Cloud – Regulatorik für Banken

Gründe und Abgründe der Cloud-Regulatorik

Liubov Khomutovskaya
Dr. Waldemar Grudzien
Moritz Treutwein

Januar 2023
Blogpost

Key Facts

- Auslagerungen in die Cloud unterliegen denselben Regelungen wie alle Auslagerungen eines Finanzinstituts, es können jedoch insb. beim Einsatz von Hyperscalern spezifische Herausforderungen bei der Umsetzung der regulatorischen Anforderungen bestehen
- Das Risikomanagement muss unbedingt auch ausgelagerte Tätigkeiten umfassen
- Je mehr kritische Prozesse und wichtige Unterstützungsfunktionen an einen Anbieter ausgelagert werden, desto höher ist die Abhängigkeit und damit die Risikokonzentration – falls daher ein Cloud-Anbieter Einfluss auf mehrere kritische Prozesse hat, steigt bei diesem das Risiko
- Ein Finanzinstitut muss die Auslagerung in die Cloud genauso stringent steuern und überwachen wie es das bei Belassung der Funktionen und Dienste im eigenen Hause tun würde
- Eine kontinuierliche Dokumentation ist in Bezug auf alle regulatorischen Verpflichtungen unbedingt einzuhalten, um die notwendigen Nachweise gegenüber der Aufsicht gewährleisten zu können

Betrachtung der Cloud-Nutzung aus Auslagerungssicht

Obgleich die Nutzung von Cloud-Angeboten den Ruf hat regulatorisch besonders betrachtet zu werden, gibt es keine speziellen Regelungen für die Cloud-Nutzung, sondern es gelten die allgemein gültigen Regelungen für Auslagerungen. Die gewohnten MaRisk[1], BAIT[2], EBA Leitlinien zu Auslagerungen gelten hier ebenso, wie bei jedem anderen Einkauf einer Bank.[3] Für eine regulatorisch konforme Cloud-Auslagerung müssen somit dieselben Schritte durchlaufen werden, die Institute bei richtiger Ausgestaltung des Auslagerungsmanagements ohnehin vorsehen. Diese wollen wir im Folgenden betrachten und ergründen, an welchen Stellen für Cloud-Angebote Herausforderungen bestehen.

Zu Beginn muss jedoch erst das Grundproblem der Aufsicht mit Einkäufen verstanden werden. Häufig fragen Institute: „Wo liegt denn das Problem? Wir wenden uns an durchgesetzte Profis auf dem Markt. Diese kennen die Technologie besser als wir und sie haben das ganze Interesse der Welt, eine gute Performance zu bieten. Es ist viel sicherer, diese Lösung einzukaufen, als selbst herzustellen“. Fair. Dem lässt sich Folgendes entgegnen:

1. Auf dem Markt setzen sich Anbieter vor allem mit visiblen Vorteilen und selten mit Informationssicherheitsaspekten gegenüber der Konkurrenz durch. Die „Profis“ müssen also keineswegs versierte Informationssicherheitsexperten in den eigenen Reihen haben, sondern könnten mit sich eben bislang nicht realisierten Risiken umgehen.[4] Die Investition in Sicherheitsaspekte darf somit vermutet werden (und ist häufig Bestandteil einer Kommunikation an den Markt bei etablierten Anbietern), ist jedoch keinesfalls ungeprüft anzunehmen.
2. Zwar sieht die Regulatorik vor, dass die Aufsicht bei wesentlichen Auslagerungen ein direktes Prüfrecht beim Dienstleister eingeräumt bekommen muss, doch kann die Ausübung besonders bei verflochtenen Vertragsbeziehungen mit mehreren Akteuren und schlechter Dokumentationslage kompliziert sein. Ebenfalls herausfordernd kann der Haftungsdurchgriff des Instituts selbst sein, da in diesem Fall das Institut die Beweislast trägt, dass beim Dienstleister verschuldete Fehler in Form von Vertragsbrüchen und Sicherheitslücken passiert sind. Die Motivation des Dienstleisters, Informationssicherheitsrisiken zu minimieren, muss demnach nicht bereits aus der Haftbarkeit heraus die höchste Stelle einnehmen. Tatsächlich investieren viele Unternehmen große Summen, um eine hinreichende Sicherheit zu gewährleisten, ein Automatismus ist dies jedoch nicht.

