BUNDESVERBAND DEUTSCHER
LEASING-UNTERNEHMEN

BDL Markgrafenstraße 19 10969 Berlin

Bundesanstalt für Finanzdienstleistungsaufsicht
per E-Mail: Konsultation-13-20@bafin.de

Deutscher Bundesbank
per E-Mail: B34_MaRisk-BAIT@bundesbank.de

Kontakt:
Dr. Matthias Pytlik
pytlik@leasingverband.de
Tel.: +49(0)30-206337-21

Berlin, 23. November 2020

Stellungnahme des BDL zum Entwurf des Rundschreibens „Bankaufsichtliche Anforderungen an die IT (BAIT)“

Sehr geehrte Damen und Herren,

als Bundesverband Deutscher Leasing-Unternehmen e.V. (BDL) begrüßen wir den konstruktiven Dialog und bedanken uns für die Möglichkeit zur Stellungnahme.

Der Bundesverband Deutscher Leasing-Unternehmen vertritt die Interessen der Leasing-Branche, die mit einem Neugeschäftsvolumen von rund 75 Mrd. EUR in 2019 mehr als die Hälfte aller außenfinanzierten Ausrüstungsinvestitionen in Deutschland realisiert. Damit leistet die Leasing-Branche einen substanziellen Beitrag für die Investitionsversorgung, insbesondere des Mittelstands. Gleichzeitig ist auch die Leasing-Branche mittelständisch geprägt. Mehr als drei Viertel aller Leasing-Unternehmen haben weniger als 50 Mitarbeiter. Selbst die größten Unternehmen der Leasing-Branche verfügen über wenig komplexe Organisationsformen.

Im Mittelpunkt des Leasing-Prozesses steht das Investitionsobjekt. Genaue Kenntnisse der Beschaffungs- und Absatzmärkte sowie der technischen und wirtschaftlichen Eigenheiten der Objekte bilden die Grundlage des Leasing-Geschäftes. Die Eigentümerstellung und das Objekt-Know-how führen dazu, dass Leasing-Geschäfte selbst bei Zahlungsstörungen oder gar Zahlungsausfällen nur selten zu Verlusten führen.

Die Refinanzierung erfolgt in der Regel durch Kredite über voll regulierte Banken. Dabei wird typischerweise eine fristenkongruente Refinanzierung angestrebt, um die Übernahme von Finanzierungsrisiken zu vermeiden. Bei der Forfaitierung gehen bis auf das Veritätshaftungsrisiko praktisch alle Risiken auf die Bank über.

Zur Verwaltung von Kundeneinlagen und zur Erfüllung von Aufgaben im Zahlungsverkehr, die ein besonderes Schutzbedürfnis und besondere Anforderungen an die Informationstechnik begründen, sind Leasing-Unternehmen gar nicht berechtigt. Banktypische IT-Risiken mit hohem Schadenspotential bestehen im Leasing nicht. Aufgrund der strukturellen Merkmale des Geschäftsmodells finden sich im Leasing zumeist auch keine zeitkritischen Anwendungen und Prozesse.

Zusammenfassend ist das Geschäftsmodell von Leasing-Unternehmen mittelständisch geprägt, in der Realwirtschaft verankert und ausgesprochen risikoarm. Der Anzahl der Mitarbeiter und dem Geschäftsmodell entsprechend verfügen diese Unternehmen über wenig komplexe Organisationsformen.

Damit unterscheiden sich Leasing-Unternehmen deutlich von Banken. Diese Unterschiede sollten daher auch in den bankaufsichtlichen Anforderungen an die IT zum Ausdruck kommen.

Es ist zu begrüßen, dass das Proportionalitätsprinzip als „evidentes Wesensmerkmal“ der BAIT angesehen und den Ausführungen in Abschnitt I Tz. 4 prominent vorangestellt wird. Die folgenden Ausführungen spiegeln diesen Ansatz jedoch nicht angemessen wider. In einzelnen Punkten wurden Gestaltungsmöglichkeiten sogar zurückgenommen.

