bankenverband

Positionspapier Outsourcing-Leitlinie

13. November 2019

Einleitung

Frank Mehlhorn
Director
+49 30 1663-2140
frank.mehlhorn@bdb.de

Tobias Tenner
Leiter Digitalisierung,
Associate Director
+49 30 1663 2323
tobias.tenner@bdb.de

Der Einsatz von Technologie in der Finanzwirtschaft ist nicht neu. Sie ist für die Branche der Finanzdienstleister gängige Alltagsarbeit. Die Geschwindigkeit mit der sich technologische Weiterentwicklungen vollziehen, ist enorm. Dies bietet Chancen auch für Banken. Eine der Möglichkeiten besteht darin, dass Banken mit FinTechs zusammenarbeiten. Wie diese Zusammenarbeit konkret verbessert werden kann, unter Einbeziehung der bankaufsichtlichen Anforderungen, dem widemt sich diese Leitlinie.

Hintergrund

Die vorliegende Leitlinie schließt an das Positionspapier „Banken und FinTechs beziehen Stellung – Stichwort Outsourcing“ aus dem Jahr 2018 an, in welchem wir die Bedeutung sowie die Herausforderungen der Zusammenarbeit zwischen Banken und FinTechs beschrieben haben. Unter dem Begriff „FinTech“ werden hier alle jungen Unternehmen verstanden, die mit Banken zusammenarbeiten, um innovative, technologiebasierte Produkte und Leistungen zum Einsatz zu bringen.

In dem Positionspapier wurde u.a. zum Ausdruck gebracht, dass es für eine produktive Zusammenarbeit zwischen Banken und FinTechs einer Leitlinie bedarf, die sich auf „Nicht-leistungsspezifische bankaufsichtliche Anforderungen“ (NLBA) [1] bezieht. Unter bankaufsichtliche Anforderungen werden im Rahmen dieser Ausarbeitung die Mindestanforderungen an das Risikomanagement (MaRisk) der BaFin verstanden, auf die aus Praktikabilitätsgründen Bezug genommen wird.[2]

Die Anwendung der Leitlinie soll bezwecken, die Zusammenarbeit zwischen Banken und FinTechs effizienter und verlässlicher zu gestalten. Insbesondere soll hierdurch ein schnellerer time-to-market für jene Produkte und Dienstleistungen erreicht werden, die Banken und FinTechs gemeinsam entwickeln. Unser Anspruch ist es, dass unsere Mitglieder die Leitlinie problemlos in der Praxis anwenden können.

Die nachfolgenden Inhalte der Leitlinie wurden mit ausgewählten Mitgliedern von Banken und FinTechs des Bankenverbandes erarbeitet. Ferner hat eine Erprobung mit weiteren Mitgliedern stattgefunden. Auch wurden die Inhalte mit dem Prüfungsverband deutscher Banken erörtert. Zudem wurden Gespräche mit der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und der Deutschen Bundesbank geführt. Den methodische Ansatz, Anforderungen an FinTechs nach dem Risikogehalt der Geschäftsaktivitäten gestaffelt abzubilden, hält die BaFin für zweckmäßig.

Parallel zu unserem Projekt „Outsourcing-Leitlinie“ wurde durch die Europäische Bankenaufsichtsbehörde (EBA) eine überarbeitete Leitlinie zu Outsourcing veröffentlicht.[3] Unsere ersten

Analysen und Gespräche mit der BaFin deuten darauf hin, dass es zu Anpassungen an den MaRisk kommen wird. Da zum aktuellen Zeitpunkt nicht geklärt ist, in welchem Umfang die BaFin Anpassungen vornehmen wird, berücksichtigen die Inhalte zu diesem Dokument die EBA-Anforderungen nicht. Zu einem späteren Zeitpunkt ist geplant, eine Bewertung hinsichtlich möglicher notwendiger Anpassungen vorzunehmen.

Herausforderungen

Wenn Banken im Wettbewerb bestehen wollen, müssen sie ein sehr breites Öko-System bedienen. Sie müssen flexibel und schnell reagieren und daher besonders die Prozesse des Onboardings systematisch und schnell umsetzen können. FinTechs stellen für die digitale Transformation von Banken wichtige Partner dar, die mit konkreten Produkten und Lösungen den Transformationsprozess beschleunigen können.

Eine der größten Herausforderungen für die Zusammenarbeit zwischen Banken und FinTechs besteht darin, dass FinTechs häufig Anforderungen erfüllen müssen, die im Verhältnis zum tatsächlichen Risiko, das die Bank zu tragen hat, überproportional hoch sind. Synergien aus einer Kooperation hingegen lassen sich zeitlich häufig erst recht spät generieren und stehen in einem Missverhältnis zum Anfangsaufwand, der sich aus den gestellten Anforderungen ergibt (vgl. Abbildung 1, linke Seite).

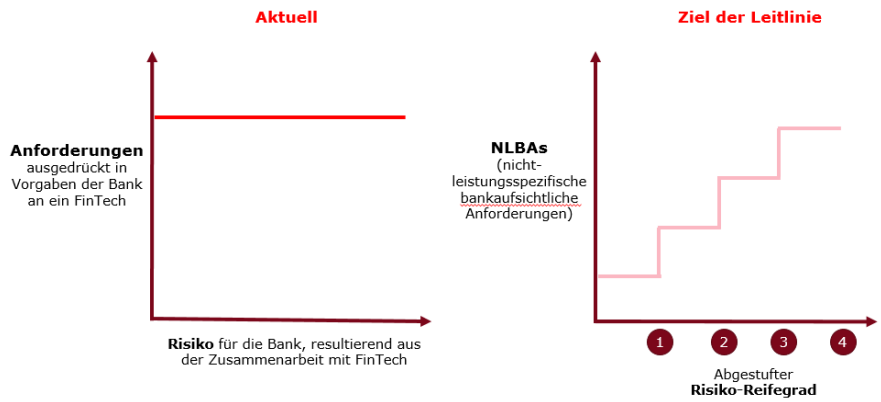


Abbildung 1: Aktuelles und angestrebtes Verhältnis von Risiko und Anforderungen in der Bank-FinTech-Zusammenarbeit

Des Weiteren stehen die FinTechs vor der Herausforderung, dass die von den Banken vorgenommenen Risikoeinschätzungen einer Kooperation nicht ausreichend transparent sind und sich dadurch die Anforderungen an das jeweilige FinTech (bei gleicher Dienstleistung bzw. gleichem Produkt) stark unterscheiden können. Selbst bei einfachen Ja- oder Nein-Fragen ist inhaltlich nicht immer klar, warum diese von der Bank gestellt werden und was konkret vom FinTech erwartet wird. Zudem ist insbesondere bei einer angestrebten Zusammenarbeit mit mehr als einer Bank zu berücksichtigen, dass sich die Risikoeinstufung, der Reifegrad, aber auch die Anforderungen

an das einzelne FinTech für gleiche Dienstleistungen sehr stark unterscheiden. Dies hat für das FinTech essentiell höhere Aufwände zur Folge.

Ergebnis der unklaren Anforderungen ist, dass das regulatorische/administrative Onboarding von FinTechs bei Banken meist 12-18 Monate dauert, während das „technische“ Onboarding nach wenigen Wochen abgeschlossen sein könnte.

Übergreifendes Ziel und Methodik

Unser Ziel ist es, die Zusammenarbeit zwischen Banken und FinTechs zu erleichtern und gleichzeitig zu beschleunigen. Die Leitlinie will dies mittels der Kombination aus den beiden nachfolgenden Schritten erreichen (vgl. Abbildung 1, rechte Seite):

i. Das Risiko aus der Zusammenarbeit von Bank und FinTech wird ermittelt und in einen entsprechenden Risiko-Reifegrad (RRG) überführt. Es gibt vier RRGe.
ii. Der RRG bestimmt die Stufe der Anforderungen, die erfüllt werden müssen. Im Anforderungskatalog werden für jeden Anforderungstypen in vier Stufen (eine Stufe pro RRG) spezifische Anforderungen festgelegt.

Wir sind der Überzeugung, dass die skizzierten Schritte (Details siehe nachfolgende Kapitel) einheitliche Erwartungen und somit auch eine bessere Vorbereitung auf die Zusammenarbeit von Banken und FinTechs zur Folge haben werden. Die daraus resultierenden Effizienzgewinne auf Seiten der Banken wie auch auf Seiten der FinTechs sollen zu einer verbesserten Wettbewerbsfähigkeit beider Partner führen und dadurch den Finanzstandort Deutschland (respekive Europa) stärken.

Angestrebte Ergebnisse

Die Outsourcing-Leitlinie des Bankenverbandes soll

1. unseren Mitgliedern mehr Sicherheit in der Auslegung und Anwendung des Proportionalitätsprinzips im Rahmen von Bank-FinTech-Auslagerungen geben,
2. als Unterstützung für die Ausgestaltung bankinterner Prozesse und Anweisungen dienen und
3. für FinTechs eine Grundlage darstellen, die an sie gestellten Anforderungen besser zu verstehen und sich dadurch zielgerichteter auf die Zusammenarbeit mit Banken vorbereiten zu können.

Je häufiger die Leitlinie in der Praxis angewendet wird, desto besser lassen sich die mit ihr verbundenen Ziele – die Zusammenarbeit zwischen Banken und FinTechs effizienter und verlässlicher zu gestalten und dabei auch einen schnelleren time-to-market zu ermöglichen – erreichen. Wir ermuntern daher neben unseren Banken und FinTechs auch deren Prüfer, sich intensiv mit der Leitlinie auseinanderzusetzen.