[1] Mindestanforderungen an das Risikomanagement
[2] Bankaufsichtliche Anforderungen an die IT
[3] S. Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter der BaFin: „Durch die Orientierungshilfe werden allerdings keine neuen Anforderungen gestellt, sondern die derzeitige aufsichtliche Praxis in solchen Auslagerungsfällen wiedergegeben.“.
[4] S. hierzu Ausführungen von Rainer Böhme, Paulina Jo Pesch und Verena Fritz in „Auswirkungen sich verändernder Wertschöpfungsketten im Finanzsektor auf die IT-Sicherheit, Projektbericht Juli 2022, S. 8.

3. Die Finanzregulatorik sieht eine Reihe von Instrumenten vor, um Risiken bei den Aufsichtsobjekten zu begegnen. So müssen Finanzinstitute eine vollständige Übersicht eigener Prozesse und unterstützender Applikationen und Infrastrukturkomponenten pflegen. Diese sind auf ihr Schutzniveau hin zu bewerten, um davon ausgehend Maßnahmen zum Schutz dieser Komponenten abzuleiten. Interne Kontrollen sollen Risiken frühzeitig erkennbar und steuerbar machen. Dienstleister, welche nicht als Aufsichtsobjekte klassifiziert sind, haben mit derartigen Regelungen wenig Berührungspunkte. Sie haben häufig keine eigene Motivation, ein ausgiebiges Risikomanagementsystem zu unterhalten. Entsprechend besteht aber hierdurch die Gefahr, dass kritische Prozesse oder unterstützende Strukturelemente an Dienstleister ausgelagert werden, die ihre eigenen Risiken nicht hinreichend kennen und somit keine Sicherheit gewährleisten können. Zwar investieren insbesonders große Unternehmen intensiv in Sicherheit, wie genau diese ausgestaltet ist und welche Risiken verbleiben, ist jedoch häufig schwer einschätzbar, denn gerade große Unternehmen zeigen sich gerne als „Black Box“. Die Nervosität der Aufsicht besteht daher darin, dass Sicherheitsmaßnahmen durch Auslagerungen einfach umgangen werden, weil das auslagernde Institut alle Risikomaßnahmen ebenso verlagert sieht, wie die Leistung selbst, der Dienstleister sich aber keineswegs an Standards der Finanzbranche gebunden fühlt und im Falle mangelhafter Vertragsgestaltung auch keine Haftung übernehmen muss. Bisweilen kommen sogar Unternehmernsverbände, die aus einer Bank und vielen nicht als Finanzinstitute zu qualifizierenden Unternehmen bestehen, auf die Idee, möglichst viele bankrelevante Prozesse und Unterstützungen in die nicht direkt regulierten Entitäten zu verlagern in der Hoffnung, so umfangreiche Risikomanagementmaßnahmen zu umgehen.

Es geht also im Grunde darum, die Anforderungen an Finanzinstitute im Hinblick auf ihre (kritischen) Finanzprozesse durchzusetzen, unabhängig davon, wo sie tatsächlich stattfinden. Und dies ist praktisch nur dann möglich, wenn der, direkt gegenüber seinen Kunden und der Aufsicht, Verantwortliche – das Finanzinstitut – den Überblick, die Steuerung und die Kontrolle über ausgelagerte Tätigkeiten behält. Das bedeutet nicht, dass Institute nicht auslagern dürfen oder alle Risiken mit unangemessenen Kosten und Aufwänden eliminieren müssen. Es bedeutet jedoch, dass die Risiken erkannt, bewertet und gesteuert werden. Wer also erhofft, den internen Aufwand im Risikomanagement, in den Kontrollfunktionen und im Vorhalten kritischen Know-Hows durch Einkäufe zu reduzieren, muss enttäuscht werden. Das geht gewissermaßen gegen die Idee von Adam Smith, denn es muss sich nicht nur derjenige mit einer Produktion befassen, der das am besten kann und die besten Ressourcen hierfür hält, sondern auch das einkaufende Finanzinstitut. Diese bittere Pille muss der Finanzmarktstabilität geschuldet geschluckt werden. Hierbei kann aber wirtschaftlich gedacht werden, indem Auslagerungs-, Risikomanagement- und IT-Prozesse möglichst effizient gestaltet werden.

