Per E-Mail
Konsultation-02-17@bafin.de; b32_marisk@bundesbank.de

Bundesanstalt für Finanzdienstleistungsaufsicht

Graurheindorfer Straße 108
53117 Bonn

Deutsche Bundesbank

Wilhelm-Epstein-Straße 14
60431 Frankfurt am Main

Deutsche Börse AG

Financial Accounting & Controling

Mergenthalerallee 61
65760 Eschborn

Postanschrift
60485 Frankfurt am Main

Telefon
+49 (0) 69-2 11-17178

Fax
+49 (0) 69-2 11-13561

Internet
Deutsche-Boerse.com

E-Mail
Marija.Kozica@
Deutsche-Boerse.com

05. Mai 2017

Konsultation 02/2017 – Entwurf der „Bankaufsichtliche Anforderungen an die IT (BAIT)“

Geschäftszeichen BA 51-K 3142-2017/0004

Sehr geehrter Herr Röseler,

sehr geehrte Damen und Herren,

am 22. März 2017 haben Sie den Entwurf eines Rundschreibens zu „Bankaufsichtliche Anforderungen an die IT“ (BAIT) zur Konsultation veröffentlicht, durch welche die MaRisk IT-spezifisch konkretisiert werden sollen.

Die Entwicklungen der Informationstechnologie in den vergangenen Jahren verlangen eine angemessene Abbildung in den aufsichtsrechtlichen Regelwerken. Die MaRisk bilden dafür grundsätzlich bereits heute eine geeignete Grundlage. Deren letzte Revision fand 2016/2017 statt und steht kurz vor der Veröffentlichung. Sofern weitere Konkretisierungen zu IT-spezifischen Themen notwendig sind, sollten diese an einer zentralen Stelle des aufsichtsrechtlichen Regelwerks verankert werden.

Wir bedanken uns für die Möglichkeit bestehenden Klärungsbedarf und Anmerkungen zu einzelnen Sachverhalten im Rahmen dieser Konsultation anbringen zu können.

Wir erkennen grundsätzlich die Bemühungen der deutschen Aufsicht an, mit den MaRisk und den BAIT IT-spezifische Fragestellungen angemessen aufzugreifen und den Instituten und deren Geschäftsleitern hierzu Vorgaben und Richtlinien zu geben. Uns erscheint jedoch die Erstellung eines eigenständigen Dokumentes für

einzelne Aspekte der IT subsidiär zu den MaRisk suboptimal. Mit dem Abwicklungsmechanismusgesetz (AbwMechG) wurde im KWG eine Rechtsverordnungsermächtigung eingefügt, die der für notwendig erachteten Rechtssicherheit der bisher in den MaRisk geregelten Sachverhalte dienen soll. Wir verweisen dazu auf unsere Stellungnahme vom 26. April 2016 zur Konsultation 02/2016. Unabhängig von der rechtlichen Ausgestaltung als BaFin-Rundschreiben oder als Rechtsverordnung, sollten jedoch die IT-spezifischen Themen mit den bisherigen Regelungen der MaRisk an einer Stelle zusammengefasst sein. Sofern die MaRisk auch weiterhin als Rundschreiben Bestand haben, könnten die IT-spezifischen Vorgaben inhaltlich z.B. als BT 3 „Besondere Anforderung an die Ausgestaltung der Informationstechnologie“ der MaRisk hinzugefügt werden. Bereits in dem Anschreiben zur Veröffentlichung der MaRisk in ihrer Fassung vom 20.12.2005[1] wird explizit darauf verwiesen, dass der modulare Aufbau der MaRisk die notwendige Flexibilität bietet, um einem zusätzlichen Regelungsbedarf durch Anpassungen oder Ergänzungen des Gesamtwerks entsprechend nachzukommen. Der modulare Aufbau wurde dabei bisher wiederholt im Rahmen der Neugestaltung der MaRisk genutzt, um die Vorgaben der §§ 25a und 25b KWG unter Berücksichtigung des zusätzlichen Regelungsbedarfs auszubauen und weiter zu spezifizieren. Dies sollte auch zur Umsetzung der IT-Spezifika genutzt werden. Der vorgelegte Entwurf der BAIT müsste dann der veränderten Struktur angepasst werden und die MaRisk müssten ebenfalls hinsichtlich möglicher Verweise auf die IT-spezifischen Vorschriften überarbeitet werden.

