Cloud: Von Stolperfalle zu Sicherheitsnetz

Regulatorische Konformität und Cloud-Sicherheit im Finanzsektor meistern

Julija Brull
Liubov Khomutovskaya
Fabian Meyer

Key Facts

- Der Finanzsektor erlebt einen Wandel - On-Premise-Lösungen gehören langsam der Vergangenheit an, cloudbasierte Dienste von Unternehmen wie Microsoft, Amazon, Google und IBM dominieren den Markt
- Regulatorisch ist der Einsatz der Cloud im Finanzsektor möglich, erfordert jedoch die Einhaltung einer Reihe regulatorischer Anforderungen, die auf europäischer Ebene gelten (z.B. BAIT, DORA)
- Finanzinstitute laufen Gefahr, die regulatorischen Mindestanforderungen nicht zu erfüllen, weil sie oft keinen ausreichenden Überblick über die zusätzlich benötigten Cloud-Anforderungen, neben den bereits bestehenden Anforderungen an die Informationssicherheit, haben
- Bei großen Projekten, wie Cloud-Transformationen, fehlen der Linienfunktion häufig die erforderlichen Kapazitäten und Erfahrungen, um alle Compliance-Aspekte abzudecken - insbesondere das Verständnis der damit verbundenen Risiken wird hier zum kritischen Faktor
- Finanzinstitute können erfolgreich Cloud-Lösungen einsetzen, wenn sie neben der Definition einer Cloud-Strategie eine Risikoanalyse durchführen, Verträge mit Cloud-Anbietern aktiv mitgestalten, interne Vorgaben und Prozesse evaluieren und anpassen und eine zusätzliche Cloud-Ausstiegsstrategie entwickeln
- Hier sollten keine Kompromisse eingegangen werden: die kontinuierliche Einbindung eines Compliance-Streams während des gesamten Transformationsprozesses in die Cloud ist das Schlüsselkriterium, um Risiken erfolgreich zu erkennen und zu minimieren

1. Der Weg der Cloud im Finanzsektor

1.1. Geht Erfolg noch ohne Cloud?

Unternehmen wie Amazon, Microsoft, IBM und Google machten den Anfang, Oracle, SAP und andere folgten und prägten den Markt für cloudbasierte Lösungen so, dass die Nachfrage von Jahr zu Jahr steigt und Cloud-Computing stetig an Relevanz gewinnt[1]. Gartner zufolge werden voraussichtlich bis zum Jahr 2026 etwa 75% der Unternehmen ein Cloud-unterstütztes Betriebsmodel einführen. Angesichts dieser Entwicklung passen Hyperscaler ihre Strategien an und bieten vermehrt cloudbasierte Dienste als integralen Bestandteil ihrer Software-Lösungen an, während on-premise Lösungen langfristig eher ersetzt werden.[2] Ein Beispiel dafür ist Microsoft, das in den letzten Jahren seine Cloud-Plattform Azure stark ausbaute und nun zahlreiche cloudbasierte Dienste anbietet. Dazu gehören auch Software-as-a-Service (SaaS)-Lösungen wie das Enterprise Resource Planning (ERP)-System Dynamics 365[3]. Auch Oracle forcierte seine Cloud-Strategie und bietet eine Vielzahl von cloudbasierten Diensten an, einschließlich SaaS-Lösungen wie Oracle Human Capital Management (HCM) Cloud und Oracle Enterprise Resource Planning (ERP) Cloud[4]. Oracle kündigte zudem an, in Zukunft verstärkt auf cloudbasierte Lösungen zu setzen und seine On-Premise-Lösungen langfristig zu reduzieren.[5] Ebenso verkündete SAP, seine Geschäftsstrategie auf Cloud-Lösungen auszurichten.[6] Das Unternehmen bietet bereits eine Vielzahl von cloudbasierten Diensten an, darunter SaaS-Lösungen wie SAP SuccessFactors und SAP S/4HANA Cloud. Diese Unternehmen sind nur einige Beispiele dafür, wie sich der Markt für Software-Lösungen von On-Premises hin zu cloudbasierten Diensten bewegt.

Wichtige bereits bekannte Treiber für die Nutzung von Cloud-Lösungen sind z.B. die einfache Bereitstellung skalierbarer Rechenleistung für die Echtzeitdatenverarbeitung sowie die Kosteneffizienz durch nutzungsbasierte Abrechnung und Vermeidung hoher Investitionen in den Betrieb eigener Infrastruktur. Ein weiterer wichtiger Faktor ist die Flexibilität der Cloud-Technologie, die es Unternehmen ermöglicht, standortübergreifend auf standardisierte Tools und Dienstleistungen zuzugreifen, was die Zusammenarbeit und den Austausch erleichtert. Die Wartung und Aktualisierung der Software wird von den Cloud-Anbietern übernommen, sodass sich die Unternehmen auf ihr Kerngeschäft konzentrieren können. Darüber hinaus ist die Sicherheit als einer der zentralen Treiber zu nennen, da Daten auf nicht transportablen Hardwaregeräten gespeichert werden und regelmäßige Aktualisierungen und Sicherheitspatches zentral gewährleistet werden. Die Cloud fördert auch Innovationen, da Unternehmen neue Produkte und Geschäftsmodelle schneller testen und einführen können. Nicht zuletzt treiben

[1] Oracle, 2023, https://www.oracle.com/de/applications/
[2] Cloudflight, 2023, https://www.cloudflight.io/de/blog/cloud-oder-nichts-der-klare-plan-von-microsoft-fuer-die-zukunft-von-office/
[3] Gartner, 2022, https://www.cloudcomputing-insider.de/zukunftstechnologien-treiben-die-cloud-ausgaben-a-7c320e4b116758ae4dbe6497a265117c/
[4] Oracle, 2023, https://www.oracle.com/de/applications/
[5] Software ONE, 2021, https://www.softwareone.com/en/blog/all-articles/2020/11/25/oracle-stops-selling-on-premise-term-licenses
[6] Forrester, 2023, https://www.forrester.com/blogs/whats-up-with-the-saps-cloudification-strategy-in-europe/

technologische Trends wie generative künstliche Intelligenz (generative AI) und Metaverse-Anwendungen derzeit das Wachstum des public Cloud Geschäfts voran.[7] Metaverse und Cloud Computing sind eng miteinander verbunden, da Unternehmen ihre virtuellen Welten auf Cloud-Infrastrukturen verlagern müssen, um vorrangig Skalierbarkeit und Verfügbarkeit und gewährleisten. Ohne diese Basis der Cloud ist der Aufbau eines Metaverse praktisch nicht realisierbar.[8]

Diese Vorteile machen die Cloud zu einer attraktiven Option für Unternehmen in der Finanzindustrie, um die digitale Transformation voranzutreiben und ihre Wettbewerbsfähigkeit zu stärken.

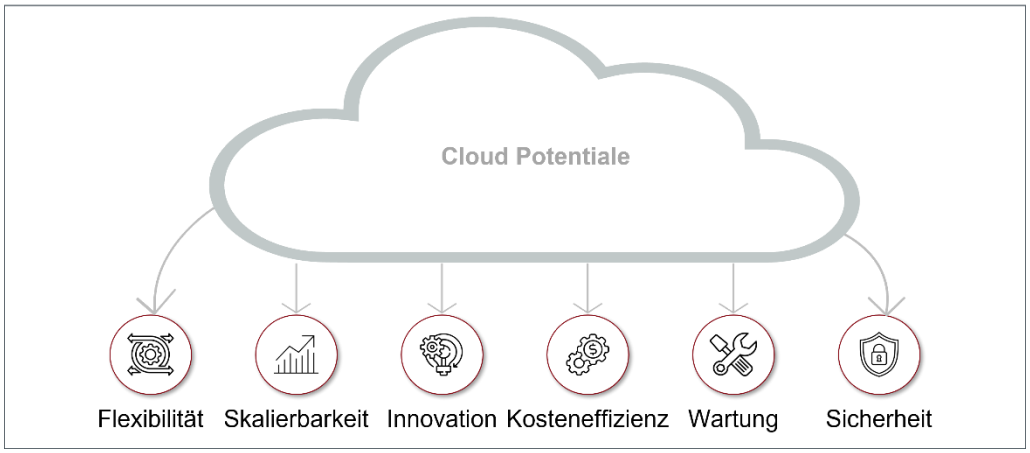

Abbildung 1: Potentiale von Cloud-Diensten für Unternehmen

Laut der Studie von Flexera aus dem Jahr 2022, in der 501 Technologieführungskräfte aus unterschiedlichen Branchen befragt wurden, entfallen 11 % (Median) ihrer gesamten IT-Ausgaben auf Cloud- und Technologie-Hosting-Lösungen. Dies stellt den zweitgrößten Anteil nach den Softwareausgaben (18% des IT-Budgets) dar. Bei den in der Studie befragten Branchen sind Finanzinstitute mit 21 % die größten Vertreter.[9]

[7] Statista, 2022, https://de.statista.com/statistik/studie/id/85672/dokument/public-cloud-report/
[8] Infoworld, 2022, https://www.infoworld.com/article/3652496/cloud-computing-and-the-metaverse.html
[9] Flexera, 2022, https://info.flexera.com/FLX1-REPORT-State-of-Tech-Spend

Zudem wird laut Gartner für 2023 erwartet, dass weltweit die Ausgaben der Endnutzer für öffentliche Cloud-Dienste auf bis zu 600 Mrd. USD steigen werden, was einem Wachstum von

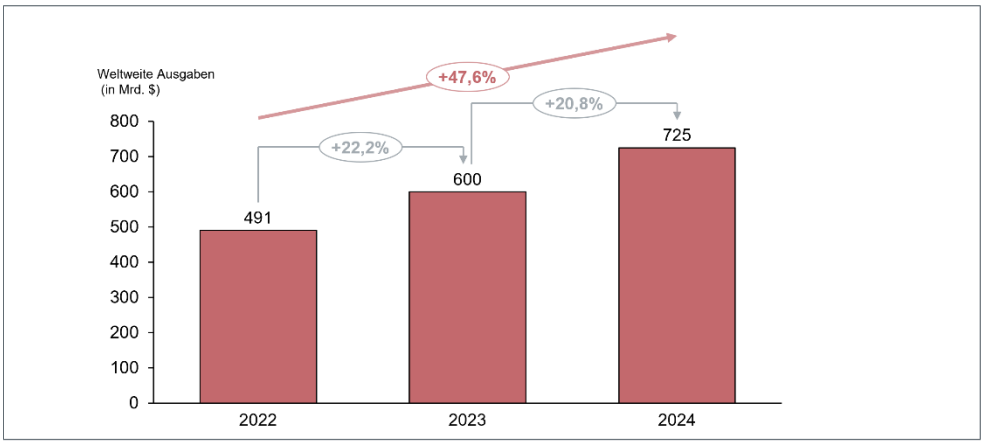

Abbildung 2: Weltweite (erwartete) Ausgaben der Endnutzer für öffentliche Cloud-Dienste 2022 – 2024[8]

etwa 22% im Vergleich zum Vorjahr (2022: 491 Mrd. USD) entspricht. Für das Jahr 2024 wird sogar ein noch stärkerer Anstieg auf 724,5 Mrd. USD im Vergleich zu 2022 prognostiziert, was einem Wachstum von fast 50% entspricht.[10]

