VÖB DIGITAL

Der Weg in die Cloud – mühsam, aber lohnend

Cloud-Computing beschreibt die Nutzung geteilter Computerressourcen – in der Regel über das Internet und geräteunabhängig. Entsprechende Dienstleistungen werden in Form von Servern, Datenspeichern oder Applikationen bereitgestellt und je nach Umfang und Einsatz abgerechnet. Für viele Finanzinstitute ist die Nutzung von Cloud-Diensten unumgänglich geworden. Gleichzeitig ist sie mit zahlreichen aufsichtlichen und regulatorischen Anforderungen verbunden.

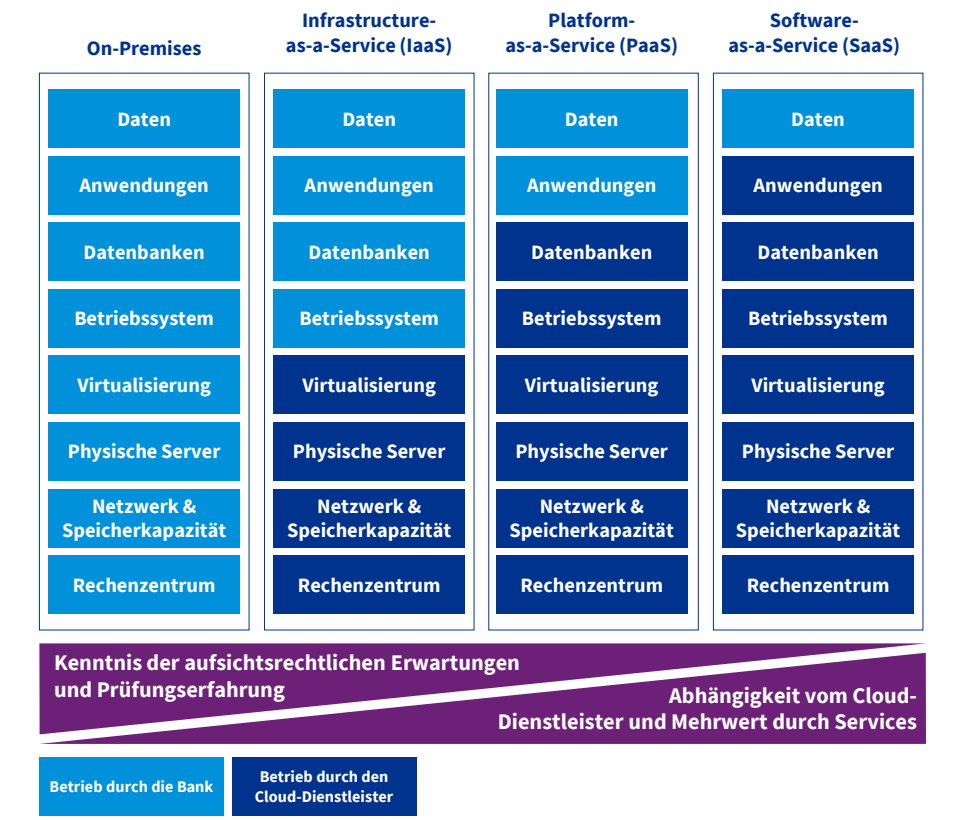
Für Banken ist Cloud-Computing ein entscheidender Innovationstreiber. Zahlreiche Institute nutzen bereits Speicher- und Rechenkapazitäten von Cloud-Dienstleistern. Im Gegensatz zu einem Betrieb in eigenen lokalen Rechenzentren („On-Premises“) können große Anbieter meist schnellere Rechengeschwindigkeiten und flexibel abrufbare Rechen- und Speicherkapazitäten bereitstellen. Diese Skalierbarkeit ermöglicht eine Leistungssteigerung je nach Bedarf und somit einen ökonomisch effizienteren Betrieb. Zudem müssen die Finanzinstitute nicht die mit eigenen Rechenzentren verbundene notwendige Technik vorhalten.

Die Leistungsfähigkeit von Cloud-Anwendungen ermöglicht es Banken, effektiv mit großen Datenvolumina zu arbeiten und sie für innovative Dienstleistungen einzusetzen. So sind bestimmte Anwendungen teilweise bereits für einzelne Kundengruppen und Dienste abrufbar. Vorteile von Cloud-Nutzungen sind beispielsweise passgenaue Management-Reports und Auswertungen, der Einsatz maschinellen Lernens bei der Betrugsbekämpfung oder bei Know-your-Customer(KYC)-Prozessen sowie komplexe Kundendatenanalysen, um einen wettbewerbsfähigen Kundenservice und individualisierte Finanzprodukte anbieten zu können. Global betrachtet betreiben einige Banken schon weite Teile ihres Kernbankensystems in der Cloud.