Gemäß des uns vorliegenden Entwurfs zu den MaRisk von Juni 2016 zu AT 7.2 Tz. 4 sind Vorgaben zum IT-Risikomanagement festgeschrieben, welche in II. Tz. 54 Satz 3 und Tz. 56 ff. BAIT aufgegriffen werden. Insbesondere II. Tz. 54 Satz 3 BAIT führt dabei jedoch zu Missverständnissen, da die Formulierung aus dem Kontext von MaRisk AT 7.2 Tz. 4 Satz 2 herausgenommen und ausschließlich in den Kontext von Auslagerungen und sonstigem Fremdbezug von IT-Dienstleistungen gestellt wird. Es entsteht somit der Eindruck, dass (i) – abweichend von MaRisk AT 9 – der Bezug von Software (sprachlich) immer als sonstiger Fremdbezug von IT-Dienstleistungen einzustufen ist und (ii) die Risikobewertung nur bei Softwarebezug durchzuführen ist. Auch sind die Anforderung nach einer Risikobewertung mit inhaltlicher Eingrenzung auf den sonstigen Fremdbezug von IT-Dienstleistungen über II. Tz. 56 und 57 BAIT aus unserer Sicht redundant zu AT 7.2 Tz. 4 MaRisk. Da anzunehmen ist, dass mit II. Tz. 54 Satz 3 BAIT weder eine Einschränkung des AT 9 noch des AT 7.2 MaRisk vorgenommen werden soll, schlagen wir die Streichung von II. Tz. 54 Satz 3 sowie eine Ergänzung des AT 7.2 Tz. 4 MaRisk vor:

[1] http://www.bundesbank.de/Redaktion/DE/Standardartikel/Aufgaben/Bankenaufsicht/risikomanagement_marisk_2005_anschreiben.html

„*Beim Bezug von Software sind die damit verbundenen Risiken, insbesondere auch im Falle einer Auslagerung oder sonstigem Fremdbezug von Software, angemessen zu bewerten*."

Die an obigem Bespiel dargestellte Verzahnung der beiden Dokumente zeigt Redundanzen und Fehlinterpretationsmöglichkeiten, die mit der Integration der BAIT in die MaRisk in einem einzigen Dokument vermieden werden sollten.

Ungeachtet dessen begrüßen wir den modularen Ansatz sowie die prinzipienorientierte Ausgestaltung der BAIT und die Fortführung des Proportionalitätsprinzips.

Nachfolgend übermitteln wir Ihnen unsere Anmerkungen im Detail.

.

1. IT-Strategie

II. Tz. 2 BAIT gibt einen Überblick über die Mindestinhalte der IT-Strategie und spezifiziert diese im Rahmen der entsprechenden Erläuterung dazu weiter. Wir begrüßen die mit der Spezifizierung der Vorgaben einhergehende größere Transparenz hinsichtlich der bestehenden Erwartungshaltung der Aufsicht an die Ausgestaltung der IT-Strategie von Instituten sowie hinsichtlich der gängigen Aufsichtspraxis. Zur Vermeidung möglicher Redundanzen und Inkonsistenzen sollte klargestellt werden, dass die IT-Strategie nicht zwingend in einem einzigen Dokument abgebildet werden muss. Vielmehr soll es möglich sein, über Verweise auf separate Dokumente in der IT-Strategie den Anforderungen an die Mindestinhalte dieser angemessen nachzukommen.

II Tz. 1 BAIT enthält bisher keine Angaben über die Form der Dokumentation der IT-Strategie. Unter Beibehaltung des Proportionalitätsprinzips befürworten wir dazu die Aufnahme einer eigenständigen Textziffer, welche die Möglichkeit einer modularen Struktur der IT-Strategie unter Nutzung weiterer Dokumenten, die ggf. detailliertere Angaben enthalten, sinngemäß wie folgt einräumt:

„Tz. 2a: Die IT-Strategie kann in einem umfassenden Dokument verankert werden oder unter Nutzung weiterer Dokumente, auf die verwiesen wird, erstellt werden. Sofern auf weitere Dokumente verwiesen wird, sind die in Tz. 2 genannten Elemente im zentralen IT-Strategiedokument zumindest überblickartig darzustellen. Statt separater Detaildokumente können detaillierte Darstellungen auch als Anhang des zentralen Dokuments ausgestaltete werden. Die Detailtiefe der IT-Strategie hat sich unter Berücksichtigung des Proportionalitätsprinzips an den Geschäftstätigkeiten des Instituts zu orientieren.“