Somit starten wir die Reise, die jede Auslagerung, und damit auch eine Auslagerung in die Cloud, zu gehen hat:

1. Dienstleisterauswahl & Klassifizierung

Sobald ein Bedarf festgestellt wird und eine Leistung (grob) beschreibbar ist, sollte sie bereits klassifiziert werden. Hierbei wird gem. § 25 KWG i.V.m. AT 9 MaRisk und Kapitel 9 BAIT eine Unterscheidung in Auslagerungen (mit oder ohne IT-Bezug) und sonstige Fremdbezüge (mit oder ohne IT-Bezug) vorgenommen. Da von dem Ergebnis dieser Einteilung unterschiedliche Anforderungen an Folgeschritte gestellt werden, sollte die Klassifizierung so früh wie möglich erfolgen. So können diese im Prozess der Dienstleisterauswahl bereits berücksichtigt werden, etwa im Rahmen des RfP[5]. Wer die Leistung erbringt, ist für die Klassifizierung erst einmal unerheblich. Maßgebliches Unterscheidungsmerkmal ist der Bankcharakter und die Dauer der ausgelagerten Prozesse. Handelt es sich um einen dauerhaften Leistungsbezug mit Bankcharakter, liegt eine Auslagerung vor. Ebenfalls werden Unterstützungsleistungen wie Wartung und Betrieb von Software, die für bankgeschäftliche Aufgaben von wesentlicher Bedeutung sind, als Auslagerungen klassifiziert. Zusätzlich kommt alles hinzu, was zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt wird.

Sonstige Fremdbezüge sind einmalig/ gelegentlich bezogene Leistungen (auch bankspezifische Leistungen), nicht banktypische Leistungen und/ oder von beaufsichtigten Unternehmen bezogene Leistungen, auch hier mit oder ohne IT-Bezug.

Bei Cloud-Diensten kann jeweils die Variante „ohne IT-Bezug“ ausgeschlossen werden. Ansonsten kann es sich aber sowohl um eine Auslagerung, als auch um einen sonstigen IT-Fremdbezug handeln, wobei die BaFin hier in der Regel von einer Auslagerung ausgehen möchte.[6] Es gelten jedoch keine neuen Kriterien für die Klassifizierung – entscheidend ist weiterhin Bank- und Risikomanagementcharakter sowie Dauer. Wird zum Beispiel eine HR-Software aus der Cloud genutzt, ist hier der für die Auslagerung notwendige Charakter regelmäßig nicht gegeben und eine Einwertung als sonstiger IT-Fremdbezug gerechtfertigt.

Das Ergebnis der Klassifizierung entscheidet über die Folgeschritte. Für sonstige Fremdbezüge ohne IT-Bezug endet hier der Weg aus Sicht des Auslagerungsmanagements. Aus Betriebs-, Datenschutz- und Fachabteilungssicht mag noch Vieles geklärt werden müssen – die auf Bankgeschäfte fokussierte Risikobetrachtung findet hier aus der Auslagerung heraus nicht statt.

Für Auslagerungen mit oder ohne IT-Bezug geht es daher mit der Risikoanalyse gem. MaRisk, für IT-Fremdbezüge mit der Risikobewertung gem. BAIT weiter.

An dieser Stelle kann nur betont werden, dass der beste Weg die Schaffung eines stabilen Fundaments des Auslagerungsmanagements ist. Das inkludiert eine in sich konsistente, verständliche und aussagekräftige Auslagerungsstrategie- und Leitlinie sowie konkrete Vorgaben für die Klassifizierung, Risikobewertung und alle Folgeschritte des Auslagerungszyklus. Je verständlicher der Prozess und die Vorgaben, desto „smoother“ laufen die häufig inhaltlich herausfordernden Folgeschritte. Kommt eine Verwirrung prozessualer und organisatorischer Art

[5] Request for Proposal
[6] S. Orientierungshilfe zu Auslagerungen, S. 5.

hinzu, sind besonders bei komplexen Vorgaben Diskussionen mit der Aufsicht sicher, die in Findings münden können. Mit der Anzahl an Auslagerungen verschärft sich dieses Risko.