Die Cloud ist ein entscheidender Faktor bei den Bemühungen der Unternehmen zur Digitalisierung und unterstützt die Umsetzung ihrer angestrebten Geschäfts- und Transformationsziele. Große Kunden von Microsoft migrierten ihre SAP-Workloads und andere „mission-critical Anwendungen“[11] bereits erfolgreich in die Azure Cloud. Dies zeigt einmal mehr, dass die Cloud inzwischen zur wichtigsten Technologieplattform für globale Unternehmen zählt. Dabei geht es nicht allein um SAP, sondern um alle wichtigen Anwendungen, die eine stark schwankende/variable oder eine hohe Arbeitslast mit sich bringen.[12] Hierbei sind natürlich auch Finanzinstitute keine Ausnahme. Mit Blick auf den europäischen Finanzmarkt sind zahlreiche Bestrebungen von Instituten zu verzeichnen, die Kernbereiche ihrer Infrastruktur in die Cloud umziehen wollen.

So kündigte die Deutsche Bank im Jahr 2020 eine mehrjährige strategische Partnerschaft mit Google Cloud an. Durch die (Teil-)Migration des Kernbankensystems in die Cloud werde eine stabilere IT und die schnellere Markteinführung neuer Produkte ermöglicht, sowie die zielgerichtete Auswirkung auf Trends und Bedürfnisse ihrer Kunden besser erreicht.[13]

Auch in der Schweiz ziehen die Banken nach. Die HSBC Private Bank Switzerland plant im Rahmen einer umfassenden Modernisierungsinitiative ihres IT-Systems ihre Dienstleistungen bis

[10] Gartner, 2022, https://www.cloudcomputing-insider.de/zukunftstechnologien-treiben-die-cloud-ausgaben-a-7c320e4b116758ae4dbe6497a265117c/
[11] Diese werden regulatorisch als sog. „wesentliche Aauslagerungen“ eingestuft und unterliegen erhöhten Anforderungen
[12] Forbes, 2018, https://www.forbes.com/sites/bobevans1/2018/02/28/microsoft-cloud-hits-superscale-as-huge-customers-migrate-mission-critical-sap-workloads-to-azure/
[13] Deutsche Bank, 2020, https://www.db.com/news/detail/20201204-deutsche-bank-and-google-cloud-sign-pioneering-cloud-and-innovation-partnership?language_id=3

Ende 2023 in die Cloud verlagern. Ein Ziel dabei ist die Steigerung der Wettbewerbsfähigkeit durch den Einsatz von Cloud-Technologie.[14]

Um im Wettbewerb erfolgreich zu bleiben und den steigenden Kundenanforderungen gerecht zu werden, definierte auch BNP Paribas in Frankreich die Beschleunigung ihrer digitalen Transformation und die Verbesserung der operativen Effizienz der Gruppe als strategische Ziele. Bereits im Jahr 2003 gründete BNP Paribas ein Joint Venture mit IBM, um ihre Cloud-Vorhaben voranzutreiben. Nach der Einführung ihrer ersten privaten IBM Cloud im Jahr 2013 wurde 2019 die Integration der IBM Cloud in dedizierte Rechenzentren von BNP Paribas angekündigt. Die Partnerschaft mit IBM und die Nutzung von IBM Hybrid Cloud-Lösungen ermöglichen es BNP Paribas ihre Dienstleistungen für Kunden zu verbessern und die Entwicklung neuer digitaler Anwendungen zu unterstützen.[15]

Zu den bereits genannten Beispielen kann eine Reihe weiterer hinzugezählt werden, z.B. der spanische Finanzdienstleister Banco Bilbao Vizcaya Argentaria (BBVA) und der Versicherer Allianz Deutschland.[16,17] Sie alle verdeutlichen, dass Cloud-Migrationen in erster Linie dazu dienen, sich noch stärker auf die Bedürfnisse der Kunden auszurichten und entlang dieser die Einführung neuer Dienste zu beschleunigen. Dies geschieht nicht nur, um mit der Konkurrenz Schritt zu halten, sondern vorrangig als Grundvoraussetzung, um sich im Wettbewerb noch stärker differenzieren zu können. Die strategische Verfolgung von Cloud-Zielen richtet sich insbesondere auf die Kernbereiche bzw. Teile des Kernbankensystems von Finanzinstituten und unterstreicht somit erneut die Bedeutung der Cloud-Technologie.[18,19]

Die Entwicklung der Zusammenarbeit von Finanzinstituten mit Cloud-Anbietern bleibt derweil jedoch nicht ohne regulatorische Folgen. Dass der digitale Wandel zu einer verstärkten Auslagerung an und Nutzung oder gar Abhängigkeit von Informations- und Kommunikationstechnologien Dienstleistungen (IKT-Dienstleistungen)[20] geführt hat, wird ebenfalls vom Europäischen Parlament und dem Rat der Europäischen Union erkannt und adressiert. Einer der Erwägungsgründe zu dem Digital Operations Resilience Act (DORA) geht auf diesen Umstand ein: „Da es unvorstellbar geworden ist, Finanzdienstleistungen ohne die Nutzung von Cloud-Computing-Diensten, Softwarelösungen und datenbezogenen Dienstleistungen zu erbringen, ist das Finanzökosystem der Union zwangsläufig immer abhängiger von bestimmten IKT-Dienstleistungen geworden, die von IKT-Dienstleistern bereitgestellt werden.“[21] Infolgedesse reagieren sowohl Gesetzgeber als auch

[14] IT-Markt, 2022, https://www.it-markt.ch/news/2022-02-17/hsbc-schweiz-will-dienste-in-die-cloud-verlagern-und-stellen-streichen
15 BNP Paribas, 2019, https://group.bnpparibas/en/press-release/bnp-paribas-signs-agreement-ibm-services-deploy-cloud-strategy
[16] BBVA, 2022, https://www.bbva.com/en/innovation/google-cloud-spotlights-bbvas-transformation-into-a-digital-enterprise/
[17] CIO, 2019, https://www.cio.de/a/cto-shell-trimmt-allianz-auf-agilitaet,3625422
[18] IT-Finanzmagazin, 2021, https://www.it-finanzmagazin.de/cloud-banken-studie-122005/
[19] Forbes, 2018, https://www.forbes.com/sites/bobevans1/2018/02/28/microsoft-cloud-hits-superscale-as-huge-customers-migrate-mission-critical-sap-workloads-to-azure/
[20] Informations- und Kommunikationstechnologien
[21] s. Erwägungsgrund 79 der DORA

Aufsichtsbehörden, indem sie robuste Auslagerungs- und Kontrollprozesse fordern, um Auslagerungsrisiken zu begegnen.

1.2. Ist Cloud im Finanzsektor regulatorisch möglich?

Der Cloud-Einsatz orientiert sich nicht nach speziell auf die Cloud abstellenden Gesetzen, sondern fügt sich in ein bestehendes Rahmenwerk für das Risikomanagement, Informationssicherheit, IT- und Auslagerungsmanagement ein. Es gibt eine Vielzahl von regulatorischen Anforderungen, die erfüllt werden müssen. Hervorzuheben ist auf EU-Ebene die DORA, die ab dem 17. Januar 2025 in Kraft tritt, sowie die bereits in Kraft getretene Datenschutz-Grundverordnung (DSGVO).[22] Auf nationaler Ebene in Deutschland sind vor allem die Mindestanforderungen an das Risikomanagement (MaRisk)[23] und Bankaufsichtlichen Anforderungen an die IT (BAIT) zu beachten. Zusätzlich zu diesen bindenden Regelungen veröffentlichten unterschiedliche Behörden und Institutionen Leitlinien, Empfehlungen und Standards, die sich mit der Gestaltung des Cloud-Einsatzes im Einklang mit den genannten Vorschriften befassen. Dies ist vor allem notwendig, da (häufig auch aus Projekt- und Technologieperspektive komplizierte) Cloud-Transformationen praktische Herausforderungen für Risiko- und Compliance-Prozesse von Instituten darstellen.

Besonders hervorzuheben sind die im Jahr 2021 von der European Securities and Markets Authority (ESMA)[24] herausgegebenen Leitlinien zur Auslagerung an Cloud-Anbieter.[25] Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) beabsichtigt, diese ESMA Leitlinien anzuwenden und sie als Maßstab bei Überprüfungen heranzuziehen.[26] Diese bindenden regulatorischen Vorgaben sowie Leitlinien und Empfehlungen konzentrieren sich auf folgende Aspekte und werden im nächsten Kapitel vertieft:

- Definition einer Strategie für den Cloud-Einsatz
- Durchführung einer Risikoanalyse und Berücksichtigung mitigierender Maßnahmen bei der Planung und Einführung von Cloud-Lösungen
- Definition interner Vorgaben an Prozesse, insbesondere zur Informationssicherheit
- Vertragsgestaltung mit dem Cloud-Anbieter
- Definition einer Ausstiegsstrategie

Der eindeutige Trend im Finanzsektor in Richtung Cloud zeigt, dass ein praktischer Druck zum Einsatz und zur Nutzung der Cloud besteht. Die Institute stehen vor der Herausforderung den Cloud-Einsatz regulatorisch konform im Einklang mit Regelungen aus unterschiedlichen Rechtsrahmen zu gestalten. Diese Herausforderungen betreffen sowohl strategische als auch

[22] DSGVO VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679
[23] Rundschreiben 10/2021 (BA) Mindestanforderungen an das Risikomanagement – MaRisk, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html
[24] ESMA50-164-4285, 2021, https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines_de.pdf
[25] ESMA50-164-4285, 2021, https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines_de.pdf
[26] BaFin, 2021, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2021/meldung_2021_06_29_Anwendung_ESMA_Leitlinien.html

operative Aspekte und lassen sich allein aus der Linienfunktion heraus schwer meistern. Geplante Cloud-Transformationen sollten daher Compliance-Aspekte von Anfang an in das Projekt einbeziehen.