Inhaltlich erachten wir die Zuordnung der gängigen Standards an denen sich das Institut orientiert, auf die Bereiche der IT, wie von II Tz. 2 lit. b) BAIT gefordert sowohl für praktisch schwierig umsetzbar, als auch für ungeeignet für eine Strategie. Stattdessen sollte lediglich die Nennung der wesentlichen IT-Standards in der Strategie erfolgen und deren Nutzung erläutert werden. Von daher bitten wir die Formulierung des lit. b) wie folgt zu erwägen:

„b) Nennung der gängigen IT-Standards, an denen sich das Institut orientiert, und Erläuterung zu deren Anwendung.“

Auch die Erläuterung zu lit. b) scheint uns zu weitegehende Anforderungen zu stellen. Die Darstellung sollte sich auf die wesentlichen Standards beschränken und die beabsichtigte Umsetzung darstellen. Eine Ermittlung eines „Erfüllungsgrades“ erscheint uns in diesem Zusammenhang nicht zielführend. Wir schlagen daher vor, die Erläuterung wie folgt zu formulieren:

„Zu b): Nennung der vom Institut angewandten wesentlichen IT-Standards und Darstellung der Anwendung der Kernelemente dieser IT-Standards im Institut.“

2. IT-Governance

Die Erläuterung zu II. Tz. 5 BAIT verwendet den Begriff einer „sich verändernde Bedrohungslage“. Es ist unklar, welche Bedrohungslage in diesem Kontext gemeint ist und zudem kann auch nur die vom Institut festgestellte Bedrohungslage in der IT-Governance berücksichtigt werden. Eine absolute Bedrohungslage ist insofern nicht abbildbar. Wir schlagen daher vor, die Erläuterung wie folgt zu modifizieren. Zudem sollte der Text sprachlich auf den Text der eigentlichen Textziffer angepasst werden:

„Hinsichtlich der angemessenen Personalausstattung, sollen insbesondere der Stand der Technik sowie von Institut vermutete aktuelle und künftige Bedrohungen für die Informationssicherheit und den IT-Betrieb berücksichtigt werden.“

Die Erläuterung zu II. Tz. 7 BAIT unterstellt sprachlich, dass das genannte Beispiel zwingend zur Anwendung kommt. Das erscheint uns nichtzutreffend. Wir bitten daher das Beispiel auch als solches z.B. wie nachfolgend beschrieben zu formulieren:

„Bei der Festlegung der Kriterien können z.B. die Qualität der Leistungserbringungen, die Verfügbarkeit, Wartbarkeit, Anpassbarkeit an neue Anforderungen, Sicherheit der IT-Systeme oder der dazugehörigen IT-Prozesse sowie deren Kosten berücksichtigt werden.“

3. Informationsrisikomanagement

Die Erläuterungen zu II. Tz. 10 BAIT erscheinen uns sehr vage. Zudem erschließt sich uns die Nennung der „räumlichen Gegebenheiten“ nicht. Ohne eine angemessene Erläuterung dürfte die Einhaltung der Anforderung aus II. Tz. 10 BAIT nur schwer umsetzbar sein und zu Auslegungs- und Interpretationsunterschieden zwischen Instituten und der Aufsicht führen. Wir bitten daher, entweder um eine angemessene Erläuterung oder eine Streichung der Anforderung. In der aktuellen Fassung trägt II. Tz. 10 BAIT nicht zu einer ausreichenden Umsetzbarkeit der Anforderungen und einer gewünschten Klarstellung des Sachverhaltes bei.

4. Informationssicherheitsmanagement

4.1. Bildung eines CERT

Zur Sicherstellung eines umfassenden Managements aller Informationssicherheits-Vorfälle erscheint uns die Bildung einer zentralen Stelle sinnvoll, die von allen Mitarbeitern und Dienstleistern umgehend zu informieren ist, die eine Analyse der Vorfälle durchführt, Maßnahmen anstößt und den Informationsprozess an die zuständigen Stellen im Institute sowie ggf. gegenüber externen Stellen und Aufsichtsbehörden koordiniert. Eine solche Stelle wird in Fachkreisen CERT (Computer Emergency Response Team genannt.