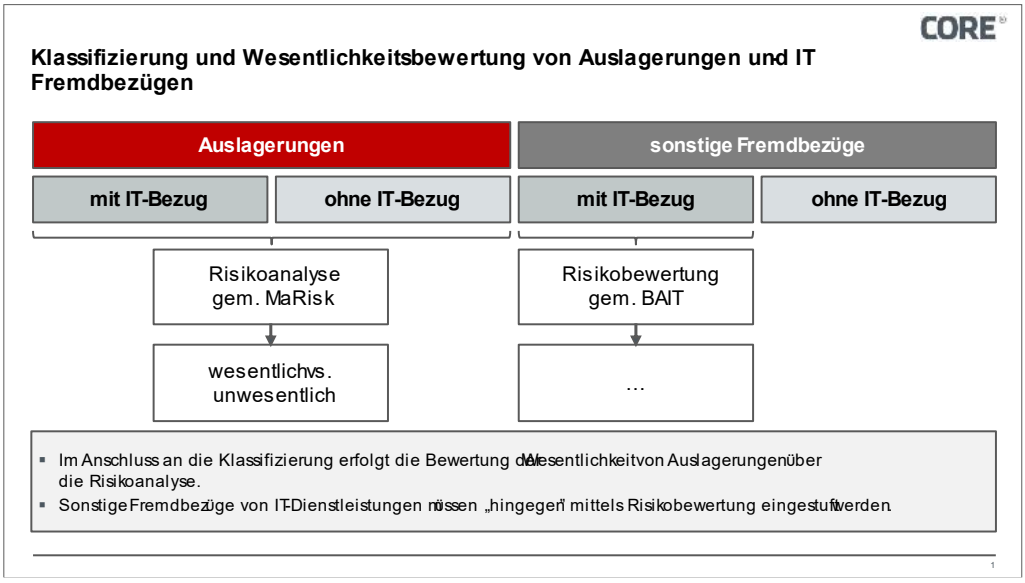

Abbildung 1: Klassifizierung und Wesentlichkeitsbewertung von Auslagerungen und IT Fremdbezügen

2. Risikoanalyse gem. MaRisk für Auslagerungen

AT 9 Tz 2 MaRisk verlangt eine Risikoanalyse von Auslagerungen. Hierbei sind wichtige Funktionen wie Datenschutzbeauftragte, Informationssicherheitsbeauftragte, Business Continuity Beauftragter, Compliance etc. einzubeziehen. Wichtig ist, dass die Risikoanalyse unabhängig erfolgen muss. Sie könnte zum Beispiel auch dazu führen, dass angesichts der analysierten Risiken eine Auslagerung nicht oder nur unter Beachtung bestimmter Risiko-minimierender Maßnahmen erfolgen darf. Sie kann auch ergeben, dass ein Teil der Auslagerung wesentlich und ein anderer unwesentlich ist. Dann sollten diese Dienstleistungen auch separat betrachtet werden, auch wenn sie an denselben Dienstleister vergeben werden.

Bei der Risikoanalyse muss neben der ausgelagerten Dienstleistung auch die Zuverlässigkeit und Qualifikation d Dienstleister betrachtet werden. Sind mehrere Leistungen an einen Dienstleister ausgelagert, so muss dies ebenfalls im Sinne einer Risikokonzentration Berücksichtigung finden.Als wesentlich sind dabei Dienstleistungen einzustufen, die nah an den Kernbereich des eigenen Angebots herankommen sowie diejenigen Dienstleistungen, die eine Kontrollfunktion für das Finanzinstitut bereitstellen. In jedem Fall muss die Einbindung ausgelagerter Prozesse in das eigene Risikomanagement Einlass finden.

Zu beachten ist, dass auch die Risiken aus Weiterverlagerungen zu bewerten sind. Die Liste der Subdienstleister muss daher bei dem Anbieter erfragt werden. Regelmäßig kommt dieses Thema leider erst bei der Vertragsgestaltung zu Tage, sodass die Risikoanalyse dann wiederholt durchlaufen werden muss.

Dies ist bei dem Einsatz der Cloud nicht anders, auch die Orientierungshilfe zu Auslagerungen an Coud Anbieter der BaFin nennt hier gegenüber der MaRisk keine neuen Anforderungen. Einzig auffällig kann man die Betonung der Risiken in Bezug auf die Gerichtsbarkeit der Länder, in denen

