Cloud Exit

Cloud Computing hat sich in vielen Organisationen – beispielsweise unter dem Schlagwort „Cloud First" – als bevorzugtes Modell für die Erbringung von IT-Dienstleistungen etabliert. Unabhängig davon, ob Infrastruktur (IaaS), Plattformen (PaaS) oder fertige Anwendungen (SaaS) aus der Cloud bezogen werden: Bei jedem dieser Bereitstellungsmodelle besteht die Gefahr der Abhängigkeit von einem einzelnen Anbieter – bei SaaS aufgrund proprietärer Datenformate und geschlossener Schnittstellen besonders ausgeprägt, bei PaaS und IaaS durch plattformspezifische Dienste und Konfigurationen ebenfalls relevant. Diese Abhängigkeit gilt es zu antizipieren. Eine gut vorbereitete Cloud-Exit-Strategie ermöglicht einen planvollen Ausstieg aus dieser Abhängigkeit, falls sich die Rahmenbedingungen ändern. Wenn im Folgenden von ***Cloud Exit*** *gesprochen wird, meinen wir den geplanten und kontrollierten Prozess, mit dem ein Unternehmen seine Daten, Anwendungen und Services aus einer bestehenden Cloud-Infrastruktur herausführt, um sie*

- *in eine andere Cloud-Umgebung,*
- *in eine hybride Lösung oder*
- *zurück in die eigene IT-Landschaft zu überführen.*

In diesem Positionspapier werden die Auslöser und Herausforderungen eines Cloud Exit aufgezeigt. Darauf aufsetzend stellen wir einen Plan für den Weg aus der Cloud dar, der neben relevanten Schritten auch rechtliche und vertragliche Fragestellungen einbezieht. Im Anhang präsentieren wir ein Beispiel, das die zuvor angesprochenen Aspekte aufgreift und anwendungsorientiert veranschaulicht.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Inhaltsverzeichnis

Cloud Computing ist großartig – warum will da jemand weg?

Man beschäftigt sich oft begeistert mit der Implementierung neuer Dienstleistungen und oft überwiegen die positiven Aspekte und Erwartungen. In unserer digitalisierten Welt verlagern viele Unternehmen ihre Services und Daten zunehmend in die Cloud. Die BaFin [[1]] hat sogar moderne Cloud-Lösungen als kostengünstige Alternative zum Betrieb traditioneller Rechenzentren anerkannt. Aus diesem Grund setzen sowohl Unternehmen als auch Institutionen, selbst in regulierten Bereichen, verstärkt auf Cloud-Lösungen verschiedener Anbieter. Doch bei der Auswahl eines Dienstanbieters sollte man auch immer einen potenziellen Ausstieg bedenken.

Wir verstehen im Folgenden unter Cloud Exit den geplanten oder ungeplanten Ausstieg eines Unternehmens aus einer Cloud-Umgebung, also die Migration von Daten, Anwendungen oder Diensten weg von einem Cloud-Anbieter – entweder zurück in ein eigenes Rechenzentrum oder zu einem anderen Cloud-Anbieter.

Die Notwendigkeit einer wohlüberlegten Exit-Strategie ist unumgänglich geworden. Die Geschwindigkeit und Agilität, die die Cloud bietet, haben zweifellos zahlreiche Vorteile für Organisationen geschaffen. Dennoch sollten wir uns bewusst sein, dass die Abhängigkeit von Cloud-Anbietern auch potenzielle Risiken birgt, die bei einem unvorhergesehenen Ausstieg aus der Cloud erhebliche Auswirkungen haben können. Wie kann ich meine Daten erhalten, wenn ich die Zusammenarbeit beenden möchte? Welche vertraglichen Aspekte werden dann wichtig? Und wie einfach ist es, die vorhandenen Daten in etwaige Nachfolge-Services zu importieren?

Damit es nicht zu bösen Überraschungen kommt, soll dieser Leitfaden Denkanstöße bieten und bei der Erstellung einer Exit-Strategie unterstützen.

- Die Bedeutung einer Exit-Strategie im Kontext von Cloud-Diensten wird durch die EU-Verordnung des Digital Operational Resilience Act (DORA) betont. DORA verlangt von Finanzinstituten und anderen regulierten Unternehmen in der EU, ihre digitale Resilienz zu stärken, indem sie Strategien für den Umgang mit Drittanbietern entwickeln. Dazu gehört auch die Bewertung von Risiken durch Cloud-Anbieter sowie die Fähigkeit, die Geschäftsprozesse trotz einer Unterbrechung oder sogar eines Ausstiegs aufrechtzuerhalten. Die Regelungen zur Geschäftskontinuität und Exit-Strategien sind Anforderungen von DORA, die vor allem sicherstellen, dass keine unkontrollierte Abhängigkeit (Vendor Lock-In) vom Cloud-Anbieter entsteht. [[19]]
- Das BSI hat im Rahmen seiner Empfehlungen zur Cloud-Sicherheit ebenfalls die Bedeutung eines geplanten Exits hervorgehoben. Im BSI-Grundschutz-Kompendium wird explizit darauf verwiesen, dass Organisationen geeignete Maßnahmen treffen sollten, um die Datenmigration sowie die Wiederherstellung der IT-Dienste zu gewährleisten. Dies schließt die Definition vertraglicher Regelungen zur Datenherausgabe und Datenlöschung ein. Zudem verweist das BSI auf die Bedeutung der Multi-Cloud-Strategie, um Abhängigkeiten von einzelnen Anbietern zu minimieren. Für Unternehmen, die unter die KRITIS-Verordnung fallen, ist die Planung eines Exits von besonderer Bedeutung, da eine hohe Verfügbarkeit und Resilienz der Systeme vorgeschrieben sind. Der Ausfall eines Cloud-Anbieters könnte massive Auswirkungen auf die Kritikalität der bereitgestellten Dienste haben. Laut der KRITIS-Richtlinie sollten Betreiber Notfallpläne und Ausweichszenarien entwickeln, um die Kontinuität sicherzustellen. Dies umfasst auch die Einhaltung strenger Sicherheitsanforderungen und die regelmäßige Überprüfung von Drittanbietern.
- Die Norm ISO/IEC 27001:2022, die den Aufbau eines Informationssicherheits-Managementsystems (ISMS) regelt, legt Wert auf Risikomanagement und die Minimierung von Risiken, die durch Drittanbieter entstehen. In diesem Kontext fordert die Norm, dass Unternehmen die Verfügbarkeit, Integrität und Vertraulichkeit von Daten auch im Falle eines Anbieterwechsels gewährleisten. Im Rahmen eines ISMS sollten daher Prozesse definiert werden, die sicherstellen, dass Daten im Einklang mit den Sicherheitsanforderungen exportiert, migriert oder gelöscht werden können. Dies betrifft insbesondere die Planung und Dokumentation eines möglichen Anbieterwechsels. [[3]]

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Um den Lock-In-Effekt zu vermeiden, sollten Unternehmen von Anfang an eine Exit-Strategie erstellen, die ihnen die Möglichkeit gibt, den Cloud-Anbieter zu wechseln oder die Services wieder intern zu erbringen. Wenn man sich jedoch bereits in einer Abhängigkeit befindet, sollte man prüfen, wie man diese reduzieren oder auflösen kann.

Eine weitere Herausforderung ist die Integration verschiedener Cloud-Angebote, die zusammen eine Lösung bilden. Was passiert, wenn einer dieser Anbieter seinen Service einstellt oder die Bedingungen ändert? Wie kann man die Kontinuität und Kompatibilität der Lösung sicherstellen?

Ein Exit-Szenario kann auch durch ein ungeplantes Ereignis ausgelöst werden, wie z. B. eine Sicherheitsverletzung, eine Insolvenz oder eine regulatorische Änderung. In diesem Fall muss man schnell und effektiv reagieren können, um die Geschäftskontinuität zu gewährleisten.

Um die Machbarkeit und die Kosten eines Exits zu bewerten, sollte man diesen regelmäßig testen. Dabei sollte man nicht nur die technischen Aspekte, sondern auch die organisatorischen und rechtlichen Implikationen berücksichtigen. Zum Test können die bekannten Szenarien ähnlich wie in einem Business-Continuity-Test abgeprüft werden (Tabletop-Test bis hin zur Durchführung einer (Teil-)Migration von Daten).

Die aktuelle Situation

Cloud Computing ist in der Unternehmenspraxis breit etabliert. Laut Bitkom Cloud Report 2026 nutzen 86 Prozent der Unternehmen in Deutschland bereits Cloud Computing, weitere 14 Prozent planen oder diskutieren den Einsatz. Lediglich 1 Prozent misst dem Thema derzeit keine Relevanz bei.