Es werden folgende drei Typen von Cloud-Auslagerungen nach dem jeweiligen Umfang an übertragenen Services unterschieden (Abb. 1). Beim Modell Infrastructure-as-a-Service (IaaS) stellt der Dienstleister die Basisinfrastruktur wie Rechenkapazität und Speicherplatz bereit. Platform-as-a-Service (PaaS) ermöglicht darüber hinaus, dass eigene Anwendungen in einer standardisierten Software-Umgebung des Dienstleisters entwickelt und betrieben werden. Bei Software-as-a-Service (SaaS) werden Anwendungen und Software bereits vollständig in der Cloud zur Verfügung gestellt. Die Modelle PaaS und SaaS bieten der Finanzwirtschaft das größte Potenzial an digitalen und innovativen Technologien, die meist rechen- und speicherintensiv sind. Gleichzeitig steigt die Abhängigkeit von Cloud-Dienstleistern kontinuierlich von IaaS über PaaS bis hin zu SaaS, verbunden mit abnehmenden organisatorischen und technischen Kontrollmöglichkeiten.

Nur wenige Branchen unterliegen so umfangreichen regulatorischen Anforderungen wie die Finanzwirtschaft. Die Sicherheit von Daten und Informationen liegt dabei im ureigenen Interesse der Institute und bildet zugleich die Grundlage für das Vertrauen von Kundinnen und Kunden. Während die aufsichtsrechtlichen

Abbildung 1: Cloud-Service-Modelle und deren Grad der Abhängigkeit vom Cloud-Dienstleister



Quelle: Erörterung im Fachgremium IT der BaFin, 2021/22

Erwartungen an eigene Rechenzentren mit den Mindestanforderungen an das Risikomanagement (MaRisk) der BaFin hinlänglich bekannt sind, stehen Finanzinstitute bei der Nutzung von Cloud-Services vor der Herausforderung, die Vorgaben gemeinsam mit ihren Dienstleistern in verteilten Rollen sicherzustellen. Dabei erfordert die Zusammenarbeit, besonders mit großen Anbietern außerhalb der Finanzbranche, passgenaue und innovationsoffene Spezialregeln.

Anforderungen der Compliance als größte Hürde

Auf dem Weg in die Cloud stellt sich für Finanzunternehmen zunächst die Frage, wie die Übertragung von Daten und Prozessen in einen Cloud-Betrieb sicher gestaltet werden kann. Branchenspezifische oder individuelle Anforderungen der stark regulierten Finanzinstitute sind häufig nicht erfüllbar, da vorwiegend große internationale Cloud-Anbieter wie Amazon, Google oder Microsoft zwar hochstandardisierte und automatisierte Services anbieten, jedoch den europäischen datenschutz- und aufsichtsrechtlichen Vorgaben nicht ausreichend gerecht werden. Daher stellen die Identifikation und Bewertung von Aus- und Weiterverlagerungsrisiken kontinuierliche Herausforderungen dar und bleiben auch nach der Wahl des Dienstleisters fester Bestandteil des weiteren IT-Risikomanagement-Prozesses. Datenschutz-Compliance, Cyber- und Ausfallsicherheit müssen ebenfalls regelmäßig geprüft und sichergestellt werden. Demnach können die Anforderungen der Cloud-Compliance mithilfe der drei Handlungsfelder Informationssicherheit, IT-Betrieb und Auslagerungsmanagement strukturiert werden.

Informationssicherheit und Internes Kontrollsystem

Rechtliche Bestimmungen zum Datenschutz, zur Datenverarbeitung und -speicherung sind stets einzuhalten. Ferner muss der Ort der Speicherung und Verarbeitung bekannt sein. Bei einem nicht vermeidbaren Datentransfer außerhalb der EU droht ein Verstoß gegen die Datenschutzgrundverordnung (DSGVO). Denn

nachdem der Europäische Gerichtshof (EuGH) das Datenschutzabkommen zwischen Europäischer Union und den USA, den Data Privacy Shield, mit dem Schrems-II-Urteil für unwirksam erklärt hatte, ist keine Rechtsgrundlage mehr für den Datentransfer zwischen EU-Firmen und großen US-amerikanischen Cloud-Anbietern bis zur Einigung auf ein neues Privacy Shield nutzbar. In der Zwischenzeit bleibt Banken und Finanzdienstleistern lediglich die Möglichkeit, sogenannte Standardvertragsklauseln einzusetzen. Hierbei handelt es sich um von der Europäischen Kommission veröffentlichte Vertragsmuster, die den Datentransfer zwischen der EU und Drittländern regeln. Diese Klauseln reichen allerdings in der Regel nicht aus, sodass sie durch angemessene technisch-organisatorische Maßnahmen (TOMs) ergänzt werden. Sie zielen darauf ab, die in der Cloud zu verarbeitenden Informationen zusätzlich vor Zugriffen Dritter zu schützen.

