



DER WEG IN DIE CLOUD

Anleitung zu einer
faktenbasierten Risikoabschätzung

Abstract

Der Schritt in die Cloud ist heute für die meisten Unternehmen, Organisationen und öffentlichen Verwaltungen sinnvoll, denn dank dem technologischen Fortschritt ist die Cloud sicher und höchst nutzenstiftend. Damit ergeben sich völlig neue Entwicklungsmöglichkeiten und Chancen.

Der Schritt in die Cloud will indes gut überlegt und geplant sein. Es gibt wie in jedem Projekt unterschiedliche Risiken, welche identifiziert und beurteilt werden müssen. Der Entscheid für die Cloud muss entsprechend auf einer sorgfältigen Risikoabwägung basieren. Das vorliegende Dokument soll Organisationen in diesem Prozess unterstützen.

Von zentraler Bedeutung ist zudem, wie sich das auslagerungswillige Unternehmen organisatorisch aufstellt. Dies hängt nicht zuletzt von Grösse und vom Umfang des Cloud-Projekts ab. Unabdingbar ist eine klare Kompetenzordnung, in die alle zuständigen Fachabteilungen eingebunden sind. Dies garantiert einen gut strukturierten Entscheidungsprozess, der nötigenfalls schnelle Entscheide von höchster Stelle erlaubt.

Beim Aufbau von Cloud-Lösungen ist stets auch das entsprechende regulatorische Umfeld zu beachten. Compliance und Governance kommt bei allen Projekten eine grosse Bedeutung zu.

© (2021) Microsoft Corporation. All rights reserved. Microsoft, Windows and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational and discussion purposes only and represents the current view of Microsoft Corporation or any Microsoft Group affiliate as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment or binding offer or acceptance of any warranties, liabilities, wrongdoing etc. on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this document.

Inhalt

1	Die Cloud – ein zentrales Element des Geschäftserfolgs.....	4
2	Compliance: Klare Vorgaben erleichtern die Kontrolle	6
3	Die Risikosicherung (Risk Assurance).....	10
4	Der Risikobeurteilungsprozess.....	14
5	Cloud-Governance	27

Abbildungen

Abbildung 1 –	Aufbau des Dokuments	5
Abbildung 2 –	Wichtigste Daten-Compliance Vorgaben	7
Abbildung 3 –	Daten können an verschiedenen Standorten verschiedenen Compliance Vorgaben unterworfen sein und die Verantwortung für die Daten kann in verschiedenen Händen sein.....	7
Abbildung 4 –	Geteilte Zuständigkeiten	10
Abbildung 5 –	Microsoft Assurance Framework.....	13
Abbildung 6 –	Beurteilung und Bewertung der Risiken.....	14
Abbildung 7 –	6 Stufen des Risikomanagement Prozesses nach ISO Norm 31000.....	15
Abbildung 8 –	Risikograde	16
Abbildung 9 –	Liste potentieller Risiken bei Cloud Migration und Betrieb.....	17
Abbildung 10 –	Risiko-Auswirkung - Tabelle zur Beurteilung.....	18
Abbildung 11 –	Eintrittswahrscheinlichkeit von Risiken: Tabelle zur Beurteilung.....	19
Abbildung 12 –	Beispiel einer Risikobeurteilungsmatrix.....	19
Abbildung 13 –	Beispiel einer Kontrolle für das Nutzerberechtigungsmanagement.....	22
Abbildung 14 –	Einbindung der Kontrollen des Cloud Providers.....	23
Abbildung 15 –	Elemente einer ausgearbeiteten Risiko-Option	25
Abbildung 15b–	Optimaler Mix aus juristischen, technischen und organisatorischen Massnahmen ..	25
Abbildung 16 –	Beurteilte Risiken, vor und nach mitigierenden Massnahmenpaketen.....	26
Abbildung 17 –	Homogenisierung der Governance Struktur zwischen Kunde und Cloudprovider.....	29
Abbildung 18 –	MVP-Ansatz für die Erarbeitung der Cloud-Governance	30

Disclaimer

Dieses Dokument enthält eine allgemeine Darstellung von Fragen, die unsere Kunden beim Einsatz von Cloud Computing Lösungen häufig stellen. Sie sollen damit in die Lage versetzt werden, die technischen und rechtlichen Hintergründe beim Einsatz einer Cloud Computing Lösung besser zu verstehen. Dieses Dokument beinhaltet keine einzelfallbezogene Prüfung individueller Rechtsverhältnisse. Für die individuelle und abschliessende rechtliche Beurteilung über die Zulässigkeit des Einsatzes von Microsoft Cloud Lösungen in einem konkreten Anwendungsfall müssen Sie daher eine separate rechtliche Beratung in Anspruch nehmen.