Dabei kommt die Private Cloud mit 64 Prozent häufiger zum Einsatz als die Public Cloud mit 53 Prozent. [[4]]

Die Herausforderungen

Trotz des Wachstums und der Vorteile, die die Cloud bietet, stehen Unternehmen vor einer Reihe von Herausforderungen, wenn es um den Ausstieg aus der Cloud geht. Die Lock-in-Effekte, unerwartete Kosten, Compliance-Probleme und Sicherheitsbedenken sind nur einige der Risiken, die es zu berücksichtigen gilt.

Vor diesem Hintergrund wird deutlich, dass eine Exit-Strategie von entscheidender Bedeutung ist, um potenzielle Risiken zu minimieren und die Handlungsfähigkeit des Unternehmens in jeder Situation zu gewährleisten. Eine gut durchdachte Exit-Strategie ermöglicht es Unternehmen, flexibel zu bleiben und ihre Daten und Dienste bei Bedarf nahtlos zu verlagern.

In diesem Leitfaden werden die wesentlichen Aspekte einer Cloud-Exit-Strategie beleuchtet, von den Auslösern, die Unternehmen dazu veranlassen können, die Cloud zu verlassen, über die strategischen Überlegungen und Kriterien bis hin zu den vertraglichen Aspekten und praxisnahen Beispielen.

Auslöser für den Cloud Exit

Mögliche Auslöser lassen sich dahingehend unterscheiden, ob sie zu einem geplanten oder ungeplanten Wechsel/ Ausstieg führen. Die Zeiträume für einen Ausstieg/ Wechsel sind im ersten Fall länger und im zweiten Fall kürzer. Insbesondere ein ungewollter Wechsel erfordert ähnliche Vorgehensweisen wie in der Notfallplanung (vgl. BSI 200-4), gegebenenfalls mit Übergangslösungen.

Die Auslöser lassen sich auf unterschiedliche Arten strukturieren:

- Langfristig (strategisch) geplanter oder kurzfristig erzwungener bzw. ungeplanter Wechsel
- Geopolitische, politische oder ökonomische Gründe (Umwelt, soziale Verantwortung)
- Probleme mit dem Geschäftspartner oder durch äußere Rahmenbedingungen induzierte Gründe

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Langfristig (strategisch) geplante Gründe für einen Wechsel

Cloud-Repatriation: Kostensenkung durch Verschiebung von Workloads in effizientere Umgebungen

Cloud Repatriation bedeutet die Rückführung von Workloads aus der Cloud in eigene Rechenzentren oder kostengünstigere Alternativen. Unternehmen entscheiden sich für diesen Schritt, wenn sie feststellen, dass die Cloud-Kosten zu hoch sind oder dass Workloads in einer hybriden oder eigenen Umgebung effizienter betrieben werden können. Dies ist besonders bei dauerhaft hohen Rechenanforderungen oder speziellen Datenverarbeitungsprozessen der Fall.

Beispiel: Ein großes Forschungsunternehmen stellt fest, dass seine langfristigen Cloud-Kosten für maschinelles Lernen und Big Data deutlich über den Erwartungen liegen. Nach der Rückführung dieser Workloads in eine eigene, speziell auf Machine-Learning-Workloads optimierte Infrastruktur kann das Unternehmen Kosten reduzieren und die Leistung steigern. Durch die Hybrid-Cloud-Strategie verbleiben nur noch Workloads in der Cloud, die aufgrund schwankenden Kapazitätsbedarfes dort wirtschaftlicher betrieben werden können, während sich für gleichbleibende ausgelastete Workloads die On-Premise-Lösung als vorteilhaft erweist.

Kurzfristig erzwungener bzw. ungeplanter Wechsel

Anbieter geht insolvent oder stellt Geschäftsbetrieb ein

Wenn ein Cloud-Anbieter in Insolvenz geht oder aus anderen Gründen seine Dienste einstellt, müssen Kunden notgedrungen eine alternative Lösung finden. Die plötzliche Einstellung von Diensten kann den Geschäftsbetrieb empfindlich stören, wenn keine Ausweichpläne existieren.

Beispiel: Im Jahr 2024 wurde im Zusammenhang mit der Insolvenz von Weltbild deutlich, dass auch Endkunden von einem erzwungenen Cloud Exit betroffen sein können: Kundinnen und Kunden verloren den Zugang zu für den eBook-Reader Tolino bereitgestellten digitalen Inhalten. Das zeigt, dass Anbieterabhängigkeiten nicht nur im B2B-, sondern auch im Endkundengeschäft erhebliche Auswirkungen haben können. [[16]]

Geopolitische, politische oder ökonomische Gründe (Umwelt, soziale Verantwortung)

Plötzliche geopolitische Ereignisse oder Sanktionen, die den Dienstzugang blockieren

Sanktionen oder politische Spannungen können dazu führen, dass Cloud-Dienste in bestimmten Regionen nicht mehr zugänglich sind oder Anbieter gezwungen sind, den Dienst in bestimmten Ländern einzustellen. Unternehmen aus sanktionierten Regionen müssen dann ihre Daten und Workloads auf Anbieter verlagern, die nicht von den Sanktionen betroffen sind.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Beispiel: Nach dem Ausbruch des Russland-Ukraine Krieg und der den darauffolgenden Sanktionen gegen Russland mussten zahlreiche russische Unternehmen und sogar einige internationale Firmen ihre Daten von westlichen Cloud-Anbietern wie Microsoft Azure und AWS abziehen. Dies führte zu einer vermehrten Nutzung inländischer Alternativen wie Yandex Cloud.

Ein weiteres prägnantes Beispiel für die Notwendigkeit einer Cloud-Exit-Strategie betrifft SAP im Zusammenhang mit dem Russisch-Ukrainischen- Krieg. Aufgrund internationaler Sanktionen gegen Russland hat SAP im Jahr 2022 beschlossen, seine Cloud-Operationen in Russland schrittweise einzustellen. Dies beinhaltete die vollständige Einstellung des Verkaufs von Produkten und Dienstleistungen in Russland und Belarus sowie die Abschaltung der Cloud-Dienste in Russland.

SAP gab russischen Unternehmen, die nicht von Sanktionen betroffen sind, die Möglichkeit, ihre Daten entweder löschen zu lassen, sie zu erhalten oder in Datenzentren außerhalb Russlands zu migrieren. Für Unternehmen, die den Migrationsweg wählten, wurde vereinbart, dass deren Verträge nach Ablauf der aktuellen Abonnementlaufzeit nicht verlängert werden. Dieser Schritt zeigt deutlich, wie geopolitische Ereignisse und Sanktionen Unternehmen zwingen können, Cloud-Dienstleistungen abrupt zu beenden und ihre Dateninfrastruktur neu zu organisieren. [[6]]

Politische Gründe (auch Umwelt, soziale Verantwortung)

Nachhaltigkeit und Umweltfreundlichkeit

Viele Cloud-Anbieter betreiben Rechenzentren mit enormem Energiebedarf, was zu einem hohen ökologischen Fußabdruck führt. Unternehmen, die klimafreundliche und nachhaltige Praktiken fördern, müssen sicherstellen, dass ihre Cloud-Anbieter ähnliche Ansprüche haben.

Beispiel: Ein großer Automobilhersteller mit einer „Zero Emissions"-Kampagne wechselt den Cloud-Anbieter, um einen Dienstleister zu wählen, der seine Rechenzentren mit erneuerbaren Energien betreibt und die CO_2-Bilanz seiner IT-Infrastruktur reduziert. Dies passt zur Strategie, eine nachhaltige Zukunft zu fördern und stärkt das Markenimage.

Ökonomische Gründe

Preiserhöhung oder Änderungen der Leistungen/AGB

Änderungen in der Preispolitik oder in den Allgemeinen Geschäftsbedingungen (AGB) eines Cloud-Anbieters können dazu führen, dass Unternehmen ihre Vertragsbeziehung überdenken. Dies gilt besonders, wenn die neuen Konditionen die ursprünglichen Erwartungen übersteigen oder die Leistungen reduziert werden. Da solche Änderungen oft angekündigt werden, ist der Zeitdruck in der Regel geringer.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Beispiel: Ein kleineres Unternehmen verlässt einen großen SaaS Cloud-Anbieter, weil dessen Preismodelle kontinuierlich angepasst und dadurch die Kosten erhöht wurden. Stattdessen entscheidet sich das Unternehmen für einen Anbieter, der stabile und berechenbare Preise sowie eine transparente Leistungsübersicht bietet.

