Stellungnahme

Stellungnahme zur Konsultation der MaRisk Novelle der Bundesanstalt für Finanzdienstleistungsaufsicht und der Deutschen Bundesbank

27. April 2016

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Steffen von Blumröder
Bereichsleiter
Banking, Financial Services & FinTechs
T +49 30 27576-126
s.vonblumroeder@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Thorsten Dirks

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

1. Einleitung

Die Bundesanstalt für Finanzdienstleistungsaufsicht hat gemeinsam mit der Deutschen Bundesbank am 19. Februar eine Konsultation zur MaRisk Novelle gestartet.

Seit der letzten Überarbeitung der MaRisk im Jahre 2012 sind aus Sicht der Aufsicht einige Themen zum Risikomanagement in den Vordergrund gerückt, die bisher noch nicht bzw. noch nicht explizit in den MaRisk verankert waren und daher als Haupttreiber einer Novellierung angesehen werden können.

Vor diesem Hintergrund ist es Bitkom ein Anliegen zur Wirksamkeit beizutragen und nachteilige Auswirkungen oder unbeabsichtigte Konsequenzen zu minimieren, die mögliche Vorteile beeinträchtigen oder den Wettbewerb verzerren.

Bitkom vertritt viele Mitglieder die Software und Software-bezogene Dienstleistungen an Finanzinstitute liefern. Die geplante Entwurf der MaRisk (der

„**MaRisk-Entwurf**") ist daher insbesondere im Hinblick auf die Regelungen zur **Auslagerung (Ziffer AT 9)** von großem Interesse für unsere Mitglieder.

Für die Gelegenheit zur Stellungnahme bedanken wir uns und nehmen diese betreffend Ziffer AT 9.1 des MaRisk Entwurfs gerne wie folgt war.

2. Auslagerung nach Ziffer AT 9

A. Standardsoftware, individuelle Software und angepasste Software

Gemäß Ziffer AT 9.1 liegt eine Auslagerung vor, „wenn ein anderes Unternehmen mit der Wahrnehmung solcher Aktivitäten und Prozesse [...] beauftragt wird, die ansonsten vom Institut selbst erbracht würden". Keine Auslagerung liegt hingegen vor, wenn es sich um einen sonstigen Fremdbezug von Leistungen handelt. Letzteren konkretisiert die Novelle wiederum dahingehend, dass „[...] vom Institut bezogene Software und diesbezügliche fachliche Unterstützungsleistungen [...] "nicht als sonstiger Fremdbezug, sondern als Auslagerung zu werten sind. Hieraus schließen wir zunächst, dass eine Auslagerung grundsätzlich nur an die Erstellung von Software bzw. an deren Anpassung anknüpfen kann.
Dieses Ergebnis erschließt sich bei einem Blick auf die folgenden Kategorien:

- **Standardsoftware** ist Software, welche keine kundenspezifischen Merkmale enthält und für eine große Anzahl von Kunden mit unterschiedlichen Anforderungsprofilen erstellt wurde. Immense Entwicklungskosten werden durch eine breite Nutzerbasis finanziert. Bei Updates und Weiterentwicklungen kann jedoch nicht auf einzelne Kundenwünsche eingegangen werden. Der Source-Code ist häufig äußerst umfangreich und ist das Ergebnis eines jahrelangen Entwicklungsprozesses. Bei Standardsoftware ist es Sache des Instituts zu evaluieren, ob die Software einem bestimmten kundenspezifischen Zweck dienlich ist oder nicht. Es handelt sich demnach um keine Dienstleistung, auf die Auslagerungsregeln passen. Das Institut erwirbt lediglich eine Lizenz ohne Einflussmöglichkeit auf die Software selbst– insbesondere wird der Source-Code dem Institut in aller Regel nicht zugänglich gemacht.

- **Individuelle Software** ist Software, die das Institut nach seinen Anforderungen in Eigenverantwortung erstellt und hierzu die Dienst-/ Werkleistung Dritter in Anspruch nimmt. Hierbei ist aus unserer Sicht zwischen der externen Unterstützung der projekthaften initialen bzw. Weiterentwicklung und der dauerhaften Fremdvergabe der Anwendungswartung zu unterscheiden. So haben die Institute für Projekte eine separate Governance etabliert (Providerauswahl, Projektmanagementprozesse, Risikomanagement, Qualität, Kostensteuerung, etc....), die aus unserer Sicht die einschlägigen Risiken auf Basis der umfangreichen im Markt vorhandenen

Erfahrung hinreichend adressiert. Dies gilt ebenso für die zur Produktivsetzung von entwickelter Software verwendeten Serviceprozesse (z. B. Change- und Releasemanagement).