1 DIE CLOUD – EIN ZENTRALES ELEMENT DES GESCHÄFTSERFOLGS

Die Zahl der Unternehmen, die auf Cloud-Anwendungen setzt, steigt kontinuierlich. Kleine wie grosse Betriebe sind überzeugt, dass die Cloud mit effizienten Abläufen und widerstandsfähigen Prozessen die Basis für schnellere Innovationen schafft. Sie ermöglicht die Auslagerung einzelner Arbeitsabläufe im Produktivitätsumfeld, fördert die Modernisierung bestehender Applikationslandschaften sowie die ganzheitliche Kundenansprache über digitale Kanäle. Selbst regulierte Unternehmen wie Finanzinstitute sind deshalb bereit, auch sensitive oder essenzielle Daten in der Public Cloud zu bearbeiten. Eine ähnliche Entwicklung lässt sich bei der öffentlichen Verwaltung und im Gesundheitsbereich beobachten, wo – wie im Bankenwesen – hohe Diskretion und Vertraulichkeit Kern der Geschäftsmodelle sind.

Heute werden auch geschäftskritische und patientenorientierte Anwendungen, die höchsten Ansprüchen an Sicherheit und rechtlich-regulatorischer Konformität entsprechen müssen, in der Cloud unterhalten. Die meisten Firmen anerkennen, dass eine professionell betriebene Public Cloud mindestens ein gleichwertiges, wenn nicht höheres Niveau an Sicherheit bietet als dass es die Firmen aus eigener Kraft bewerkstelligen könnten. Immer mehr Geschäftsleitungen und Verwaltungsräte haben verstanden, dass Cloud-basierte Infrastrukturen einen wichtigen Beitrag zur Sicherung des künftigen Geschäftserfolgs darstellen und damit von hochgradig strategischer Relevanz sind.

Die Cloud ist sicher

Zweifel bezüglich der Datensicherheit galten vor nicht allzu langer Zeit noch als einer der Hauptgründe, die Cloud nicht zu nutzen. Dass diese Zweifel weitgehend beseitigt werden konnten, ist nicht zuletzt einem allgemeinen Digitalisierungsschub und der Maturität der Cloud-Technologie geschuldet.

Doch trotz sicherer und besserer Technologie ist es auch heute unabdinglich, den Weg in die Cloud genau zu planen. Verschiedene Gesichtspunkte sind zu beachten, von der Technologiewahl über organisatorisch-kulturelle Aspekte bis zur Einhaltung von konkreten Anforderungen wie etwa gesetzliche Vorgaben oder (industrie-)spezifische Regulierungen. Als Beispiele seien hier das Schweizer Datenschutzgesetz, die Rundschreiben der Eidgenössischen Finanzmarktaufsicht FINMA oder der Schutzbedarf von kritischen Daten genannt. Zunehmend wichtig für die Beurteilung eines spezifischen Cloud-Projekts werden jüngst auch Entwicklungen auf internationaler Ebene, konkret die Diskussionen rund um «Schrems II» oder der faktische Wegfall des «Privacy Shield Abkommens» zwischen der Schweiz und den USA. Beide Themen betreffen die rechtlichen Rahmenbedingungen für grenzüberschreitende Datentransfers, insbesondere wenn diese ausserhalb von Europa oder in Länder mit einem niedrigeren Datenschutzniveau stattfinden.

