BaFin Journal

BaFin

Informationen der Bundesanstalt
für Finanzdienstleistungsaufsicht

April 2018

Interview

Dr. Thorsten Pötzsch: „Wir beschäftigen uns mit dem gesamten potenziellen Lebenszyklus am Kapitalmarkt“

Seite 14

IT-Sicherheit

Aufsicht konkretisiert IT-Anforderungen an die Versicherungswirtschaft

Seite 24

Lebensversicherung

Jährliche Standmitteilungen: Information und Schutz der Verbraucher

Seite 19

Cloud-Computing

Aufsichtsrechtliche Vorgaben zu Informations- und Prüfungsrechten sowie Kontrollmöglichkeiten

Seite 29

Themen

© BaFin

BaFin-Tech

Konferenz zur Digitalisierung in Berlin: Zwischen Wettbewerb, Kooperation und Verbraucherschutz

Seite 34

In Artikeln mit diesem Zeichen finden Sie Informationen zum Verbraucherschutz. In der Rubrik Verbraucher lesen Sie Warnungen und aktuelle Kurzmeldungen dazu.

KF = Kredit- und Finanzdienstleistungsinstitute; **VP** = Versicherer und Pensionsfonds;
WM = Wertpapierfirmen und Märkte; **AW** = Abwicklungsthemen; **ÜG** = Übergreifendes

Editorial

Liebe Leserinnen und Leser,

seit Anfang des Jahres ist Dr. Thorsten Pötzsch Exekutivdirektor des neuen Geschäftsbereichs „Abwicklung" bei der BaFin. Dazu gehören neben den Abwicklungsfunktionen die Themen Erlaubnispflicht und Verfolgung unerlaubter Geschäfte sowie Geldwäscheprävention. Im Interview ab Seite 14 erläutert Pötzsch, was ihn an der neuen Aufgabe reizt, welche Herausforderungen er erwartet und welche Themen ihm besonders am Herzen liegen.

Verbrauchern, die eine Lebensversicherung abgeschlossen haben, möchte ich den Beitrag ab Seite 19 ans Herz legen. Dort erfahren sie, auf welche Informationen ihres Versicherers sie Anspruch haben. Der Beitrag gibt zudem einen Ausblick auf bevorstehende Änderungen und beschreibt, wie die BaFin den Schutz der Versicherungsnehmer sicherstellt.

Daneben steht die aktuelle Ausgabe ganz im Zeichen der fortschreitenden Digitalisierung. Der Beitrag ab Seite 24 geht ausführlich auf die Versicherungsaufsichtlichen Anforderungen an die IT ein, die die BaFin derzeit konsultiert. Sie sollen künftig – analog zu den BAIT für den Bankensektor – der zentrale Baustein der IT-Aufsicht über alle Versicherungsunternehmen und Pensionsfonds in Deutschland sein.

Zu den IT-Technologien, denen die Aufsicht erhebliche Bedeutung beimisst, zählt das Cloud-Computing. Dabei werden IT-Ressourcen nicht innerhalb des Unternehmens betrieben, sondern durch einen externen Dienstleister, in der Regel über ein internetbasiertes, dynamisch nutzbares System. Der Beitrag ab Seite 29 erläutert, welche aufsichtsrechtlichen und regulatorischen Vorgaben dabei zu beachten sind und welche Schritte die BaFin unternommen hat, um diese zu konkretisieren.

Diese und viele weitere Themen standen im Fokus der zweiten BaFin-Tech, die vergangene Woche in Berlin stattfand. Anderthalb Jahre nach der ersten Konferenz dieser Art diskutierte die BaFin erneut mit Vertretern neuer und etablierter Unternehmen der Finanzindustrie sowie Experten aus Praxis und Wissenschaft über die Folgen der Digitalisierung und finanztechnologische Innovationen. Mehr dazu erfahren Sie ab Seite 34.

Eine interessante Lektüre wünscht Ihnen

Sabine Reimer

Dr. Sabine Reimer

© Bernd Roselieb

Dr. Sabine Reimer, Leiterin Kommunikation

IT-Sicherheit

Aufsicht konkretisiert IT-Anforderungen an die Versicherungswirtschaft

© iStockphoto.com/ mattjeacock

VP Mitte März hat die BaFin den Entwurf des Rundschreibens „Versicherungsaufsichtliche Anforderungen an die IT" (VAIT) zur Konsultation gestellt (siehe BaFinJournal März 2018). Stellungnahmen hierzu nimmt sie noch bis zum 20. April entgegen.

Die VAIT sollen künftig – ebenso wie die BAIT für den Bankensektor (siehe BaFinJournal November 2017 und Januar 2018) – der zentrale Baustein der IT-Aufsicht über alle Versicherungsunternehmen und Pensionsfonds in Deutschland sein. Sie richten sich primär an die Geschäftsleitungen der Unternehmen.

Unternehmen, die dem Anwendungsbereich von Solvency II unterliegen, müssen sich darüber hinaus weiterhin auch an die Mindestanforderungen an die Geschäftsorganisation (MaGo) halten. Für Versicherungs-Zweckgesellschaften im Sinne des § 168 Versicherungsaufsichtsgesetz (VAG) sowie den Sicherungsfonds im Sinne des § 223 VAG gelten die VAIT nicht.