Probleme mit dem Geschäftspartner oder durch äußere Rahmenbedingungen induzierte Gründe

Ein solcher Grund kann sein, dass ein Cloud-Anbieter nicht mehr zu den favorisierten strategischen Partnern gehört, da man sich auf einen anderen Cloud-Anbieter fokussieren möchte, da dieser z. B. eine bessere weltweite Abdeckung mit Rechenzentren bietet.

Ein anderer Grund kann sein, dass der Cloud-Anbieter wiederholt das benötigte Service-Level oder die benötigte Service-Verfügbarkeit unterschreitet.

Cloud-Exit mit Plan

Schon bei der Erstellung der Cloud-Strategie sollte die Exit-Strategie mit entsprechenden Exit-Optionen erstellt werden, inklusive entsprechender Risikoabschätzung.

Die Vorbereitung eines möglichen Wechsels sollte bereits im Rahmen der initialen Cloud-Strategie erfolgen. Eine fundierte Exit-Strategie stellt sicher, dass Unternehmen im Falle eines Anbieterwechsels die Kontrolle über ihre Daten und Workloads behalten und die Auswirkungen auf den Betrieb minimieren können. Dies umfasst folgende Aspekte:

Frühe Integration der Exit-Strategie in die Cloud-Planung

Eine Exit-Strategie ist mehr als eine Notfallmaßnahme und sollte als zentraler Teil der Cloud-Strategie betrachtet werden. Dies schließt ein, dass Unternehmen bereits bei der Auswahl eines Anbieters klare Kriterien definieren, die festlegen, wann und unter welchen Bedingungen ein Wechsel erfolgen würde. Eine frühzeitige Planung ermöglicht es, spezifische technische und organisatorische Maßnahmen zu implementieren, die den Daten- und Workload-Transfer im Ernstfall vereinfachen.

Durchführung einer umfassenden Risikoabschätzung

Die Risikoanalyse identifiziert die potenziellen Szenarien und Gründe, die zu einem Wechsel führen könnten, wie z. B. Sicherheitsvorfälle, regulatorische Änderungen, Preiserhöhungen oder Anbieterinsolvenz. Diese Szenarien werden hinsichtlich ihrer Wahrscheinlichkeit und möglichen Auswirkungen bewertet. Eine systematische Bewertung gibt Einblicke in die Schwachstellen der bestehenden Cloud-Umgebung und ermöglicht es, präventive Maßnahmen zu ergreifen.

Festlegung von Exit-Kriterien und Entscheidungsprozessen

Um im Ernstfall schnelle Entscheidungen zu ermöglichen, sollten klare Exit-Kriterien definiert werden. Diese Kriterien legen fest, unter welchen Bedingungen ein Wechsel eingeleitet wird und wie Entscheidungsprozesse ablaufen. Beispielsweise könnten Exit-Kriterien an die Nichterfüllung von Service-Level-Agreements (SLAs), Compliance-Verstöße oder signifikante Kostensteigerungen geknüpft sein.

Dokumentation von Daten-Portabilität und Interoperabilität

Ein kritischer Aspekt jeder Exit-Strategie ist die Sicherstellung der Daten-Portabilität und Interoperabilität der Workloads, um Abhängigkeiten zu reduzieren. Unternehmen sollten sicherstellen, dass Daten in offenen Formaten gespeichert und Anwendungen so konzipiert sind, dass sie sich nahtlos in eine andere

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Umgebung migrieren lassen. Hierzu gehört auch die Einhaltung von Standards und Schnittstellen, die eine Migration auf alternative Plattformen erleichtern.

Test und Validierung der Exit-Prozesse

Eine dokumentierte Exit-Strategie allein reicht nicht aus – regelmäßige Tests und Validierungen sind unerlässlich, um die Praxistauglichkeit der Exit-Strategie zu überprüfen. Ähnlich wie bei einem Business-Continuity-Plan/Notfallplan sollte die Exit-Strategie in regelmäßigen Abständen auf Funktionsfähigkeit getestet werden, um sicherzustellen, dass die Migration ohne wesentliche Unterbrechungen oder Datenverluste abläuft. Pilot-Umzüge oder Sandbox-Tests können wertvolle Einblicke in mögliche Hindernisse geben und Optimierungen ermöglichen.

Kriterien vor der Nutzung

Um den Ausstieg aus einer Cloud-Lösung einfacher zu gestalten, sollten einige Kriterien bereits im Vorfeld (idealerweise bereits vor Einführung der Cloud-Lösung) geprüft werden.

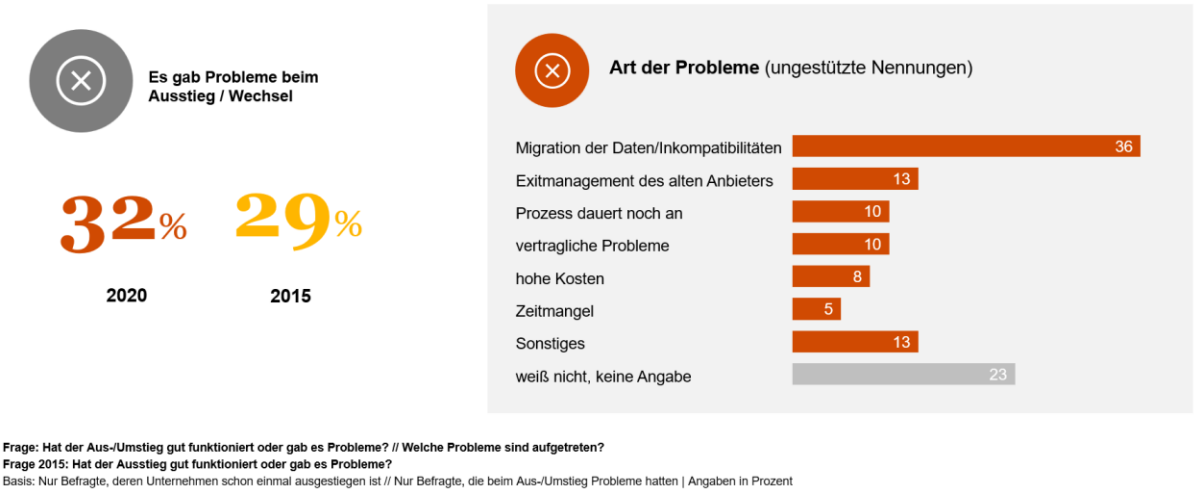

Abbildung 1: Probleme beim Wechsel des Cloud-Dienstes

Diese sind auch gegebenenfalls regelmäßig während des Betriebs der Lösung zu aktualisieren (analog zum Notfallplan). Denn gemäß der Umfrage von ISACA und PwC von 2021 [[7]], gaben 29 % der Befragten im Jahr 2020 an, Probleme beim Ausstieg/Wechsel gehabt zu haben. Um etwaigen Herausforderungen zu begegnen, sollen folgende wichtigste Kriterien eine Hilfestellung darstellen:

- Vergleichbare Cloud-Services auf dem Markt prüfen (Abhängigkeitsrisiko senken),
- Voraussetzung für eine Datenmigration prüfen (u. a. offene Standards, Tools von Anbietern, Metadaten, Komplexität zur Aufbereitung von Daten, Netzwerklatenz, potenzielle Störungen beim Datentransfer),
- Ressourcenbedarf für eine mögliche Exit-Strategie (Zeit, Speicherkapazität, Aufwand für Datenkonvertierung oder Datenmigration),
- sowie rechtliche und vertraglich einzuhaltende Aspekte wie z. B. Datenschutz, Data Residency oder GoBD (u. a. Aufbewahrungsfristen). [[21]]

Im Folgenden werden die genannten Kriterien detailliert beschrieben:

Vergleichbare Services auf dem Markt

Damit die Migration zu einer anderen SaaS-Lösung überhaupt möglich ist, bedarf es eines vergleichbaren Produkts auf dem Markt. Daher sollte man vor der Verwendung von SaaS-Lösungen prüfen, ob es im Bedarfsfall alternative Produkte gibt, zu denen man wechseln könnte.

Achtung: Vorsicht bei Alleinstellungsmerkmalen, die zwar Entscheidungsgründe bei der (Erst-)Auswahl sein können, aber andererseits einen Vendor-Lock-In begünstigen!

Voraussetzungen für eine Datenmigration

Laut einer Umfrage der ISACA in Zusammenarbeit mit PwC [[7]] wurden bei 36 % der problematischen Wechsel des Cloud-Anbieters Probleme mit inkompatiblen Daten bei der Migration angegeben. Dieser Wert bezog sich auf allgemeine Cloud-Wechselprojekte. Bei SaaS liegen die Werte vermutlich noch höher.