2. Regulatorische Anforderungen an den Cloud-Einsatz von Strategie bis Umsetzung

Im nächsten Abschnitt werden die regulatorischen Anforderungen an den Cloud-Einsatz näher betrachtet. Anschließend wird ein Framework vorgestellt, welches deren Berücksichtigung bei Cloud-Transformationen sicherstellt.

2.1 Anforderungen an die Cloud-Strategie

Institute sind auf Basis nationaler und europäischer Vorgaben verpflichtet, eine Cloud-Strategie zu definieren, die im Einklang mit ihrer IT- und Geschäftsstrategie steht. Dies sieht die Ziff. 1 BAIT vor und benennt als Mindestinhalte folgende:

- Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation des Instituts sowie IT-Dienstleistungen und sonstige wichtige Abhängigkeiten von Dritten
- Zuordnung der gängigen Standards, an denen sich das Institut orientiert, auf die Bereiche der IT und der Informationssicherheit
- Ziele, Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation
- Strategische Entwicklung der IT-Architektur
- Aussagen zum IT-Notfallmanagement unter Berücksichtigung der Informationssicherheitsbelange
- Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten)

Die DORA wiederum fordert in Art. 6 Abs. 8 eine Strategie für die digitale operationale Resilienz, mit einer Darlegung der Umsetzung des regulatorischen Rahmens, einschließlich Methoden für das Management von IKT-Risiken und die Erreichung spezifischer IKT-Ziele. Sowohl die „ESMA Leitlinien zur Auslagerung an Cloud-Anbieter“ als auch die „BaFin Orientierungshilfe“ fordern eine klare Strategie für Auslagerungen an Cloud-Anbieter insofern Cloud-Nutzung erfolgt. Diese soll insbesondere auf die Bereiche Informations- und Kommunikationstechnologie, Informationssicherheit und operatives Risikomanagement eingehen.[27]

Unternehmen müssen daher eine fundierte Analyse von Zielen, Risiken sowie Maßnahmen zur Zielerreichung und Risikomitigation durchführen, um eine Basis für ihre Cloud-Strategie zu schaffen.

[27] S. ESMA Leitlinien, Tz. 12

2.2 Risikoanalyse

Bei der Definition der Cloud-Strategie sind bereits erste Überlegungen zur Risikobewertung und zur Risikokonzentration erforderlich.

Wie bei den bestehenden Anforderungen der MaRisk, BAIT und der European Banking Authority (EBA)-Leitlinien zu Auslagerungen, fordert die DORA zusätzlich zu den allgemeinen Risikoüberlegungen des Cloud-Einsatzes eine gründliche Risikoanalyse vor dem Abschluss eines jeden spezifischen Vertrages.[28] Zusammenfassend müssen bei der Risikoanalyse für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen folgende Aspekte berücksichtigt werden:

- IKT-Konzentrationsrisiko (im Zusammenhang mit weiteren bestehenden oder geplanten Auslagerungen, insbesondere wenn diese beim selben Cloud-Anbieter bezogen werden)[29]
- Ersetzbarkeit des Dienstleisters[30]
- Potenzielle Auswirkungen auf:
    - operationelle Risiken (Ziff. 8.5 BAIT fordert hier u.a. die Berücksichtigung möglicher Sicherheits- oder Kompatibilitätsprobleme sowie Aspekte der Datensicherungen der betroffenen IT-Systeme)
    - rechtliche Risiken
    - Risiken für die Einhaltung der Vorschriften
    - Reputationsrisiken des Instituts
    - Risiken für Informations- und Kommunikationstechnologie, Informationssicherheit und Fortführung des Geschäftsbetriebs
    - potenzielle Einschränkungen der Kontrolle für das auslagernde Institut[31]

Zusätzlich zur Risikobetrachtung sieht Art. 29 Abs. 1 lit. b) DORA eine Abwägung von Nutzen und Kosten alternativer Cloud-Lösungen vor, z. B. die Nutzung verschiedener IKT-Drittdienstleister. Letztlich muss eine Abwägung zwischen den erwarteten Vorteilen, einschließlich bedeutender Risiken, die verringert oder besser gesteuert werden können, und den möglichen bedeutsamen Risiken, die sich aus der Vereinbarung über die Auslagerung an Cloud-Anbieter ergeben, vorgenommen werden.[32]

---

[28] S. DORA, EG 66: „Dem förmlichen Abschluss vertraglicher Vereinbarungen sollte eine gründliche Analyse vor Vertragsabschluss zugrunde liegen und diesem vorausgehen, insbesondere indem der Fokus auf Aspekte wie die Kritikalität oder Bedeutung der durch den geplanten IKT-Vertrag unterstützten Dienste, die erforderlichen aufsichtlichen Genehmigungen oder sonstigen Bedingungen, das damit verbundene mögliche Konzentrationsrisiko sowie die Anwendung der Sorgfaltspflicht bei der Auswahl und Bewertung von IKT-Drittdienstleistern gelegt wird, und indem potenzielle Interessenkonflikte bewertet werden."; S. insb. auch Artt. 8, 28 und 29 DORA; s. zusätzlich Tz. 19 lit. b) der ESMA Leitlinien für Auslagerungen an Cloud-Anbieter; S. auf nationaler Ebene auch AT 9 MaRisk sowie Ziff. 7 BAIT

[29] Art. 28 Abs. 4 lit c) und Art. 20 Abs. 1 lit b) DORA

[30] Art. 29 Abs. 1 a) DORA (Verordnung (EU) 2022/2554)

[31] S. Tz. 20 und 21 ESMA Leitlinien für Auslagerungen an Cloud-Anbieter; s. auch AT 8.2 MaRisk

[32] S. Tz. 21 lit b) ESMA Leitlinien für Auslagerungen an Cloud-Anbieter; S. auch Tz. 66 EBA-Leitlinien zu Auslagerungen

Für die Risikobewertung ist ein Due-Diligence-Prozess zwingend vorgesehen,[33] wobei die Anforderungen an die Informationssicherheit bei kritischen Dienstleistungen den höchsten Standards entsprechen müssen.[34] Dabei kann auf Zertifizierungen nach internationalen Standards und auf externe oder interne Prüfberichte zurückgegriffen werden.

Die Risikobewertung ist gem. Art. 5 Abs. 2 lit iii) dem Leitungsorgan des Instituts zu berichten.

Eine Risikoauswertung kann dazu führen, dass von der geplanten Auslagerung Abstand genommen werden muss. Wird die Auslagerung jedoch weiter forciert, sind Maßnahmen zur Minderung identifizierter Risiken zu ergreifen (z.B. Einsatz von Verschlüsselungstechnologien in Kombination mit einer geeigneten Schlüsselmanagementarchitektur).[35]

2.3 Vertragsgestaltung

Vorgaben zur Vertragsgestaltung mit Cloud-Anbietern ergeben sich sowohl aus der DORA als auch der MaRisk und sind ergänzend zu den EBA-Leitlinien zu Auslagerungen zu betrachten. Insbesondere bei Cloud-Lösungen, die kritische Funktionen und Prozesse[36] unterstützen, sollten folgende Mindestinhalte vertraglich vereinbart werden, wobei hier aus Sicht der Autoren besonders relevante aufgeführt sind:

- eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Drittdienstleister bereitzustellen hat[37]
- Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz einschließlich des Schutzes personenbezogener Daten
- Bestimmungen über die Sicherstellung des Zugangs zu Daten bei Insolvenz des Anbieters sowie nach Vertragsbeendigung inkl. Sicherstellung der Rückgabe der Daten in einem passenden Format
- Beschreibungen der Dienstleistungsgüte mit präzisen quantitativen und qualitativen Leistungszielen innerhalb der vereinbarten Dienstleistungsgüte, um dem Finanzunternehmen eine wirksame Überwachung von IKT-Dienstleistungen und das unverzügliche Ergreifen angemessener Korrekturmaßnahmen zu ermöglichen
- Berichtspflichten des IKT-Drittdienstleisters gegenüber dem Finanzunternehmen, einschließlich der Meldung aller Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittdienstleisters, IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß den vereinbarten Leistungsniveaus wirksam bereitzustellen, auswirken könnten

[33] Tz. 19 lit. c und Tz. 22 ESMA Leitlinien für Auslagerungen an Cloud-Anbieter
[34] S. DORA, EG 66: „Betreffen vertragliche Vereinbarungen kritische oder wichtige Funktionen, so sollten Finanzunternehmen darauf achten, dass IKT-Drittdienstleister die aktuellsten und höchsten Standards für die Informationssicherheit anwenden."; Art. 28 Abs. 5: „Finanzunternehmen dürfen vertragliche Vereinbarungen nur mit IKT-Drittdienstleistern schließen, die angemessene Standards für Informationssicherheit einhalten. Betreffen diese vertraglichen Vereinbarungen kritische oder wichtige Funktionen, so berücksichtigen die Finanzunternehmen vor Abschluss der Vereinbarungen angemessen, ob die IKT- Drittdienstleister die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit anwenden."
[35] S. Tz. 64 und 68 EBA-Leitlinien zu Auslagerungen
[36] Auch für nicht-kritische Services werden Mindestinhalte in Art. 30 Abs. 2 DORA vorgesehen
[37] Art. 30 Abs. 2 DORA

- Kündigungsrechte und Ausstiegsstrategien, insbesondere die Festlegung eines verbindlichen angemessenen Übergangszeitraums
- Verpflichtung des IKT-Drittdienstleisters, sich an den Threat-Led-Penetration-Tests (TLPT) des Instituts zu beteiligen und uneingeschränkt daran mitzuwirken
- Anforderungen an die Daten- und Systemsicherheit[38]
- Standort bzw. die Standorte der Datenspeicherung und Datenverarbeitung[39]

Es wird die Verwendung von Standardvertragsklauseln empfohlen, die von staatlichen Behörden oder von Organen der Union entwickelt wurden. Darunter zählt insbesondere die Verwendung der von der Kommission entwickelten Vertragsklauseln für Cloud Computing Dienste für Finanzunternehmen und IKT-Drittdienstleister.[40]

2.4 Interne Vorgaben, Steuerung und Kontrolle

Institute müssen interne Vorgaben zum Informationsschutz definieren und Prozesse entsprechend gestalten. So sieht AT 7.2 MaRisk vor, dass die technisch-organisatorische Ausstattung, die IT-Systeme (Hard- und Software-Komponenten), die zugehörigen IT-Prozesse und die sonstigen Bestandteile des Informationsverbundes, die Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit der Daten sicherstellen müssen.[41] Bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse ist auf gängige Standards zurückzugreifen.