Wir erachten es für sinnvoll, unter Beachtung des Proportionalitätsprinzips, die Einrichtung eines solchen Teams vorzuschreiben. Bei kleinere Instituten kann dies ggf. mit der Funktion des Informationssicherheitsbeauftragen verschmolzen werden. Die Funktion des CERT sollte auslagerbar sein und innerhalb einer Gruppe oder sogar eines Konzerns auch zentral betrieben werden dürfen. Als einen Kernbaustein schlagen wir die Einfügung einer Textziffer 18a in BAIT Abschnitt II wie folgt vor:

„18a Unter Berücksichtigung von Größe und Komplexität der Geschäftsaktivitäten eines Instituts, ist zur Sicherstellung einer zentralen Sammlung und Koordinierung IT-sicherheitsrelevanter Vorfälle ein Computer Emergency Response Team (CERT) zu etablieren."

4.2 Aufgaben des CERT

Die Aufgaben des CERT sollten in der BAIT (bzw. MaRisk) grob beschrieben werden. Das CERT sollte eine zentrale Sammlung, Sicherung und Bewertung der eingegangenen Vorfälle nachkommen sowie daran anschließend, alle als sicherheitsrelevante Sachverhalte bewertete Vorfälle, sofern materiell, an den Informationssicherheitsbeauftragten melden. Wir schlagen die ein sinngemäße Ergänzung einer weiteren Textziffer wie folgt vor:

„18b Das CERT dient als zentrale Sammelstellung für alle Informationssicherheits-Vorfälle, bewertet diese, leitet Gegenmaßnahmen zur Wahrung oder Wiederherstellung der Informationssicherheit ein und sorgt für die zielgerichtete Information der zuständigen Stellen im Institut, der Geschäftsleitung sowie, sofern erforderlich, externer Stellen und / oder Aufsichtsbehörden."

In den Erläuterungen zu II. Tz. 18b BAIT sollte festgehalten werden, dass die Beschäftigten des Institutes sowie dessen IT-Dienstleister verpflichtet sind, das CERT unverzüglich und umfassend über IT-sicherheitsrelevante Vorfälle, die das Institut betreffen, zu unterrichten haben.

4.3 Aufgaben des Informationssicherheitsbeauftragten

II. Tz. 19 BAIT verlangt die Errichtung der Funktion eines Informationssicherheitsbeauftragten, welcher nach II. Tz. 19 Satz 3 BAIT u.a. die Überprüfung und Überwachung der Einhaltung der in der IT-Strategie, der Informationssicherheitsrichtlinie und den Informationssicherheitskonzepten aufgeführten Ziele und Maßnahmen sicherzustellen hat.

Die IT-Strategie geht weit über die Belange der Informationssicherheit hinaus. Es

kann daher nach unserer Auffassung nicht Aufgabe des Informationssicherheitsbeauftragten sein, die Einhaltung der in der IT-Strategie aufgeführten Ziele und Maßnahmen allumfassend sicherzustellen. II. Tz. 19 Satz 3 BAIT muss daher auf die Belange der Informationssicherheit (*„…des Instituts niedergelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl …*“) eingeschränkt werden.

Darüber hinaus ist entsprechend der vorgeschlagenen Ergänzungen hinsichtlich der Bildung eines CERT, der fünfte Gliederungspunkt der Erläuterung zu II. Tz. 20 BAIT (Unterrichtung des Informationssicherheitsbeauftragten) zu modifizieren. Die unmittelbare Information des Informationssicherheitsbeauftragten sollte unseres Erachtens durch eine Information an das CERT ersetzt werden und die Pflicht zur Information des Informationssicherheitsbeauftragten sollte einerseits dann durch das CERT und andererseits bei materiellen Vorfällen erfolgen.:

„Als vom CERT als materiell eingestufte, IT-sicherheitsrelevant Vorfälle werden dem Informationssicherheitsbeauftragten unmittelbar und basierend auf definierten Eskalationsprozessen gemeldet. Eine Information weniger risikobehafteten IT-sicherheitsrelevanten Vorfälle erfolgt durch das CERT and den Informationssicherheitsbeauftragten im Rahmen der regelmäßigen Berichterstattung.“

5. Benutzerberechtigungsmanagement

Zum Zwecke einer zu den Vorgaben der MaRisk konsistenten Ausgestaltung der BAIT folgen diese dem modularen Aufbau der MaRisk und bedienen sich, abgesehen von wenigen Ausnahmen, der in den MaRisk verwendeten Begrifflichkeiten, was wir ausdrücklich begrüßen.