die Leistungen erbracht oder Daten verarbeitet werden, sehen. Bei Datenschützern in Deutschland klingeln alle Glocken. Von „etwaigen Zugriffsmöglichkeiten auf Daten durch andere Jurisdiktionen“ ist die Rede. Seit Schrems II ist Verarbeitung personenbezogener Daten in den USA Grundlage für viele Diskussionen. In aller Kürze besteht die Befürchtung der Datenschutz-Aufsicht, darin, dass personenbezogene Daten in den Clouds der Hyperscaler von US-Geheimdiensten ohne rechtliche Grundlage angefragt und dann unter Bruch der DSGVO-Prinzipien und einhergehend mit Risiken für europäische Bürger in einem Drittland verarbeitet werden. Unter Beschuss kommt hier besonders der Einsatz von Hyperscalern. In anderen Branchen, in denen sensible personenbezogene Daten (Minderjährigendaten, Gesundheitsdaten, etc.) en masse verarbeitet werden, ist dieses Thema bei jedem Management auf strategischer Ebene angekommen, da die Datenschutzaufsichten teils rigoros durchgreifen. So wurde in Brandenburg der Einsatz von Teams an Schulen kurzerhand verboten[7]. In der Finanzbranche ist dieses Thema (noch) nicht in ähnlicher Weise eskaliert und es besteht Hoffnung, dass es in absehbarer Zukunft auf politischer Ebene oder durch den Markt gelöst wird. Dennoch sind Institute gut beraten, beim Einsatz von Cloud-Anbietern, die durch Konzernstrukturen mit US-amerikanischen Unternehmen verbunden sind, die Datenschutzrisiken in der Betrachtung nicht zu kurz kommen zu lassen und vertraglich (Abschluss von Auftragsverarbeitungsverträgen) sowie in der Steuerung zu berücksichtigen.

Ein weiterer wichtiger Punkt: die Risikoanalyse ist auch nach Vertragsschluss während der Zusammenarbeit regelmäßig zu prüfen und bei Änderungen zu aktualisieren. Häufig wird die Risikoanalyse in eine (digitale) Schublade gelegt und verstaubt dort. Das ist natürlich nicht Sinn der Übung und fällt bei BaFin Audits regelmäßig negativ auf. Simpel gesagt müssen die wichtigen Risiken diejenigen Personen im Unternehmen erreichen, die etwas von ihnen verstehen und die diese durch interne Maßnahmen oder durch Einwirkung auf den Dienstleister mitigieren können.

3. Risikoanalyse gem. BAIT

Für die Risikoanalyse gem. Tz 9.2 BAIT bestehen für das Institut mehr Freiheiten. „Art und Umfang einer Risikobewertung kann das Institut unter Proportionalitätsgesichtspunkten nach Maßgabe seines allgemeinen Risikomanagements flexibel festlegen.“ Hier kann also eine Risikoanalyse „light“ durchgeführt werden, die bei größeren Risiken im Einzelfall natürlich doch größere umfänge annehmen muss. Für Cloud-Lösungen gilt nichts anderes.

4. Notfallpläne

Des Weiteren müssen für wichtige ausgelagerte Prozesse und Unzerstützungsfunktionen Vorkehrungen getroffen werden, damit der Geschäftsbetrieb aufrechterhalten werden kann, falls ein Anbieter die Dienste nicht oder in unannehmbarer Form erbringt.[8] Besonders in der Risikobetrachtung aufzunehmen ist das Szenario, in dem der Dienstleister kurzfristig ausfällt.

Es muss klar festgelegt sein, wie die Stabilität der Dienstleistungen des Finanzinstituts in diesen Fällen gewahrt bleibt. Das heißt, Maßnahmen zur Mitigation von Ausfallrisiken müssen festgelegt

[7] https://www.tagesspiegel.de/potsdam/landeshauptstadt/arger-uber-verbot-von-microsoft-produkten-7960036.html
[8] EBA Recommendations on Cloud Outsurcing, S. 12

werden, z.B. sollten etwaige Migrationsleistungen vertraglich geregelt sein und Alternativen (andere Dienstleister oder Eigenübernahme) feststehen. Je mehr Prozesse von einem Dienstleister abhängig sind, desto kritischer wird diese Planung. Hier greift in der Praxis ein interessanter Effekt, dem unbedingt entgegengewirkt werden sollte: wenn eine Abhängigkeit vom Dienstleister klar besteht und ein Ausfall tatsächlich probelmatisch wäre, befassen sich Institute sich damit am liebsten gar nicht, da sie befürchten, eine „ehrliche“ Risikoanalyse würde dokumentieren, dass Risiken erkannt wurden und der Anbieter dennoch gewählt wurde. Das mag in anderen Bereichen haftungstechnisch für die Geschäftsführung sinnvoll sein, ist es in diesem Fall jedoch nicht. Das Institut hat die Möglichkeit, gewisse Risiken zu akzeptieren. Sie müssen allerdings analysiert und wo möglich, müssen sie für den Notfall Alternativen beobachtet bzw. bereitgehalten werden. Letztlich muss klar sein, ob das Institut an einem Ausfall zu Grunde gehen oder mittelschwere Verluste tragen würde. Das betrifft die ebenfalls zu klärende Frage, welchen Umfang das Risiko in den einzelnen Szenarien annehmen kann.