Den BAIT liegt vielmehr ein Maßstab zugrunde, der sich (unverändert) an der durchschnittlichen Größe von Banken orientiert und den Anforderungen an eine proportionale Ausgestaltung für Leasing-Unternehmen nicht gerecht wird. Damit drohen der Leasing-Branche Vorgaben, die zu einer existenziellen Hürde werden können. Der infolgedessen einsetzende Konsolidierungsdruck in der Branche führt wiederum dazu, dass dem Mittelstand flexible und passgenaue Investitions- und Finanzierungsformen verloren gehen.

Mit dem Protokoll zum 1. Gesprächskreis Leasing und Factoring wurde klargestellt, dass für das Petitum, Leasing-Unternehmen vom Anwenderkreis der BAIT auszunehmen, kein Verhandlungsspielraum gesehen wird. Mit den Ausführungen in der Anlage möchten wir daher anregen, deutlicher als bisher, dem Proportionalitätsprinzip im Rahmen der BAIT Rechnung zu tragen, um Leasing-Unternehmen eine angemessene Form der Umsetzung der primär bankaufsichtlichen Anforderungen an die IT zu ermöglichen. Ergänzungen analog den MaRisk, die auf große und komplexe Institute abstellen, können hierbei ein Ansatzpunkt sein, einheitliche aufsichtliche Anforderungen an die IT für einen breiten Anwenderkreis beizubehalten und dennoch eine angemessene Differenzierung zu ermöglichen.

Für weitere Informationen auch im Rahmen eines persönlichen Gespräches stehen wir jederzeit gerne zu Ihrer Verfügung.

Mit freundlichen Grüßen

Bundesverband Deutscher
Leasing-Unternehmen e. V.

Dr. Claudia Conen
Hauptgeschäftsführerin

Dr. Matthias Pytlik
Referatsleiter
Betriebswirtschaft und Regulatorik

Anlage

Stellungnahme des BDL zum Entwurf des BaFin-Rundschreibens
„Bankaufsichtliche Anforderungen an die IT (BAIT)“

Anlage

Tz.	Petita des BDL
1.	**IT-Strategie**
1.2	**Petitum:** Wir regen an, Inhalt und Abgrenzung der IT-Strategie nach Tz. 1.2. und der Informationssicherheitsleitlinie nach Tz. 4.2. überschneidungsfrei darzulegen. Ergänzend regen wir die Klarstellung an, ob zwingend zwei Dokumente erforderlich sind oder eine integrierte Darstellung möglich ist. Der Hinweis gemäß Tz. 4.2., dass die Informationssicherheitsleitlinie in Einklang mit den Strategien zu stehen hat, bedarf der Konkretisierung. **Begründung**: Die stärkere Einbindung von Informationssicherheitsaspekten in der IT-Strategie kann zu Dopplungen und Überschneidungen zur Informationssicherheitsleitlinie führen, erhöht den Pflegeaufwand und vermischt Verantwortlichkeiten. Sofern zwei separate Dokumente erwartet werden, sollte die Abgrenzung klar und der Verweis möglich sein.
2.	**IT-Governance**
3.	**Informationsrisikomanagement**
3.3.	**Petitum:** Wir regen die Klarstellung in Tz. 3.3. (Erläuterung) an, dass die Berücksichtigung von Vernetzungen im Informationsverbund mit Dritten keine über das Auslagerungsmanagement nach AT 9 MaRisk und Abschnitt 9 BAIT hinausgehenden Anforderung darstellt. Die Klarstellung kann durch Streichung des Hinweises in den Erläuterungen erreicht werden. **Begründung:** Die Verpflichtung zur Berücksichtigung der Vernetzung führt zu einem kaum abgrenzbaren Kreis der Bestandteile eines Informationsverbundes. Dadurch steigt die Unsicherheit in Bezug auf die Erfüllung der damit verbundenen aufsichtlichen Pflichten. Darüber hinaus sind die Pflichten gemäß AT 9 MaRisk und Abschnitt 9 BAIT ausreichend und der Hinweis in Tz. 3.3. (Erläuterung) somit redundant.
3.5.	**Petitum:** Wir bitten um Klarstellung, wie das Informationsrisikomanagement aufbau- und ablauforganisatorisch in die bestehenden Strukturen insbesondere mittelständischer Leasing-Unternehmen einzubinden ist und welche Beziehung/Abgrenzung zwischen dem Informationsrisikomanagement und dem Informationssicherheitsbeauftragten besteht. **Begründung:** In Tz. 3.2. wird die Umsetzung des Informationsrisikomanagements unverändert aus Tz. 9 BAIT (alt) übernommen, allerdings wird die Aufgabenbeschreibung des Informationsrisikomanagements in Tz. 3.5. und Tz. 3.9. konkretisiert. Dabei korrespondiert die nun sehr konkrete Aufgabenbeschreibung nicht mehr mit der abstrakt-systemischen Umsetzung in Tz. 3.2. Wir gehen davon aus, dass mit den neuen Aufgaben im Informationssicherheitsmanagement nicht die aufsichtliche Erwartung verknüpft wird, eine zusätzliche Funktion einzurichten.
3.9.	**Petitum:** Der Hinweis auf die kompetenzgerechte Genehmigung der Behandlung von Informationsrisiken sollte gestrichen werden. **Begründung:** Es bleibt unklar, was mit der Vorgabe zur kompetenzgerechten Genehmigung der Behandlung von Informationsrisiken gemeint bzw. wie der Prozess zu gestalten ist. Darüber hinaus sollte die Behandlung aller Risikoarten konsistent erfolgen.