Auch sind diese Vorgaben gem. Ziff. 3 BAIT zu überprüfen. Bei Auslagerungen muss ebenfalls ein Soll-Ist-Abgleich auf Basis interner Vorgaben erfolgen. Dies ist die Grundlage für eine laufende Risikobewertung und ein effizientes Risikomanagement. Häufig sind die internen Vorgaben eines Finanzinstituts jedoch nicht auf die Cloud-Nutzung ausgelegt. Daher müssen die ausgewählten Standards um Cloud-Spezifika ergänzt und die internen Prozesse unter Berücksichtigung der regulatorischen Anforderungen angepasst werden.[42] Nach der Orientierungshilfe der BaFin sollten beaufsichtigte Unternehmen vor einer Auslagerung in die Cloud zunächst ihre internen Prozesse auf deren Eignung prüfen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt zur Ergänzung der internen Vorgaben mindestens Sicherheitsanforderungen aus dem BSI Anforderungskatalog *Cloud Computing Compliance Criteria Catalogue (C5)* heranzuziehen.[43]

---

[38] S. Tz. 82 der EBA Leitlinien zu Auslagerungen (EBA/GL/2019/02)
[39] Art. 30 Abs. 2 lit b) DORA; Hierbei sollte gem. Tz. 83 EBA Leitlinien zu Auslagerungen (EBA/GL/2019/02) ein risikobasierter Ansatz gewählt werden – nach Möglichkeit sollte dieser innerhalb der EU bzw. in einem sicheren Drittstaat erfolgen
[40] S. EG 75 DORA
[41] S. auch Ziff. 4.3 BAIT: Auf Basis der Informationssicherheitsleitlinie und der Ergebnisse des Informationsrisikomanagements sind konkretisierende, den Stand der Technik berücksichtigende Informationssicherheitsrichtlinien und Informationssicherheitsprozesse zu definieren.
[42] Vgl. auch Tz 29 ESMA Leitlinien: Eine Firma sollte in ihren internen Richtlinien und Verfahren sowie in der schriftlichen Auslagerungsvereinbarung mit dem Cloud-Anbieter Anforderungen an die Informationssicherheit festlegen und die Einhaltung dieser Anforderungen fortlaufend überwachen, einschließlich des Schutzes vertraulicher, personenbezogener oder anderweitig sensibler Daten.
[43] Kriterienkatalog Cloud Computing C5:2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2

Darüber hinaus ist sicherzustellen, dass Transparenz über die Aufgaben- und Verantwortlichkeitsverteilung hinsichtlich der Informationssicherheit zwischen Unternehmen und Cloud-Anbieter besteht.[44] Auch sind Vorgaben für interne Maßnahmen bei Cloud-Nutzung festzulegen, insbesondere in den Bereichen Identitäts- und Zugriffsverwaltung sowie Verschlüsselung.

Die Einhaltung der Vorgaben ist anschließend zu überprüfen, wobei auch Zertifikate und Sammelprüfungen herangezogen werden können, sofern diese eine ausreichende Transparenz über die jeweiligen Dienstleistungen bieten.[45]

2.5 Ausstiegsstrategie

Gem. Art. 28 Abs. 8 DORA sind für kritische oder wichtige Dienste bzw. für Cloud-Anbieter, die diese Dienste erbringen, Ausstiegsstrategien zu erstellen. Damit soll sichergestellt werden, dass z.B. bei einer Verschlechterung der Qualität ein Wechsel oder eine Internalisierung der Aufgaben mit verhältnismäßigem Aufwand möglich bleibt. Die darf nicht zu einer unverhältnismäßigen Unterbrechung der eigenen Dienstleistungen für die Kunden oder zur Verletzung regulatorischer Pflichten führen.[46] Insbesondere bei einer One-Cloud-Strategie[47] können Abhängigkeiten entstehen, die diese Ziele gefährden. Daher ist es entscheidend, Regelungen zur Datenmigration im Falle eines Anbieterwechsel so zu gestalten, dass ein reibungsloser Übergang möglich ist. Eine Multi-Cloud-Strategie[48] kann hier besonders hilfreich sein. Die Ausstiegsstategie aus einem Vertragsverhältnis mit einem Cloud-Dienstleister sollte mindestens folgende Aspekte umfassen:

- Ziele der Ausstiegsstrategie
- Auslösende Ereignisse zur Einleitung der Ausstiegsstrategie
- Business Impact Assessment (BIA) inkl. Angaben, welche Ressourcen zur Durchführung der Ausstiegsstrategie notwendig wären
- Aufgaben und Verantwortlichkeiten für die Durchführung
- Prüfung der Angemessenheit (Abwägung der Risiken bei Durchführung sowie bei Nicht-Durchführung)
- Erfolgskriterien für die Übertragung

[44] S. Tz. 30 ESMA; Datenschutzquelle: „Zu beachten ist, dass das reine Vorliegen von Zertifikaten nicht hinreichend aussagekräftig ist. Vielmehr muss sich der Cloud-Anwender anhand der in den Zertifizierungs- bzw. Gütesiegelverfahren erarbeiteten Gutachten, Berichte und Analyseergebnisse darüber Klarheit verschaffen, ob und in welchem Umfang sich der Untersuchungsgegenstand auf cloudspezifische Datenschutz- und IT-Sicherheitsrisiken bezieht und dabei die vom Cloud-Anbieter zur Verfügung gestellten Dienste (IaaS, PaaS oder SaaS) geprüft wurden“
[45] S. Tz. 92 f. EBA Leitlinien zu Auslagerungen (EBA/GL/2019/02)
[46] S. auch Tz. 31 ff. ESMA Leitlinien und Tz. 106 ff. EBA Leitlinien zu Auslagerungen
[47] Eine One-Cloud-Strategie bezeichnet die Konsolidierung aller Cloud-Dienste und Ressourcen einer Organisation auf einer einzigen Plattform, um Kosten zu reduzieren, die Verwaltung zu vereinfachen und die Integration zu erleichtern
[48] Eine Multi-Cloud-Strategie ermöglicht es Unternehmen, verschiedene Cloud-Dienste von verschiedenen Anbietern zu kombinieren, um die spezifischen Anforderungen ihrer Anwendungen zu erfüllen und die Abhängigkeit von einem einzelnen Anbieter zu verringern

3. Transition zur sicheren Cloud schaffen

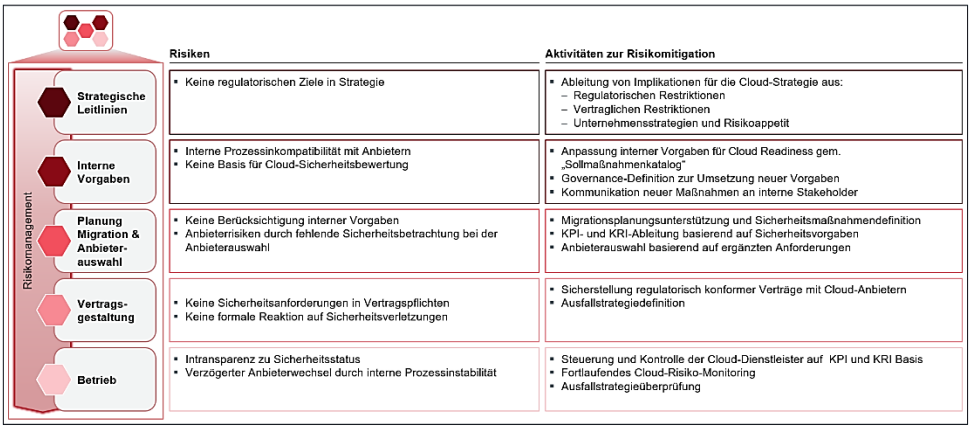

Abbildung 3: Compliance Management Framework

Die aufgeführten Anforderungen müssen im Cloud-Transformationsprozess umgesetzt werden. Dabei ist zu berücksichtigen, dass das Risikomanagement ein kontinuierlicher Prozess ist. In allen Phasen der Coud-Transformation, von der Strategie bis zum Betrieb, müssen Risiken identifiziert und analysiert werden. Darauf aufbauend muss die Ableitung von Mitigationsmaßnahmen sowie deren Umsetzung erfolgen. Daher können generische Anforderungen nicht vordefiniert und dem Projekt übergeben werden. Vielmehr ist die ganzheitliche Integration eines Compliance-Streams in den Cloud-Transformationsprozess erforderlich. Dieser adressiert die Risiken in den jeweiligen Dimensionen und führt folgende Aktivitäten durch:

3.1. Strategische Leitlinien

Bereits bei der strategischen Ausrichtung besteht die Gefahr, dass regulatorische Anforderungen nicht erfüllt werden. Dies ist z.B. der Fall, wenn die Strategie überhaupt nicht dokumentiert ist, nicht zu den anderen Strategien (z.B. Geschäftsstrategie) des Instituts passt oder nicht den erforderlichen Mindestanforderungen genügt. Besonders gravierend ist es, wenn bereits ein Zielbild definiert wurde, das im Ergebnis nicht regulatorisch konform ausgestaltet werden kann. Daher sollte der Compliance-Stream an dieser Stelle der Cloud-Journey Ableitungen aus regulatorischen Restriktionen, vertraglichen Pflichten gegenüber Kunden oder Anbietern sowie dem Risikoappetit und den anderen Unternehmensstrategien einbringen. Dies muss unter Berücksichtigung der zu diesem Zeitpunkt bereits bekannten Risiken erfolgen. Aus diesen Risiken sind Leitplanken für den weiteren Prozess abzuleiten. Während die planungs- und unternehmensspezifischen Risiken im Laufe der konkreten Planung und des gesamten Prozesses identifiziert werden, sollten die allgemein mit der Cloud-Nutzung verbundenen Risiken bereits zu diesem Zeitpunkt bewertet und in die Strategie und Planung einbezogen werden. Anlage 1 listet einige dieser Risiken auf.

3.2. Interne Vorgaben

Sobald das Zielbild definiert ist und feststeht, dass ein Cloud-Einsatz forciert werden soll, müssen die internen Vorgaben dahingehend überprüft werden, ob sie für einen Cloud-Einsatz geeignet sind. Dabei kann es vorkommen, dass bestehende Prozesse zwar die Anforderungen erfüllen, aber nicht mit den Prozessen der Cloud-Anbieter vereinbar sind. Beispielhaft anzuführen sind hier verpflichtende Anbindungen an intern genutzte Tools für Incident- und Change-Management-Prozesse. Diese Prozesse sollten daher im Rahmen einer sog. „Cloud-Readiness-Prüfung“ auf Anpassungsbedarf geprüft werden. Bei der Anpassung der internen Prozesse müssen natürlich die zugrunde liegenden Anforderungen weiterhin gewährleistet bleiben.