Warum ist Datenmigration grundsätzlich wichtig?

Daten werden aus verschiedenen Gründen migriert, beispielsweise um folgende Zwecke zu erfüllen:

- Daten oder Ressourcen konsolidieren
- Speicherkosten senken
- Altdaten archivieren
- Dateneigentum übertragen
- Daten in neuen Applikationen weiter nutzen
- Konformität von Daten mit Regularien verbessern

Diese Gründe gelten auch beim Cloud-Exit.

Welche typischen Herausforderungen bei der Datenmigration sind zu meistern?

Problematisch ist oft, dass unklar ist, in welchem Format die Daten vorliegen und ob ein Datentransfer verlustfrei möglich ist, da die Daten in Clouds oft anders strukturiert bzw. formatiert sind (proprietäre Formate). [[18]]

Durch die Reform des Datenschutzrechts in Europa wird ein neues rechtliches Instrument eingeführt, das den Export vereinfachen soll. Gemäß Artikel 20 der EU-Datenschutzgrundverordnung hat jede natürliche Person das „Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“. Zwar geht die DSGVO hier explizit auf natürliche Personen ein, jedoch sind die dadurch geschaffenen Lösungen auch für juristische Personen nutzbar. Für eine rechtssichere und praktikable Datenmigration bleibt es jedoch erforderlich, in Verträgen mit Cloud-Anbietern explizite Regelungen zu Exportformaten, Schnittstellen und Exit-Szenarien festzuhalten. [[17]]

(Offene) Standards

Standardisierte Schnittstellen zum Auslesen der eigenen Daten ermöglichen eine Migration auch ohne Mithilfe des bisherigen Anbieters. Wenn zudem die Datenstrukturen (für Stammdaten wie Adressen, interne Konfigurationen wie Workflows oder Berechtigungsgruppen) an einem offenen Standard angelehnt sind, sind weniger komplexe Transformationen zwischen unterschiedlichen Datenmodellen erforderlich.

OpenAPI-Spezifikation für Cloud-APIs

Viele Cloud-Anbieter verwenden OpenAPI, um ihre APIs standardisiert bereitzustellen. Dies ermöglicht die einfache Integration und den Zugriff auf Cloud-Daten.

AWS API Gateway: Unterstützt die OpenAPI-Spezifikation, wodurch Daten und Dienste zwischen AWS und anderen Plattformen migriert werden können.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Google Cloud APIs: Viele Google Cloud-Dienste, wie Cloud Storage oder BigQuery, bieten standardisierte OpenAPI-basierte Endpunkte. [[8]]

OData bei Enterprise-Cloud-Diensten

OData (Open Data Protocol) ist ein gängiger Standard, der in vielen Cloud-basierten Unternehmenslösungen verwendet wird. Es ermöglicht den einheitlichen Zugriff auf Daten in verschiedenen Cloud-Diensten.

Microsoft Azure: OData wird für Dienste wie Azure API Management und Dynamics 365 verwendet, um standardisierten Datenzugriff zu gewährleisten.

SAP Cloud: Die SAP Business Technology Platform unterstützt OData für nahtlose Datenmigrationen zwischen Cloud- und On-Premise-Systemen. [[9]]

SQL-Standards in Cloud-Datenbanken

Cloud-basierte Datenbankdienste setzen auf SQL-Standards, um Daten Portabilität und Interoperabilität zu fördern.

Google BigQuery: Unterstützt SQL-ähnliche Abfragen und ermöglicht den Export von Daten in andere Datenbanken.

Amazon RDS: Nutzt relationale Datenbanken (z. B. MySQL, PostgreSQL), die ANSI SQL-konform sind, was die Migration zu anderen Plattformen vereinfacht. [[10]]

CSV als Exportformat in Cloud-Services

CSV ist ein gängiges Format, das von nahezu allen Cloud-Diensten als Exportoption angeboten wird, um Daten für die Migration bereitzustellen.

Google Workspace: Google Sheets bietet den Export von Daten im CSV-Format, was die Übertragung in andere Cloud- oder On-Premise-Systeme erleichtert.

AWS S3: Unterstützt die Speicherung und den Export von tabellarischen Daten im CSV-Format. [[11]]

FHIR (Fast Healthcare Interoperability Resources) in Cloud-Healthcare-Lösungen

FHIR wird in Cloud-basierten Gesundheitsdiensten verwendet, um den Austausch von Gesundheitsdaten zwischen Plattformen zu ermöglichen.

Google Cloud Healthcare API: Unterstützt FHIR, um Patientendaten in verschiedenen Cloud- und On-Premise-Systemen zu teilen.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Microsoft Azure Health Data Services: Ermöglicht die Nutzung von FHIR zur Integration und Migration von Gesundheitsdaten. [[12]]

JSON und XML in Cloud-APIs

JSON und XML sind Standardformate für Datenexporte und werden von nahezu allen Cloud-APIs verwendet.

AWS Lambda: Nutzt JSON als Standardformat für den Datenaustausch zwischen Lambda-Funktionen und anderen AWS-Diensten.

Azure Functions: Unterstützt JSON und XML für die Interaktion mit externen Systemen. [[13]]

ISO 20022 für Cloud-basierte Finanzdienste

Finanzdienste, die auf Cloud-Dienste setzen, wie Zahlungsplattformen oder Bankenlösungen, verwenden ISO 20022 für den Datenaustausch.

AWS Financial Services Cloud: Unterstützt ISO 20022 für Finanzdatenübertragungen.

Google Cloud for Financial Services: Ermöglicht den standardisierten Austausch von Zahlungs- und Transaktionsdaten gemäß ISO 20022. [[14]]

Betriebskontinuität

Auf Basis der geschaffenen maschinenlesbaren Formate ist der Export jedoch nicht zwingend interoperabel. Eine Datentransformation wird nötig. Die damit verbundenen Aufwände, etwa bei JSON zu XML-Konvertierungen, erfordern eine detaillierte, zeitliche Planung. Betriebsabläufe müssen daher frühzeitig betrachtet, Benutzer involviert und im Prozess informiert werden, um eine reibungslose Betriebskontinuität sicherzustellen.

Systemausfälle und Störungen

Durch die Konvertierung von Quell- zu Zieldaten können Anpassungsfehler auftreten. Eine Migration von virtuellen Maschinen kann zu Treiberkonflikten im Ziel-Hypervisor führen. Obligatorische Datenfelder im Zielsystem können im Quellsystem nicht vorhanden sein.

Diese Problemfälle sind im Voraus durch Tests und genaue Planung der Datenmigration zu validieren. Systemausfälle können so auf Teilbereiche eingegrenzt werden. Damit muss das Zielsystem bereits bei Erstellung der Exit-Strategie hinreichend bekannt sein.

Aufwände für die Migration

Wie schon unter Betriebskontinuität erwähnt, entstehen durch die nötigen Datentransformationen Aufwände. Üblicherweise können Transformationen jedoch gut automatisiert werden. Die dafür nötigen Aufwände sind je nach Anbieter, Komplexität der Umgebung und Datenvolumen nicht leicht zu quantifizieren. Auch ist die bisherige Praxis (z. B. Weltbild (Pakalski, 2024)) davon geprägt, den Kunden wenig Vorlauf zu bieten. Ein Exit kann sehr kurzfristig notwendig werden, wenn der Dienstleister zahlungsunfähig wird

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

und ein Insolvenzverfahren einleitet (siehe oben). Hyperscaler schalten zum Beispiel rigoros ganze Accounts bei ausbleibender Zahlung ab. Eine Migration würde hier nicht nur interne, sondern auch wegen fehlender kurzfristiger Kapazitäten, externe Kosten verursachen. Bei einer konkreten Exit-Strategie sind diese Kosten zumindest grundlegend evaluiert.

Datensicherheit

Beim Export dieser Daten ist das Gesamtsystem während des Migrationszeitraums nicht über die bekannte Governance geschützt. Es entstehen kurzzeitige Veränderungen der Rechte und Rollen. Die damit verbundene Vulnerabilität des Systems stellt eine weitere Herausforderung dar. Die Daten müssen auch hier entsprechend den Schutzzielen sicher gespeichert und verarbeitet werden.

- Daten dürfen lediglich von autorisierten Benutzern gelesen werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten als auch während der Migration.
- Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.
- Verhinderung von Systemausfällen. Der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.

Ein besonderes Schutzziel im Zuge des Cyber Resilience Act betrifft die Resilienz: Widerstandsfähigkeit und Belastbarkeit gegenüber Ausspähungen, irrtümlichen oder mutwilligen Störungen sowie absichtlichen Schädigungen (Sabotagen) Invalid source specified..