Bei Cloud-Hyperscalern stellt sich mitunter die Herausforderung, dass wenige Alternativen bestehen. Umso wichtiger ist es, eine genaue Analyse der dennoch vorliegenden Möglichkeiten zu fahren und für die wichtigsten Prozesse zu definieren, wie sie möglichst zügig bei einem Dienstleister-Ausfall wieder stabil zu beziehen wären.

Wichtig ist auch, interne KPIs[9] und KRIs[10] festzulegen, welche das Leistungsniveau und die verbundenen Risiken steuerbar machen: Welche Schlechtleistung löst welches Risiko aus? Ab wann wird ein Ausstiegsplan ausgelöst? Diese Fragen müssen bei der Steuerung berücksichtigt werden und insbesondere eine klare Verknüpfung zu den vertraglich festzulegenden SLAs haben.

5. Vertragsgestaltung

Für wesentliche Auslagerungen hält die MaRisk eine ganze Reihe an notwendigen Vertragsbestandteilen vor. Auf eine Aufzählung wird hier verzichtet und auf AT 9 Tz. 7 MaRisk verwiesen. Stattdessen konzentriert sich dieser Beitrag auf die Herausforderungen, die diesbezüglich regelmäßig bei Verhandlungen mit großen Cloud-Anbietern bestehen. Zusammenfassend lässt sich jedoch sagen: diese Herausforderungen sind in der Regel lösbar, erfordern mitunter aber große Verhandlungsaufwände, die bei der Planung des Einsatzes eines Dienstleisters berücksichtigt werden müssen. Für den Bezug von standardisierten Lösungen halten Hyperscaler zudem Anlagen für regulierte Institute bereit, die Minimalanforderungen in Bezug auf Informations- und Reportingpflichten sowie Weisungsrechte enthalten. Vor Vertragsschluss dürfen allenfalls vorbereitende Handlungen getroffen werden, die Erbringung der Dienstleistungen darf jedoch keinesfalls vor Vertragsschluss vorgenommen werden.

a) Leistungsgegenstand, SLAs

   Bereits in dieser fundamentalen Forderung liegen häufig die ersten Herausforderungen. Viele Anbieter beschreiben ihre Leistungen eher Marktbroschürenhaft, sodass am Ende nicht klar wird, welche Funktionalitäten und Leistungen eigentlich geschuldet sind. Es

[9] Key Performance Indicators
[10] Key Risk Indicators

sollte darauf geachtet werden, dass konkrete Leistungen und Mitwirkungspflichten eindeutig den Parteien zugeordnet werden. Sofern einzelne Leistungsbestandteile nicht eindeutig beschreibbar sind, weil sie noch gemeinsam ausgearbeitet werden müssen , muss klar festgelegt werden, wie diese erarbeitet werden und welche Rahmenbedingungen bereits feststehen (z.B. bzgl. Hauptfunktionalitäten, Preis, etc.).

Eine weitere Herausforderung ist häufig, dass Dienstleister sich vorhalten, die Leistungsbeschreibung einseitig anzupassen. Bei Lösungen, die auf dem Markt breit angeboten werden, soll dem Dienstleister die Weiterentwicklung entsprechend vorbehalten bleiben. In diesem Fall müssen Mechanismen vertraglich vereinbart werden, die verhindern, dass das Institut an die Abnahme der Leistung auch dann gebunden ist, wenn für ihn Verschlechterungen mit der jeweiligen Aktualisierung einhergehen, etwa weil regulatorische Anforderungen durch die Änderung nicht mehr erfüllt werden können. Neben der Bereitstellung initial vereinbarter und noch regelkonformer Leistung kann auch das Kündigungsrecht zur Lösung herangezogen werden.