Gemäß AT 3 Tz. 1 MaRisk liegt bereits jetzt - unabhängig von der internen Zuständigkeit - die Verantwortung für die ordnungsgemäße Geschäftsorganisation bei der Geschäftsleitung. Diese wird ihrer Verantwortung nur gerecht, wenn sie u.a. erforderliche Maßnahmen zur Begrenzung der Risiken trifft. Einen besonderen Genehmigungsprozess für Informationsrisiken vorzugeben ist daher nicht erforderlich und korrespondiert auch nicht mit den Vorgaben zur Behandlung anderer Risikoarten. Ein Genehmigungsprozess für Informationsrisiken sollte daher nicht explizit gefordert werden.

3.10 **Petitum:** Die Pflicht zur Information über Bedrohungen des Informationsverbundes ist angemessen. Der Zusatz „laufend“ sollte jedoch ersatzlos gestrichen werden.

Begründung: Es ist kaum möglich, den Nachweis darüber zu erbringen, dass Institute sich „laufend“ im Sinne von „kontinuierlich“ informieren. Eine dem Risiko angemessene Informationspflicht liegt im eigenen Interesse jeden Institutes und folgt bereits aus übergeordneten Grundsätzen einer ordnungsgemäßen Geschäftsorganisation. Die Pflicht zur Information über Bedrohungen des Informationsverbundes ist daher ausreichend.

4. Informationssicherheitsmanagement

4.4. **Petitum:** Der Hinweis auf das Informationssicherheitsmanagement-Team in den Erläuterungen ist zu streichen oder auf „große und komplexe Institute“ zu beschränken.

Begründung: Es bleibt unklar, wie die aufsichtliche Empfehlung zur Einrichtung eines Informationssicherheitsmanagement-Teams zu verstehen ist. Es bleibt auch unklar, welche Aufgaben dieses Team übernehmen soll.

Der bloße Hinweis, dass ein solches Team eingerichtet werden „kann“, befördert die Erwartung, dass ein solches Team unabhängig von den institutsspezifischen Gegebenheiten auch eingerichtet werden „sollte“. Damit drohen insbesondere an kleine und wenig komplexe Institute mit risikoarmen Geschäftsmodell, überzogene Anforderungen bei der Prüfung gestellt zu werden.

Grundsätzlich gilt, dass die Personalausstattung den betriebsinternen Erfordernissen, den Geschäftsaktivitäten und der Risikosituation angemessen sein muss. Ferner ist die Ressourcenausstattung des Informationssicherheitsbeauftragten Gegenstand von Tz. 4.5. Die Personalausstattung ist damit angemessen geregelt.