Metadaten

Wenn Metadaten (physische Adressen, Signaturen, Audit Trails [Integrität], Zeitstempel) nicht portiert werden können, müssen alternative Wege zur Sicherung der Datenintegrität geplant und umgesetzt werden (z. B. Bulk-Signatur migrierter Datensätze, Export in ein Read-only-Archiv). Schnittstellen zu und von anderen Systemen müssen dabei gegebenenfalls angepasst werden.

Wenn historische Daten (Vorversionen) proprietär abgelegt wurden, ist auch hier eine Alternativlösung zur Sicherung der Integrität einzuplanen.

Aufbereitete Daten

Wurden im alten System Daten in weiterverarbeiteter Form verwendet (z. B. spezielle Indizierung oder KI-Modelle), muss geklärt werden, inwieweit diese berechneten Daten migriert werden können oder dürfen.

Ressourcenbedarf (Zeit, Speicherkapazität, Personal)

Der Bedarf an Ressourcen (z. B. Speicherplatz oder Kommunikationsbandbreite) wird neben der Datenstruktur auch durch den Umfang der in der Cloud gespeicherten Informationen bestimmt. Während im Normalbetrieb die Bandbreite für Datentransfers ausreichend dimensioniert sein sollte, kann es im Falle einer vollständigen Migration aller Daten zu Engpässen kommen (zumal andere Kunden womöglich zur gleichen Zeit diese Kapazitäten nutzen möchten). Daher sollte auch eine lokal beim Anbieter durchgeführte Kopie auf physische Datenspeicher in Betracht gezogen werden. Entsprechende Vereinbarungen sind vorab vertraglich zu regeln.

Mitarbeiter oder Dienstleister, die die Datenmigration durchführen, sollten entsprechend geschult und erfahren sein, um diese Tätigkeit effizient durchführen zu können.

Rechtliche und vertragliche Aspekte

Letztendlich zählt zwischen zwei Parteien, was vertraglich bindend festgehalten wurde. Daher ist es entscheidend zu prüfen, ob die relevanten Aspekte vertraglich festgehalten wurden. Beispielsweise sollen neben den oft standardisierten Themen wie Datenschutz und GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern) auch Themen wie Dateneigentümerschaft oder ein möglicher Wechselservice geprüft werden. Denn gerade auch die rechtliche Klärung über die Besitzverhältnisse der

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Daten kann im Falle einer Trennung zwischen einem Unternehmen und einem Cloud -Anbieter eine entscheidende Rolle dabei spielen, ob man alle Daten und Services durch den Wechsel verliert oder nicht. [[21]]

In Cloud-Verträgen sind nicht nur die Verpflichtungen des Cloud-Anbieters, sondern auch die Verpflichtungen des Cloud-Nutzers geregelt. Beispielsweise enthält der Datenverarbeitungsvertrag (Data Processing Agreement) Rechte und Pflichten des Datenverantwortlichen. Dieser bleibt auch bei Cloud-Szenarien üblicherweise der Kunde. Von daher ist es notwendig, die Verträge mit Cloud-Anbietern auch auf eigene Verantwortlichkeiten hin zu prüfen. Diese eigenen Verantwortlichkeiten können sich auch auf technische Aspekte oder Kooperationsaspekte wie Mitwirkungspflichten beziehen. Solche Mitwirkungspflichten können den Exit-Fall betreffen, indem z. B. Fristen und Möglichkeiten zur Daten-Extraktion geregelt sind. Dabei ist darauf zu achten, dass nicht nur der Extrakt von Primärdaten geregelt ist, sondern auch der Extrakt von notwendigen Sekundärdaten wie Änderungsbelegen oder Sicherheitslogs.

Praxisbeispiel von Exit Vertragsregelungen mit einem Cloud-Anbieter:

Im Falle eines Vertragsendes, sowie nach schriftlicher Aufforderung durch Aufsichtsbehörden, verpflichtet sich der Cloud-Anbieter, alle vom Kunden bereitgestellten Daten in einem gängigen, maschinenlesbaren Format innerhalb von 30 Tagen nach Vertragsbeendigung zur Verfügung zu stellen. Die Datenbereitstellung erfolgt über einen sicheren Übertragungsweg, den der Kunde vorgibt. Nach erfolgreicher Übergabe löscht der Provider sämtliche Kundendaten gemäß den geltenden Datenschutzbestimmungen. Im Falle einer ausdrücklichen schriftlichen Aufforderung durch Aufsichtsbehörden, verpflichtet sich der Cloud-Anbieter zudem, ab dem Datum der Kündigung die angeforderten Onlinedienste weiterhin bereitzustellen. Während dieses Zeitraums stellt der Cloud-Anbieter die Onlinedienste gemäß den Bestimmungen des Beitritts bereit und der Kunde bezieht und bezahlt diese weiterhin gemäß den Bestimmungen des Beitritts. Darüber hinaus kann der Kunde während dieses Zeitraums die Kundendaten über die Standardprozesse und -tools des Cloud-Anbieters abrufen.

Des Weiteren sind beim Abschluss von Cloud-Verträgen die geltenden, und so weit absehbar, auch zukünftigen rechtlichen Rahmenbedingungen zu berücksichtigen. Steht z. B. fest, dass Unternehmen der DORA (Digital Operations Resilience Act) Verordnung unterliegen, sind sowohl bestehende als auch künftige Verträge mit Cloud-Anbietern höchstwahrscheinlich ebenfalls betroffen. In diesem Zusammenhang sind die entsprechenden DORA-Anforderungen zu berücksichtigen und Exit-Strategien vorzubereiten. [[19]]

Besonderes Augenmerk ist auf die jeweiligen Datenkategorien zu legen, die in der Cloud verarbeitet werden sollen. Mit den Datenkategorien können sich auch die rechtlichen Rahmenbedingungen des Vertrags ändern. Das gleiche gilt für den Ort der Datenverarbeitung und Datenspeicherung (Data Residency, Jurisdiction). Wird z. B. die Kategorie „gesundheitsbezogene Daten“ neu in das Cloud-Szenario aufgenommen, ändern sich u. U. die rechtlichen Anforderungen. Dies kann z. B. Änderungen in den Anforderungen an Daten-Extraktionen bedeuten, welche im Cloud-Exit-Fall von essenzieller Bedeutung sein können.

In der EU regelt u. a. der EU Data Act viele der o. g. Aspekte. Der EU Data Act ist seit dem 11. Jan. 2024 in Kraft. Er bietet Übergangsfristen für einige Teile und erlaubt eine schrittweise Einführung. Der EU Data Act enthält Anforderungen an Cloud-Anbieter, einheitliche vertragliche sowie technische Standards bereitzustellen, so dass es Cloud-Kunden erleichtert wird, zwischen Cloud-Anbietern zu wechseln. Bei Infrastructure-as-a-Service-(IaaS-)Anbietern geht dies so weit, dass Werkzeuge angeboten werden müssen, die bei der Portierung von Programmen und Daten zu anderen Cloud-Anbietern unterstützen.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Cloud-Exit Pläne

Cloud-Exit Pläne enthalten Handlungsanweisungen, um in einem Cloud-Exit-Fall handlungsfähig zu sein. Da der Cloud-Exit unterschiedliche Szenarien umfassen kann, sind verschiedene Arten von Exit-Plänen erforderlich. Im Folgenden ist eine Überschicht verschiedener Cloud-Exit Pläne aufgeführt.

Die Aktualität der Pläne sollte regelmäßig überwacht werden.

Kategoriespezifische Pläne

In diesen Plänen sind grundsätzliche Aspekte enthalten, was beim Exit von verschiedenen Kategorien von Cloud-Service-Modellen zu beachten ist, d. h. „Exit von Cloud SaaS“, „Exit von Cloud PaaS“, „Exit von Cloud IaaS“.

Situationsspezifische Pläne

In diesen Plänen sind grundsätzliche Aspekte enthalten, was in verschiedenen Situationen zu beachten ist, z. B. Cloud-Anbieter stellt Service ein, kann auf Grund von Sicherheitsvorfällen nicht mehr als vertrauenswürdig betrachtet werden, ist insolvent usw.

Cloud-Anbieter-spezifische Pläne

Diese Pläne enthalten Anweisungen, wie bei einem Exit von einem bestimmten Cloud-Anbieter vorzugehen ist. Hierbei können u. a. auch technische Spezifikationen des Cloud-Anbieters eine Rolle spielen, die bei einer Übertragung der Daten zu einem alternativen Anbieter relevant sind.