Eine uns aufgefallene Ausnahme zur konsistenten Begriffsverwendung zwischen BAIT und MaRisk findet sich im Rahmen des Benutzerberechtigungsmanagements. Den Vorgaben des AT 4.3.1 Tz. 2 MaRisk folgend, hat die Vergabe von Berechtigungen nach dem „Sparsamkeitsgrundsatz („Need-to-know-Prinzip“)“ zu erfolgen. Im Gegensatz dazu wird in den diesen Vorgaben spezifizierenden BAIT unter II. Tz. 25 BAIT das „Prinzip der minimalen Rechtevergabe“ als maßgebliches Prinzip im Rahmen der Rechtevergabe genannt.

Obwohl ersichtlich ist, dass den unterschiedlichen Begrifflichkeiten eine identische Absicht zugrunde liegt, nämlich die Vermeidung einer nicht notwendigen Vergabe von Berechtigungen, erscheint uns die Verwendung gleicher Begrifflichkeiten sinnvoll. Wir bitten daher die bereits in den MaRisk verwendeten Begrifflichkeiten auch in den BAIT zu verwenden. Sollte der Verwendung der zuvor genannten unterschiedlichen Begrifflichkeiten jedoch auch inhaltlich voneinander abweichende Zielsetzungen zugrunde liegen, bitten wir um eine Erläuterung dieser.

6. IT-Projekte, Anwendungsentwicklung

II. Tzn. 37 – 46 BAIT enthalten Vorgaben, die im Rahmen der Anwendungsentwicklung bzw. im Falle einer Nutzung von Anwendungen umzusetzen sind. Während die Vorgaben zur Nutzung von Anwendungen unabhängig davon ausgestaltet sind, ob es sich dabei um fremdbezogene oder selbst entwickelte Anwendungen handelt und folglich grundsätzlich nach Produktivsetzung der entsprechenden Anwendung umzusetzen sind (darunter insbesondere II. Tzn. 38, 39, 43-46 BAIT), ist nicht eindeutig ersichtlich, welche der Anforderungen, die sich explizit auf die Anwendungsentwicklung (insbesondere II. Tzn. 37, 40, 41) beziehen, im Falle fremdbezogener Anwendungsentwicklung zu erfüllen sind.

Es ist uns z.B. unklar, wie im Falle fremdbezogener Anwendungsentwicklung Vorkehrungen zur Verhinderung einer unbeabsichtigten Veränderung oder beabsichtigten Manipulation der Anwendung im Anwendungsentwicklungsprozess ausgestaltet werden sollen (II. Tz. 41 BAIT). Auch kann ein Teil der Anforderungen beim Bezug von Standardsoftware nicht zur Anwendung gebracht werden. Eine entsprechende Klarstellung in Abschnitt II. 6. BAIT ist aus unserer Sicht notwendig.

Eine Klarstellung der anzuwendenden Vorschriften könnte auch in Abschnitt II. 8. BAIT erfolgen.

7. IT-Betrieb

– Keine Anmerkungen –

8. Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen

In Bezug auf II. Tzn. 54 - 59 BAIT stellen sich uns auch im Zusammenspiel mit AT 9 der MaRisk eine Reihe von Detailfragen bzw. erachten wir die vorgeschlagenen Regelungen für nicht adäquat:

8.1 Cloud-Dienstleistungen

II. Tz. 54 Satz 2 BAIT betont die Geltung der Auslagerungsreglungen „insbesondere“ für Cloud-Dienstleistungen. Es ist unklar, warum die Anforderungen des AT 9 MaRisk für Cloud-Dienstleistungen bedeutender ist, als für andere Sachverhalte. Ein aufsichtsrechtlich als Auslagerung eingestufter Sachverhalt bleibt eine Auslagerung und es bedarf unserer Meinung nach keiner Betonung, dass „insbesondere für Auslagerungen von IT-Dienstleistungen .. (Cloud-Dienstleistungen)“ die Auslagerungsregelung gelten. Es bleibt daher unklar, was der Zweck des Satzes 2 ist. Sofern hiermit klarstellend erläutert werden soll, dass Cloud-Dienstleistungen aufsichtsrechtlich – ggf. unabhängig vom Inhalt der Cloud-Dienstleistung und damit ohne Prüfung auf die Anwendbarkeit des § 25b KWG – als Auslagerung zu klassifizieren sind, so sollte dies auch der Inhalt des Satzes sein. Allerdings lehnen wir eine solche weitreichende Interpretation einerseits ab und müsste dies andererseits

unserer Ansicht nach in AT 9 der MaRisk erläutert werden. In jedem Fall erscheint uns die Streichung des Satzes 2 in seiner jetzigen Form geboten.