Zudem möchten wir die Leitlinie fortlaufend weiterentwickeln. Daher soll sie nach Erproben in der Praxis in eine laufende Überprüfung und gegebenenfalls Anpassung überführt werden.

Überblick über die Leitlinie

Die Leitlinie wurde auf Grundlage von geltenden regulatorischen Anforderungen sowie Best Practices erarbeitet. Sie basiert auf den zwei Teilsegmenten „RRG-Modell“ (i) und „Anforderungskatalog“ (ii). Die Teilsegmente sind nacheinander anzuwenden.

Das RRG-Modell dient der Risikoeinstufung der Bank-FinTech-Zusammenarbeit in vier einzelne RRGe. Zur Ermittlung der RRGe ist ein Fragenkatalog mit 18 Fragen zu beantworten. Die Fragen unterteilen sich in Risiko- und Auswirkungsfragen. Bei jeder Frage kann aus verschiedenen Antwortoptionen ausgewählt werden. Aus der jeweils gewählten Option resultiert eine Punktzahl, die im Anschluss gewichtet wird. Die Gesamt-Risiko-Punktzahl und die Gesamt-Auswirkungs-Punktzahl werden multipliziert, um eine Gesamt-Punktzahl zu erhalten. Diese Gesamt-Punktzahl entspricht einem der vier RRGe, die sich jeweils in einer Spannbreite „von … bis …“ bewegen.

Der Anforderungskatalog ist ein Katalog konkreter, risikoproportionaler Anforderungen, die ein FinTech in einer bestimmten Bank-Kooperation zu erfüllen hat.

Die Anforderungen sind analog ebenfalls in vier Stufen unterteilt, wobei jede Stufe einem RRG zugewiesen ist, d.h. für RRG 1 sind in Stufe 1 „x“ Anforderungen zu erfüllen; für RRG 2 sind in Stufe 2 „y“ Anforderungen zu erfüllen. Die formulierten Anforderungen bauen aufeinander auf.

Das Vorgehen sowie die Segmente wurden mittels Use Cases (UCs) auf ihre Praxistauglichkeit erprobt. Die UCs stellen einen unmittelbaren, praktischen Bezug zu tatsächlich existierenden Fallkonstellationen einer Zusammenarbeit zwischen Bank und FinTech her.

Leitlinienmodell im Detail: Risiko-Reifegradmodell

Erläuterung der Logik des Risiko-Reifegradmodells

Übersicht

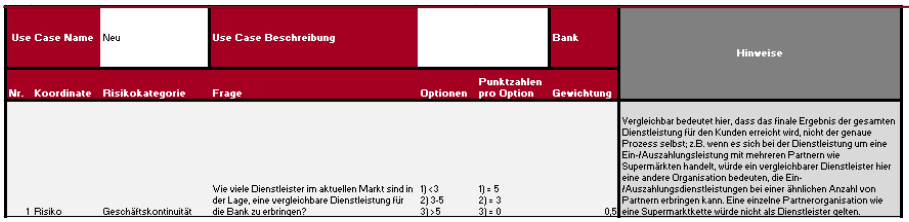
Das RRG-Modell dient der differenzierten und leistungsspezifischen Risikoeinschätzung der zu erbringenden Dienstleistung eines FinTechs. Ziel ist es, mithilfe eines Fragenkatalogs einen entsprechenden RRG zu ermitteln.

Da die Zusammenarbeit zwischen Banken und FinTechs oft viel dynamischer ist als jene zwischen Banken und traditionellen Dienstleistern, ist vorgesehen, dass – abhängig von der Intensivierung des Leistungsbezugs bzw. der Zusammenarbeit – die RRG-Bewertung anhand des RRG-Modells regelmäßig durchgeführt wird. Somit können sich auch die entsprechenden Anforderungen ändern.

Der Fragenkatalog

Das Kernstück des RRG-Modells bildet ein Fragenkatalog von 18 Fragen zur Einordnung einer Leistungsbeziehung von FinTech und Bank in einer der vier RRGe. Der Fragenkatalog wurde nach den folgenden Kriterien erstellt:

- Eindeutigkeit der Fragen und Antwortoptionen für den Anwender;
- Relevanz aller Fragen am Beispiel etablierter UCs von Banken mit FinTechs;
- schnelle Einordnung von UCs in einen RRG;
- Transparenz und Handlungssicherheit über Einstufung in eine RRG für FinTechs und Banken;
- Allgemeingültigkeit im Sinne der Anwendbarkeit auf die jeweiligen Einzelfälle der unterschiedlichen (beteiligten) Banken



Use Case Name	Neu	Use Case Beschreibung		Bank	Hinweise
Nr.	Koordinate	Risikokategorie	Frage	Optionen	Punktzahlen pro Option	Gewichtung	
1	Risiko	Geschäftskontinuität	Wie viele Dienstleister im aktuellen Markt sind in der Lage, eine vergleichbare Dienstleistung für die Bank zu erbringen?	1) <3 2) 3-5 3) >5	1) = 5 2) = 3 3) = 0	0,5	Vergleichbar bedeutet hier, dass das finale Ergebnis der gesamten Dienstleistung für den Kunden erreicht wird, nicht der genaue Prozess selbst; z.B. wenn es sich bei der Dienstleistung um eine Ein-/Auszahlungsleistung mit mehreren Partnern wie Supermärkten handelt, würde ein vergleichbarer Dienstleister hier eine andere Organisation bedeuten, die Ein-/Auszahlungsdienstleistungen bei einer ähnlichen Anzahl von Partnern erbringen kann. Eine einzelne Partnerorganisation wie eine Supermarktkette würde nicht als Dienstleister gelten.

Abbildung 2: Beispiel Frage vom Fragenkatalog *(siehe Anhang 1, Blatt 1 für den Gesamtkatalog)*

Die Fragen wurden in einem strukturierten Ansatz entwickelt. (Die Methodik der Herleitung ist im Kapitel „Validierungsprozess des Risiko-Reifegradmodells“ näher erläutert.)

Auf der Basis der allgemeingültigen Risikokategorien einer Dienstleistung:

- Geschäftskontinuität,
- aufsichtsrechtliche Anforderungen,
- Leistungserbringung seitens FinTech,
- Leistungserbringung seitens Bank,
- Informationssicherheit

wurden entsprechende Fragen- und Antwortoptionen zusammengestellt. Die fünf Risikokategorien ermöglichen sowohl die eindeutige Strukturierung der Fragen als auch die Gewährleistung eines hohen Abdeckungsgrades des RRG-Modells. Um eine hohe Güte des Ergebnisses sicherzustellen, ist es unumgänglich, alle 18 Fragen zu beantworten.

Jede Frage ist einer der Koordinaten des Modells „Risiko“ oder „Auswirkung“ zugeordnet.[4] Die Bandbreite der Fragen wird bei dem Thema „Informationssicherheit“ besonders deutlich: Die fünf Fragen decken die Art des Server Hostings, die Region der Serverstandorte, die Datenklassifizierung, das Niveau der Datengenauigkeit und die Auswirkungen einer Datenschutzverletzung ab.

Darüber hinaus wurden die Fragen und Antworten dediziert auf die Leistungsbeziehung von FinTechs (im Vergleich zu traditionellen Dienstleistern) zugeschnitten.

- Die Zahl der Antwortoptionen wurde an den kleinen FinTech-Markt angepasst, sprich: gegenüber vergleichbaren Dienstleistern im Markt entsprechend reduziert.[5]
- Die Frage der finanziellen Stabilität des FinTech zielt, abweichend von den gängigen Prüfmodellen der Banken, auf die Dauer des Fundings in Verbindung mit der Gesellschafterstruktur ab.

Jede Frage ist mit Antwortoptionen hinterlegt und – wo notwendig – zur Sicherstellung größtmöglicher Transparenz mit zusätzlichen Hinweisen erläutert. Wenn die Optionen – zum Beispiel „niedrig“, „mittel“ und „hoch“ – ohne weitere Erläuterung erscheinen, soll es für diese Fragen keine quantitative Abstufung geben, da dies je Bank individuell ist. Es sollte aber in der gelebten Praxis dazu führen, dass die Bank dem FinTech

erklärt, warum die Einschätzung so ausfällt. Dies sorgt für Transparenz und gegenseitiges Verständnis.

Aus der Beantwortung der Fragen ergeben sich die einzelnen Punktzahlen, die entsprechend der Bedeutung für die Banken im Rahmen des Projektes noch einmal gewichtet und damit praxisnah justiert werden (Standard = 1, Minimum = 0,5, Maximum = 4). Die gewichteten Einzel-Punktzahlen ergeben in der Summe jeweils eine Gesamtrisiko- und eine Gesamtauswirkungs-Punktzahl, wobei in beiden Koordinaten jeweils eine Maximal-Punktzahl von 50 erreicht werden kann.