Zudem kommt es regelmäßig vor, dass die internen Vorgaben der Informationssicherheit nicht die spezifischen Anforderungen an Cloud-Prozesse und -Betrieb enthalten. Diese sind entsprechend zu ergänzen. Anlage 2 beleuchtet spezifische Anforderungen an die Cloud-Nutzung aus Sicht der Informationssicherheit.

3.3. Planung der Migration und Anbieterauswahl

Bei der Migrationsplanung sind den Hauptbeteiligten die (neuen) Vorgaben häufig nicht ausreichend bewusst. Der Compliance-Stream sollte in diesem Stadium unterstützen, diese neuen Vorgaben und Prozesse in der Migrationsplanung sicherzustellen. Ebenso sind die regulatorischen Anforderungen an die Anbieterauswahl zu berücksichtigen. Nicht zuletzt sind häufig Schnittstellen und Konfigurationen entsprechend den Sicherheitsvorgaben zu gestalten, auch in diesem Bereich ist eine enge Zusammenarbeit der Verantwortlichen mit dem Compliance-Stream erforderlich.

3.4. Vertragsgestaltung

Die Vertragsgestaltung mit Cloud-Anbietern erfolgt selten auf Basis der Vertragsmuster des Instituts. Insofern muss vor Vertragszeichnung eine gründliche Überprüfung der Abbildung regulatorischer Grundlagen erfolgen. Typischerweise halten Cloud-Anbieter bereits regulatorisch konforme Templates für regulierte Kunden vor – dennoch sollte für eine zeitliche Komponente für Vertragsgestaltung eingeplant werden, da kommunizierte Anpassungsbedarfe häufig nicht zügig verhandelbar sind.

3.5. Betrieb

Während des Betriebs muss eine kontinuierliche Steuerung und Kontrolle der Dienstleister erfolgen. Identifizierte Schwachstellen müssen in das Risikomanagement überführt und Mitigationsmaßnahmen geplant und umgesetzt werden. Hierzu sind die Erkenntnisse aus dem Transformationsprojekt geordnet in die Linie zu überführen.

Ein regulatorisch konformer Cloud-Einsatz ist bei angemessener Planung und ausreichender Einbindung des dedizierten Compliance-Streams möglich. Die Verunsicherung auf dem Markt ist jedoch verständlich, denn gerade an dieser Stelle werden oft Fehler gemacht, die später teilweise

nur mit großem Aufwand korrigiert werden können. Die Cloud Security Alliance ordnet einige der relevantesten Risiken des Cloud-Einsatzes dem Verantwortungsbereich des Cloud-Nutzers zu.[49]

Ranking	Ursachen für verwirklichte Risiken
1	Unzureichende ID, Zugangsberechtigung, Zugangs- und Schlüsselverwaltung, privilegierte Konten
2	Unsichere Schnittstellen und APIs
3	Fehlkonfiguration und unzureichende Änderungskontrolle
4	Fehlende Cloud-Sicherheitsarchitektur und -strategie
5	Unsichere Softwareentwicklung
6	Unsichere Ressourcen von Drittanbietern
7	Systemschwachstellen
8	Versehentliche Offenlegung/Veröffentlichung von Cloud-Daten
9	Fehlkonfiguration und Ausnutzung von Serverless- und Container-Workloads
10	Organisierte Kriminalität/Hacker/APT
11	Exfiltration von Cloud-Speicherdaten

Abbildung 4: Die häufigsten Herausforderungen im Cloud Computing

4. Fazit

Langfristig ist die Auseinandersetzung mit Cloud-Technologien und deren Einsatz für die meisten Institute unumgänglich, um wettbewerbsfähig zu bleiben. Hierbei muss die Einhaltung von regulatorischen Anforderungen, teils speziell geltend für ausgelagerte Cloud-Technologien bei Finanzinstituten, gewährleistet sein. Um schwerwiegende Konsequenzen aus regulatorischen Verstößen der Institute als Cloud-Nutzer zu vermeiden, sollten Cloud-Vorhaben auf Basis der zuvor erarbeiteten Cloud-Strategie und im Rahmen eines Projekts ausreichend geplant und streng gesteuert werden. Nur so werden Compliance-Aspekte von Anfang bis Ende berücksichtigt und unterstützen zusätzlich die Umsetzung der IT- und Cloud-strategischen Leitlinien des Unternehmens.

Geschieht dies nicht, entstehen sogenannte Compliance-Schulden: Erst zu einem späten Zeitpunkt wird visibel, dass eine bereits erfolgte (technische) Umsetzung nicht alle regulatorischen Anforderungen erfüllt. Diese mitten in der Transformation oder gar im Nachhinein zu korrigieren, gestaltet sich meist schwieriger und kostspieliger als zu Beginn. Insbesondere noch nicht oder nur unzureichend umgesetzte technologische Compliance-Aspekte sind mit hohen Kosten für die Nachbesserung verbunden. Darüber hinaus bestehen auch Risiken in dem Zeitraum bis zur eigentlichen Nachbesserung. In diesem Zusammenhang wird bei behördlichen Prüfungen häufig bemängelt, dass Risiken nicht frühzeitig erkannt und gemindert wurden und das Risikomanagement daher mangelhaft ist. Dies wiederum kann bekanntlich zu gravierenden

[49] Copyright 2022, Cloud Security Alliance – S. 6, https://cloudsecurityalliance.org/research/working-groups/top-threats/

Sanktionen der Aufsichtsbehörden führen, die von Risikorückstellungen bis hin zu Wachstumsbeschränkungen reichen.[50]

Der Einsatz eines end-to-end Compliance-Streams im Transformationsprozess ist daher eine wesentliche Maßnahme, um die im vorliegenden Artikel beschriebenen Mindestanforderungen zu erfüllen und Compliance-Schulden gar nicht erst entstehen zu lassen. Er gewährleistet, dass die Ressourcen, die für die eigentliche Cloud-Migration erforderlich sind, ausschließlich mit dieser Aufgabe betraut sind während regulatorische Maßnahmen gleichzeitig eingehalten werden. Als Folge werden relevante Risiken frühzeitig berücksichtigt und mitigiert.

Der Compliance-Stream beweist das, was die zu beachtende Regulatorik so vehement verlangt: ein starkes Risikobewusstsein und -management.

[50] Bußgelder der BaFin erreichen mitunter Millionenhöhe. Eine Übersicht verhängter Sanktionen findet sich auf der Webseite der BaFin unter https://www.bafin.de/DE/Aufsicht/BoersenMaerkte/Massnahmen/massnahmen_sanktionen_node.html#ID_7946462.

ANLAGE 1: Relevante Risiken, die bei Finanzinstituten adressiert sein müssen

Unternehmen müssen die mit der Cloud-Nutzung verbundenen Risiken unter Berücksichtigung unternehmensinterner und -externer Faktoren projektbezogen identifizieren und bewerten. Insofern kann eine Cloud-Risikoanalyse nicht fertig „von der Stange“ gekauft werden, sondern muss begleitend zur Cloud-Journey erstellt werden. Einige Risiken sind jedoch in den meisten Fällen relevant und sollten daher bei geplanten Cloud-Auslagerungen immer betrachtet und durch die Definition von Mitigationsmaßnahmen adressiert werden.

Das BSI hat umfangreiche Anforderungen und Empfehlungen entwickelt, um Cloud-Risiken zu minimieren und einen sicheren Betrieb in der Cloud zu gewährleisten.

Im Folgenden werden, in Anlehnung an diese Publikation sowie ergänzend dazu, die wichtigsten Risiken dargestellt. Außerdem wird aufgezeigt, welche spezifischen Anforderungen sowohl der Cloud-Kunde als auch der Cloud-Anbieter erfüllen müssen, um diesen Risiken wirksam zu begegnen.

Migration:

Jede Migration birgt das Risiko der Störung oder gar des temporären Ausfalls von Geschäftsprozessen. Häufig tritt die Situation auf, dass eine Migration nur verzögert durchgeführt werden kann, während der bisherige Cloud-Anbieter jedoch bereits gekündigt ist und ein sicheres Fallback-Szenario nicht zur Verfügung steht. Die Strategie des Instituts sollte daher Aspekte wie die IT-Architektur, das Datenformat, das Zielsystem und die Rückholbarkeit berücksichtigen. Darüber hinaus ist es wichtig, den Rückholprozess zu dokumentieren und Vorkehrungen für eine zügige Umsetzung der Ausstiegsstrategie zu treffen, falls bereits während der Migration gravierende Probleme auftreten.

Ausfall:

Gerade bei erfolgreichen Hyperscalern scheint ein Ausfall undenkbar. Gegenüber Aufsichtsbehörden ist dieses Argument schwer durchzusetzen. Zum einen, weil spektakuläre Fälle in der Vergangenheit gezeigt haben, dass selbst DAX-Konzerne vor einer Pleite nicht gefeit sind. Zum anderen, weil es besonders bei der Betrachtung von Hyperscalern keineswegs fernliegt, dass z.B. journalistische Enthüllungen dazu führen können, dass Institute ihre Dienste schlicht nicht mehr anbieten dürfen, weil sie sonst selbst Kundenrechte verletzen würden. Man stelle sich nur vor, eine Enthüllung, wie es sie im Fall Meta[51] (Facebook-Mutterkonzern) gab, würde eine gezielte und massive Zusammenarbeit eines Cloud-Anbieters mit US-Geheimdiensten aufdecken. Der Cloud-Kunde sollte daher eine langfristige Business Continuity Management (BCM)-Strategie entwickeln, die je nach Kritikalität der Dienste variiert. Dabei können verschiedene Maßnahmen in Betracht gezogen werden, wie beispielsweise Backup-Lösungen beim Cloud-Kunden selbst, die Implementierung eines hybriden Modells oder die Bereitstellung einer reduzierten Gesamtleistung durch eine Kopie der Datenbank als

[51] Meta muss aufgrund eines Verstoßes gegen die DSGVO eine Rekordstrafe von 1,2 Milliarden Euro zahlen, da das Unternehmen persönliche Informationen von EU-Bürgern nicht ausreichend vor amerikanischen Geheimdiensten geschützt hat; Handelsblatt, 2023, https://www.handelsblatt.com/technik/it-internet/facebook-mutter-rekordstrafe-fuer-meta-in-eu-datenschutzstreit-/29163242.html

Notfallbetrieb. Diese Vorkehrungen stellen sicher, dass geschäftskritische Prozesse auch im Falle eines Ausfalls weiterlaufen.