5. Operative Informationssicherheit

1. Petitum: Die Anwendung des in Abschnitt I. Tz. 4 vorangestellten Proportionalitätsprinzips sollte für Tz. 5.3., 5.4. und 5.5. klargestellt werden, indem die Pflicht zur Einführung eines Security Information and Event Management Systems auf große und komplexe Institute beschränkt wird.

Begründung: Mit Tz. 5.3., 5.4. und 5.5 wird de facto die Einrichtung eines Security Information and Event Management Systems (SIEM) gefordert, in dessen Mittelpunkt das in den Erläuterungen zu Tz. 5.5. aufgeführte Security Operation Center steht (SOC). Für große und komplexe Institute kann SIEM ein angemessenes Konzept sein, um auf Sicherheitsvorfälle zu reagieren und Schäden an der IT Infrastruktur vorzubeugen. Instituten mit keinen oder nur wenigen zeitkritischen Anwendungen und Prozessen sowie geringem Risikopotential, ist dieses Konzept jedoch nicht angemessen und von kleinen Instituten auch nicht leistbar.

2. Petitum: Wir regen die ergänzende Klarstellung an, dass die Vorgaben zur operativen Informationssicherheit auch durch Dritte im Rahmen einer Auslagerung erbracht werden können.

Begründung: Insbesondere kleine und mittelständische Leasing-Unternehmen nutzen Auslagerungen des IT-Betriebes einschließlich der IT-Infrastruktur, um sich externe Expertise zu erschließen, zu der aufgrund der fokussierten Geschäftsaktivitäten sonst i.d.R. kein Zugang besteht. Sofern an der Einführung von Tz. 5. grundsätzlich festgehalten wird, ist diesem Umstand Rechnung zu tragen, indem die Möglichkeit zur Auslagerung der Pflichten gemäß Tz. 5 grundsätzlich vorgesehen wird.

Andernfalls drohen die Anforderungen insbesondere kleine und mittelständische Institute vor unüberwindbare Hürden zu stellen, wodurch die betroffenen Unternehmen aus dem Markt gedrängt werden. Selbst bei Verbleib im Markt belasten die Anforderungen kleine und mittelständische Institute überproportional, wodurch dem Konsolidierungsdruck in der mittelständisch geprägten Leasing-Branche zusätzlich Vorschub geleistet wird. Dem Proportionalitätsgrundsatz folgend ist die zusätzliche Belastung im Hinblick auf Größe, Risiko und Komplexität jedoch nicht angemessen, sondern leistet einer Konzentration im Finanzmarkt Vorschub, die die Vielfalt und die Stabilität des Finanzmarktes einschränkt.

Zudem weisen wir darauf hin, dass die Vorgaben gemäß Tz. 5 umfangreiche Anpassungen der Verträge mit Dritten erfordern, die nur mit längeren Umsetzungsfristen zu erfüllen sind. Wir regen „Augenmaß“ und angemessene Fristen von mindestens zwei Jahren an.

6. Identitäts- und Rechtemanagement

6.2. **1. Petitum:** Dem Proportionalitätsprinzip folgend sollten Berechtigungskonzepte in kleinen, wenig komplexen Instituten oder bei risikoarmen Geschäftsaktivitäten auf den Kreis der privilegierten Benutzer beschränkt werden können.

Begründung: Die formale Organisation von Zugriffsrechten ist insbesondere in großen und komplexen Instituten notwendig und ergänzt bzw. ersetzt dort die persönliche Kontrolle. In kleinen, wenig komplexen Instituten mit risikoarmen Geschäftsmodell kann die formale Organisation der Zugriffsrechte jedoch auf den Personenkreis beschränkt werden, der über weitreichende Eingriffsrechte verfügt (privilegierte Benutzer). Andernfalls werden kleine Institute mit einem Aufwand für die Verwaltung von Zugriffsrechten belastet, dem kein angemessener Nutzen gegenübersteht.