Frage 18 ist von besonderer Bedeutung, da sie quasi außerhalb des RRG-Modells liegt; sie dient dazu, den RRG, der aus den vorangegangenen 17 Fragen ermittelt wurde, entsprechend dem Risikoappetit der Bank potenziell nach oben anzupassen. Sie ist eine Ja-Nein-Frage, bei der die Option „Ja“ den Effekt hat, die Risikopunktzahl zu erhöhen (mit der Option „Nein“ kann aus den anderen Fragen immer noch die Gesamtrisiko-Punktzahl von 50 erreicht werden). Dieser Ansatz ist deshalb sinnvoll, weil im Rahmen der Erprobungen festgestellt wurde, dass UCs zu einem RRG führen können, der nicht der Bedeutung in der Praxis entspricht: Der ermittelte RRG war geringer als die Einstufung der Vertragsbeziehung durch die Bank. Dies ist aufgrund der verschiedenen Geschäftsmodelle der Banken plausibel (im vorliegenden Fall White-Label-Bank) und spiegelt sich auch in dem prinzipienorientierten Ansatz bankaufsichtlicher Anforderungen wider.

Das Risiko-Reifegradmodell konkret

Die beiden dem RRG-Modell zugrunde liegenden Koordinaten „Risiko“ und „Auswirkung“ erlauben es nicht nur, das Risiko der spezifischen FinTech-Dienstleistung für die Bank einzuschätzen, sondern darüber hinaus auch die zu erwartenden Auswirkungen der Dienstleistungs- und Dienstleisterrisiken auf die Bank mit einzubeziehen.

Beispielhaft bedeutet dies (bei gleichen absoluten Punktzahlen), dass eine FinTech-Dienstleistung mit einer hohen Risiko-Punktzahl und einer geringen Auswirkungs-Punktzahl in den gleichen oder ähnlichen RRG eingestuft wird wie eine FinTech-Dienstleistung mit einer geringen Risiko-Punktzahl und einer hohen Auswirkungs-Punktzahl.

Im grafischen Modell werden nach der Beantwortung des Fragenkatalogs die Gesamtrisiko- und Gesamtauswirkungs-Punktzahlen getrennt auf der x-Achse (Risiko) und der y-Achse (Auswirkung) erfasst. Hieraus ergibt sich der jeweilige RRG der spezifischen FinTech-Dienstleistung für die Bank.

Insgesamt wurden, abhängig von den Punktzahlen, vier RRGe definiert, die grafisch im Koordinatensystem als Kurven abgetragen und farblich von „grün“ (RRG 1=Minimum) bis „rot“ (RRG 4=Maximum) dargestellt werden.

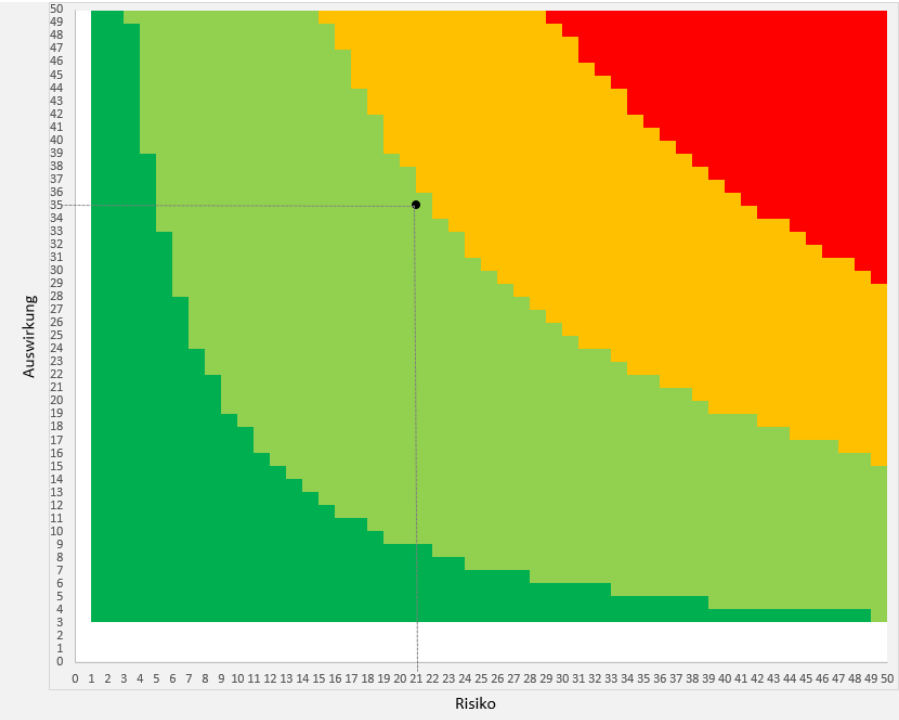


Abbildung 3: Risiko-Reifegradmodell

Für die einzelnen RRG ergeben sich die Schwellwerte als Produkt aus Risiko- und Auswirkungs-Punktzahl wie folgt:

Abbildung 4: Risiko-Reifegrade udn Schwellwerte

Der in Abbildung 3 dargestellte RRG eines Beispiels berechnet sich daher folgendermaßen:

Risiko (21) x Auswirkung (35) = 735, was RRG 2 entspricht.

Nach erfolgter RRG-Bestimmung können die Anforderungen an das FinTech direkt im Anforderungskatalog vertikal abgelesen werden. Risikoadjustiert erhöhen sich die Anforderungen sukzessive von RRG 1 bis RRG 4. Die Anforderungen nehmen grundsätzlich direkten Bezug zu den regulatorischen Maximalanforderungen an Auslagerungen.

Beschreibung Risiko-Reifegrade

Nachfolgende Beschreibungen zu den RRGe sind beispielhaft und dienen der Veranschaulichung im RRG sowie der Abstufung der RRGe untereinander.

Risiko-Reifegrad 1

Unter RRG 1 ist die risikoärmste Stufe der Zusammenarbeit zwischen FinTech und Bank zu verstehen. In diesem RRG wird die Leistung des FinTechs im Regelfall einen nur eingeschränkten Produktumfang oder begrenzten Nutzerkreis umfassen. Leistungen dieses RRGs sind gegebenenfalls nicht als Auslagerung im Sinne des § 25b KWG/MaRisk AT9 einzustufen, soweit nicht mit echten Kundendaten produktiv gearbeitet wird.

Risiko-Reifegrad 2

Im RRG 2 befindet sich die Kooperation zwischen FinTech und Bank bereits in einem fortgeschrittenen Stadium. Der Leistungsumfang bzw. die Leistungsreichweite im Kundenstamm oder bei den internen Prozessen der Bank ist zwar eingeschränkt, aber bei überschaubarem Risiko weiter gefasst als im RRG 1. Die Dienstleistung des FinTechs besteht weitgehend eigenständig und ist wenig verzahnt mit der System- und Prozesswelt der Bank. Die Leistung kann als Auslagerung gem. § 25b KWG/MaRisk AT9 eingestuft sein. Im Regelfall wird es sich hierbei um eine nicht-wesentliche[6] Auslagerung handeln.

Risiko-Reifegrad 3

Der RRG 3 beschreibt eine weit fortgeschrittene Kooperation zwischen FinTech und Bank, bei der die Ausprägung oder das Umfeld der Leistung ein erhöhtes Risiko für die Bank darstellt, beispielsweise aufgrund enger rechtlicher Vorgaben an die Leistung, einer höheren Abhängigkeit vom FinTech oder aufgrund des erweiterten Leistungsumfangs. Die Einbindung in die System- und Prozesswelt der Bank ist in der Regel (weit) fortgeschritten und die Leistung steht einer Vielzahl von Bankkunden mit unterschiedlichstem Leistungsumfang zur Verfügung bzw. hat umfangreiche Auswirkungen auf die internen Prozesse der Bank. Darüber hinaus ist die Leistung sehr wahrscheinlich auch als Auslagerung im Sinne von § 25b KWG/MaRisk AT9 einzustufen und weist in diesem Aspekt erhöhte Risikoeinschätzungsnotwendigkeiten auf. Bankspezi-

fisch kann es sich hierbei bereits um eine als wesentlich eingestufte Auslagerung handeln.

Risiko-Reifegrad 4

Die Kooperation zwischen FinTech und Bank hat die höchste Ausprägung erreicht. Aus dem Risiko, also der vom FinTech bereitgestellten Leistung, ergibt sich eine hohe Risikorelevanz für die Bank, zum Beispiel dadurch, dass das Leistungsangebot vom für den überwiegenden Teil der Bankkunden genutzt wird und die Kunden alternativlos auf die Dienstleistung angewiesen sind. Weiterhin könnte die Leistung des FinTechs zwingend erforderlich sein, um Kernbankprozesse durchzuführen oder zu unterstützen, zum Beispiel den Zahlungsverkehr oder Wertpapiertransaktionen. Im RRG 4 wird die Leistung üblicherweise als wesentliche Auslagerung gem. § 25b KWG/MaRisk AT9 bewertet.

Leitlinie im Detail: Anforderungskatalog

Abgrenzung NLBA von LBA

In der Einleitung dieses Dokuments wurde darauf hingewiesen, dass sich diese Leitlinie auf „Nicht-leistungsspezifische bankaufsichtliche Anforderungen“ (NLBA) bezieht. Um die Leitlinie übersichtlich zu halten, wird nur auf „Anforderungen“ und einen „Anforderungskatalog" verwiesen, doch gemeint sind immer NLBA. Daher ist es angebracht, diesen Begriff weiter zu erläutern.

NLBA grenzen sich von den „Leistungsspezifischen bankaufsichtlichen Anforderungen“ (LBA) dadurch ab, dass sie unabhängig von spezifischen Produkten als generelle Anforderungen der Banken an FinTechs gerichtet werden. Mehrheitlich handelt es sich dabei um Anforderungen an die ordnungsmäßige Geschäftsorganisation (basierend auf KWG §25a) sowie um regulatorische Anforderungen mit unmittelbarem Bezug zur Auslagerung (beispielsweise gemäß MaRisk).