Anwendungsspezifische Pläne

Diese Pläne enthalten Anweisungen, wie beim Exit von einer bestimmter Cloud-Anwendung bzw. Cloud Service eines bestimmten Cloud-Anbieters vorzugehen ist.

Überprüfung und Tests der Cloud-Exit-Strategien und Pläne

Da Exit-Strategien und Exit-Pläne einen wesentlichen Teil der Geschäftsfortführungsplanung darstellen, ist eine regelmäßige Überprüfung, sowie Testen – insbesondere der konkreten Exit-Pläne – unabdingbar. Im Rahmen einer Multi-Cloud-Strategie kann dieser Test auch die Übertragung der Daten von einem Cloud-Anbieter zum anderen (alternativen) Cloud-Anbieter beinhalten.

Fazit und Ausblick

In dem Positionspapier wurden die wesentlichen Aspekte einer Cloud-Exit-Strategie herausgearbeitet. Eine solide Exit-Strategie ist von entscheidender Bedeutung, um die Abhängigkeit von Cloud-Anbietern zu verringern und die Flexibilität des Unternehmens zu gewährleisten. Es wurden zudem die Risiken beleuchtet, die mit einem Cloud-Exit verbunden sind (wie z. B. Datenverlust, Komplexität der Migration und potenzielle Kostensteigerungen).

Mit Blick auf die hohen Abhängigkeiten von Cloud-Providern verfügen lediglich 29 Prozent der befragten Unternehmen über geregelte Exit-Strategien. [[5]]. Das bedeutet, dass mehr als zwei Drittel der befragten Unternehmen kein klares vertragliches Vorgehen für den Ausstieg definiert haben, was ein erhebliches Risiko für Vendor-Lock-in und Compliance-Probleme darstellt.

Eine gründliche Planung und Vorbereitung im Unternehmen sind daher unerlässlich, um diese Herausforderungen erfolgreich zu bewältigen.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Anhang: Cloud Exit-Strategie – beispielhafte Herangehensweise

Werden in einem Unternehmen wichtige Kernaufgaben an Cloud-Anbieter ausgelagert, entsteht dadurch eine Abhängigkeit, die bei Wegfall des Anbieters oder einzelner Services signifikante Unterbrechung der eigenen Geschäftsprozesse und -tätigkeit zu Folge haben kann.

Gesetzlicher Rahmen

DORA verlangt von Unternehmen, insbesondere im Finanzsektor, robuste Maßnahmen zur operativen Resilienz. Die Abhängigkeit von Cloud-Anbietern ist ein zentraler Bestandteil, da diese oft als kritische Drittanbieter eingestuft werden. Cloud-Exit-Strategien sollten Teil des unternehmensweiten Risikomanagements sein, um DORA-Vorgaben zu erfüllen. [[19]]

Unternehmen, die als kritische Infrastrukturen eingestuft werden, müssen eine hohe Verfügbarkeit und Sicherheit ihrer Systeme gewährleisten. Ein Ausfall von Cloud-Diensten könnte wesentliche Teile der Infrastruktur gefährden. Eine Cloud-Exit-Strategie ist essenziell, um den Betrieb auch bei Wegfall von Cloud-Services aufrechtzuerhalten.

Der EU Cyber Resilience Act (CRA) legt den Fokus auf Cybersicherheit und Resilienz in der Nutzung digitaler Produkte und Services, was auch Cloud-Dienste umfasst. Bei der Implementierung einer Cloud Exit-Strategie sollten auch Cybersicherheitsaspekte berücksichtigt werden, insbesondere der Schutz sensibler Daten während der Migration zu alternativen Anbietern, die Gewährleistung von Interoperabilität und die Nutzung standardisierter Datenformate, der sichere Entzug bzw. Transfer von Zugriffsrechten, die lückenlose Dokumentation aller Maßnahmen sowie die verpflichtende sichere Löschung von Daten beim bisherigen Anbieter. Unternehmen sollen sicherstellen, dass Cloud-Dienste den CRA-Vorgaben entsprechen, bestehende Abhängigkeiten in der Lieferkette berücksichtigt und geeignete Maßnahmen zur Erkennung, Meldung und Bewältigung von Cyberangriffen implementiert sind.

Die NIS2-Richtlinie fordert von Unternehmen eine robuste IT-Sicherheitsstrategie und erhöht die Anforderungen an die Resilienz kritischer Dienstleistungen, einschließlich der Abhängigkeit von Drittanbietern wie Cloud-Diensten. Eine Cloud Exit-Strategie ist Teil der Risikomanagementmaßnahmen, die NIS2 erfordert, um die Geschäftskontinuität sicherzustellen.

Eine Cloud Exit-Strategie ist ein zentrales Element, um die Anforderungen von DORA, KRITIS, CRA und NIS2 zu erfüllen. Die Hauptmaßnahmen umfassen:

- Identifikation kritischer Abhängigkeiten von Cloud-Diensten.
- Entwicklung und regelmäßige Aktualisierung von Exit Plänen.
- Sicherstellung von Cybersicherheit während des Exits.
- Schulung der Verantwortlichen und klare Zuweisung von Rollen und Verantwortlichkeiten.
- Vertragliche Absicherung mit Cloud-Anbietern hinsichtlich Exit Szenarien.

Diese Vorgaben erhöhen nicht nur die Sicherheit und Resilienz, sondern sichern auch die Compliance mit regulatorischen Anforderungen.

Um diesen Abhängigkeiten vorzubeugen, sollte auf Unternehmensebene eine Cloud-Exit-Strategie implementiert werden, die Augenmerk auf die Abhängigkeit zu Cloud-Anbietern und deren möglichem Wegfall legt. Viele Unternehmen regeln die erlaubte und nicht-erlaubte Nutzung von Cloud Services in einer unternehmensweiten Cloud-Strategie oder Cloud-Policy. In diese eingebettet muss der Fall betrachtet werden, dass Cloud Services unvorhergesehen wegfallen, d. h. Anbieter ihren Dienst einstellen, ihren Kunden kündigen, insolvent sind, etc. Um eine Cloud-Exit-Strategie unternehmensweit zu implementieren, sind in den folgenden Bereichen Aspekte zu berücksichtigen und umzusetzen.

Die Hauptelemente der Cloud-Exit-Strategie sind, den verschiedenen Unternehmungsfunktionen bzw.-rollen Verantwortung innerhalb der Cloud-Exit-Strategie zu zuordnen, sowie Cloud-Exit-Pläne zu erstellen und zu pflegen.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Rollen und Verantwortlichkeiten

Beim Erstellen einer Cloud Exit-Strategie spielen verschiedene Abteilungen und Rollen im Unternehmen eine entscheidende Rolle. Eine enge Zusammenarbeit und die klare Zuweisung von Verantwortlichkeiten sind unerlässlich, um einen reibungslosen Übergang sicherzustellen.

Unternehmensleitung / Geschäftsführung (CEO)

Diese hat dafür Sorge zu tragen, dass in der unternehmensweiten Cloud Strategie das Thema Cloud-Exit verankert ist.

Verantwortlichkeiten: Die Unternehmensleitung (CEO, Vorstand) trägt die letztendliche Verantwortung für die strategische Entscheidung, die Cloud-Infrastruktur oder einen bestimmten essenziellen Cloud-Anbieter zu verlassen. Diese Entscheidung kann durch viele Faktoren motiviert sein, wie steigende Kosten, Sicherheitsbedenken, Veränderungen im Geschäftsmodell oder regulatorische Anforderungen. Die Geschäftsführung legt die übergeordneten Ziele des Cloud-Exits fest, wie z. B. die Verbesserung der Datenkontrolle oder die Senkung langfristiger Betriebskosten. Sie autorisiert auch das Budget und stellt sicher, dass ausreichend Ressourcen zur Verfügung stehen, um die Strategie ohne wesentliche Geschäftsunterbrechungen umzusetzen. Zusätzlich ist die Geschäftsführung dafür verantwortlich, Risiken wie mögliche Datenverluste oder Ausfallzeiten zu bewerten und zu minimieren.

Einbindung: Die Unternehmensleitung ist von Beginn an beteiligt, da sie sicherstellen muss, dass der Exit in die Gesamtstrategie des Unternehmens eingebettet ist. Sie trifft entscheidende Freigaben, überwacht die Risikobewertung und unterstützt die Kommunikationsstrategie intern wie extern.