Intention

Ziel der VAIT ist es, insbesondere für das Management der IT-Ressourcen sowie das Informationsrisiko- und das Informationssicherheitsmanagement einen für die Geschäftsleitungen der Unternehmen verständlichen und flexiblen Rahmen zu schaffen. Sie sollen außerdem dazu beitragen, das IT-Risikobewusstsein in den Unternehmen und gegenüber deren IT-Dienstleistern zu erhöhen.

Linkempfehlung zum Thema
Die Konsultation der VAIT finden Sie unter:
www.bafin.de » Recht & Regelungen » Konsultationen

Die VAIT machen transparent, welche Erwartungen die BaFin in Bezug auf die Steuerung und Überwachung des IT-Betriebs an die Unternehmen hat, einschließlich des hierfür notwendigen Berechtigungsmanagements. Zudem regeln sie die Anforderungen an das IT-Projektmanagement und die Anwendungsentwicklung, was auch die individuelle Datenverarbeitung in den Fachbereichen umfasst. Insgesamt adressieren die VAIT all jene Themen, die die BaFin aufgrund der Erkenntnisse aus ihrer IT-Aufsichts- und -prüfungspraxis als besonders bedeutend ansieht.

Interpretation der Aufsichtsnormen

Das Rundschreiben enthält Hinweise zur Auslegung der VAG-Vorschriften zur Geschäftsorganisation, die sich auf die technisch-organisatorische Ausstattung der Unternehmen beziehen. Es konkretisiert also, was die Aufsicht unter einer angemessenen technisch-organisatorischen Ausstattung der IT-Systeme (Hard- und Software) versteht, und zwar unter besonderer Berücksichtigung der Anforderungen an die Informationssicherheit. Da inzwischen viele Unternehmen IT-Services von Dritten beziehen – entweder in Form von Ausgliederungen oder sonstiger Dienstleistungsbeziehungen –, sind auch dazu Anforderungen in den VAIT formuliert.

Die erhöhte Transparenz der aufsichtlichen Anforderungen soll den Unternehmen helfen, in Bezug auf die IT eine ordnungsgemäße Geschäftsorganisation sicherzustellen. Die prinzipienorientierten Anforderungen stellen jedoch keinen vollständigen Vorgabenkatalog dar und sind deshalb nach Regelungstiefe und -umfang nicht abschließend. Jedes Unternehmen bleibt folglich auch jenseits der Konkretisierungen durch die VAIT verpflichtet, auf gängige IT-Standards abzustellen sowie den Stand der Technik zu berücksichtigen.

Bei der Umsetzung der Anforderungen an die Geschäftsorganisation und somit auch der Ausgestaltung der Strukturen, IT-Systeme und Prozesse spielt das Proportionalitätsprinzip eine erhebliche Rolle. Die Anforderungen sind also auf eine Weise zu erfüllen, die der Wesensart, dem Umfang und der Komplexität der Risiken gerecht wird, die mit der Tätigkeit des Unternehmens einhergehen.

IT-Risikobewusstsein schärfen

Wie bereits erwähnt, verfolgen die VAIT – wie auch die BAIT – darüber hinaus das zentrale Ziel, das IT-Risikobewusstsein in den Unternehmen zu schärfen. Ein besonderer Fokus liegt auf den Führungsebenen.