Hieraus ergibt sich der Vorteil, unabhängig von der individuellen Zusammenarbeit eines FinTechs mit einer Bank vereinheitlichte Anforderungen an die FinTechs zu adressieren, da beispielsweise für die Einhaltung des Business Continuity Managements immer bestimmte Voraussetzungen zu erfüllen sind.

Durch eine vierstufige Aufteilung der Anforderungen (RRG 1 = Stufe 1 bis RRG 4 = Stufe 4) wird eine einheitliche Orientierungshilfe zur Implementierung dieser Anforderungen beim FinTech geschaffen.

Anforderungen wie zum Beispiel die Ausgestaltung von Verträgen oder die Vereinbarung von Service Levels sind im Gegensatz dazu als LBA zu sehen. Auch Anforderungen im Hinblick auf den EU-Datenschutz und die Geldwäscheprävention gehören zu den LBA, weil sie von sehr spezifischen

Aspekten der Zusammenarbeit abhängig sind. Für solche LBA ist es nicht möglich, eine Abstufung per RRG vorzunehmen. Sie bleiben daher im Rahmen dieser Leitlinie unberücksichtigt.

Herleitung der Anforderungen und deren Abstufung

Der Anforderungskatalog enthält die folgenden Anforderungstypen, die einen wesentlichen Bestandteil der auslagerungsrelevanten bankaufsichtlichen Anforderungen umfassen.

1) Business Continuity Management,
2) interne Kontrollen,
3) Informationssicherheit, unterteilt in
    a. Governance,
    b. Berechtigungskonzept,
    c. physische Sicherheit,
4) Organisationsrichtlinien und Dokumentation,
5) Revisionstätigkeit,
6) Vendormanagement.

Der folgende Abschnitt beschreibt die grundsätzliche Methodik zur Herleitung und Abstufung der Anforderungstypen. Er umfasst die Benennung der Standards, aus denen die Anforderungen grundsätzlich abgeleitet werden, und die Dimensionen, die für die Untergliederung und Abstufung der Anforderungen notwendig sind. Eine detaillierte Darstellung der im Fokus dieser Dokumentation befindlichen Anforderungstypen sowie deren ausformulierte Anforderungen je Stufe finden sich im Anhang 1, Blatt 3.

Ausgangspunkt für die Beschreibung der durch das FinTech einzuhaltenden und durch die Bank sicherzustellenden Anforderungen für die jeweiligen Anforderungstypen ist stets die für die jeweilige Bank geltende Regulatorik.

In Deutschland zugelassene Kreditinstitute haben nach § 25a Abs. 1 KWG „Besondere organisatorische Pflichten“ sicherzustellen, die wiederum durch weitere Verwaltungsvorschriften – wie das Rundschreiben der BaFin zu den Mindestanforderungen an das Risikomanagement (MaRisk) – oder durch internationale bzw. nationale Sicherheitsstandards konkretisiert werden. Beispiele für Sicherheitsstandards sind der IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder der internationale Sicherheitsstandard ISO/IEC 2700X der International Organization for Standardization. Den betrachteten Anforderungstypen dieser Dokumentation liegen (beispielhaft) die folgenden Standards zugrunde.

Anforderungstyp	Mindeststandard
Business Continuity Management (BCM)	AT 7.3 MaRisk – „Notfallkonzept“; BSI-Standard 100-4
Internes Kontroll-system (IKS)	AT 4.3 MaRisk – „Internes Kontrollsystem“; COSO Rahmenwerk[7]
Informationssi-cherheit (IS) ■ Governance ■ Berechitugngs-konzept ■ Physische Sicherheit	AT 7.2 Abs. 1 und 2 MaRisk „Technischor-ganisatorische Ausstattung“; Bankaufsichtliche Anforderungen an die IT (BAIT), insbesondere Abschnitt 2 bis 5 ITGrundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI), insbesondere BSI-ISO 27001 Ggf. weitere internationale Standards wie NIST, PCI, DSS

Die aufgeführten Standards setzen für den jeweiligen Anforderungstyp stets die maximale Anforderung und geben somit den Rahmen für die Stufe 4 vor. Daraus sollte allerdings nicht geschlossen werden, dass die Standards endgültig oder allumfassend sind. Der Feedback-Review-Zyklus (siehe Kapitel „Ausblick“) der vorliegenden Leitlinie ermöglicht Anpassung der Standards.

Grundsätzlich gilt für Stufe 4, dass der Grad der Kooperation von FinTech und Bank sehr hoch ist (siehe Kapitel „Beschreibung Risiko-Reifegrade“) und somit Prozesse und Datenströme als eng verzahnt anzusehen sind. Sofern Prozesse oder Systeme bei einem Beteiligten fehlerhaft agieren oder sogar ausfallen, ist folglich mit einer unmittelbaren Auswirkung (Ansteckung) auf den Kooperationspartner zu rechnen. Dementsprechend sind in Stufe 4 die höchsten Sorgfaltspflichten anzusetzen, die sich wiederum aus der Konkretisierung der für Banken geltenden „Besonderen organisatorischen Pflichten“ ergeben.

> *Am Beispiel des Anforderungstyps „Informationssicherheit – Governance“ und wie im Anhang 1 weiter beschrieben wäre die Governance u.a. entsprechend den Prinzipien und Anforderungen des IT-Grundschutzkatalogs des BSI, insbesondere der BSI-ISO 27001, auszugestalten. Dies würde u.a. bedeuten, eine eigenständige Organisationseinheit einzurichten und für die Tätigkeit qualifiziertes Personal abzustellen, das sich mit Themen der Informationssicherheit befasst und diese im Tagesgeschäft sicherstellt.*

Die Organisationseinheit hätte entsprechende Risikomanagement-, Störfallmanagement- oder Schulungsprozesse zu definieren, zu dokumentieren, durchzuführen und zu etablieren.

Für den Anforderungstyp „Business Continuity Management“ (BCM) hätten Banken beispielsweise dem deutschen BSI-Standard 100-4 zum Notfallmanagement zu folgen. In Stufe 4 wären dann für die Zwecke des Notfallmanagements der grundsätzliche BCM-Regelkreis umzusetzen, sodass BCM-Pläne in Bezug auf Gebäude, IT und Personen zu beschreiben sowie die entsprechenden BCM-Pläne des FinTechs und der Bank aufeinander abzustimmen wären. Ferner wären dazu Krisenhandbücher, Richtlinien, Organisationscharts sowie Kontaktdetails für den Krisenfall anzufertigen.

Ausgehend von Stufe 4 ergeben sich die weiteren Stufen. Hierzu sind die Mindestanforderungen von Stufe 4 risikoorientiert unter Berücksichtigung der Dimensionen „Grad der organisatorischen Bedeutung“ und „Grad der strukturellen Umsetzung“ bis auf Stufe 1 abzustufen. Die Einführung der beiden Dimensionen ist notwendig, um letztlich die Nachvollziehbarkeit für Dritte – v.a. Banken, Aufsichtsbehörden und Prüfungsgesellschaften – zu gewährleisten und der teilweise subjektiven Experteneinschätzung zwischen RRG 1 und 4 objektive Bandbreiten zu geben.

Der Grad der organisatorischen Bedeutung ordnet die einzelnen Mindestanforderungen aus Stufe 4 implizit den für einen (Risiko-)Management-Kreislauf wesentlichen Bestandteilen (A) Governance (einschl. Wissenstransfer/Training), (B) Identifizierung, Steuerung und Überwachung sowie (C) Validierung und Anpassung zu. Diesen Kategorien wird dann untereinander ein relativer Rang zugewiesen. Eine hohe Bedeutung kommt dabei (A) und (B) zu, während (C) eine niedrigere Bedeutung hat. Bestandteile mit einer hohen relativen Bedeutung sind grundsätzlich auch in den unteren RRG-Anforderungen aufzunehmen, während dies für Bestandteile mit einer niedrigen Bedeutung nicht erforderlich ist (vgl. Abbildung 5).

	(A)	(B)	(C)
Stufe 4	X	X	X
Stufe 3	X	X	X
Stufe 2	X	X	(X)
Stufe 1	(X)	(X)	

Abbildung 5: Anforderungen je Risiko-Reifegrad

Während der Grad der organisatorischen Bedeutung darauf abzielt, Anforderungen grundsätzlich zu definieren, steht der Grad der strukturellen Umsetzung für eine qualitative Dimension im Sinne einer qualitativ umfangreichen bzw. vereinfachten Umsetzung. Ein hoher Grad der strukturellen Umsetzung analog Stufe 4 erfordert eine strukturierte, umfassende oder standardisierte Umsetzung, während für einen niedrigen Grad, wie in Stufe 1, eine einzelfallbasierte oder vereinfachte Implementierung ausreichen würde. Allerdings bleibt für die Abstufung zwischen den beiden Extremen (4 und 1) unverändert eine grundsätzliche Experteneinschätzung unabdingbar, da die Dimension letztlich nur die Bandbreiten für die Abstufung vorgibt (vgl. Abbildung 6). Diese ist in jedem Fall durch die Bank ausreichend zu begründen.