8.2 Bezug von Software

II. Tz. 54. Satz 4 BAIT erscheint uns redundant zu den Vorschriften der MaRisk und der intendierte Sinn ist sprachlich nicht eindeutig (siehe unsere Anmerkungen in der Einleitung dieser Stellungnahme).

8.3 Anwendungsentwicklung

Wir möchten im Kontext der Auslagerung von Anwendungsentwicklung einerseits unsere bereits in der Konsultation 02/2016 geäußerten Anmerkungen wiederholen und andererseits auf den zu Abschnitt II. 6. BAIT in dieser Stellungnahme geäußerten Klarstellungsbedarf verweisen.

8.4 Vorgaben zum sonstiger Fremdbezug von IT-Dienstleistungen

II. Tzn. 55 – 59 BAIT enthalten Vorgaben für den sonstigen Fremdbezug von IT-Dienstleistungen. Entsprechende der Definitorik aus MaRisk AT 9 handelt es sich damit um Bezug von Dienstleistungen Dritter, die nicht als Auslagerung einzustufen sind.

Die Vorgaben von II. Tzn. 55 – 59 BAIT gelten allgemein und beinhalten keinerlei Proportionalität. Sie sind daher auf jeden sonstigen Fremdbezug (von IT-Dienstleistungen) unabhängig von Inhalt, Umfang und Dauer der Dienstleistung anzuwenden. Das lehnen wir entschieden ab.

Auch Abschnitt II. 8. BAIT muss dem generellen Proportionalitätsprinzip folgen. Die im Entwurf vorgeschlagenen Regelungen gehen z.B. über die Anforderungen für unter Risikogesichtspunkten nicht wesentliche Auslagerungen hinaus. Dies kann nicht gewollt sein.

Der Sinn einer „strategischen“ Steuerung von Verträgen des sonstigen Fremdbezugs von IT-Dienstleistungen nach II. Tz. 55 BAIT erschließt sich uns nicht. Hier führt die Vorschrift eher zur Unklarheit als zu einer Konkretisierung aufsichtlicher Vorgaben. Zudem sollte eine solche Steuerung – falls überhaupt erforderlich – nur für wesentliche und dauerhaften Fremdbezug vorgeschrieben werden.

Der Imperativ des II. Tz. 56 BAIT („jeden“) erscheint ebenfalls überzogen. Hier muss eine angemessene Einschränkung festgelegt werden. Hier wird insbesondere das krasse Missverhältnis der Regelungen für den sonstigen Fremdbezug von IT-Dienstleistungen und IT-Auslagerungen mehr als deutlich. Wir lehnen daher den Vorschlag zu II. Tz. 56 BAIT in seiner jetzigen Form ebenfalls entschieden ab.

Der sonstige Fremdbezug von IT-Dienstleistungen beinhaltet zu einem substantiellen Anteil kurzfristige Vertragsbeziehungen z.B. im Rahmen der Anwendungsentwicklung. Eine kurzfristige Vertragsbeziehung steht im klaren Widerspruch zu einer Notwendigkeit einer regelmäßigen Überprüfung, wie diese in II. Tz 58 BAIT gefordert wird. Eine regelmäßige Überprüfung kann daher nur bei einem Vertragsverhältnis sinnvoll eingeforderter werden, dass auf längere Dauer angelegt ist, nach unserem Verständnis also über einen Zeitraum von mindestens einem Jahr vereinbart ist bzw. durch ein- oder mehrmalige Verlängerung mehr als ein Jahr besteht. II. Tz. 58 BAIT sollte daher in Bezug auf regelmäßige Überprüfungen von ggf. durchzuführen Risikobewertungen (siehe oben) auf langfristigen sonstigen Fremdbezug von IT-Dienstleistungen beschränkt werden und die „Fristigkeit“ in den Erläuterungen näher beschrieben werden.

9. Inkrafttreten und Übergangsfristen

Die konkretisierenden Vorgaben der BAIT stellen z.T. neue, bisher nicht absehbare Anforderungen dar, welche von Instituten angemessen umzusetzen sind.

Es ist daher notwendig, den Zeitpunkt des Inkrafttretens der BAIT klar zu definieren und darüber hinaus festzulegen, welche Übergangsfristen den Instituten bis zur vollständigen Einhaltung der neuen Vorgaben gewährt werden.

Wir würden uns über die Berücksichtigung unserer Anmerkungen im weiteren Verlauf der Ausgestaltung der BAIT freuen. Für etwaige Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen,

Jürgen Hillen Marija Kozica