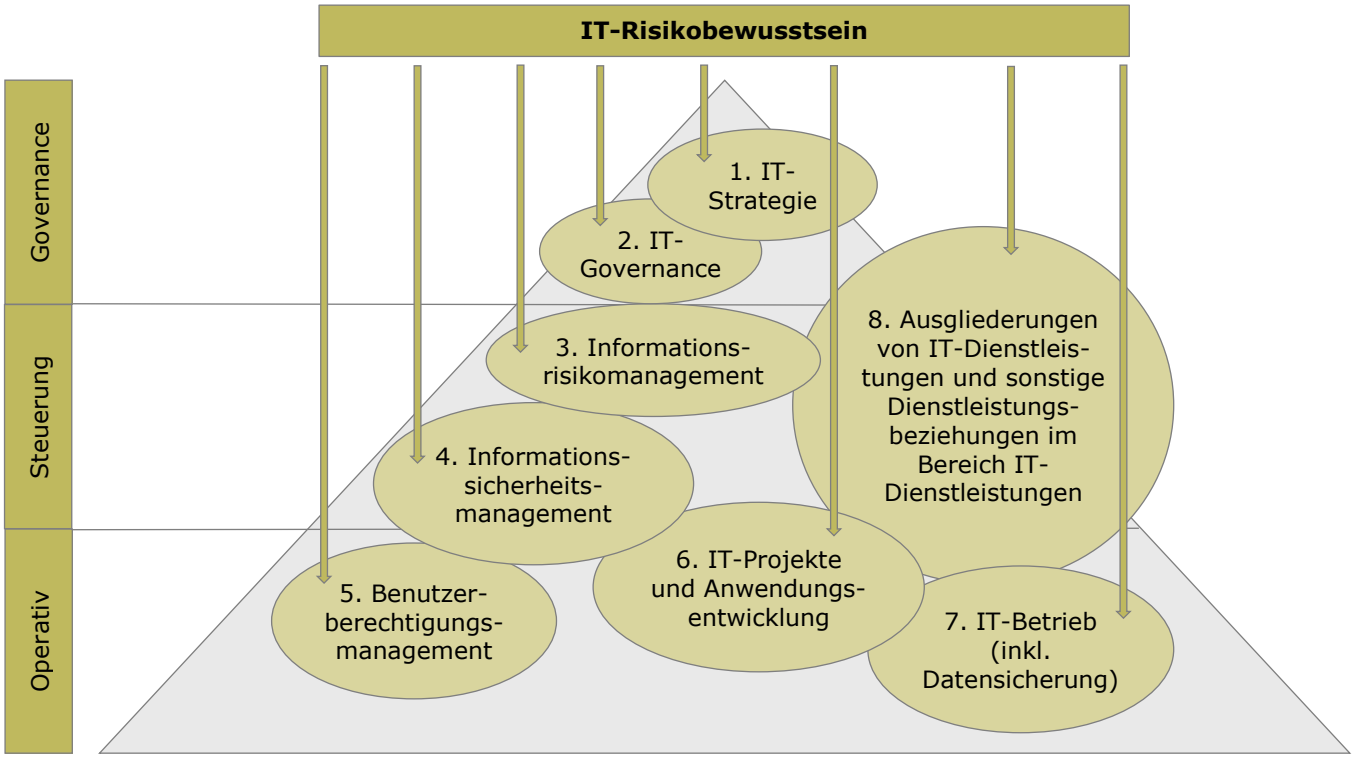
Unter dem Begriff IT-Risiko versteht die Aufsicht das bestehende und künftige Risiko von Verlusten aufgrund der Unzweckmäßigkeit oder des Versagens der Hard- und Software technischer Infrastrukturen, welche die Verfügbarkeit, Integrität, Zugänglichkeit und Sicherheit dieser Infrastrukturen oder von Daten beeinträchtigen können.

Das Erfordernis der Schaffung von Risikotransparenz und die Auseinandersetzung mit dem IT-Risiko auf allen Ebenen des Unternehmens zieht sich durch alle Themenmodule der VAIT und ist integraler Bestandteil der einzelnen IT-Anforderungen (siehe Grafik Seite 26).

IT-Strategie

In Bezug auf die IT-Strategie steht die Anforderung im Vordergrund, dass sich die Geschäftsleitung mit den strategischen Implikationen der verschiedenen Aspekte der IT für die Geschäftsstrategie regelmäßig auseinandersetzt. Hierzu gehört neben der Aufbau- und Ablauforganisation der IT und der Ausgliederung von IT-Dienstleistungen beziehungsweise sonstigen Dienstleistungsbeziehungen beispielsweise auch der strategische Umgang mit der individuellen Datenverarbeitung (IDV) in den Fachbereichen.

Schärfung des IT-Risikobewusstseins durch die VAIT



Durch die Festlegung der IT-Strategie sowie durch daraus abgeleitete Maßnahmen zur Erreichung der Strategieziele, die unternehmensintern in geeigneter Weise zu kommunizieren sind, wird auch die Klarheit über die Bedeutung der IT für die Durchführung der Versicherungsgeschäfte geschaffen, die für das IT-Risikobewusstsein notwendig ist.

IT-Governance

Die Geschäftsleitung ist dafür verantwortlich, dass auf Basis der IT-Strategie die Regelungen zur IT-Aufbau- und -Ablauforganisation festgelegt und bei Veränderungen der Aktivitäten und Prozesse zeitnah angepasst werden. Sie hat zudem deren wirksame Umsetzung sicherzustellen. Dies gilt auch für die Schnittstellen zu wichtigen Ausgliederungen.

Das Unternehmen hat dafür Sorge zu tragen, dass insbesondere das Informationsrisiko- und das Informationssicherheitsmanagement, der IT-Betrieb und die Anwendungsentwicklung angemessen mit Personal ausgestattet sind. Dies ist aus Sicht der Aufsicht wichtig, damit das Risiko einer qualitativen oder quantitativen Unterausstattung dieser Bereiche frühzeitig erkannt und möglichst umgehend behoben werden kann. Interessenkonflikte innerhalb der IT-Aufbau- und -Ablauforganisation sind zu vermeiden. Auch hierfür ist eine angemessene Personalausstattung notwendig.

Informationsrisikomanagement

Jedes Unternehmen hat im Rahmen des Managements der Informationsrisiken den jeweiligen Schutzbedarf zu ermitteln, auf dieser Grundlage Soll-Maßnahmen festzulegen, diese mit den wirksam umgesetzten Ist-Maßnahmen abzugleichen und Anpassungen vorzunehmen, sofern dies erforderlich ist.