Abbildung 6: Grad der strukturellen Umsetzung je Risiko-Reifegrad

Rückgreifend auf die beiden zuvor angeführten Beispiele zu „Informationssicherheit – Governance“ und „BCM“, ergeben sich daraus die folgenden beispielhaften Abstufungen.

> *Im Falle des Anforderungstyps „Informationssicherheit – Governance“ bleiben über alle RRG die Mindestanforderungen mit einer hohen organisatorischen Bedeutung bestehen.*

Das bedeutet im Einzelfall, dass unter (A) „Governance“"immer ein Information Security Officer zu benennen ist, der je nach RRG in der strukturellen Umsetzung von Vollzeitarbeitskraft auf Teilzeitarbeitskraft abgestuft wird. Weiter bedarf es entsprechender Rahmenwerke oder Richtlinien, die ebenfalls qualitativ differenziert werden. In Stufe 3 wird noch ein Aktualisierungs- und Genehmigungsprozess zu allen Dokumenten gefordert, während in Stufe 2 das Vorhandensein entsprechender Dokumente genügt und in Stufe 1 sogar eine generelle Richtlinie ausreichen würde.

Unter (B) „Identifizierung, Steuerung und Überwachung“ bleiben als Kernbestandteile über alle RRG der Joiner-Mover-Leaver-Prozess (Zugriffs- und Zutrittsrechte) sowie das Störfallmanagement eine Grundanforderung an das (kooperierende) FinTech. Eine Abstufung erfolgt dabei ebenfalls in der Dimension der strukturellen Umsetzung, im Sinne der Qualität und der Anzahl an Maßnahmen; beispielsweise werden in Stufe 3 zusätzlich eine Funktionstrennung sowie ein Sicherheitsrisikomanagement in Bezug auf Identifizierung und Verhinderung gefordert. Ferner ist das Störfallmanagement in Stufe 1 nur noch individuell für den Einzelfall durchzuführen und nicht strukturiert wie in den übrigen RRG.

Für (C) „Validierung und Anpassung“ reduzieren sich die umfangreichen Anforderungen der Stufe 4 entsprechend dem Grad ihrer organisatorischen Bedeutung auf vereinfacht umzusetzende Anforderungen, sodass in RRG 3 lediglich Rahmenwerke und Richtlinien zu überprüfen und zu aktualisieren sind und in den folgenden Stufen (RRG 1 und 2) diese Tätigkeiten nicht mehr als harte Mindestanforderungen gelten. Hintergrund ist die nicht-systematische und nicht eng verzahnte Kooperation zwischen FinTech und Bank und das damit geringe bzw. marginale Risiko für die Prozesse oder den operativen Betrieb der Bank.

In Hinblick auf den Anforderungstyp „BCM“ ergibt sich ein ähnliches Bild. Über die Stufen 2 und 3 bleiben unverändert Anforderungen für (A) Governance und (B) Identifizierung, Steuerung und Überwachung, zum Beispiel BCM-Prozesse oder BCM-Pläne, bestehen. Jedoch unterscheiden sich die Anforderungen wie bereits bei „Informationssicherheit – Governance“ nach Grad der strukturellen Umsetzung. BCM-Prozesse müssen entsprechend der Risikoeinschätzung beispielsweise in Stufe 3 vollständig; in Stufe 2 vereinfacht („bekannt und eingeschränkt“) implementiert sein.

Ferner gelten abweichend zum Beispiel „Informationssicherheit – Governance“ für die Stufe 1 keinerlei Mindestanforderungen. Unter der Annahme, dass in diesem RRG kein systematischer Austausch von (Test-) Daten erfolgt und sich eine Kooperation und erste Verzahnung von Prozessen zwischen FinTech und Bank erst in der Anbahnung befinden, ergibt sich folglich auch kein Risiko für die Bank oder ihre Geschäftsprozesse im Falle eines Notfalls beim FinTech.

Ein etwaiges Testing der BCM-Pläne als Maßnahme der Kategorie (C) „Validierung und Anpassung“ wäre sowohl in Stufe 3 und 2 durchzuführen, würde aber ebenfalls über den Grad der strukturellen Umsetzung abgestuft werden. In Stufe 3 wären derartige Tests regelmäßig unter Abstimmung mit der Bank durchzuführen, während in Stufe 2 diese nicht mehr systematisch, sondern gegebenenfalls im Einzelfall zu erfolgen hätten.

Anwendung in der Praxis

Für die Anwendung in der Praxis möchten wir im Folgenden einige konkrete Empfehlungen aussprechen.

Anwendung in Grenzfällen

In Fällen, in denen ein RRG-Ergebnis an der Schwelle zum nächst höheren RRG liegt, werden im Regelfall die Anforderungen der höheren Stufe risikoorientiert herangezogen. Dies kann zu mehr Aufwand seitens des FinTechs führen. Allerdings ist dies immer dann zweckdienlich, wenn sich die Zusammenarbeit zwischen Bank und FinTech perspektivisch weiterentwickeln soll, da mit zunehmender Einbindung der FinTech-Dienstleistung das Risiko sowie die Auswirkung für die Bank und damit zugleich auch die zu erfüllenden Anforderungen steigen.

Darüber hinaus gilt zu beachten, dass es bei der individuellen Betrachtung der Bank-FinTech-Zusammenarbeit notwendig sein kann, einen Anforderungstyp auf einer höheren Stufe abzustellen, als dies die eigentliche RRG-Einstufung erfordert (konservative Betrachtung). Beispielsweise kann eine Geschäftskontinuitäts-Anforderung über den bei anderen Anforderungstypen erforderlichen Grad hinausgehen; es wird dann von der generellen RRG-Einstufung zu dieser spezifischen Anforderung abgewichen (z.B. kann die FinTech-Dienstleistung insgesamt im RRG 2 liegen, hat aber abweichend die Stufe 3 hinsichtlich BCM zu erfüllen). Diese Vorgehensweise trägt den komplexen Möglichkeiten einer Bank-FinTech-Zusammenarbeit und den vielschichtigen regulatorischen Anforderungen Rechnung. Es muss jedoch erwähnt werden, dass diese Abweichung nicht der Regelfall sein sollte.

Empfehlung an Banken

1. **Implementierung der Leitlinie in die Praxis des Auslagerungsmanagements- und controllings einer Bank:** Vor der Einführung der Leitlinie in das bankeigene Auslagerungsmanagement empfiehlt sich ein Erproben der Leitlinie mit den in der Bank bestehenden Verfahren und Methoden anhand von konkreten Auslagerungssachverhalten der Bank. Auch kann es zunächst ratsam sein, für die Bewertung einer Bank-FinTech-Auslagerung parallel sowohl die bestehenden Verfahren als auch die Leitlinie zu verwenden. Weiterhin empfiehlt sich die frühzeitige Einbindung der Geschäftsleitung sowie der relevanten Funktionen (Risikocontroling-Funktion, Compliance, Interne Revision, Informationssicherheits- und Datenschutzbeauftragter), da diese die Risikostrategie und -tragfähigkeit der Bank verantworten und die Anwendung der Leitlinie vertreten müssen.

2. **Anwendung der Leitlinie für einzelne Bank-FinTech-Auslagerungen – eine individuelle Betrachtung bleibt unabdingbar:** Auch wenn durch die Leitlinie eine Grundlage für eine einheitlichere Behandlung bestimmter Anforderungstypen über Banken hinweg geschaffen werden soll und sie sich mit dem RRG einer anschaulichen und einfachen Methodik bedient, bleibt festzuhalten, dass eine individuelle Analyse des jeweiligen Auslagerungssachverhalts durch die Bank und gegebenenfalls notwendige konkrete Anpassungen bei den Anforderungen an das FinTech durchaus möglich sind. Deshalb sollte der RRG (und die entsprechende Anforderungsgüte) als ein Orientierungspunkt verstanden werden, der durch zahlreiche Praxiserfahrungen und das Erproben anhand konkreter UCs abgeleitet wurde. Dies bedeutet jedoch nicht, dass Anforderungen über verschiedene Anforderungstypen hinweg zwangsweise immer nur innerhalb desselben RRGs entnommen werden können. Insofern es die konkrete Ausgestaltung der Bank-FinTech-Zusammenarbeit und die damit einhergehende Risikoeinschätzung erfordern, können bei einzelnen Anforderungstypen auch Anforderungen aus einer geringeren bzw. höheren Stufe sinnvoll sein.