Mangelhaftes Löschen:

Insbesondere bei Hyperscalern ist zu befürchten, dass Daten nicht nur zweckgebunden verwendet werden und eine Löschung nicht wie vorgeschrieben erfolgt.[52] Im Hinblick auf die datenschutzkonforme Löschung von Daten sind klare vertragliche Vereinbarungen zwischen dem Cloud-Kunden und dem Cloud-Anbieter von entscheidender Bedeutung. Der Cloud-Kunde muss konkrete Regelungen zur Dokumentation des Löschprozesses, zur Rückgabe der Hardware sowie zu technischen und organisatorischen Grenzen treffen. Insbesondere im Insolvenzfall ist es wichtig, im Vorfeld zu klären, wer für die ordnungsgemäße Löschung der Daten verantwortlich ist. Der Cloud-Anbieter wiederum trägt die Verantwortung für die dokumentierte Durchführung der Datenlöschung gemäß den vertraglichen Vereinbarungen. Dabei sind Aspekte wie Backup-Lösungen, Zweitrechenzentren, die Einbindung von Subunternehmern und die Berücksichtigung von Metadaten zu berücksichtigen. Eine umfassende Dokumentation des Löschprozesses ist unabdingbar, um die Nachvollziehbarkeit und die Einhaltung der Datenschutzbestimmungen zu gewährleisten. Eine klare Verteilung der Verantwortlichkeiten und die Berücksichtigung dieser Aspekte stellen sicher, dass die Löschung von Daten sowohl im Regelbetrieb als auch im Falle einer Insolvenz des Cloud-Anbieters ordnungsgemäß erfolgt und die datenschutzrechtlichen Anforderungen erfüllt werden.

Fehlende/nicht ausreichende Leistung:

Insbesondere bei Hyperscalern sind personelle Ressourcen selten ein Problem. Allerdings können diese bei Bedarf nicht sofort zur Verfügung stehen, da im Vorfeld keine Vereinbarungen über optionale Zusatzleistungen oder Zeitfenster getroffen wurden. Daher ist wichtig, dass der Cloud-Kunde klare Regelungen für Preise sowie vertraglich garantierte und optionale Unterstützungsleistungen festlegt. Es sollten auch Empfehlungen zur Vorbereitung einer Ausstiegsstrategie bei der Nutzung von Cloud-Diensten und eine Regelung für die Übernahme von Mitarbeitern in Betracht gezogen werden.

Es ist ratsam, klare Vereinbarungen über die Kostenstruktur und die Bereitstellung von zusätzlicher Ressourcen im Vertrag zu treffen, um unvorhergesehene Engpässe zu vermeiden und kontinuierliche Unterstützung zu gewährleisten. Auf der anderen Seite liegt es in der Verantwortung des Cloud-Anbieters, sicherzustellen, dass die notwendigen Ressourcen zur Verfügung stehen, um zusätzliche optionale Leistungen oder Zeitfenster bereitzustellen. Dies kann den Einsatz von qualifiziertem Personal, die Bereitstellung von Hardware oder andere technische Anforderungen umfassen. Eine effektive Kommunikation und enge Zusammenarbeit zwischen dem Cloud-Kunden und dem Cloud-Anbieter sind für eine erfolgreiche Umsetzung unerlässlich.

[52] S. etwa die Bewertung der DSK zu Microsoft: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf, S. 6

Änderung der Rechtsgrundlage:

Aufgrund neuer oder geänderter rechtlicher Anforderungen kann es vorkommen, dass bestimmte Cloud-Dienste oder Cloud-Anbieter nicht mehr genutzt werden dürfen. Beispielsweise kann ein neues Gesetz dazu führen, dass ein Unternehmen einen Rechtsverstoß begeht, wenn es Cloud-Dienste eines Anbieters nutzt. Dies kann zu Strafzahlungen und einer möglichen Unterbrechung der Geschäftstätigkeit führen. Um solche Risiken zu vermeiden, ist es für den Cloud-Kunden wichtig, über ein Sonderkündigungsrecht und eine gut ausgearbeitete Ausstiegsstrategie zu verfügen, um schnell reagieren zu können. Der Cloud-Kunde muss in der Lage sein, flexibel auf sich ändernde rechtliche Anforderungen zu reagieren und gegebenenfalls den Cloud-Anbieter zu wechseln oder bestimmte Dienste einzustellen. Auf der anderen Seite liegt es in der Verantwortung des Cloud-Anbieters, auch unter schwierigen Rahmenbedingungen weiterhin Unterstützungsleistungen zu erbringen. Auch wenn neue regulatorische Anforderungen und die damit verbundenen Veränderungen Herausforderungen mit sich bringen können, ist es wichtig, dass der Cloud-Anbieter bestmögliche Unterstützung bietet und bei der Umsetzung der Austiegsstrategie hilft. Dies kann beispielsweise die Bereitstellung von Informationen, Schulungen oder technischer Expertise umfassen.

Fristlose Kündigung aus einem besonderen Grund:

Sowohl eine Kündigung durch den Cloud-Anbieter als auch eine Kündigung durch den Cloud-Nutzer ist möglich. Bei einer fristlosen Kündigung aus besonderem Grund (wie beispielsweise schwere Vertragsverletzung, wiederholtes Fehlverhalten oder grobe Fahrlässigkeit) gelten besondere Anforderungen für den Cloud-Anbieter und den Cloud-Kunden. Der Cloud-Anbieter muss eine vertraglich festgelegte Mindestübergabefrist entsprechend der Migrationsstrategie vereinbaren und die Möglichkeit bieten, kritische Dienstleistungen unverzüglich in eine private oder alternative public Cloud zu verlagern. Darüber hinaus sind Empfehlungen zur Vorbereitung einer Ausstiegsstrategie bei der Nutzung von Cloud-Diensten wichtig. Der Cloud-Kunde erwartet trotz einer schwierigen Geschäftsbeziehung weiterhin Unterstützungsleistungen durch den Cloud-Anbieter.

Im Falle einer fristlosen Kündigung aus wichtigem Grund gelten für den Cloud-Anbieter und den Cloud-Kunden bestimmte Anforderungen. Der Cloud-Anbieter muss eine vertraglich festgelegte Mindestübergangszeit auf Basis der Migrationsstrategie vereinbaren und bei kritischen Dienstleistungen die Möglichkeit einer sofortigen Überführung in eine private oder alternative public Cloud anbieten. Darüber hinaus sind Empfehlungen zur Vorbereitung einer Exit-Strategie bei der Nutzung von Cloud-Diensten wichtig. Der Cloud-Kunde wiederum erwartet trotz einer schwierigen Geschäftsbeziehung weiterhin Unterstützungsleistungen durch den Cloud-Anbieter.

Fristlose Kündigung wegen Insolvenz:

Für den Fall, dass die Unterstützungsleistung durch den Cloud-Anbieter wegfällt, sei es aufgrund der Nichtexistenz des Unternehmens oder aufgrund behördlicher Vorgaben, ist der Cloud-Kunde verpflichtet, die Wirtschaftlichkeit zu prüfen. Es sollten Vereinbarungen mit dem Insolvenzverwalter getroffen werden, um die Übernahme bzw. das Ausleihen von Personal für den On-Premise-Betrieb zu ermöglichen, sowie Regelungen für die sofortige Überführung kritischer Dienstleistungen in die private Cloud oder eine alternative public Cloud.

Datensouveränität in der Cloud:

Es ist von entscheidender Bedeutung, dass Cloud-Dienste im Hinblick auf die Vertraulichkeit und Integrität der Daten angemessen gesichert sind. Hier kommt die Verschlüsselung ins Spiel. Das Prinzip „Bring your own key (BYOK)“ ist seit langem etabliert, es besteht jedoch die Gefahr, dass die Schlüssel aufgrund ihres Speicherortes oder ihrer Generierung keinen ausreichenden Schutz bieten. Um solche Risiken zu mitigieren, haben Anbieter an verschiedenen Konzepten gearbeitet, auch in Zusammenarbeit mit nationalen Anbietern, welche die Datensouveränität gewährleisten. Anbieter wie Google in Zusammenarbeit mit T-Systems oder Arvato Systems sind in Deutschland dabei, Lösungen für stark regulierte Branchen zu entwickeln. Für die Datensouveränität sind vor allem Transparenz und Kontrolle entscheidend, um eine bewusste und aktive Steuerung der eigenen Daten bei der Erhebung, Speicherung, Nutzung und Verarbeitung zu ermöglichen. Souveräne Clouds stellen sicher, dass Unternehmen selbstbestimmt mit ihren Daten umgehen und dadurch regulatorische Anforderungen besser erfüllen können.[53]

Vendor Lock-In:

Insbesondere bei einer One-Cloud-Strategie besteht die Gefahr, dass sich das Unternehmen stark an einen bestimmten Cloud-Anbieter bindet, da z.B. der Großteil der Daten in der Cloud liegt und bei einem Wechsel erhebliche technologische Inkompatibilitäten auftreten können. Ein Wechsel zu einem anderen Anbieter wird dadurch erschwert und kann hohe Kosten verursachen. Auf mögliche Ausfälle kann so kaum reagiert werden. Hier bedarf es einer starken Ausstiegsstrategie, die auch einen ständigen Dialog mit alternativen Cloud-Anbietern beinhalten sollte.

Hacker-Angriffe:

Große Cloud-Anbieter bieten eine attraktive Angriffsfläche für Hacker. Daher ist es wichtig, dass Cloud-Anbieter angemessene Sicherheitsmaßnahmen implementieren und regelmäßige Audits durchführen, um die Vertraulichkeit und Integrität der Daten zu gewährleisten. Als Nachweis können Zertifizierungen und Berichte dienen, die von potenziellen Cloud-Kunden vorab geprüft werden sollten.

[53] Datacenter Insider, 2023, https://www.datacenter-insider.de/guter-vorsatz-zum-neuen-jahr-souveraenitaet-a-28ca80f2c50f06aa4691e45c3dc9debe/

ANLAGE 2: Cloud-Anforderungen zur Informationssicherheit

Aus den in Kapitel 2 aufgeführten Themenblöcken zu den regulatorischen Anforderungen, die ein reguliertes Institut bei der Cloud-Transformation zu beachten hat, kann sich die Umsetzung einer adäquaten Ergänzung der internen Prozesse und Maßnahmen als sehr anspruchsvoll erweisen. Dies liegt daran, dass sie auf bestehenden Unternehmensstrukturen aufbauen und gleichzeitig die spezifischen Lücken identifizieren müssen, die für die Auslagerung an einen Cloud-Anbieter relevant sind.