Die hierdurch erhöhte Transparenz der Risikosituation und gegebenenfalls die Akzeptanz des Restrisikos durch die Geschäftsleitung ist die zentrale Anforderung zur Schärfung des IT-Risikobewusstseins im Unternehmen und gegenüber IT-Dienstleistern.

Informationssicherheitsmanagement

Unter Berücksichtigung der Risikosituation ist die Geschäftsleitung dafür verantwortlich, eine Informationssicherheitsleitlinie zu beschließen und innerhalb des Unternehmens angemessen zu kommunizieren. Auf Basis dieser Leitlinie sind konkretisierende Informationssicherheitsrichtlinien und -prozesse mit den Teilprozessen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren, die den Stand der Technik berücksichtigen.

In der Funktion des Informationssicherheitsbeauftragten sieht die Aufsicht das zentrale Element für die Einhaltung der Anforderungen und die Überwachung der Informationssicherheit innerhalb des Unternehmens und gegenüber Dritten. Die Funktion ist aufbau- und ablauforganisatorisch angemessen unabhängig auszugestalten, um Interessenkonflikte bei der Bewertung der Informationssicherheit zu vermeiden. Dies stärkt auch das IT-Risikobewusstsein der Geschäftsleitung und aller Beschäftigten im Unternehmen.

Benutzerberechtigungsmanagement

Das Unternehmen hat ein Benutzerberechtigungsmanagement einzurichten. Dieses muss sicherstellen, dass Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Unternehmens entspricht. Es ist ein Berechtigungskonzept schriftlich festzulegen. Im Hinblick auf die Vergabe von Berechtigungen an Benutzer hat dieses Konzept sicherzustellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt. Auch das trägt zur Verbesserung des IT-Risikobewusstseins bei.

Dies gilt auch für den Rezertifizierungsprozess, in dem die eingeräumten Berechtigungen regelmäßig überprüft werden. Dies ermöglicht es, Abweichungen von den genannten Maßgaben zu identifizieren und Berechtigungen gegebenenfalls anzupassen.

IT-Projekte und Anwendungsentwicklung

IT-Projekte sind angemessen zu steuern, insbesondere unter Berücksichtigung der Risiken im Hinblick auf Dauer, Ressourcenverbrauch und Qualität. Auch das Portfolio der IT-Projekte ist angemessen zu überwachen und zu steuern. Dabei ist zu berücksichtigen, dass auch aus gegenseitigen Abhängigkeiten verschiedener Projekte Risiken resultieren können.

Bereits bei der Entwicklung von Anwendungen sind nach Maßgabe des Schutzbedarfs angemessene Vorkehrungen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der in diesem Programm zu verarbeitenden Daten nachvollziehbar sicherstellen. Diese Vorgaben dienen auch dazu, das Risiko einer versehentlichen Änderung oder einer absichtlichen Manipulation der Anwendung zu reduzieren.

Aus Sicht der BaFin ist es notwendig, dass die Unternehmen für Anwendungen, die die Endbenutzer in den Fachbereichen entwickeln oder betreiben, ein angemessenes Verfahren zur Klassifizierung beziehungsweise Kategorisierung auf der Basis des Schutzbedarfs festlegen und sich Regeln für den Umgang mit solchen Anwendungen geben. Dies schafft die erforderliche Transparenz in Bezug auf die Risiken, die aus IDV-Anwendungen resultieren.

Darüber hinaus erwartet die Aufsicht, dass die Unternehmen ein zentrales Register der kritischen beziehungsweise wesentlichen Anwendungen führen. Dieses Register hat zumindest die Anwendungen zu beinhalten, die zur Identifizierung, Bewertung, Überwachung und Steuerung der Risiken sowie zur Berichterstattung über diese Risiken eingesetzt werden oder die für die Durchführung anderer versicherungstypischer Tätigkeiten von Bedeutung sind.

Hinweis

Keine Umsetzungsfrist

Die VAIT enthalten keine neuen Anforderungen an die Unternehmen und ihre IT-Dienstleister, sondern erläutern beziehungsweise konkretisieren lediglich bereits bestehende aufsichtliche Anforderungen. Darum sind keine Umsetzungsfristen vorgesehen.

IT-Betrieb

Die Berücksichtigung der Risiken, die aus dem Betrieb veralteter IT-Systeme – sowohl Hard- als auch Software – entstehen können, trägt ebenfalls wesentlich zur Stärkung des IT-Risikobewusstseins bei. Möglich ist ein solches (Produkt)-Lebenszyklus-Management jedoch nur, wenn die Komponenten der IT-Systeme einschließlich der Bestandsangaben entsprechend verwaltet werden. Hierfür sollten Unternehmen, für die dies gemäß dem Proportionalitätsprinzip geboten ist, ein digitales Verzeichnis nutzen, beispielsweise eine Configuration Management Database (CMDB).

Um unternehmerische beziehungsweise Reputationsschäden minimieren zu können, sind geeignete Kriterien festzulegen, nach denen die Geschäftsleitung über ungeplante Abweichungen vom Regelbetrieb (Störungen), deren Ursachen, die eingesetzten Notfallmaßnahmen zur Aufrechterhaltung oder Wiederherstellung des Geschäftsbetriebs sowie die Beseitigung der einschlägigen Mängel zu informieren ist. Dies ermöglicht es ihr, stets einen angemessenen Überblick über die IT-Risiken zu haben.