3. **Laufende Überwachung der FinTech-Auslagerung und regelmäßige „Neu“-Bewertung des RRG:** Geschäftsbeziehungen zwischen Banken und FinTechs sowie die damit einhergehenden Auslagerungssachverhalte entwickeln sich unter Umständen dynamischer, als dies bei „klassischen“ Auslagerungen der Fall ist. Insbesondere bei Ausla-

gerungen an FinTechs, für die zum Start der Kooperation zunächst ein geringer RRG festgestellt wurde und bei denen daher eine geringere Stufe von Anforderungen für das FinTech gelten, kann eine regelmäßige „Neu“-Bewertung des RRGs erforderlich sein, um sicherzustellen, dass die Umsetzung der Anforderungen auf FinTech-Seite proportional zum Risiko der Bank erfolgt. Zudem könnte es bestimmte Anlässe geben, bei denen es erforderlich ist, andere Modelle und Prozesse zur Bewertung bzw. Steuerung der Kooperation zu nutzen. Anlässe für Änderungen an der Serviceleistung könnten sein:

a. Zusätzlicher Service außerhalb der EU
b. Umgebung für Cloud-Dienste wird gewechselt
c. Risikoappetit der Bank ändert sich; z.B. weil der Marktanteil oder der Revenue-Anteil basierend auf der Dienstleistung des FinTech steigt
d. FinTech wird aufgekauft / Änderung der Gesellschafterstruktur

Empfehlung an FinTechs

Für FinTechs bieten sich drei konkrete Anwendungsmöglichkeiten der Leitlinie an, die sich über verschiedene Unternehmensphasen erstrecken:

1. **Von der Gründungsphase bis zur Marktreife - Wissensvermittlung und frühzeitiger Einbezug von Anforderungen in die Unternehmensplanung:** Insbesondere in der frühen Unternehmensphase verfügen FinTechs oft nur über geringes Wissen und wenige Erfahrungen bezüglich bankaufsichtsrechtlicher Anforderungen und deren Umsetzung bei Auslagerungen. Die Leitlinie kann daher als eine praxisorientierte Informationssammlung und handlungsorientierte Anleitung aus der Anwendersicht eines FinTechs genutzt werden. Die Leitlinie eignet sich konkret, um frühzeitig Anforderungstypen zu identifizieren und einen planbaren Weg – im Sinne einer Roadmap zur Einhaltung aufsichtsrechtlicher Anforderungen – aufzuzeigen. Bankaufsichtliche Anforderungen können dadurch frühzeitig und laufend im Rahmen der Ressourcenplanung und -allokation sowohl in der Produktentwicklung als auch für den organisatorischen Aufbau des FinTechs berücksichtigt werden.

2. **Vorbereitung auf konkrete Kooperationen mit Banken und ständige Begleitung innerhalb einer Geschäftsbeziehung:** Die Leitlinie bietet FinTechs die Möglichkeit, nach bestem Wissen ein „Self-Assessment“ durchzuführen und dabei die Perspektive der Bank einzunehmen, um konkrete aufsichtsrechtliche Anforderungen, die für die

Zusammenarbeit mit der Bank zu erwarten sind, abzuleiten. Dies kann wiederum dazu genutzt werden, um bereits im Rahmen der Geschäftsanbahnung einen Soll-Ist-Abgleich zwischen zu erwartenden Anforderungen und bestehender Umsetzung durchzuführen und somit mögliche Handlungs- und Anpassungsbedarfe frühzeitig zu identifizieren und sich darauf vorzubereiten. Die Leitlinie berücksichtigt die Risikoproportionalität aufsichtsrechtlicher Anforderungen, sodass sie auch laufend im Rahmen einer bestehenden und sich dynamisch entwickelnden Geschäftsbeziehung zur Ableitung der Anforderungen genutzt werden kann – denn in der Regel gilt: je bedeutender und wichtiger die Geschäftsbeziehung für eine Bank wird, desto höher werden der RRG und, damit einhergehend, steigende aufsichtsrechtliche Anforderungen an das FinTech.

3. **Vorbereitung auf eine eigene Lizenz**: FinTechs, deren Geschäftsmodelle erlaubnispflichtig sind, arbeiten in der Anfangsphase oft mit einem anderen, bereits lizensierten Unternehmen zusammen („license/banking as a service“). Je länger ein solches FinTech am Markt besteht und je etablierter sein Geschäft wird, desto vorteilhafter kann die Beantragung einer eigenen Lizenz sein. Auch hier kann die Leitlinie als eine Roadmap verstanden werden, die über die verschiedenen RRG hinweg eine Entwicklung hin zur Erfüllung zumindest gewisser, wenn auch nicht aller Voraussetzungen für eine eigene Erlaubnis aufzeigt (z.B. bezüglich Unternehmenssteuerung, interner Kontrollmechanismen, Risikomanagement, organisatorischen Aufbaus und Ablaufs).

Ausblick

Der Bankenverband strebt an, dass die Leitlinie von möglichst vielen seiner Mitglieder angewendet wird. Zudem möchten wir die Leitlinie fortlaufend weiterentwickeln. Wenn die Leitlinie (grundsätzlich) auf breite Akzeptanz bei unseren Mitgliedern stößt und zur praktischen Anwendung kommt, ist vorgesehen, einen systematischen Feedback-Loop zu etablieren. Dieser sollte idealerweise elektronisch erfolgen, standardisierte Dokumente umfassen und verschiedene Auswertungsmöglichkeiten bieten. Gleichzeitig wollen wir unseren Mitgliedern Unterstützung bei der Anwendung geben, zum Beispiel durch telefonischen Support.

Die an der Ausarbeitung der Leitlinie beteiligten Vertreter können sich perspektivisch die Entwicklung eines Zertifikats auf Basis der Leitlinie vorstellen. Ein Zertifikat soll die Regulierungsgüte eines FinTechs in Bezug auf die Einhaltung einer Stufe von Anforderungen bescheinigen. Es könnte beispielsweise dazu genutzt werden, sich wiederholende Prüfungsauf-

wände seitens der Banken und FinTechs zu reduzieren. Zur weiteren Umsetzung wird der Bankenverband gemeinsam mit seinen Mitgliedern Vorschläge erarbeiten.

Definitionen

Anforderungstyp

Klasse von „Nicht-leistungsspezifischen bankaufsichtlichen Anforderungen“, z.B. BCM, Interne Kontrollen, Informationssicherheit.

Auslagerung

Nach MaRisk.
Im Titel dieses Dokuments und in Bezug auf europäische Maßnahmen wird das Synonym „Outsourcing“ verwendet.

Auswirkung

Koordinate des RRG-Modells.
Meint den Effekt, der eintritt, wenn das Risiko zum Tragen kommt.
Eine Frage im Fragenkatalog lautet z.B.: „Wie hoch ist der Zeitaufwand für einen Wechsel zu einem alternativen Dienstleister?“; gemeint ist der Effekt für die Bank ausgedrückt in/bezogen auf Zeit.

Bank

Nach § 1 Abs. 1 KWG.
Umfasst alle Mitgliedsbanken des BdB.

Dimension

Beschreibt die wesentlichen Aspekte, die im Prozess der Anforderungs-Abstufung berücksichtigt wurden.

FinTech

Im Rahmen dieser Leitlinie definieren wir als FinTech ein junges Unternehmen, das mit Banken zusammenarbeitet, um innovative, technologiebasierte Produkte und Leistungen zum Einsatz zu bringen.
Umfasst die meisten außerordentlichen Mitglieder des BdB.

Grad der organisatorischen Bedeutung

Eine Dimension, die zur Ableitung der Anforderungsabstufungen verwendet wurde.
Ordnet die einzelnen Mindestanforderungen aus Stufe 4 implizit den für einen (Risiko-)Management-Kreislauf wesent-

lichen Bestandteilen (A) Governance (einschl. Wissenstransfer/ Training), (B) Identifizierung, Steuerung und Überwachung sowie (C) Validierung und Anpassung zu.

Grad der strukturellen Umsetzung

Dimension, die zur Ableitung der Anforderungsabstufungen verwendet wurde.
Intendiert, eine qualitative Dimension im Sinne einer qualitativ umfangreichen bzw. vereinfachten Umsetzung zu geben.

Koordinaten

Die x- und y-Achsen unseres RRG-Modells (Risiko und Auswirkung).

LBA

Kurzform von „Leistungsspezifische bankaufsichtliche Anforderungen“.
Anforderungen, die von sehr spezifischen Aspekten der Zusammenarbeit abhängig sind und für die es nicht möglich ist, eine Abstufung vorzunehmen, z.B. Datenschutz- und Geldwäsche-Anforderungen.
LBA bleiben im Rahmen dieser Leitlinie unberücksichtigt.

NLBA

Kurzform von „Nicht-leistungsspezifische bankaufsichtliche Anforderungen“.
NLBAs sind Anforderungen, die unabhängig von Produkten/ Dienstleistungen als generelle Anforderungen der Banken an FinTechs gerichtet werden. Mehrheitlich handelt es sich dabei um Anforderungen an die ordnungsmäßige Geschäftsorganisation (basierend auf KWG §25a) sowie um regulatorische Anforderungen mit unmittelbarem Bezug zur Auslagerung (beispielsweise gemäß MaRisk).
NLBA werden im Rahmen dieser Leitlinie in einem Katalog risikobasiert konkretisiert und abgestuft.

Onboarding

Standardisiertes Vorgehen vom ersten Kontakt (Anbahnung) bis zur Realisierung der Kooperation und/oder Auslagerung. Ermöglicht eine risikoangemessene und kooperationsunabhängige, qualitativ gleichbleibende Entscheidung über das Eingehen von Kooperationen und Auslagerungen.

Option

Eine Antwortmöglichkeit im Fragenkatalog des RRG-Modells.

Punktzahl

Jeder Option im Fragenkatalog des RRG-Modells entspricht eine Punktzahl.
Jede Punktzahl wird so gewichtet, dass die Gesamt-Risiko- und Gesamt-Auswirkungs-Punktzahlen jeweils maximal 50 betragen.
Die Gesamt-Punktzahl ist das Produkt aus der Gesamt-Risiko-punktzahl und der Gesamt-Auswirkungs-Punktzahl.