Ergänzungen von regulatorischen Maßnahmen bei Cloud Nutzung

Abbildung 5: Themenauszug über erforderliche Ergänzungen von C5-Maßnahmen zum bestehenden ISO-Maßnahmenset

Im folgenden Abschnitt werden die spezifischen Anforderungen an die Cloud-Nutzung aus Sicht der Informationssicherheit beleuchtet. Gemäß den Vorgaben der BAIT sind Finanzinstitute dazu aufgefordert, ihre Sicherheitsanforderungen anhand anerkannter Standards wie ISO 27001/27002 umzusetzen. Im Bereich der Cloud-Technologie ist der C5-Standard als anerkannter Maßstab etabliert. Es ist von besonderer Bedeutung, die Abweichungen zwischen diesem Standard und den ISO-Richtlinien darzustellen, da der C5-Standard zusätzliche Kriterien für Cloud-Dienstleister von Finanzinstituten offenlegt. Dies ermöglicht ein besseres Verständnis der spezifischen Ergänzungen, die für den Einsatz von Cloud-Diensten in der Finanzbranche gelten. Der hier aufgeführte Auszug dieser Ergänzungen orientiert sich ebenfalls an der ISO 27002- Struktur und gliedert sich in organisatorische, physische, technische Anforderungen sowie Anforderungen zur Personalsicherheit.

Organisatorische Anforderungen

MaRisk und BAIT fordern ein Informationsrisikomanagement und verweisen zur konkreten Ausgestaltung auf gängige Standards wie ISO270XX. Diese Regelungen (z.B. Aufbau eines Informationsverbundes, Durchführung einer Schutzbedarfsanalyse, Definition eines Sollmaßnahmenkatalogs und Durchführung eines Soll-Ist-Abgleichs) richten sich primär an regulierte Institute. Die neuere Regulierung in Form der DORA fordert nun auf europäischer Ebene, in Anlehnung an den C5-Standard, ein umfassendes Risikomanagement - auch direkt von Cloud-Anbietern.

Damit werden Cloud-Anbieter in die Pflicht genommen, Risiken zu erfassen, die die Schutzziele der Informationssicherheit für den Cloud-Kunden gefährden können. Dabei sind Faktoren wie Datenverarbeitung, -speicherung und -übertragung zu berücksichtigen. Eine Besonderheit ist die Trennung von Ressourcen, die von verschiedenen Kunden genutzt werden. Die Risikobewertung im Zusammenhang mit Cloud-Technologien ist jährlich vom Risikoeigentümer durchzuführen.[54]

Darüber hinaus muss der Cloud-Anbieter über strukturierte und dokumentierte Informationssicherheitsrichtlinien verfügen. Sind Ausnahmen von den darin enthaltenen Richtlinien und Anweisungen erforderlich, muss der Anbieter ein formelles Risikobewertungsverfahren durchführen, das regelmäßig überprüft wird.[55]

Die Richtlinien sind auch für die Planung und Durchführung von Audits relevant. Sie betreffen beispielsweise

- Aktivitäten, die z.B. bei einer Wartung den Cloud-Dienst beeinträchtigen und außerhalb von Lastspitzen durchzuführen sind,
- qualifiziertes Personal, welches regelmäßige interne Audits umsetzt, um die Compliance des Informationssicherheitsmanagementsystems zu überprüfen, und
- identifizierte Schwachstellen, die risikobewertet werden müssen und die entsprechende Maßnahmenableitung bedeuten.[56]

In Bezug auf das Asset Management muss der Cloud-Anbieter eine konsistente Erfassung der Werte (Assets) über den gesamten Lebenszyklus sicherstellen. Der Umgang mit den physischen Assets der Mitarbeiter unterliegt einer zentralen Verwaltung, die u.a. die Verteilung von Software, Daten und Richtlinien ermöglicht. Unter Assets versteht der ISO-Standard alles, was für die Organisation einen Wert darstellt (physisch und digital). Um dieses Verständnis in der Organisation transparent zu machen, kann z.B. eine Erläuterung im Rahmen eines Glossars o.ä. bereitgestellt werden.[57]

Beim Rechte- und Rollenmanagement sind einige Ergänzungen zum ISO-Standard für die Cloud-Nutzung relevant. So ist beim Zugriffsmanagement darauf zu achten, dass Zugriffsberechtigungen bei Änderungen im Aufgabenbereich der Mitarbeitenden rechtzeitig entzogen werden. Dies betrifft sowohl interne als auch externe Mitarbeitende und darüber hinaus auch Systemkomponenten, die bei automatisierten Autorisierungsprozessen eine Rolle spielen. Bei privilegierten Zugriffsberechtigungen müssen die Berechtigungen spätestens 48 Stunden nach Inkrafttreten der Änderung angepasst werden. Darüber hinaus sind die Zugriffsberechtigungen mindestens einmal jährlich daraufhin zu überprüfen, ob sie dem tatsächlichen Aufgaben- bzw. Einsatzbereich entsprechen. Abweichungen sind spätestens sieben Tage nach Feststellung zu bearbeiten.[58]

Eine weitere und essenzielle Anforderung für Finanzinstitute mit Cloud-Auslagerung ist die Benachrichtigung bei unberechtigtem Zugriff auf Kundendaten. Ist ein solcher Zugriff (ausnahmsweise) erfolgt, muss der Cloud-Anbieter den Cloud-Kunden unverzüglich darüber

[54] Kriterienkatalog Cloud Computing C5:2020, OIS-06 und OIS-07
[55] Kriterienkatalog Cloud Computing C5:2020, SP-01 – SP-03
[56] Kriterienkatalog Cloud Computing C5:2020, COM-02, COM-03
[57] Kriterienkatalog Cloud Computing C5:2020, AM-01 – AM-03
[58] Kriterienkatalog Cloud Computing C5:2020, IDM-04 – IDM-05

informieren. Dabei sind Angaben zu Anlass, Zeitpunkt, Dauer, Art und Umfang des Zugriffs zu machen.[59]

Eine eher naheliegende Anforderung im Bereich des Rechte- und Rollenkonzeptes ist die geordnete Authentifizierung von Nutzern und Systemkomponenten, die in der Verantwortung des Cloud-Anbieters liegt. In der Produktionsumgebung ist eine Zwei- oder Mehrfaktor-Authentifizierung erforderlich.[60]

Für das Management von kryptographischen Schlüsseln enthält die ISO 27002 bereits eine Liste von Maßnahmen, wie z.B. die Erstellung, Verteilung, Speicherung sowie Änderung von Schlüsseln. Darüber hinaus definiert der C5-Standard weitere ergänzende Maßnahmen, um ein sicheres Schlüsselmanagement im Verantwortungsbereich des Cloud-Anbieters zu gewährleisten. Dazu gehören die sichere Speicherung der Schlüssel, z.B. durch die Separierung des Schlüsselverwaltungssystems von der Applikations- und Middleware-Ebene, und die Beschreibung der Zugriffsautorisierung. Auch müssen Richtlinien inkl. Konditionen für das Ändern oder Aktualisieren von Schlüsseln festgelegt werden. Für den Fall, dass Pre-Shared Keys verwendet werden, sind prozessuale Besonderheiten aufzuführen, die zur Sicherheit ihrer Verwendung beitragen.[61]

Der C5-Standard greift gezielt das Thema Ermittlungsanfragen staatlicher Stellen auf und weist auf organisatorische Anforderungen hin, die so dezidiert im ISO 27001 Standard nicht erwähnt werden. Lediglich bei der technischen Umsetzung der Protokollierung und des Loggings von Ereignissen, die als Beweismittel herangezogen werden können, findet sich gelegentlich ein Hinweis auf rechtliche Ermittlungen. Die folgenden Aspekte sind daher als Ergänzung sinnvoll.

Sollten Ermittlungsanfragen staatlicher Stellen an den Cloud-Anbieter herangetragen werden, muss dieser sicherstellen, dass sein Personal die Anwendbarkeit und Rechtsgültigkeit dieser Anfrage juristisch bewertet. Der Cloud-Kunde ist unverzüglich über die Ermittlungsanfrage zu informieren (soweit dies dem Cloud-Anbieter seinerseits rechtlich möglich ist). Der Cloud-Anbieter darf den Zugriff auf die Daten des Cloud-Kunden nur bei Vorliegen einer gültigen Rechtsgrundlage und streng beschränkt auf die für die Ermittlungsanfrage relevanten Daten gewähren. Nicht relevante Daten werden anonymisiert oder pseudonymisiert.[62]

Personalsicherheit

Zum Thema Personalsicherheit deckt der ISO 27002 Standard die Kerninhalte weitgehend ab. Ein kleinerer vertraglicher Aspekt betrifft die Verpflichtung der Mitarbeitenden zur Informationssicherheit. Gemäß dem C5-Standard sind alle Mitarbeitenden des Cloud-Anbieters verpflichtet, die Richtlinien zur Informationssicherheit einzuhalten und diese vor dem Zugriff auf Kundendaten oder Systemkomponenten nachweislich zu akzeptieren. Die Kontrolle der Einhaltung durch den Anbieter ist beim jeweiligen Finanzinstitut zu implementieren.[63]

[59] Kriterienkatalog Cloud Computing C5:2020, IDM-07
[60] Kriterienkatalog Cloud Computing C5:2020, IDM-08 – IDM-09
[61] Kriterienkatalog Cloud Computing C5:2020, CRY-04
[62] Kriterienkatalog Cloud Computing C5:2020, INQ-01 – 04
[63] Kriterienkatalog Cloud Computing C5:2020, HR-02

Physische Anforderungen

Bezüglich der genutzten Rechenzentren des Cloud-Anbieters sind ebenfalls Anforderungen zu erfüllen. Sofern physische Sicherheitsmaßnahmen aus Standards wie ISO/IEC 22237, ISO9001, EN50600 bereits unabhängig von der Cloud-Nutzung gelten, ist hier ein individueller Abgleich erforderlich, welche Anforderungen zusätzlich für Cloud-Anbieter gelten. Wurden bisher keine etablierten Standards in diesem Bereich befolgt, gelten für Cloud-Anbieter zumindest die nachfolgend aufgeführten Aspekte.