IT-Dienstleistungen

Vor der Ausgliederung von IT-Dienstleistungen und auch vor Vereinbarung anderer IT-Dienstleistungsbeziehungen sind Risikoanalysen durchzuführen. Nur so können die Unternehmen die Risikosituation vollständig ermitteln und Konzentrationsrisiken im Zusammenhang mit IT-Dienstleistungen erkennen.

Des Weiteren erwartet die Aufsicht, dass die Maßnahmen, die aus der Risikoanalyse abgeleitet werden, in die Gestaltung der Verträge mit einfließen.

Weiterentwicklung und Ausblick

Die modulare Struktur der VAIT gibt der Aufsicht die notwendige Flexibilität für Anpassungen oder Ergänzungen, wenn dies künftig aufgrund neuer internationaler oder nationaler Anforderungen mit IT-Bezug erforderlich werden sollte.

Derzeit prüft sie beispielsweise, ob die wesentlichen Elemente der Cybersicherheit, die die G-7-Staaten im Oktober 2016 veröffentlichten, durch Anpassungen der VAIT umgesetzt werden können. Diese betreffen unter anderem das Thema IT-Notfallmanagement inklusive Test- und Wiederherstellungsverfahren. Des Weiteren plant die BaFin – in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) –, ein spezielles Modul „Kritische Infrastrukturen" (siehe BaFinJournal August 2017) zu erarbeiten und in die VAIT zu integrieren. Dieses soll ausschließlich für die Betreiber kritischer Infrastrukturen gemäß Änderungsverordnung zur BSI-Kritisverordnung gelten, ohne dass diese über Gebühr zusätzlich belastet werden.

Die BaFin plant, zeitnah eine englische Übersetzung der VAIT zu veröffentlichen. Im Zuge der geplanten europaweiten Harmonisierung der Anforderungen an die IT-Systeme im Versicherungssektor wird sie die VAIT aktiv in den Diskussionsprozess einbringen. ■

Autor
Dr. Jens Gampe
BaFin-Grundsatzreferat für IT-Aufsicht und Prüfungswesen

Cloud-Computing

Einhaltung der aufsichtsrechtlichen Vorgaben zu Informations- und Prüfungsrechten sowie Kontrollmöglichkeiten

ÜG Im Rahmen der fortschreitenden Digitalisierung ist neuen IT-Technologien wie Cloud-Computing (siehe Infokasten Seite 30) eine erhebliche aufsichtliche Bedeutung beizumessen. Dabei ist es wichtig, dass insbesondere die beaufsichtigten Unternehmen im Finanzsektor und auch die Aufsicht technische Innovationen verstehen, um deren Einfluss auf das Geschäftsmodell, die Risikotragfähigkeit und die Erlaubnispflicht beurteilen zu können. Nur so ist es möglich, den spezifischen Gefahren, die mit dem Einsatz neuer IT-basierter Entwicklungen einhergehen, aufsichtlich und regulatorisch gerecht zu werden.

Aufgrund der wachsenden Bedeutung des Themas und der zunehmenden Unsicherheit im Finanzsektor bei der Anwendung der aufsichtsrechtlichen Vorgaben hat die BaFin kürzlich wichtige Schritte unternommen, um den regulatorischen Rahmen für Cloud-Computing zu konkretisieren.

Regulatorischer Rahmen

Die beaufsichtigten Unternehmen haben bei der Nutzung von Cloud-Computing die jeweiligen aufsichtsrechtlichen Anforderungen an Auslagerungen (Kreditinstitute) beziehungsweise Ausgliederungen (Versicherungsunternehmen) einzuhalten.

Der erste Schritt zur Konkretisierung des regulatorischen Rahmens für Cloud-Computing war die Veröffentlichung des Rundschreibens „Bankaufsichtliche Anforderungen an die IT" (BAIT) (siehe BaFinJournal November 2017 und Januar 2018). Die BAIT stellen klar, dass AT 9 der Mindestanforderungen an das Risikomanagement der Banken (MaRisk) auch für die Nutzung solcher Cloud-Dienste gilt, die eine Auslagerung von IT-Dienstleistungen darstellen. Das bedeutet, dass die aufsichtsrechtlichen Anforderungen an eine Auslagerung gemäß § 25b Kreditwesengesetz (KWG) in Verbindung mit AT 9 MaRisk entsprechend der jeweiligen Einzelfallprüfung einzuhalten sind.

In den nächsten Monaten wird die BaFin auch ihre Erwartungshaltung an Versicherungsunternehmen und Pensionsfonds per Rundschreiben konkretisieren. Derzeit befinden sich die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) in der öffentlichen Konsultation (siehe Seite 24). Analog zu den BAIT stellt auch dieses Rundschreiben klar, dass bei der Nutzung von Cloud-Diensten die aufsichtsrechtlichen Anforderungen zu Ausgliederungen einzuhalten sind, die für das jeweilige Unternehmen gelten.

