

Tz. 55

Die Vorgabe, dass Verträge betreffend den sonstigen Fremdbezug von IT-Dienstleistungen strategisch analog zu den Auslagerungsverträgen bzgl. IT-Dienstleistungen zu steuern sind, sehen wir als zu weitgehend an. Eine analoge Steuerung ist unter Berücksichtigung des Proportionalitätsprinzips nicht angemessen.

Formulierungsvorschlag zur linken Spalte:

„Die Verträge betreffend den sonstigen Fremdbezug von IT-Dienstleistungen sind strategisch ~~analog den Auslagerungsverträgen bzgl. IT-Dienstleistungen~~ angemessen zu steuern."

Die Aussage in den Erläuterungen „Vertragsevidenz im Einklang mit den Vorgaben der IT-Strategie des Instituts" ist unverständlich. Wir bitten um klare Formulierung des Gewollten.

Tz. 56

Wir bitten die Erwartungshaltung der Aufsicht an eine Risikobewertung - auch in Abgrenzung zu der in AT 9 MaRisk geforderten Risikoanalyse - zu erläutern. Eine Risikobewertung für jeglichen sonstigen Fremdbezug unabhängig davon, für welche Aufgaben in der Bank dieser bezogen wird, halten wir für zu weitreichend. Bei mehreren gleichartigen Fremdbezügen (z.B. IT-Beratereinsatz) sollte nicht jedes Mal eine neue Risikobewertung inklusive Einbindung der Sonderfunktionen notwendig sein.

In Tz. 56 ist zudem unklar, welche Aussage das Wort "auch" hat.

Formulierungsvorschlag zur linken Spalte:
„Für den sonstigen Fremdbezug von IT-Dienstleistungen, der für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung ist, ~~Wegen der grundlegenden Bedeutung der IT für das Institut ist auch für jeden sonstigen Fremdbezug von IT-Dienstleistungen~~ ist vorab eine Risikobewertung durchzuführen. Für gleichartige Formen von Fremdbezug kann auf bestehende Risikobewertungen zurückgegriffen werden."

Daneben sollte klargestellt werden, dass es sich hierbei nur um feste Dienstleistungs-/Wartungsverträge handeln kann, nicht um Einzelbeauftragungen.

Tz. 57

Wir gehen davon aus, dass hierunter nicht Standardverträge zum Bezug von Software und Hardware fallen (vgl. Tz. 54). Banken sind auf Software und Hardware von Quasi-Monopolisten wie Microsoft, SAP, Oracle u.ä. angewiesen, denen keine Vertragsbedingungen diktiert werden können, obwohl sie nicht risikofrei sind. Die Alternative wäre jedoch eine viel risikoreichere Eigenentwicklung oder das Ausweichen auf abhängige Kleinunternehmen.

Nur wenn sich aus der Risikobewertung tatsächlich Maßnahmen ableiten, ist zudem eine Berücksichtigung in der Vertragsgestaltung notwendig. Die Verwendung des Begriffs „Restrisiken" ist zudem missverständlich (siehe unsere Anmerkungen zu den Tzn. 14 und 15).

Formulierungsvorschlag zur linken Spalte:
„Die ggf. aus der Risikobewertung zum sonstigen Fremdbezug von IT-Dienstleistungen abgeleiteten Maßnahmen sind angemessen in der Vertragsgestaltung (sofern darstellbar) zu berücksichtigen. ~~Vom Institut akzeptierte und genehmigte Restrisiken werden überwacht und~~Die Ergebnisse der Risikobewertung fließen, sofern relevant, in den Prozess des Managements der operationellen Risiken ein ~~überführt~~."

In den MaRisk wird eine Einbindung von Dienstleistungen ins Notfallmanagement lediglich bei zeitkritischen Auslagerungen gefordert (AT 7.3 Tz 1). Dieser Passus sollte in den Erläuterungen ergänzt werden.

Formulierungsvorschlag zur rechten Spalte:
„Dies beinhaltet beispielsweise Vereinbarungen zum Informationsrisikomanagement, zum

Informationssicherheitsmanagement und bei zeitkritischen Aktivitäten und Prozessen zum Notfallmanagement, ~~die im Regelfall den Zielvorgaben des Instituts entsprechen~~. ..."

Tz. 58

Eine Risikobewertung sollte nur anlassbezogen, z.B. bei Vertragsverlängerung oder bei gesetzlichen Änderungen wiederholt werden müssen, nicht regelmäßig.

Formulierungsvorschlag zur linken Spalte:
„Die Risikobewertungen in Bezug auf den sonstigen Fremdbezug von IT-Dienstleistungen sind ~~regelmäßig und~~ anlassbezogen zu überprüfen und ggf. ~~inkl. der Vertragsinhalte und~~ anzupassen."