Der Cloud-Anbieter muss die Sicherheitsanforderungen für Räumlichkeiten und Gebäude nach den anerkannten Regeln der Technik dokumentieren. Diese Anforderungen müssen Gefahren, wie fehlerhafte Planung, unbefugten Zutritt und Stromausfall berücksichtigen. Nutzt der Cloud-Anbieter Räumlichkeiten oder Gebäude Dritter, so sind die Sicherheitsanforderungen an diese Dritten zu stellen und deren Umsetzung zu überprüfen.[64]

Der Cloud-Dienst selbst muss an mehreren Standorten und in ausreichender Entfernung voneinander bereitgestellt werden, um (betriebliche) Redundanz zu gewährleisten. Die Standorte müssen den Sicherheitsanforderungen des Cloud-Anbieters entsprechen und so ausgelegt sein, dass sie die Verfügbarkeitsanforderungen des Dienstgüteabkommens erfüllen.[65]

Die Räumlichkeiten und Gebäude des Cloud-Dienstes sind physisch gesichert und vor unbefugtem Zutritt geschützt. Die Zugangskontrolle wird durch ein geeignetes System geregelt. Es gibt auch Schutzmaßnahmen gegen Feuer und Rauch. Darüber hinaus müssen Cloud-Anbieter Maßnahmen zur Ausfallsicherung wie Redundanz, unterbrechungsfreie Stromversorgung und regelmäßige Wartung der Versorgungseinrichtungen umsetzen und überprüfen.[66]

Die Betriebsparameter der technischen Versorgungseinrichtungen und die Umgebungsparameter der Räumlichkeiten gemäß den Sicherheitsanforderungen des eigenen Sicherheitskonzeptes müssen durch den Cloud-Dienstleister überwacht und geregelt werden. Verlassen diese Parameter den zulässigen Regelbereich, muss das entsprechende Personal oder autorisierte Systemkomponenten des Anbieters automatisch informiert werden, um umgehend Maßnahmen zur Rückführung in den Regelbereich einzuleiten.[67]

Technische Anforderungen

Die technischen Anforderungen des C5 erzeugen neben den organisatorischen Anforderungen das wesentliche Delta zum ISO-Standard. Die Themenfelder sind vielfältig und betreffen den Regelbetrieb, die Kommunikationssicherheit und die Produktsicherheit.

Der Cloud-Anbieter muss einen effektiven Schutz vor Schadsoftware durch den Einsatz aktueller Schutzsoftware und regelmäßiger Updates gewährleisten. Es gibt Richtlinien und Anweisungen zur Protokollierung und Überwachung von Ereignissen auf Systemkomponenten. Darüber hinaus stellt der Cloud-Anbieter Richtlinien für den sicheren Umgang mit Metadaten bereit, um die Privatsphäre der Cloud-Kunden zu schützen.[68]

[64] Kriterienkatalog Cloud Computing C5:2020, PS-01
[65] Kriterienkatalog Cloud Computing C5:2020, PS-02
[66] Kriterienkatalog Cloud Computing C5:2020, PS-03 – 06
[67] Kriterienkatalog Cloud Computing C5:2020, PS-07
[68] Kriterienkatalog Cloud Computing C5:2020, OPS-05, OPS-10 – OPS-11

Darüber hinaus gewährleistet der Cloud-Anbieter die Sicherheit und Verwaltung der Protokolldaten. Die Daten werden in geeigneter Form gespeichert, um eine zentrale Auswertung zu ermöglichen, und gelöscht, wenn sie nicht mehr benötigt werden. Es erfolgt eine Authentifizierung zwischen den Protokollierungsservern und den zu protokollierenden Werten, um die Integrität und Authentizität der Informationen sicherzustellen. Die Übertragung erfolgt verschlüsselt oder über ein separates Administrationsnetz. Der Anbieter überwacht die Systeme kontinuierlich und sendet bei Ausfällen automatische Benachrichtigungen, um die Probleme zu bewerten und zu beheben.[69]

Die Systemkomponenten, für die der Cloud-Anbieter verantwortlich ist, werden gemäß Branchenstandards gehärtet und die spezifischen Härtungsvorgaben für jede Komponente dokumentiert. Darüber hinaus werden die Daten der Cloud-Kunden, die auf gemeinsam genutzten virtuellen und physischen Ressourcen gespeichert und verarbeitet werden, nach einem dokumentierten Konzept und einer Risikoanalyse strikt separiert. Dies dient der Vertraulichkeit und Integrität der Daten.[70]

Für den Themenblock „Portabilität und Interoperabilität“ ist es relevant zu berücksichtigen, dass eine sichere Schnittstellenkommunikation erfolgt. Der Cloud-Dienst ermöglicht die Kommunikation mit anderen Cloud-Diensten oder IT-Systemen der Cloud-Kunden von dokumentierten Schnittstellen. Dabei werden standardisierte Kommunikationsprotokolle verwendet, um die Vertraulichkeit und Integrität der übertragenen Informationen zu gewährleisten. Die Kommunikation über unsichere Netze muss verschlüsselt erfolgen.[71]

Zur Identifikation von Schwachstellen sind Sicherheitstests (Penetrationstests) unerlässlich. Diese muss der Dienstleister mindestens einmal jährlich durchführen. Im Rahmen einer Risikoanalyse werden die relevanten Systemkomponenten für die Tests ausgewählt. Zudem werden die für den Cloud-Dienst verantwortlichen Systemkomponenten mindestens monatlich automatisiert auf bekannte Schwachstellen überprüft. Erkannte Schwachstellen werden nach definierten Kriterien bewertet und entsprechende Maßnahmen zur Behebung oder Milderung innerhalb festgelegter Zeitfenster gemäß den Richtlinien zum Umgang mit Schwachstellen umgesetzt.[72]

Kommunikationssicherheit

Der ISO-Standard legt bereits umfangreiche Sollmaßnahmen für die Kommunikationssicherheit fest. Zusätzlich werden im Folgenden weitere ergänzende Maßnahmen aufgeführt, die entweder nicht in den ISO-Richtlinien enthalten sind oder im C5-Rahmenwerk näher beschrieben werden. Es empfiehlt sich, die im Unternehmen bzw. beim Cloud-Anbieter bereits kommunizierten Maßnahmen und deren Implementierungsgrad individuell zu prüfen, um festzustellen, ob spezifische Ergänzungen erforderlich sind.

Der Cloud-Anbieter implementiert technische Schutzmaßnahmen, um Netzwerkangriffe und Distributed-Denial-of-Service (DDoS)-Angriffe zu erkennen und darauf zu reagieren. Die Daten werden in ein SIEM-System übertragen, um korrelierende Ereignisse zu identifizieren und

[69] Kriterienkatalog Cloud Computing C5:2020, OPS-14, OPS-17
[70] Kriterienkatalog Cloud Computing C5:2020, OPS-23 – OPS-24
[71] Kriterienkatalog Cloud Computing C5:2020, PI-01
[72] Kriterienkatalog Cloud Computing C5:2020, OPS-19, OPS-22

entsprechende Maßnahmen zu ergreifen. Für die internen Verbindungen im Netzwerk des Cloud-Anbieters bestehen spezifische Sicherheitsanforderungen, einschließlich der Separierung von Sicherheitszonen, Kommunikationsbeziehungen, erlaubten Protokollen und der Trennung des Datenverkehrs zu Administrations- und Überwachungszwecken. Diese Anforderungen werden dokumentiert und kommuniziert.[73]

Hinsichtlich der Netzwerkarchitektur werden die Cloud-Netzwerke entsprechend einer Risikobewertung in vertrauenswürdige und nicht vertrauenswürdige Netzwerke unterteilt und durch Sicherheitszonen separiert. Darüber hinaus erfolgt eine Zugangskontrolle zu den Netzwerkperimetern auf Basis einer Sicherheitsbewertung entsprechend den Anforderungen der Cloud-Kunden.

Zur logischen und physischen Trennung von Cloud-Kundennetzwerken werden Managementkonsolen und Infrastruktur in separaten Netzen betrieben. Diese Netze sind durch Multi-Faktor-Authentifizierung geschützt. Netzwerke für Migration und virtuelle Maschinen sind ebenfalls von anderen Netzen separiert. Der Kundendatenverkehr in gemeinsam genutzten Netzen wird nach einem Segmentierungskonzept auf Netzebene segregiert.[74]

Im nächsten Themenblock Produktsicherheit geht es darum, den Cloud-Kunden aktuelle Informationen über die sichere Konfiguration des Cloud-Produkts (-Dienstes) sowie über bekannte Schwachstellen zur Verfügung zu stellen. Dazu kann beispielsweise ein Online-Register dienen, auf das der Kunde Zugriff hat. Dort werden auch verfügbare Software-Updates sowie Informationen zur Sicherheit des Dienstes, zum Datenzugriff und zur Funktionalität aufgeführt. Die protokollierten Daten sind geschützt und können vom Cloud-Kunden gelöscht werden.[75]

Um eine sichere Interaktion zwischen Benutzern, IT-Komponenten und Anwendungen zu gewährleisten, muss der Dienstleister starke Authentisierungsmechanismen an allen Zugangspunkten anbieten. Darüber hinaus wird ein effizientes Session-Management eingesetzt, um Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität zu schützen.[76]

Passwörter werden cloudseitig vertraulich behandelt, wobei Länge und Komplexität technisch erzwungen werden. Die serverseitige Speicherung erfolgt sicher mit starken Hash-Funktionen und Salt-Werten.[77]

Für die unverzügliche Behebung eventueller Schwachstellen, muss der Zugriff auf die Funktionen des Cloud-Dienstes durch Zugriffskontrollen eingeschränkt werden. Diese sind regelmäßig zu überprüfen. Bei virtuellen Maschinen oder Containern, die von Cloud-Kunden betrieben werden, stellt der Cloud-Anbieter sicher, dass der Kunde die Auswahl der Images einschränken kann und über Änderungen informiert wird.[78]

[73] Kriterienkatalog Cloud Computing C5:2020, COS-01 – COS-02
[74] Kriterienkatalog Cloud Computing C5:2020, COS-05 – COS-06
[75] Kriterienkatalog Cloud Computing C5:2020, PSS-03 – PSS-04
[76] Kriterienkatalog Cloud Computing C5:2020, PSS-05 – PSS-06
[77] Kriterienkatalog Cloud Computing C5:2020, PSS-07
[78] Kriterienkatalog Cloud Computing C5:2020, PSS-08

Julija Brull ist Senior Transformation Manager bei CORE. Sie verfügt über mehrjährige Beratungserfahrung im Technologiesektor. Ihre Schwerpunktthemen umfassen strategisches Project Management, Organisationsentwicklung und -transformationen sowie Informationssicherheit.

Mail: julija.brull@core.se

Liubov Khomutovskaya ist Expert Director 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

Fabian Meyer ist Managing Partner bei CORE. In der Klientendimension verantwortet er die Umsetzung komplexer IT-Projekte mit Schwerpunkten Digitalisierung im Bankensektor, Merger & Akquisitions, Payments und Transaction Banking. Fabian betreut eine Vielzahl an Klienten aus der Finanzindustrie und verfügt über mehrjährige Beratungserfahrung im Technologiesektor.

Mail: fabian.meyer@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