Zusätzlich zu einer Beschreibung, was geschuldet ist, müssen klare Messgrößen zur Messung der Güte der Leistungsbereitstellung vereinbart werden. Ebenso muss klar sein, welche Konsequenzen bei einer Unterschreitung greifen, etwa Vertragsstrafen sowie Kündigungsmöglichkeiten des Instituts. Intern müssen die SLAs mit den festgelegten KPIs und KRIs einen funktionalen Kontroll- und Steuerungsmechanismus ermöglichen.

b) Ort der Leistungserbringung bzw. der Datenverarbeitung

Wie oben erwähnt spielen insbesondere bei Cloud-Anbietern mit Drittlandbezug datenschutzrechtliche Aspekte eine Rolle. Daher ist es wichtig festzuhalten, wo die Daten des Institus verarbeitet werden (dürfen) und welche Sicherheitsmaßnahmen zu ihrem Schutz zu ergreifen sind.

c) Weiterverlagerungen

Bereits für die Risikobewertung spielen Weiterverlagerungen eine Rolle. Große Unternehmen sträuben sich teils, die volle Transparenz über Weiterverlagerungen einzuräumen. Da extensive Auslagerungen jedoch vieles von dem aushöhlen können, was mit dem Dienstleister erreicht wurde, müssen bereits feststehende Subdienstleister aufgezeigt und neue, sofern möglich, unter einen Erlaubnisvorbehalt gestellt werden.

d) Informations- und Prüfrechte des Instituts

Die Forderung der Möglichkeit von Audits durch das Institut selbst sowie durch die Aufsicht des Instituts lösen regelmäßig Begeisterung auf Seiten der Dienstleister aus. Gerade Hyperscaler können nicht zulassen, dass alle ihre Kunden separat Prüfungen durchführen und somit viele Ressourcen für die Beantwortung ähnlicher Fragen in alle Richtungen vorgehalten werden müssen. Zulässig ist jedoch der Anschluss an Initiativen wie etwa die „Collaborative Cloud Audit Group“, die kollektiv Audits bei Cloud-Anbietern durchführen. Dies reduziert den Aufwand für alle Beteiligten deutlich.

Abseits der Prüfungen vor Ort sollte mit dem Dienstleister abgestimmt werden, durch welche Berichte dieser die Einhaltung der Anforderungen der Informationssicherheit, des BCM, des Datenschutzes, etc. nachweisen wird und zu welchen Fristen entsprechende Berichte bereitgestellt werden. Andernfalls besteht die Gefahr, dass Berichte später angefragt, die Bereitstellung seitens der Dienstleister jedoch mit Kosten verbunden wird.

e) Kündigungsmodalitäten

Hier ist insbesondere die Anknüpfung an die interne Exit-Strategie zu beachten, mithin etwaige Migrationsleistungen zu vereinbaren, die z.B. bei einem Dienstleisterwechsel nach Kündigung zu erbringen sind.

Nicht zu unterschätzen ist, dass die Kündigungsmöglichkeit als ultima ratio für verschiedene Szenarien herangezogen werden kann und sollte. So etwa für regulatorische Änderungen, die die Nutzung der Dienstleistung unmöglich machen, bei Forderung der Kündigung durch die Aufsicht und bei Schlechtleistungen.

f) Governance

Je enger die Zusammenarbeit, desto wichtiger ist es, Grundregeln für die diese festzulegen. Eskalationsprozesse, Rollen, Gremien und Abstimmungstreffen sollten entsprechend bereits vertraglich vereinbart werden, um eine effiziente Steuerung des Dienstleisters gewährleisten zu können.

g) Rechtswahl und Gerichtsstand

Alle Bemühungen um inhaltlich rechtssichere Vertragsgestaltung können in der Praxis in Gefahr geraten, wenn das Recht oder der Gerichtsstand außerhalb der Europäischen Union liegen. Insbesondere ist die für deutsche Finanzinstitute geltende Regulatorik Gerichten in Deutschland vertraut, in der EU zumindest in ähnlicher Form gut bekannt. Außerhalb der EU sind viele Vorgaben nicht vertraut und eine Durchsetzung könnte auf Hindernisse stoßen.

h) Anerkennung von Zertifizierungen

Auch wenn die Auslagerungs-Dienstleister über anerkannte Sicherheitszertifikate verfügen, entbindet es die Finanzinstitute nicht von eigenen Prüfungshandlungen.