Zudem müssen Kontrollen des Cloud-Dienstleisters in das Interne Kontrollsystem (IKS) der Bank einfließen, sodass deren Wirksamkeit regelmäßig geprüft werden kann. Dabei können Zertifikate des Dienstleisters zwar für das Monitoring herangezogen werden, aber reichen als alleinige Überwachungshandlung nicht aus. Die Wirksamkeit des IKS eines Dienstleisters ist ebenfalls zu prüfen. Da sich aufgrund des hohen Aufwands eine eigenständige Überprüfung nur schwer umsetzen lässt, ist hierfür das Heranziehen von externen Zertifikaten notwendig.

IT-Betrieb

Die Abhängigkeiten und Zusammenhänge der IT-Systeme der Bank sind mit der Hardware des Cloud-Dienstleisters im Konfigurationsmanagement zu berücksichtigen – insbesondere auch als Basis für das Risikomanagement und die Notfallvorsorgeplanung. Zudem müssen Notfallkonzepte erstellt und mit dem Dienstleister abgestimmt werden. Veränderungen an IT-Systemen wie der Austausch von Hardware-Komponenten sind durch das Institut zu steuern und zu dokumentieren. Der Dienstleister muss zudem Störungen im Regelbetrieb beheben und ihre Ursachen nachverfolgen und analysieren.

Insgesamt wird aufsichtlich eine aktive Dienstleistersteuerung vom beauftragenden Institut gefordert, die unter anderem mit einem ineinandergreifenden Incident- und Problem-Management-Prozess eine kontinuierliche Überwachung der Einhaltung der Dienstleistungserbringung und der einhergehenden Risiken ermöglicht.

Auslagerungsmanagement

Weisungsrechte eines Instituts gegenüber einem Cloud-Dienstleister sind vertraglich zu vereinbaren, sofern sie über eine entsprechende Leistungsbeschreibung nicht bereits eindeutig definiert und Bestandteil des Dienstleistungsvertrages sind. Zudem sind uneingeschränkte Informations- und Prüfrechte – auch für die Aufsichtsbehörden – vertraglich zu verankern. Wenn ein Cloud-Dienstleister Subunternehmen beauftragt, sind diese Weiterverlagerungen vorab zu genehmigen beziehungsweise Modalitäten für mögliche Weiterverlagerungen vertraglich festzulegen. Schließlich sind angemessene Kündigungsrechte und -fristen, zum Beispiel bei wesentlichen Änderungen sowie ein Kündigungsrecht aus wichtigem Grund, beispielsweise auf begründetes Verlangen der Aufsicht, zu vereinbaren. In diesem Zusammenhang ist eine Exit-Strategie mit Handlungsoptionen und Ausstiegsprozessen zu definieren und regelmäßig auf ihre Durchführbarkeit zu prüfen. Hinsichtlich der aufsichtsrechtlich geforderten Analyse von Auslagerungsrisiken ist es problematisch, dass der konkrete Speicherort in verteilten Cloud-Lösungen aufgrund der Virtualisierung häufig nicht konkret bestimmbar oder gegebenenfalls lediglich regional eingrenzbar ist. Hier besteht die Notwendigkeit der Aufsicht, traditionelle Bewertungsparameter modernen, innovativen Cloud-Lösungen anzupassen – selbstverständlich in der Steuerungshoheit der Bank und strategisch sowie konzeptionell prüfbar verankert.

Abbildung 2: Zusammenfassung der Handlungsfelder

Feld	Thema	Quellen
Informationssicherheit/IKS	Datensicherheit/ -schutz	EBA Guidelines on Outsourcing Tz. 75 + 84 BaFin Mindestanforderungen an das Risikomanagement (MaRisk) AT 9 Tz. 7 BaFin Orientierungshilfe zu Auslagerungen an Cloud-Anbieter Kap. V. 5 Datenschutzgrundverordnung (DSGVO) Art. 45 (1)
IT-Betrieb	Konfigurationsmanagement	Bankaufsichtliche Anforderungen an die IT (BAIT) 7 Tz. 46
	Notfallmanagement	MaRisk AT 7.3 Tz. 1
	Change Management	BAIT 7 Tz. 48–49
	Incident- / Problem-Management	BAIT 7 Tz. 50
Auslagerungen	Weisungsrechte	BaFin Orientierungshilfe Kap. V. 4 MaRisk AT 9 Tz. 7
	Prüfrechte / Pooled Audits	BaFin Orientierungshilfe Kap. V. 2 + 3 MaRisk AT 9 Tz. 7 b + c EBA G. Tz. 87, 89, 91
	Weiterverlagerungen	EBA G. Tz. 78 MaRisk AT 9 Tz. 7–8
	Kündigungsmodalitäten	MaRisk AT 9 Tz. 7 BaFin Orientierungshilfe Kap. 6
	Exit-Strategie	MaRisk AT 9 Tz. 6 BaFin Orientierungshilfe Kap. V. 6 EBA G. Tz. 107