Kein Einstieg in die Cloud ohne faktenbasierte Risikoabschätzung

Fakt ist: Jedes Cloud-Projekt bedarf einer sorgfältigen Abwägung der Chancen und Risiken, insbesondere was den Schutzbedarf der ausgelagerten Anwendungen und Datenbestände sowie die Einhaltung der relevanten rechtlichen und regulatorischen Anforderungen betrifft. Gefordert ist indes nicht nur eine saubere Risikobeurteilung der Cloud-Auslagerung, sondern auch ein nachgelagertes Risikomanagement. Genau an dieser Stelle setzt dieses Dokument an. Es bietet eine Orientierungshilfe, wie eine Risikoeinschätzung an die Hand genommen werden kann und es zeigt auf, wie die rechtlich-regulatorischen Anforderungen in den Kontrollrahmen einer Cloud-Plattform eingefügt und belastbar beurteilt werden können. Es fragt, welche organisatorischen, technischen und vertraglichen Massnahmen vorhanden sind, und inwieweit diese Massnahmen gegebene Anforderungen effektiv adressieren können, beispielsweise die Verhinderung von nicht-autorisiertem Zugriff auf Datenbestände. Es geht also um die grundlegende Methodologie einer faktenbasierten Risikoabschätzung und was dabei beachtet werden soll.

Wichtig zu verstehen ist in diesem Zusammenhang die strikte Arbeitsteilung zwischen dem Kunden und dem Cloud-Anbieter. Ziel ist es, dem Kunden so viel Transparenz und belastbare Evidenz bereitzustellen, dass dieser informiert beurteilen und entscheiden kann. Dabei gilt immer ein Grundsatz: Die Verantwortung zur abschliessenden Beurteilung liegt beim Kunden. Dem Cloud-Anbieter hingegen sind rechtsverbindliche Aussagen zur Konformität einer spezifischen Implementation strikte untersagt.

Daraus leitet sich der zweite Anspruch des vorliegenden Dokuments ab: Es soll als Wegweiser dienen, die relevanten Informationen, Audit-Berichte und technischen Illustrationen schnell zu finden. Dies auch in Anerkennung des Umstands, dass viele Kunden nicht über spezifische Risiko- oder Rechtsabteilungen mit entsprechenden Kernkompetenzen verfügen.

Microsoft bietet Cloud-Services aus Datenzentren in der Schweiz

Microsoft ist seit über 30 Jahren in der Schweiz tätig, verfügt heute über ein Netzwerk von über 4'600 lokal verankerten Partnerfirmen und pflegt regelmässigen und vertrauenswürdigen Kontakt mit Regulatoren und Aufsichtsbehörden. Wir hören zu und sind bestrebt, die Bedenken unserer Kunden zu verstehen und entsprechend darauf zu antworten. Deshalb hat Microsoft auch entschieden, eigene Cloud-Services aus Datenzentren in der Schweiz anzubieten und die ruhenden Daten spezifischer Services innerhalb des Landes zu lagern. Dasselbe gilt für industriespezifische Vertragszusätze wie das Financial Services Amendment, das wir mit unseren Schweizer Finanzkunden in Anerkennung der lokalen Besonderheiten abschliessen.

Beide Initiativen dienen unseren Kunden als zusätzliche Kontrollelemente, wenn es um die Identifikation, Beurteilung und das Management etwaiger Risiken geht. Sie sind Teil unseres Bestrebens, die hiesigen Firmen bestmöglich zu unterstützen, zukunftsorientiert und rechtskonform von den Vorteilen der Hyperscale Cloud zu profitieren. Dass dieses Angebot breit aufgenommen wird, zeigt nicht zuletzt die wachsende Liste an Schweizer Unternehmen, welche ihre Cloud-Dienste aus den lokalen Rechenzentren beziehen. Davon stammt über die Hälfte aus regulierten Industrien, also der Finanzwirtschaft, dem Gesundheitswesen oder dem Bereich der öffentlichen Hand.

Wir sind uns bewusst, dass die Themen, die im Rahmen einer Risikobeurteilung adressiert werden müssen, mitunter sehr anspruchsvoll sind. Wir haben uns im Rahmen dieses Papiers deshalb zu einer vereinfachten Darstellung entschieden, welche beliebig erweitert werden kann. Die wesentlichen Grundlagen der Cloud sind soweit erläutert, dass kein einschlägiges Vorwissen notwendig ist. Entsprechende Musterformulare oder Vorgehensansätze haben wir als Templates beigelegt.

Die möglichen Nutzungsvarianten der Cloud sind sehr breit. Das Dokument wird darum nicht allen Ansprüchen genügen. Auf wichtige, weitere Dokumente wird verwiesen.