2. Petitum: Die Festlegung von Zutrittsrechten sollte nur für Räume notwendig sein, die für die Informationsverarbeitung relevant sind. Darüber hinaus sollte erläuternd klargestellt werden, dass Einzelräume im Rahmen eines Raumkonzeptes auch zu Gruppen von Räumen zusammengefasst werden können, für die dann gruppenweite Zugriffsrechte festgelegt werden.

Begründung: Dem erheblichen Aufwand, für alle Räume Zutrittsrechte festzulegen und zu verwalten, steht kein angemessener Nutzen gegenüber.

7. IT-Projekte und Anwendungsentwicklung

8. IT-Betrieb

8.8. **Petitum:** Das Leistungs- und Kapazitätsmanagement von IT-Systemen ist auf wesentliche und/oder kritische Teile von Systemen zu beschränken.

Begründung: Ein angemessenes Leistungs- und Kapazitätsmanagement steht im Eigeninteresse jedes Leasing-Unternehmens. Die Verwaltung aller IT-Systeme ist dazu jedoch nicht erforderlich, sondern mit einem Aufwand verbunden, dem kein angemessener Nutzen gegenüber. Insbesondere kleine und mittlere Unternehmen werden durch den formalen Dokumentationsaufwand überproportional belastet, ohne dass dem ein angemessener Mehrwert gegenübersteht.

9. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

10. IT-Notfallmanagement

Petitum: Die neuen, umfangreichen Vorgaben zum IT-Notfallmanagement erfordern deutliche Anpassungen und Erweiterungen auch von bestehenden Auslagerungsvereinbarungen bei einer Vielzahl von Leasing-Unternehmen. Eine Umsetzungsfrist von mindestens 2 Jahren ist daher angemessen.

10.1. **Petitum:** Statt „aufeinander abgestimmte Notfallkonzepte“ bei Auslagerung von zeitkritischen Aktivitäten vorzuschreiben, sollten auslagernde Unternehmen bei Auslagerung von zeitkritischen Aktivitäten zur Prüfung verpflichtet werden, dass die Notfallkonzepte der Auslagerungsunternehmen den eigenen Vorgaben/Ansprüchen genügen.

Begründung: Die Anforderung an „aufeinander abgestimmte Notfallkonzepte“ bei Auslagerungen ist eine Forderung, die in der Praxis nicht immer erfüllt werden kann. So bieten bspw. große Cloud-Anbieter einen identischen Service ggf. in verschiedenen Abstufungen allen Kunden an – eine Abstimmung oder gar individuelle Anpassung ist nicht vorgesehen. Unser Vorschlag, auf die Prüfung von Notfallkonzepten abzustellen, erfordert keine Abstimmung, sondern stellt von vornherein sicher, dass die Notfallkonzepte passgenau sind.

10.4 **Petitum**: Statt „mindestens jährliche IT-Notfalltests“ für alle Systeme vorzuschreiben, sollte bei der Prüfung der Wirksamkeit der Notfallpläne auf einen mehrjährigen, risikobasierten Prüfzyklus abgestellt werden, so dass im Turnus mehrerer Jahre alle Szenarien aufeinander abgestimmt getestet werden können.

Begründung: Alle Notfallpläne mindestens jährlich vollständig zu testen, ist nicht angemessen und auch kaum leistbar. Dies gilt insbesondere vor dem Hintergrund, dass sich die Anzahl der Tests und Szenarien auf Basis der Anforderungen aus Tz. 10.1. und Tz. 10.3. im Vergleich zur aktuellen Situation noch erhöhen wird. Ein abgestimmter Prüfzyklus ist dagegen machbar und auch ausreichend.

10.5 **Petitum:** Die implizite Anforderung, zwei redundant ausgelegte Rechenzentren zu betreiben, ist auf große und komplexe Institute zu beschränken.

Begründung: Die strikte Anforderung zweier redundanter Rechenzentren ist von kleinen Instituten nicht erfüllbar und unter Maßgabe der Proportionalität auch nicht angemessen. Statt explizit auf Rechenzentren kann auf redundant ausgelegte Systeme oder auf eine Notfallwiederherstellungsumgebung abgestellt werden.