Finanzabteilung (CFO)

Verantwortlichkeiten: Die Finanzabteilung überwacht die finanziellen Aspekte des Cloud-Exits. Dazu gehört die Erstellung von Budgetplänen, die Bewertung der finanziellen Auswirkungen des Wechsels auf die Geschäftsbilanz und die Überwachung der laufenden Kosten des Projekts. Die Finanzabteilung arbeitet eng mit der IT und der Geschäftsführung zusammen, um sicherzustellen, dass der Cloud-Exit wirtschaftlich sinnvoll ist und langfristig Kosteneinsparungen ermöglicht. Sie analysiert auch potenzielle Kostentreiber, wie zusätzliche Hardware-Investitionen oder laufende Lizenzkosten, und stellt sicher, dass die Cloud Exit-Strategie im Rahmen des Budgets bleibt.

Einbindung: Die Einbindung der Finanzabteilung in eine Cloud Exit-Strategie ist von entscheidender Bedeutung, da dieser Prozess erhebliche finanzielle Auswirkungen auf das Unternehmen haben kann. Die Finanzabteilung, angeführt vom CFO (Chief Financial Officer), ist verantwortlich für die Bewertung, Überwachung und Steuerung aller finanziellen Aspekte des Exits. Ihre Einbindung erfolgt in mehreren Phasen des Prozesses, um die wirtschaftliche Tragfähigkeit zu gewährleisten und finanzielle Risiken zu minimieren.

IT-Leitung (CIO / CTO) - Operating Office

Verantwortlichkeiten: Der CIO (Chief Information Officer) oder CTO (Chief Technology Officer) trägt die technische Gesamtverantwortung für den Cloud-Exit. Dies umfasst die Überprüfung der technischen Anforderungen, die Auswahl einer neuen oder angepassten Infrastruktur und die detaillierte Planung der Migration. Dabei muss die IT-Leitung sicherstellen, dass die gewählte Infrastruktur den spezifischen Anforderungen des Unternehmens entspricht und zukünftige Wachstumsbedürfnisse abdeckt. Die IT-Leitung ist außerdem für die Koordination der internen IT-Teams verantwortlich, die an der technischen Umsetzung arbeiten. Sie muss sicherstellen, dass die Systeme während des Exit Prozesses verfügbar bleiben und dass Notfallpläne für den Fall von Störungen oder Systemausfällen bestehen. Zusätzlich ist die IT-Leitung für die Kosteneffizienz des Projekts und die Auswahl geeigneter Technologien verantwortlich, die sowohl wirtschaftlich als auch technisch tragfähig sind.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Einbindung: Die IT-Leitung ist kontinuierlich eingebunden, von der Vorab-Planung über die Entscheidungsfindung bis hin zur Steuerung der technischen Umsetzung. Sie arbeitet mit der Geschäftsführung und den technischen Teams zusammen, um alle strategischen und technischen Aspekte zu verbinden.

Cloud-Architekten

Verantwortlichkeiten: Cloud-Architekten sind für die Planung und technische Ausgestaltung des Cloud-Exits verantwortlich. Sie analysieren und identifizieren, welche Komponenten migriert, umgestaltet oder durch On-Premise- oder hybride Lösungen ersetzt werden müssen. Sie entwickeln detaillierte Migrationspläne, die sicherstellen, dass Daten und Anwendungen effizient und ohne Datenverlust auf die neue Infrastruktur übertragen werden. Dies erfordert eine genaue Analyse der bestehenden Anwendungen, die Identifizierung von Abhängigkeiten und die Erstellung eines Exit Plans, der potenzielle Engpässe und Risiken berücksichtigt. Cloud-Architekten müssen auch geeignete Alternativen zur Cloud auswählen (z. B. eigene Rechenzentren, Hybrid-Cloud-Modelle) und eng mit den Sicherheitsexperten zusammenarbeiten, um sicherzustellen, dass die neue Architektur den Sicherheitsstandards des Unternehmens entspricht.

Einbindung: Die Cloud-Architekten sind von Anfang an aktiv beteiligt und übernehmen die technische Leitung bei der Planung und Umsetzung der Migration. Ihre Arbeit ist maßgeblich für die Risikominderung und den Erfolg der Migration verantwortlich.

Sicherheitsbeauftragte (CISO / IT-Sicherheitsbeauftragter)

Verantwortlichkeiten: Der CISO (Chief Information Security Officer) oder IT-Sicherheitsbeauftragte hat die Verantwortung, alle Sicherheitsaspekte des Cloud-Exits zu überwachen. Dies umfasst die Sicherstellung der Datenintegrität während der Migration, den Schutz vor Sicherheitslücken und die Einhaltung von Datenschutzanforderungen (z.B. DSGVO, HIPAA). Der Sicherheitsbeauftragte prüft, wie Daten sicher übertragen und in der neuen Umgebung geschützt werden können. Dazu gehört die Verschlüsselung von Daten während der Migration, die Implementierung von Sicherheitskontrollen in der neuen Infrastruktur sowie die Überwachung und Vermeidung von Schwachstellen. Darüber hinaus muss der CISO gewährleisten, dass die Sicherheitsrichtlinien des Unternehmens auf die neue Infrastruktur übertragen werden und dass interne und externe Bedrohungen kontinuierlich überwacht und adressiert werden.

Einbindung: Der Sicherheitsbeauftragte wird bereits in der frühen Planungsphase eingebunden, um Sicherheitsanforderungen und Risiken frühzeitig zu berücksichtigen. In der Vertrags- und Designphase prüft er Service Level Agreements (SLAs), die Sicherheitsarchitektur sowie Berechtigungskonzepte. Während der Umsetzung ist er intensiv eingebunden: Er überwacht die Einhaltung der definierten Sicherheitsmaßnahmen, begleitet Migrationstests und sorgt für den sicheren Entzug von Zugriffsrechten beim bisherigen Anbieter. Vor dem Go-Live erteilt er auf Basis erfüllter Sicherheitskriterien den Freigabevermerk. Auch nach Abschluss bleibt er in Monitoring, Incident-Response und Nachweisdokumentation aktiv, um die Sicherheit nachhaltig zu gewährleisten.

Recht & Compliance

Verantwortlichkeiten: Die Abteilung für Recht und Compliance spielt eine wichtige Rolle, um sicherzustellen, dass der Cloud-Exit rechtlich und regulatorisch abgesichert ist. Dies umfasst die Analyse der Vertragsbedingungen mit dem Cloud-Anbieter, einschließlich Kündigungsfristen, Kosten für vorzeitige Vertragsauflösungen und die Verpflichtungen des Anbieters in Bezug auf Datenspeicherung und -löschung. Compliance-Verantwortliche prüfen auch, ob der Exit Prozess mit gesetzlichen Anforderungen wie der DSGVO oder branchenspezifischen Vorschriften (z. B. im Gesundheitswesen oder Finanzwesen) im Einklang steht. Zudem sorgt diese Abteilung dafür, dass alle Datenschutzrichtlinien, die das Unternehmen betreffen, eingehalten werden und potenzielle rechtliche Risiken im Zusammenhang mit der Datenübertragung minimiert werden.

Einbindung: Diese Abteilung muss frühzeitig involviert sein, um sicherzustellen, dass alle rechtlichen und regulatorischen Aspekte identifiziert und adressiert werden. Sie bleibt während des gesamten Prozesses aktiv, um sicherzustellen, dass Änderungen im Plan oder in der technischen Umsetzung konform sind.

Projektmanager

Verantwortlichkeiten: Der Projektmanager steuert den gesamten Cloud-Exit-Prozess und sorgt dafür, dass alle beteiligten Parteien koordiniert zusammenarbeiten. Er wird dann aktiv, wenn bereits erstellte Exit Pläne (siehe Kapitel ‚Cloud-Exit-Pläne') zur Ausführung kommen. Der Projektmanager entwickelt einen detaillierten Projektplan, der alle Meilensteine, Zeitpläne und Ressourcenanforderungen abdeckt. Der Projektmanager überwacht die Fortschritte, stellt sicher, dass das Projekt innerhalb des Budgets bleibt, und identifiziert sowie adressiert Risiken und Abweichungen vom Plan. Er koordiniert die Kommunikation zwischen den Abteilungen (IT, Recht, Finanzen, Sicherheit etc.) und sorgt dafür, dass regelmäßige Status-Updates und Berichte an die Unternehmensleitung geliefert werden. Der Projektmanager ist auch für die Nachverfolgung verantwortlich, um sicherzustellen, dass der Exit wie geplant durchgeführt und abgeschlossen wird.

Einbindung: Der Projektmanager wird von Anfang an eingebunden und bleibt bis zur vollständigen Umsetzung und Nachbereitung des Cloud-Exits aktiv. Seine Rolle ist entscheidend für den reibungslosen Ablauf des Projekts.