Risiko

Eine Koordinate des RRG-Modells.Bezieht sich auf ein mögliches Wagnis, welches die Bank negativ beeinflusst.Eine Frage des Fragenkatalogs lautet z.B.: „Gibt es alternative Dienstleister/FinTechs im Markt?“. Hier ist das Wagnis gemeint, dass es keine Option für die Bank gibt, den Service/das Produkt anderweitig zu generieren.Für gewöhnlich werden bei der Ermittlung von Risiken auch Wahrscheinlichkeiten berück-sichtigt. Unser RRG-Modell sieht dies nicht vor – u.a. deshalb nicht, weil wir ein leicht anwendbares und in der Praxis selbst-verständlich nutzbares Modell zur Verfügung stellen wollen. Unser Fokus liegt zudem auf den Auswirkungen und dann im weiteren Verlauf auf den Anforderungen an ein FinTech.

Risikoappetit

Bezieht sich auf Frage 18 im RRG Modell.Bestimmt, in welchem Umfang die Bank bereit ist, Risiken einzugehen, die sich aus einer Kooperation mit einem FinTech ergeben können.

Risikoeinschätzung

Ergebnis des RRGs.Bewertung aus Sicht der Bank bezüglich des Risikos einer bestimmten Kooperation mit einem FinTech.

Risikokategorien

Kategorien von Fragen im Fragenkatalog des RRG-Modells.

RRG

Kurzform von Risiko-Reifegrad.
Risikoeinschätzung der spezifischen Bank-FinTech-Kooperation.

RRG-Modell

Modell, um den RRG einer Bank-FinTech Kooperation zu ermitteln.Besteht aus einem Fragenkatalog von Risiko- und Auswirkungsfragen und einem grafischem Modell, in dem Gesamt-Risiko- und Gesamt-Auswirkungs-Punktzahlen vom Fragenkatalog getrennt auf der x-Achse (Risiko) und der y-Achse (Auswirkung) erfasst werden.

Schwellwert

Abgrenzung zwischen den einzelnen vier RRG als Gesamt-Punktzahl.

Stufe

Bezieht sich auf den Anforderungskatalog.
Jeder Anforderungstyp ist in vier Stufen von Anforderungen unterteilt, welche dem jeweilige RRG entsprechen.

time-to-market

Zeit, die verstreicht, bis eine Produktidee oder ein Dienstleistungsangebot, das von Bank und FinTech gemeinsam entwickelt wird, zur Marktreife gelangt ist, sodass eine Platzierung des Produktes bzw. der Dienstleistung am Markt erfolgen kann

UC

Kurzform von Use Case.
Stellt einen unmittelbaren, praktischen Bezug zu einer tatsächlich existierenden Fallkonstellation einer Kooperation zwischen Bank und FinTech her.

White-Labelling

Bereitstellung einer Bank-Infrastruktur (inklusive der dazugehörigen Banklizenz) an Drittparteien, die für ihre Kunden wie eine Bank agieren.
Die White-Label-Bank bietet ihre Bankdienstleistung nicht den eigentlichen Endkunden (im B2C-Sinne) an, sondern lediglich den Drittparteien bzw. den Partnern (im B2B-Sinne).

Zusammenarbeit/ Kooperation

Operative Zusammenarbeit von Bank und FinTech in unterschiedlicher Intensität, zeitlicher Dauer und Zielrichtung zwischen rechtlich selbstständigen Unternehmen. Unterschiedliche Intensitätsstufen sind möglich; bspw. Informationsaustausch, Gemeinschaftsarbeiten mit/ohne Ausgliederung einer (mehrerer) Unternehmensfunktion(en), Gemeinschaftsgründung.
Bank und FinTech bringen Produkte und Leistungen gemeinsam zum Einsatz.
Inkludiert mehrere Modelle, z.B. Fintech-as-a-service, White-Labelling und gemeinsame Neuentwicklung.
Neben Produkten und Dienstleistungen, die am Markt angeboten werden, sind auch Produkte und Dienstleistungen gemeint, die die Bank intern zur Anwendung bringt.

ANHANG 1 - Leitlinienmodell (Excel-Dokument)

Das Excel-Dokument wird auf individuelle Anfrage seitens der Mitglieder durch den Bankenverbandes übmittelt. Senden Sie uns gern eine E-Mail an bab_buero@bdb.de, Stichwort „BdB POL - Anforderung des Excel-Dokumentes“.

ANHANG 2: Validierungsprozess des Risiko-Reifegradmodells

Das RRG-Modell wurde durch reale UCs zwischen Banken und FinTechs iterativ validiert. Ziel war ein methodisch-systematisches Vorgehen, bei dem die Ergebnisse der Arbeit für jeden objektiv nachvollziehbar und wiederholbar waren.

Unter stringenter Anwendung des iterativen Vorgehens wurde jeder Teilschritt des Modells gemeinsam erarbeitet und in Diskussionen innerhalb der Projektgruppe im Hinblick auf die Zielsetzung kritisch hinterfragt. Basierend auf den fünf Risikokategorien (Geschäftskontinuität, aufsichtsrechtliche Anforderung, Leistungserbringung seitens FinTech, Kunde und Informationssicherheit) wurden zunächst maßgebliche Fragen aller beteiligter Institute gesammelt. Im Anschluss daran wurden die Fragen in der gesamten Projektgruppe mehrfach diskutiert, Redundanzen eliminiert und Fragen zusammengefasst, um das Modell überschaubar zu halten. Hierbei blieb die breite Spannweite der Fragen das Ziel der Herangehensweise.

Weiterer Bestandteil der Arbeit war die Einteilung der Fragen in die Koordinaten „Risiko“ und „Auswirkung“. In zwei separaten Arbeitsgruppen wurden zunächst die Fragen und Optionen der beiden Koordinaten weiterentwickelt, anschließend wieder im Gesamtplenum diskutiert und mit ersten UCs erprobt. Bei der Erprobung der UCs wurden die verwendeten Begriffe genauer definiert und Formulierungen geschärft, um eine möglichst hohe Antworteindeutigkeit bei den Modellanwendern zu erzielen.

Nachdem die Fragen, Optionen und Punktzahlen vordefiniert waren, wurde das Modell anschließend anhand von UCs aus den Banken validiert und die entsprechenden RRG ermittelt. Die RRG wurden mit den aktuellen Bewertungen innerhalb der Banken abgeglichen.

Insbesondere jene Fälle mit Diskrepanzen zwischen aktueller Bewertung der Auslagerung in den Banken und der Bewertung nach dem RRG-Modell wurden in der Projektgruppe analysiert und die Gründe der Abweichungen ermittelt.

Häufig waren die Ursachen durch Ungenauigkeiten der Fragstellungen bzw. des Interpretationsspielraums der

Antworten bedingt. Infolgedessen wurden in iterativen Schleifen alle Fragen einschließlich der Optionen individuell überprüft und im Ergebnis

- um- bzw. präziser formuliert,
- mit einer anderen Frage zusammengefasst,
- die Antworten validiert,
- die Optionen überprüft und konkretisiert und
- wurde die Gewichtung der Frage diskutiert,

um die Eindeutigkeiten der Fragen und deren Antworten zu gewährleisten. Darüber hinaus wurden die Optionen und das Scoring auf die Belange von FinTechs und deren Spezifika angepasst.

Insgesamt wurde das RRG-Modell mit 17 UCs validiert. Die UCs wurden in Einzelarbeit und in der Projektgruppe intensiv und wiederholt geprüft. In einem konkreten Fall wurde eine bestehende Auslagerung jeweils durch das FinTech und die Bank individuell und unabhängig voneinander anhand des RRG-Modells bewertet, abgeglichen und diskutiert. Sofern sich Abweichungen ergaben, wurde die Ursache erhoben und kritisch im Kontext des RRG-Modells reflektiert. Abweichungen ergaben sich ausschließlich aus einem unterschiedlichen Verständnis der tatsächlichen Dienstleistungskomponente, sodass sich entsprechende Abweichungen nach der Vereinheitlichung des Verständnisses auflösten. Insbesondere an diesem Beispiel wurde deutlich, dass das RRG-Modell eindeutig und einfach anzuwenden ist. Im Austausch der Bewertungen konnten die Sichtweisen schnell ausgetauscht und erklärt werden und dienten der Transparenz der Bewertung.

Nach Abschluss aller Validierungen sind die UCs und ihre RRG erklärbar, nachvollziehbar und mehrheitlich mit den Bewertungen innerhalb der Banken vergleichbar.

ANHANG 3: Validierungsprozess des Anforderungskatalogs

Der folgende Abschnitt beschäftigt sich mit der Validierung der Abstufungen der einzelnen Anforderungstypen pro RRG.

Der RRG (von 1-4) ist eine Risikoeinschätzung der Zusammenarbeit zwischen Bank und FinTech in einem spezifischen Fall. Er ergibt sich aus den Antworten einer Reihe von Fragen (siehe Kapitel „Erläuterung der Logik des Risiko-Reifegradmodells“). Der RRG leitet zur Stufe (1-4) der Anforderungen über, die ein FinTech einhalten muss.

Zur Plausibilisierung unseres Modells haben wir drei exemplarische UCs ausgewählt und für drei Anforderungstypen (Business Continuity Management, Interne Kontrollen sowie Informationssicherheit) die Angemessenheit der Stufe von Anforderungen erprobt.