Die Aufsicht wird außerdem evaluieren, inwieweit hinsichtlich der bestehenden aufsichtsrechtlichen Anforderungen an Auslagerungen beziehungsweise Ausgliederungen Anpassungsbedarf besteht.

Definition

Cloud-Computing

Beim Cloud-Computing werden IT-Ressourcen nicht innerhalb des Unternehmens betrieben, sondern durch einen externen Dienstleister. Dies geschieht in der Regel über ein internetbasiertes, dynamisch nutzbares System. Die damit verbundene Möglichkeit, Kosten einzusparen und technische Expertise zu nutzen, sorgt für ein erhöhtes Interesse von Unternehmen an Cloud-Lösungen.

Orientierungshilfe geplant

Insbesondere aufgrund von Gesprächen mit beaufsichtigten Unternehmen, die den Bedarf im Finanzsektor an einer aufsichtlichen Einschätzung von Cloud-Computing deutlich gemacht haben, wird die BaFin darüber hinaus im Laufe des Jahres eine spezielle Orientierungshilfe zum Thema veröffentlichen. Diese wird den Markt detailliert über die aufsichtsrechtlichen Anforderungen informieren, die mit der Nutzung von Cloud-Diensten verbunden sind. Mit diesem weiteren Schritt will die BaFin den Unternehmen mehr Sicherheit bei der Anwendung der aufsichtlichen Vorgaben geben.

Im Vorgriff auf die Orientierungshilfe behandelt der vorliegende Artikel einige aus aufsichtsrechtlicher Sicht wesentliche Aspekte: die Einhaltung der uneingeschränkten Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten der Aufsicht und der uneingeschränkten Informations- und Prüfungsrechte der beaufsichtigten Unternehmen.

Aufsichtsrechtliche Vorgaben

Beaufsichtigte Unternehmen, die die Nutzung eines Cloud-Dienstes beabsichtigen, haben vorab zu prüfen, inwieweit dabei die aufsichtsrechtlichen Anforderungen an Auslagerungen beziehungsweise Ausgliederungen zu beachten sind.

Ergibt die Prüfung, dass es sich unter Risikogesichtspunkten um eine wesentliche Auslagerung beziehungsweise wichtige Ausgliederung handelt, so haben Kreditinstitute bei der Vertragsgestaltung §§ 25a und 25b KWG in Verbindung mit AT 9 Tz. 7 und 8 MaRisk einzuhalten, Versicherungsunternehmen Artikel 274 Absätze 3 bis 5 der Delegierten Verordnung zu Solvency II, § 32 des Versicherungsaufsichtsgesetzes (VAG) und Rn. 237 ff. der Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGO, siehe BaFinJournal Februar 2017). Diese enthalten insbesondere Regelungen zu angemessenen beziehungsweise uneingeschränkten Informations- und Prüfungsrechten.

Uneingeschränkte Informations- und Prüfungsrechte

Einige beaufsichtigte Unternehmen haben der BaFin Entwürfe zu Auslagerungsverträgen über die Nutzung von Cloud-Diensten vorgelegt. Dabei ging es

etwa um die Nutzung von Rechenleistung, Speicherplatz und Web-Anwendungen.

Aus den Entwürfen wurde deutlich, dass insbesondere die Informations- und Prüfungsrechte der Aufsicht und der beaufsichtigten Unternehmen vertraglich nicht vollständig umgesetzt waren. Dies ist aber besonders deswegen wichtig, weil viele der derzeit am Finanzmarkt tätigen Anbieter von Cloud-Lösungen ihren Firmensitz in Staaten außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums haben. Aber auch deutsche Cloud-Anbieter unterstehen selbst nicht der Aufsicht, so dass die Aufsichtsgesetze keine unmittelbare Anwendung finden. Die Durchsetzung der aufsichtsrechtlichen Bestimmungen ist daher nur auf der Grundlage entsprechender vertraglicher Rechte möglich.

Informations- und Prüfungsrechte der Kreditinstitute

Die vertragliche Einräumung uneingeschränkter Informations- und Prüfungsrechte gegenüber den Cloud-Anbietern ist insbesondere mit Blick auf die IT-Sicherheit der Institute von besonderer Bedeutung.

Bei Auslagerungen, die unter Risikogesichtspunkten nicht wesentlich sind, sind die allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 25a Absatz 1 KWG zu beachten (siehe AT 9 Tz. 3 MaRisk). Ist die Nutzung eines Cloud-Dienstes als wesentliche Auslagerung einzustufen, sind im Auslagerungsvertrag angemessene Informations- und Prüfungsrechte der Internen Revision sowie externer Prüfer als uneingeschränkte Rechte einzuräumen (AT 4.4.3. Tz. 4 MaRisk). Nur durch den uneingeschränkten Zugang zu den Cloud-Anbietern – zum Beispiel zu Geschäftsräumen, Rechenzentren, Servern und Mitarbeitern – ist es den beaufsichtigten Unternehmen möglich, ihre Informations- und Prüfungsrechte ordnungsgemäß wahrzunehmen. Daher sind insbesondere Vor-Ort-Prüfungen unerlässlich.