- **Angepasste Software** ist Standardsoftware, die punktuell im Rahmen bestimmter Vorgaben modifiziert oder über Schnittstellen mit anderer Software ergänzt wurde. Sofern die Anpassung oder Ergänzung aus unserer Sicht wie im vorhergehenden Punkt zu behandeln, nämlich nur dann als Auslagerung, wenn eine permanente Fremdvergabe der Wartung und Weiterentwicklung der angepassten Software vorliegt, nicht aber im Falle der projekthaften Unterstützung durch Dritte.

B. Verbindung der Software mit Dienstleistungen durch Dritte

Gleiches gilt für die „Verbindung" von Software mit Dienstleistungen durch Dritte. Prinzipiell finden bei Dienstleistungen, die im Zusammenhang mit Software erbracht werden, die allgemeinen Regelungen von Ziffer AT 9.1 des MaRisk Entwurfs Anwendung. Einer Sonderregelung für Software bedarf es nach unserer Ansicht nicht. Eine Vorschrift dahingehend, jeglichen Bezug von Software als eine Auslagerung zu qualifizieren, allein wenn im Zusammenhang auch Dienstleistungen durch Dritte bezogen werden, erscheint überschießend.

Zum einen wird jegliches IT-Outsourcing in mehr oder weniger enger Verbindung mit Software erbracht. Die vorgeschlagene Regelung würde daher dazu führen, dass jeglicher Bezug von Standardsoftware automatisch den Regelungen einer Auslagerung unterfällt.

Zum anderen ist es marktüblich, dass Standardsoftware meist im Zusammenhang mit Dienstleistungen vertrieben wird, die einen untergeordneten bzw. unterstützenden Charakter aufweisen. Es erscheint unangemessen, dass der Bezug von Standardsoftware bereits deswegen als Auslagerung zu qualifizieren ist, weil üblicherweise Softwareinstallation bzw. Dienstleistungen der sog. „Software Maintenance" ebenfalls erbracht werden.

Entscheidend sollte sein, dass das Wesensmerkmal der entsprechenden Software die Risikosteuerung bzw, die Kernbankleistung ist, also eine Bankleistung untrennbar mit ihr verbunden ist. Nach dem aktuellen Wortlaut würde z. B. ein Tabellenkalkulationsprogramm welches minimal an Bedürfnisse des Institutes angepasst ist, unter dem Wortlaut des Vorschlages subsumierbar sein.

C. Folgen des derzeitigen Entwurfs

Wenn projekthafte Entwicklung unter Einbeziehung Dritter oder der Bezug von Software als Auslagerung bzw. Teil einer solchen und damit potenziell „wesentlichen Auslagerung" qualifiziert wird, ist das Institut gehalten die Regelungen von Ziffer AT 9.7 des MaRisk Entwurfs durchzusetzen. Hierzu gehört insbesondere die Sicherstellung der uneingeschränkten Informations- und Prüfungsrechte der BaFin bei den Herstellern von Standardsoftware sowie den bei der projekthaften Anpassung beteiligten Unternehmen bzw. Einzelpersonen.

D. Formulierungsvorschlag zu Anm. zu Ziffer AT 9.1 des MaRisk Entwurfs

Vor diesem Hintergrund schlagen wir folgende Änderungen zur Anmerkung von Ziffer AT 9.1 des MaRisk Entwurfs vor:

> Nicht als sonstiger Fremdbezug, sondern als Auslagerung einzustufen sind jedoch vom Institut dauerhaft, d. h. nicht im Rahmen eines einmaligen Vorhabens an einen Dritten vergebene Entwicklungs- und Anpassungsleistungen von Software und diesbezügliche fachliche Unterstützungsleistungen, die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt werden oder für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung sind (Kernbanksysteme), sofern und soweit sie individuell an die bankspezifischen Bedürfnisse eines Instituts (und seiner verbundenen Unternehmen) angepasst oder entwickelt wird.