6. Dienstleistersteuerung- und Überwachung

Nur allzu häufig wird der Vertrag bei Abschluss sauber im Legal-Ordner abgelegt und erst bei ensthaften Problemen wieder rausgeholt. Richtigerweise müssen aber alle Mitwirkungspflichten und die vereinbarten SLAs an intern Verantwortliche kommuniziert und mit internen KPIs und KRIs verknüpft werden. Ein laufendes Tracking der Ergebnisse ist notwendig, um eine Übersicht darüber zu haben, ob die wichtigen Prozesse stabil verlaufen oder Risiken ausgesetzt sind. Vertraglich vereinbarte Mechanismen sowie interne Sicherungsmaßnahmen müssen entsprechenmd eingesetzt und betrachtet werden. Pro wesentlichen Dienstleister wird sodann jährlich ein Bericht über die erbrachte Leistung und wichtige Ereignisse und Kontrollergebnisse

erstellt und der Geschäftsleitung bekannt gegeben. Auch unterjährlich muss ein angemessenes Berichtswesen gewährleistet werden.

Eigentlich müssten die Cloud Anbieter reguliert werden, da hier der Hebel falsch angesetzt wird: die Verantwortung wird auf die Institute abgewälzt, die gegenüber den Hyperscalern aber kaum Verhandlungsmacht haben. Ein anderer Fall wäre eine direkte Regulierung der Hyperscaler durch die Aufsicht – und genau das ist das Ziel der DORA[11].

7. Fazit

Der Einsatz von Cloud-Diensten ist in der Finanzbranche keineswegs verboten, relevant wird die Cloud-Charakteristik jedoch bei Risikokonzentrationen durch Auslagerungen an einen Anbieter oder wenn intern kein Know-How zur Steuerung und Kontrolle besteht. Für jedes Finanzinstitut ist sowohl ein gutes Auslagerungsmanagement und Informationssicherheitsmanagement geboten. Ein gutes Auslagerungsmanagement-Framework wird desto kritischer, je mehr Auslagerungen stattfinden, während das Informationssicherheitsmanagement auch mit wachsender Anzahl an IT-Auslagerungen nicht an Bedeutung verlieren darf. Letzteres ist vor allem der Tatsache geschuldet, dass Auslagerungen nicht von der Pflicht der Steuerung und Kontrolle über alle kritischen Prozesse sowie deren Unterstützungsinstrumente entbinden. Aus Management-Perspektive ist es wichtig, vor Auslagerungen an Hyperscaler und ausländische Unternehmen ohne Erfahrung mit der deutschen/ europäischen Finanzindustrie hinreichend Zeit für eine Vertragsverhandlung einzuplanen.

[11] Digital Operational Resiliance Act, in unseren zwei Blogposts zu DORA beschreiben wir DORA gesamthaft und stellen die Neuerungen für den Finanzsektior dar: https://core.se/de/blog/dora-regulation-der-technologien-im-finanzsektor resp. https://core.se/de/blog/dora-deltabetrachtung.

Verfasser

Waldemar Grudzien ist Expert Partner bei CORE und Gründer der Regulation and Compliance Practice. Er wurde in Elektrotechnik promoviert und verfügt über ein Diplom in VWL. Schwerpunkte seiner Arbeit sind Informationssicherheit und Datenschutz – in Theorie und Praxis, inklusive der Tätigkeit als ISB und DSB in verschiedenen Klientensituationen. Er unterstützt Klienten im Aufbau und sicherem Betrieb zertifizierungsfähiger ISMS.

Mail: waldemar.grudzien@core.se

Liubov Khomutovskaya ist Senior Legal Expert bei CORE. Sie ist Wirtschaftsjuristin und arbeitet schwerpunktmäßig im Bereich Verhandlung und Gestaltung von IT-Verträgen sowie zu Themen der Informationssicherheit.

Mail: liubov.khomutovskaya@core.se

Moritz Treutwein ist **Transformation Manager** bei CORE. Sein Beratungsschwerpunkt ist Banking & Capital Markets, dabei umfasst seine Expertise unter anderem die Steuerung und Umsetzung von Geschäftsfelderweiterungen im Rahmen von IT-Implementierungsprojekten, Audit Remediations, sowie die Entwicklung digitaler Geschäftsmodelle. Darüber hinaus ist er Informationssicherheitsbeauftragter bei CORE.

Mail: moritz.treutwein@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se