Keine Einschränkung der Rechte

Damit das Unternehmen seine Rechte wirksam ausüben kann, dürfen diese nicht vertraglich eingeschränkt werden. Gestufte Informations- und Prüfungsverfahren stellen eine solche Einschränkung dar und entsprechen weder den Anforderungen der MaRisk noch den Empfehlungen der Europäischen Bankenaufsichtsbehörde EBA (siehe Infokasten Seite 32). Eine Einschränkung liegt in der Regel auch vor, wenn die Ausübung einer Prüfung von der wirtschaftlichen Zumutbarkeit (Commercially Reasonable) abhängig gemacht wird. Auch eine vertragliche Verpflichtung, zunächst auf standardisierte Prüfungsberichte der Cloud-Anbieter zurückzugreifen, ist eine unzulässige Einschränkung von Informations- und Prüfungsrechten.

Die Nutzung von Management-Konsolen eignet sich zwar für bestimmte Kontrollen, beispielsweise für die Überprüfung der Einhaltung der Service-Level-Agreements im laufenden Betrieb. Sie kann jedoch keine Prüfungen der Internen Revision ersetzen, da über Management-Konsolen nur auf Informationen zurückgegriffen werden kann, die der Cloud-Anbieter

Links zum Thema

Kreditwesengesetz
www.gesetze-im-internet.de

MaRisk
www.bafin.de » Recht & Regelungen » Verwaltungspraxis

BAIT
www.bafin.de » Recht & Regelungen » Verwaltungspraxis

Empfehlungen der EBA
www.eba.europa.eu

Delegierte Verordnung zu Solvency II
www.eur-lex.europa.eu

Versicherungsaufsichtsgesetz
www.gesetze-im-internet.de

MaGo
www.bafin.de » Recht & Regelungen » Verwaltungspraxis

VAIT (Konsultation)
www.bafin.de » Recht & Regelungen » Konsultationen

zur Verfügung stellt. Für die Interne Revision eines Instituts muss es jedoch auch möglich sein, darüber hinausgehende Informationen zu erhalten, die für die Prüfung erforderlich sind.

Erleichterungen

Um die Prüfungen bei wesentlichen Auslagerungen effektiver zu gestalten – sowohl für Institute als auch für Cloud-Anbieter, die für mehrere Institute tätig sind –, akzeptiert die BaFin gemäß BT 2.1 Tz. 3 MaRisk auch Sammelprüfungen. Bei solchen können die Prüfungen durch die Interne Revision eines oder mehrerer der auslagernden Institute beziehungsweise durch einen von diesen Instituten beauftragten Dritten durchgeführt werden, sofern diese Revisionstätigkeit den Anforderungen von AT 4.4 und BT 2 MaRisk genügt.

Darüber hinaus kann ein Institut gemäß BT 2.1 Tz. 3 MaRisk Prüfungen durch die Interne Revision des Cloud-Anbieters durchführen lassen oder einen Dritten damit beauftragen, sofern die anderweitig durchgeführte Revisionstätigkeit die Anforderungen von AT 4.4 und BT 2 MaRisk erfüllt. Die Interne Revision des auslagernden Instituts hat sich jedoch regelmäßig davon zu überzeugen, dass die genannten Voraussetzungen eingehalten werden. Die Prüfungsergebnisse, die für das auslagernde Institut relevant sind, sind an dessen Interne Revision weiterzuleiten.

Dies steht auch im Einklang mit den EBA-Empfehlungen und führt dazu, dass der Organisationsaufwand für die Institute und den Cloud-Anbieter verringert wird. Die Bündelung von Prüfungsressourcen auf Seiten der Institute trägt auch der Sorge der Cloud-Anbieter vor einem „Prüftourismus" Rechnung.

Prüfungsverfahren

Entscheidet sich ein Institut dafür, die Prüfung nicht selbst oder nicht allein durchzuführen, darf dies nicht zu einer Einschränkung des Prüfungsrechts führen. Die Informations- und Prüfungsrechte der Internen Revision des auslagernden Instituts müssen vollständig vertraglich vereinbart sein.

Dem Informations- und Prüfungsrecht des auslagernden Instituts genügt es nicht, wenn der Cloud-Anbieter lediglich Zertifikate oder sonstige Nachweise der Einhaltung anerkannter Standards vorlegt. Es muss die Möglichkeit haben, Einfluss auf den Informations- und Prüfungsumfang zu nehmen. Dies stimmt mit den Empfehlungen der EBA überein, die entsprechende Anforderungen an einen Rückgriff auf Zertifikate und Prüfungsberichte des Cloud-Anbieters stellen.

Informations-/Prüfungsrechte und Kontrollmöglichkeiten der Aufsicht

Darüber hinaus sind uneingeschränkte Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten der Aufsicht bezüglich der ausgelagerten Aktivitäten und Prozesse vertraglich zu vereinbaren. Insbesondere dürfen die Prüfungen der Aufsicht nicht davon abhängig gemacht werden, ob sie für den Cloud-Anbieter wirtschaftlich zumutbar sind.