Folgenden drei UCs wurden ausgewählt:

1) RRG 2 ==> Barzahlungs-Zusatzdienstleistung
2) RRG 3 ==> Kontowechselservice
3) RRG 4 ==> vollumfängliche IT Dienstleistung mit großen Abhängigkeiten und umfangreichen (=allen) Kundendienstleistungen für Privatkunden

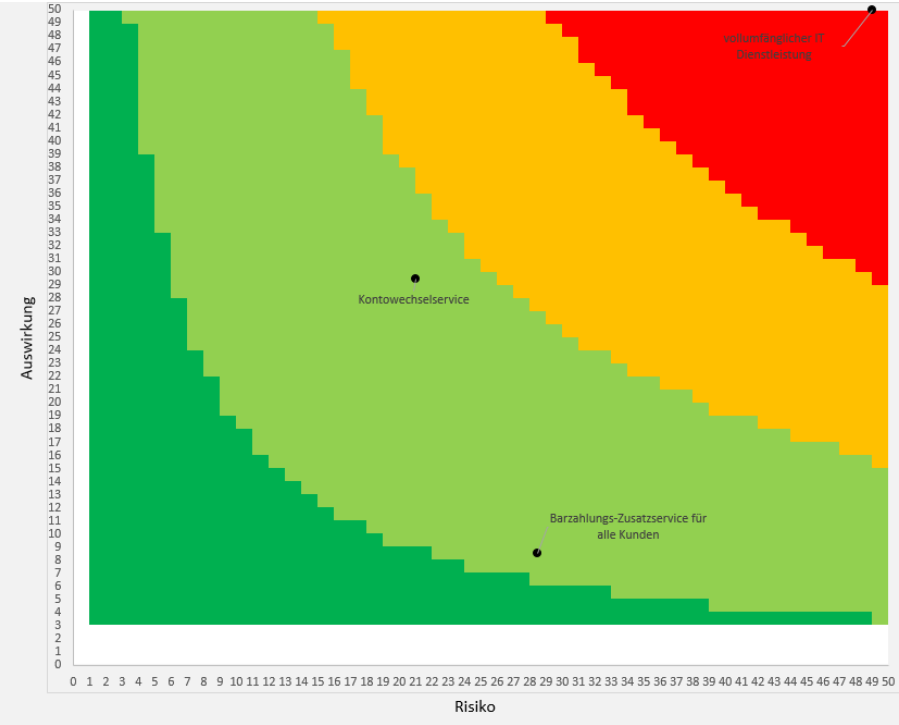


Abbildung 8: Graphik zu UC Beispiele benutzt im Validierungsprozess des Anforderungskatalogs

1. Risiko-Reifegrad 2 | Use Case: Barzahlungs-Zusatzdienstleistung

Die Bewertung der Barzahlungs-Zusatzdienstleistung im RRG-Modell ergibt eine Einwertung im RRG 2, d.h. Auswirkung und Risiko sind für die Bank, die die Dienstleistung auslagert, moderat. Dies ist für die zugrundeliegende Dienstleistung plausibel, da den Kunden der Bank immer noch andere Ein- und Auszahlungsoptionen zur Verfügung stehen.
Die konkreten Anforderungen, die an das FinTech in Stufe 2 gestellt werden, können dem Anhang 1 entnommen werden.

2. Risiko-Reifegrad 3 | Use Case: Kontowechselservice[8]

Der UC „Kontowechselservice“ wurde mittels des RRG-Modells mit erhöhtem Risiko und Auswirkung für die Bank bewertet und entsprechend im RRG 3 eingestuft. Ein anderer, zweiter UC „Kontowechselservice“ wurde hingegen mit einem geringeren Risiko und Auswirkung bewertet, so dass dieser im RRG 2 einzuordnen ist. Das mag überraschen, ist aber plausibel und folgerichtig, da das Risiko bzw. die Auswirkung beeinflussende Kriterien wie Kosten beim Wechsel der Dienstleistung oder die Art und Weise des Hostings in höheren Anforderungen an die Informationssicherheit oder Geschäftskontinuität führen können und somit eine höhere Stufe bei den Anforderungstypen erfordern.
Die konkreten Anforderungen, die an das FinTech in Stufe 3 gestellt werden, können dem Anhang 1 entnommen werden.

3. Risiko-Reifegrad 4 | Use Case: Vollumfängliche IT-Dienstleistung mit großen Abhängigkeiten und umfangreichen (=allen) Kundendienstleistungen für Privatkunden

Diese IT-Dienstleistung erlangt eine Einstufung im RRG 4. Dies bedeutet, dass Auswirkung und Risiko der angebotenen Dienstleistung für die auslagernde Bank entsprechend hoch sind und dies somit hohe Anforderungen an das FinTech erfordert. Dies ist ebenfalls plausibel, da es sich bei dem herangezogenen UC um kein “echtes FinTech” handelt, sondern um ein etabliertes Auslagerungs-Unternehmen, mit auf die Banken ausgelegten, vollumfänglichen Prozessen und Strukturen. Das Auslagerungs-Unternehmen erfüllt die Anforderungen gemäß Stufe 4.
Hintergrund für die Auswahl dieses UCs ist, dass derzeit sehr wenige FinTechs mit ihren Dienstleistungen einen so fortgeschrittenen RRG in dessen Lebenszyklus erreicht haben. Die konkreten Anforderungen, die in Stufe 4 gestellt werden, können dem Anhang 1 entnommen werden.

[1] Der Begriff NLBA wird im Kapitel „NLBA Abgrenzung von LBA“ ausführlicher definiert. Von hier an sind alle Verwendungen von "Anforderung" als NLBA zu verstehen.
[2] Auf der Basis von § 25a KWG, der die organisatorischen Pflichten von Instituten mit Blick auf das institutsinterne Risikomanagement regelt, geben die MaRisk einen Rahmen für das Management aller wesentlichen Risiken vor. Sie sollen u.a. das Verwaltungshandeln der jeweiligen aufsichtlichen Mitarbeiter vereinheitlichen. Für die Institute ergeben sich aus dem prinzipienorientierten Ansatz der MaRisk Spielräume für eine individuelle Umsetzung. Jede Bank muss daher für sich prüfen, welcher Teil der Anforderung in welcher Form umgesetzt wird. Je nach Bank können bzw. müssen dies – bezogen auf den Umfang – mehr oder weniger Anforderungen sein. Eine fortwährende Überprüfung der eigenen Anforderungen an die tägliche Praxistauglichkeit sollte erfolgen.
[3] Die EBA hat am 25. Februar 2019 die finale Version ihrer Guidelines on Outsourcing (EBA/GL/2019/02) veröffentlicht. Mit diesen Guidelines soll ein harmonisierter Regelungsrahmen für sämtliche Institute geschaffen werden, für welche die EBA mit einem Mandat ausgestattet ist. Dies bedeutet, dass die EBA-Guidelines – anders als noch die alten CEBS-Leitlinien zu Auslagerungen – auch für Zahlungsinstitute und E-Geld-Institute gelten. Die EBA-Guidelines werden am 30. September 2019 wirksam, sehen jedoch gewisse Übergangsregelungen vor, die den Instituten für die Umsetzung bestimmter Anforderungen Zeit verschaffen, um sich auf die durchaus erheblichen Änderungen der Anforderungen bei Auslagerungen einzustellen.
[4] Bei bestimmten Fragen wird ein Bezug zu „Kunde“ hergestellt. Dies meint i.d.R. externe Kunden. Möglich ist auch, dass als Kunde die Mitarbeiter der Bank (Nutzer) zu subsumieren sind; abhängig von der Dienstleistung bzw. dem Produkt.
[5] Eine Frage lautet z.B. „Wie viele Dienstleister im aktuellen Markt sind in der Lage, eine vergleichbare Dienstleistung für die Bank zu erbringen?“. Eine Antwortoption lautet „größer 5“. Das Risiko ist gering, da ausreichend viele andere Anbieter im Markt existieren. Im Vergleich zu der traditionellen Dienstleistung Geld- und Wertransport, sind beispielsweise in der Bundesvereinigung Deutscher Wert- und Gelddienste über 30 Firmen vermerkt.
[6] Die Bank muss mittels Risikoanalyse prüfen, welche Risiken mit der geplanten Maßnahme überhaupt verbunden sind und ob diese Risiken in einer Gesamtschau wesentlich oder unwesentlich sind. Dabei können unterschiedlichste Aspekte eine Rolle spielen (konkreter Gegenstand der Auslagerung, Auswirkungen der Maßnahme auf das Institut, Ort der Leistungserbringung, Komplexität der geplanten Maßnahme, Eignung potenzieller Dienstleister etc.). Schließlich wird mittels Risikoanalyse - quasi als deren Ausfluss - auch festgestellt, ob eine Auslagerung als wesentlich oder unwesentlich anzusehen ist. Im Ergebnis wird sich die Bank mithilfe der Risikoanalyse der Risiken durch die Auslagerung bewusst.
[7] Mit der Veröffentlichung Anfang September 2017 hat COSO (The Committee of Sponsoring Organizations of the Treadway

Commission) sein aktualisiertes Modell „Enterprise Risk Management – Integrating with Strategy and Performance“ veröffentlicht, welches die Bedeutsamkeit der Verzahnung zwischen Strategie, Risikomanagement und Unternehmenserfolg hervorhebt.
[8] Wir haben eine Validierung bei diesem UC durchgeführt und hierbei zwei Bank-FinTech UC herangezogen. Es handelte sich dabei um zwei verschiedene Banken und FinTechs.

Kontakt

Bundesverband deutscher Banken
Postfach 040307
10062 Berlin
+49 30 1663-0
bankenverband@bdb.de
bankenverband.de