Quelle: Erörterung im Fachgremium IT der BaFin, 2021/22

Der Weg in die Cloud lohnt sich – trotz hoher Anforderungen

Cloud-Services haben in der Finanzbranche in den letzten Jahren erheblich an Bedeutung gewonnen. Der hohe Grad an Standardisierung über alle Kundengruppen hinweg und die daraus resultierenden Skaleneffekte bringen nicht nur potenzielle Effizienzgewinne mit sich, sondern auch qualitative Vorteile gegenüber klassischen Infrastruktur-Bereitstellungsmodellen. Denn neue digitale Bankdienste und Anwendungen, beispielsweise auf Basis von Künstlicher Intelligenz, sind oftmals nur durch die von Cloud-Anbietern ermöglichte Rechenleistung zu verwirklichen. Um eine sichere Nutzung der Cloud zu gewährleisten, müssen die verschiedenen organisatorischen, prozessualen und regulatorischen Anforderungen in den drei beschriebenen Handlungsfeldern der IT-Governance bzw. Compliance Informationssicherheit, IT-Betrieb und Auslagerungsmanagement erfüllt werden.

Ob zukünftig jede Bank von Cloud-Dienstleistungen profitieren kann, hängt davon ab, inwieweit Institute hinsichtlich der hohen gesetzlichen und aufsichtsrechtlichen Konformitätsanforderungen entlastet werden. In der Praxis können durch eine gemeinschaftliche Prüfung von Dienstleistern Doppelprüfungen vermieden werden (Audit-Pools). Das ist ein erster Schritt, der jedoch regulatorisch verankerte Entlastungen nicht ersetzen kann. Hierzu zählen beispielsweise Zertifizierungen von Dienstleistern und die dringend notwendige Verabschiedung eines neuen transatlantischen Datenschutzrahmens.

VÖB DIGITAL

UNSERE POSITIONEN

Wir fordern eine Entlastung der Institute bei der Nutzung von Cloud-Dienstleistungen beispielsweise mittels standardisierter Zertifizierungen. Diese sollten im Sinne eines risikobasierten Ansatzes nach Art und Kritikalität der verarbeiteten Daten und ausgelagerten Prozesse ausgestaltet sein.

Wir unterstützen die Initiative der EU, weiterhin den Datentransfer in US-amerikanische Unternehmen über Standardvertragsklauseln zu ermöglichen. Diese Maßnahmen reichen jedoch nicht aus, um ein akzeptables Datenschutzniveau zu erreichen. Wir begrüßen daher die in diesem Jahr erfolgte politische Einigung zwischen der EU und den USA auf einen erneuerten transatlantischen Datenschutzrahmen. Dieser sollte schnellstmöglich ausgearbeitet werden.

Wir betrachten die europäische Initiative GAIA-X zur Förderung der Dateninfrastruktur als eine Möglichkeit zur Stärkung der digitalen Souveränität der EU gegenüber den außereuropäischen Digitalkonzernen. Das Projekt sollte jedoch deutlich besser finanziert und weniger bürokratisch ausgestaltet werden. Andernfalls wird es keine Alternative zu den preislich attraktiven und leistungsfähigen Angeboten der US-amerikanischen Konzerne im Bereich Cloud-Computing bieten.

Über VÖB Digital

Die Digitalisierung verändert das Bankgeschäft tiefgreifend und stellt Banken vor enorme Herausforderungen, denen es aktiv zu begegnen gilt. Diesen Transformationsprozess wollen wir mit unserem Newsletter VÖB Digital beleuchten – aber auch aktiv mitgestalten. Mit VÖB Digital zeigen wir nicht nur Herausforderungen, sondern auch Chancen auf, suchen nach Lösungen und stellen Entwicklungsperspektiven dar.

Sie wollen VÖB Digital abonnieren?

*Dann schreiben Sie bitte eine E-Mail an **presse@voeb.de.** Geben Sie einfach den Betreff „Anmeldung VÖB Digital“ an.*

*Alle VÖB-Newsletter sowie weitere VÖB-Publikationen können Sie unter **www.voeb.de/publikationen** abonnieren und downloaden.*

IMPRESSUM
Bundesverband Öffentlicher Banken Deutschlands, VÖB
Lennéstraße 11, 10785 Berlin
Telefon: 030 8192-0
E-Mail: presse@voeb.de | Internet: www.voeb.de
Redaktion: Bereich Zahlungsverkehr und Informationstechnologie
Redaktionsschluss: 21. November 2022
Foto: shutterstock, whiteMocca
Registernummer im Transparenz-Register der EU: 0767788931-41