Die Aufsicht muss die Cloud-Anbieter genauso kontrollieren können, wie dies das Gesetz gegenüber dem beaufsichtigten Unternehmen vorsieht. Dies umfasst insbesondere auch die Möglichkeit von Vor-Ort-Prüfungen.

Prüfungsrechte von Versicherungsunternehmen und Aufsicht

Auch bei der Ausgliederung durch Versicherer gilt, dass dem Unternehmen und der Aufsicht uneingeschränkte Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten vertraglich eingeräumt werden müssen.

Auf einen Blick

Empfehlungen der EBA

Cloud-Computing ist kein rein nationales Thema. Ende 2017 veröffentlichte die Europäische Bankenaufsichtsbehörde EBA Empfehlungen, die Kreditinstitute ab dem 1. Juli 2018 bei Auslagerungen an Anbieter von Cloud-Services beachten sollen (siehe BaFinJournal Januar 2018). Ziel ist ein einheitlicher europäischer Rahmen im Umgang mit Cloud-Computing.

Für die Feststellung, ob eine Ausgliederung auf den Cloud-Anbieter vorliegt, ist maßgeblich, ob und welche Funktionen oder Versicherungstätigkeiten betroffen sind. Eine Kontrolle hat nicht nur bei der Ausgliederung wichtiger, sondern nach § 32 Absatz 1, 2 und 4 VAG auch bei nicht wichtigen Funktionen und Versicherungstätigkeiten zu erfolgen. Hierbei sind nach Rn. 255 MaGo die Vorgaben aus Artikel 274 der Delegierten Verordnung zu Solvency II also über den Wortlaut hinaus auch auf nicht wichtige Funktionen und Versicherungstätigkeiten anwendbar, soweit sie universellen Charakter haben.

Die Ausführungen, die zuvor zur Einschränkung von Informations- und Prüfungsrechten gemacht wurden, gelten hier ebenso. Insbesondere ist es in der Regel als Einschränkung zu werten, wenn das Versicherungsunternehmen vertraglich dazu verpflichtet wird, zunächst auf existierende standardisierte Prüfungsberichte des Cloud-Anbieters zurückzugreifen. Ein gestuftes Verfahren entspricht nicht den aufsichtlichen Anforderungen an Versicherungsunternehmen. Eine Einschränkung liegt auch dann vor, wenn Prüfungen von wirtschaftlicher Zumutbarkeit abhängig sind.

Die BaFin erwägt derzeit, es auch Versicherungsunternehmen zu ermöglichen, bestimmte Prüfungsrechte gegenüber dem Cloud-Anbieter per Sammelprüfung gemeinsam mit anderen Versicherern wahrzunehmen. Dabei wäre zu unterscheiden zwischen der uneingeschränkten Einräumung der Prüfungsrechte – also insbesondere der Möglichkeit, Vor-Ort-Prüfungen durchzuführen – und der Ausgestaltung des Prüfungsverfahrens. Auch hier dürfte die Wahl des Prüfungsverfahrens nicht zur Einschränkung des Prüfungsrechts führen. ■

Hinweis

BaFin-Tech

Auf Seite 34 finden Sie den ausführlichen Bericht zur diesjährigen BaFn-Tech-Konferenz, die vergangene Woche in Berlin stattfand. Neben zahlreichen weiteren Themen rund um die Digitalisierung kam das Thema Cloud-Computing dort ebenfalls zur Sprache.

Autor
Nadine Rademacher
BaFin-Grundsatzreferat für IT-Aufsicht und Prüfungswesen

Impressum

Herausgeber

Bundesanstalt für
Finanzdienstleistungsaufsicht (BaFin)
Gruppe Kommunikation
Graurheindorfer Straße 108, 53117 Bonn
Marie-Curie-Straße 24 – 28, 60439 Frankfurt am Main
Internet: www.bafin.de

Redaktion und Layout

BaFin, Interne Kommunikation und Internet
Redaktion: Rebecca Frener
Tel.: +49 (0) 228 41 08 22 13
Kathrin Jung
Tel.: +49 (0) 228 41 08 16 28
Layout: Christina Eschweiler
Tel.: +49 (0) 228 41 08 38 71
E-Mail: journal@bafin.de

Designkonzept

werksfarbe.com | konzept + design
Humboldtstraße 18, 60318 Frankfurt am Main
www.werksfarbe.com

Bezug

Das BaFinJournal* erscheint jeweils zur Monatsmitte auf der Internetseite der BaFin. Mit dem Abonnement des Newsletters der BaFin werden Sie über das Erscheinen einer neuen Ausgabe per E-Mail informiert. Den BaFin-Newsletter finden Sie unter: www.bafin.de » Newsletter.

Disclaimer

Bitte beachten Sie, dass alle Angaben sorgfältig zusammengestellt worden sind, jedoch eine Haftung der BaFin für die Vollständigkeit und Richtigkeit der Angaben ausgeschlossen ist.

Ausschließlich zum Zweck der besseren Lesbarkeit wird im BaFinJournal auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen sind somit geschlechtsneutral zu verstehen.