Risikomanagement

Die Prozesse zum Risikomanagement sind zu ergänzen und durch sie ist sicherzustellen, dass das Risiko des Cloud-Exits erfasst, bewertet, überwacht und regelmäßig an das Management gemeldet wird. Dabei sind Markt- und Anbietertrends im Cloud-Segment einzubeziehen, d.h. auch externe Daten zu berücksichtigen.

Verantwortlichkeiten: Das Risikomanagement ist für die Identifikation, Bewertung und Überwachung aller Risiken im Zusammenhang mit der Cloud Exit-Strategie verantwortlich. Es analysiert potenzielle technische, finanzielle, operationelle, sicherheitsbezogene und regulatorische Risiken und entwickelt Strategien zur Risikominderung. Dazu gehören das Festlegen von Maßnahmen zur Risikobehandlung sowie die laufende Überwachung des Risikostatus während der Umsetzung des Exits. Zudem führt das Risikomanagement Szenarioanalysen durch, um potenzielle Worst-Case-Szenarien zu simulieren und präventiv zu handeln.

Einbindung: Das Risikomanagement arbeitet eng mit allen relevanten Abteilungen wie IT, Finanzen, Recht und Compliance zusammen, um sicherzustellen, dass Risiken aus allen Perspektiven erkannt und adressiert werden. Es ist in alle Phasen des Cloud-Exit-Prozesses eingebunden – von der Planung bis zur Nachbearbeitung – und informiert die Geschäftsleitung regelmäßig über den Risikostatus und potenzielle kritische Entwicklungen.

Internal Audit/ Kontrollfunktion

Die interne Audit Abteilung hat die effektive Definition und Ausführung der Cloud-Exit-Strategie und der beteiligten Geschäftsbereiche regelmäßig zu auditieren und entsprechenden Berichte zu erstellen und Mitigationen zu verfolgen.

Verantwortlichkeiten: Die interne Audit-Abteilung ist für die unabhängige Überprüfung und Bewertung der Prozesse und Kontrollen rund um die Cloud-Exit-Strategie verantwortlich. Sie sorgt dafür, dass die definierten Richtlinien, Risiken und Kontrollen eingehalten werden, und stellt die Integrität und Transparenz des gesamten Prozesses sicher. Dazu gehört die Prüfung der Einhaltung interner Vorgaben sowie regulatorischer Anforderungen, die Überwachung der Risikominderungsmaßnahmen und die Sicherstellung, dass keine wesentlichen Mängel im Exit-Prozess bestehen.

Einbindung: Internal Audit ist während des gesamten Cloud-Exits als unabhängige Instanz eingebunden, führt regelmäßige Audits und Kontrollen durch und berichtet direkt an die Geschäftsführung oder den Vorstand. Sie arbeitet in Abstimmung mit dem Risikomanagement, der IT und der Finanzabteilung, um sicherzustellen, dass Risiken angemessen bearbeitet werden und die Exit-Strategie im Einklang mit den internen Kontrollen und externen Vorgaben steht.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Fachbereich / Anwendungsverantwortliche - Einkauf/ Lieferantensteuerung /

Verantwortlichkeiten: Die Fachabteilungen sind für die Überprüfung und Definition der Anforderungen für ihre spezifischen Anwendungen und Geschäftsprozesse verantwortlich. Sie müssen sicherstellen, dass die Anwendungen, die in der Cloud betrieben werden, entweder in die neue Infrastruktur migriert oder durch geeignete Lösungen ersetzt werden. Sie sind auch dafür zuständig, die betrieblichen Auswirkungen des Cloud-Exits zu minimieren und sicherzustellen, dass keine kritischen Prozesse unterbrochen werden. Anwendungsverantwortliche arbeiten eng mit den IT-Teams zusammen, um sicherzustellen, dass alle Funktionalitäten erhalten bleiben und die Performance auf dem gewünschten Niveau bleibt.

Einbindung: Diese Abteilungen sind während der Planungs- und Migrationsphase intensiv eingebunden, um die Anforderungen ihrer Anwendungen zu kommunizieren und ihre ordnungsgemäße Funktion nach der Migration sicherzustellen.

Externe Dienstleister / Berater

Verantwortlichkeiten: Externe Berater und Dienstleister können spezifisches Fachwissen einbringen, insbesondere bei der Planung der Migration oder bei der technischen Umsetzung. Sie bieten Expertise in den Bereichen Cloud-Infrastruktur, Datensicherheit, Migrationsstrategien oder spezifische Technologien, die im Unternehmen nicht vorhanden sind. Sie unterstützen auch bei der Risikobewertung und bieten unabhängige Beratung zu Best Practices, was die Planung und Durchführung des Cloud-Exits optimiert. Dienstleister können auch bei der Schulung von Mitarbeitern oder bei der Bereitstellung technischer Ressourcen helfen.

Einbindung: Externe Berater werden typischerweise punktuell hinzugezogen, um das interne Team zu ergänzen und ihre Expertise bei speziellen Herausforderungen einzubringen.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Abbildungsverzeichnis

Quellen

[1] BaFin: Rundschreiben 10/2017 (BA) – Bankaufsichtliche Anforderungen an die IT (BAIT), Fassung vom 16.08.2021
[2] BSI-Grundschutz-Kompendium, BSI, Edition 2023 (https://www.bsi.bund.de/grundschutz)
[3] ISO/IEC 27001:2022 – Information security management systems
[4] Bitkom Research: Cloud Report 2026 – Status Quo & Trends in Wirtschaft und Politik, 2026, DOI: 10.64022/2026-cloud-report-2026
[5] Ganowski, T. / Zillmann, M.: Lünendonk-Studie „IT-Sourcing-Trends 2025/2026“, Lünendonk & Hossenfelder GmbH, September 2025
[6] SAP SE: SAP Continues to Stand in Solidarity with Ukraine, März 2022 (https://news.sap.com/2022/03/sap-continues-to-stand-in-solidarity-with-ukraine/)
[7] ISACA Germany Chapter / PwC: Cloud Governance in Deutschland – Herausforderungen und Erfolgsfaktoren, ISACA, 2021
[8] OpenAPI Initiative (https://www.openapis.org/)
[9] OData – Open Data Protocol (https://www.odata.org/)
[10] ISO/IEC 9075:2023 – Database languages SQL (ANSI SQL Standard)
[11] Shafranovich, Y.: RFC 4180 – Common Format and MIME Type for CSV Files, IETF, 2005 (https://www.rfc-editor.org/rfc/rfc4180)
[12] HL7 International: FHIR Release 4 (https://www.hl7.org/fhir/)
[13] JSON.org: Introducing JSON (https://www.json.org/)
[14] ISO 20022 – Financial services: Universal financial industry message scheme (https://www.iso20022.org/)
[15] Pakalski, I.: Wenn 8,5 Millionen Windows-Geräte die Welt im Griff haben, Golem.de, 21.07.2024
[16] Golem.de: Weltbild stellt Geschäftsbetrieb ein – eBook-Kunden verlieren Zugang zu Tolino-Inhalten, 2024
[17] Horn, N. / Riechert, A.: Praktische Umsetzung des Rechts auf Datenübertragbarkeit – Rechtliche, technische und verbraucherbezogene Implikationen, 3. Aufl., Stiftung Datenschutz, Leipzig, 2018
[18] UP KRITIS: Empfehlungen zur Vorbereitung einer Exit-Strategie bei Nutzung von Cloud-Dienstleistungen, Version 1.0, März 2022 (https://www.bsi.bund.de/dok/1042922)
[19] Europäisches Parlament / Rat der EU: Verordnung (EU) 2022/2554 – Digital Operational Resilience Act (DORA), 14.12.2022
[20] Europäisches Parlament / Rat der EU: Verordnung (EU) 2023/2854 – EU Data Act, 13.12.2023
[21] BMF: GoBD – Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form, 28.11.2019

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Autorenteam

- Edgar Röder – Leiter der Fachgruppe
- Fabian Mrowka – stellv. Leiter der Fachgruppe
- Alexander Biehl
- Andrea Schröder
- Christian Konradt
- Davor Basic
- Gerald Suffel
- Jan-Hendrik Porth
- Lars Hawranek
- Lukas Merz
- Michael Herrmann
- Philipp Werner
- Stephan Schmidt
- Stephan Zimmer
- Vassilios Tsioupas
- Wijayakulasingam Nagushaanth

Möchten Sie zu diesem Positionspapier mit uns Kontakt aufnehmen? Dann schreiben Sie uns bitte an: FG-CloudComputing@isaca.de

Interessieren Sie sich für weitere Veröffentlichungen des ISACA Germany Chapter? Dann besuchen Sie uns jetzt auf: https://www.isaca.de/publikationen/publikationen/alle-publikationen.html