Das Dokument orientiert sich an folgendem Ablauf:

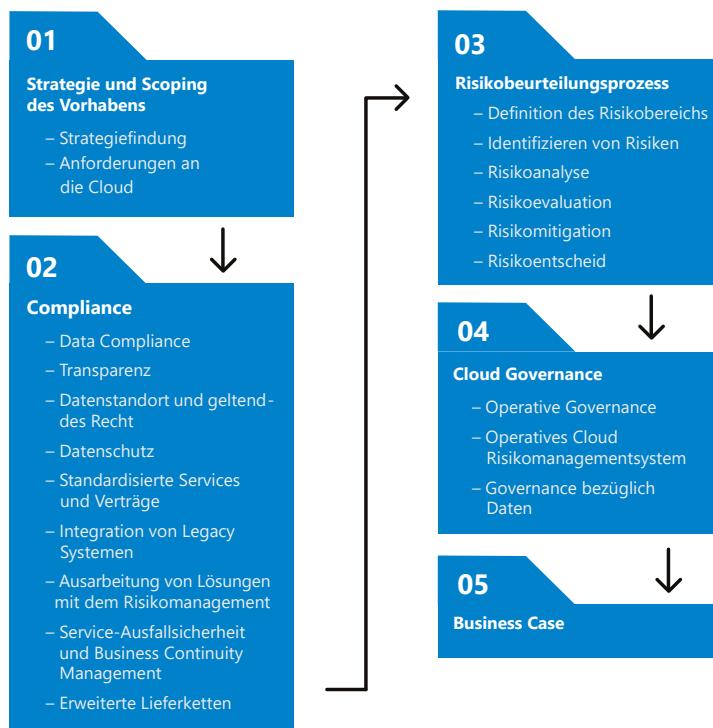


Abbildung 1 – Aufbau des Dokuments

2 COMPLIANCE: KLARE VORGABEN ERLEICHTERN DIE KONTROLLE

Was heisst Compliance?

Compliance beschreibt die Einhaltung aller gesetzlichen Bestimmungen sowie interner Richtlinien durch Unternehmen und ihre Mitarbeiter. Compliance bedeutet damit aber auch, dass Unternehmen ihre Produkte- und Serviceanbieter in ihrer Lieferkette so weit kontrollieren, dass diese Vorgaben eingehalten werden können.

Data Compliance in der Übersicht

Für diverse Arten von Daten bestehen Compliancevorschriften, die es einzuhalten gilt. Die folgende Tabelle gibt eine Übersicht über die wichtigsten Vorgaben:

Daten-Art	Schweizerische Vorgaben	
Personendaten und besonders schützenswerte Personendaten	Nachweis der Notwendigkeit der Datenbearbeitung Unterstellen der Personendaten unter adäquaten Schutz Information der Datensubjekte bez. Datenbearbeitung und Lokation der Daten Auskunfts- und Löschrechte Datenminimierung und Löschung	Schweizerisches Datenschutzgesetz DSGVO
Bankdaten	Nachweis der Klassifizierung und des besonderen Schutzes der Bankkundendaten Sicherstellung, dass der Regulator innert nützlicher Frist in seinem Rechtsraum die Daten verfügbar hat und auf diese zugreifen kann	BankG FINMA Rundschreiben
Finanzdaten aus Bilanz und Erfolgsrechnung	Aufbewahrungspflicht für Bilanz und Erfolgsrechnung Auskunftspflicht und Sicherstellung, dass der Regulator innert nützlicher Frist in seinem Rechtsraum die Daten verfügbar hat und auf diese zugreifen kann.	GebüV OR
Steuerdaten	Aufbewahrungspflicht für Steuer und insbesondere MwSt Daten. Auskunftspflicht und Sicherstellung, dass der Regulator innert nützlicher Frist in seinem Rechtsraum die Daten verfügbar hat und auf diese zugreifen kann	MWSTG
Exportkontrolldaten	Erhebung und Speicherung von Daten, welche der Exportkontrolle unterstellt Güter und deren einzelne Bestandteile betreffen (z.B. Militärische oder sog. Dual-Use Güter) Aufbewahrungspflicht, Auskunftspflicht und Sicherstellung, dass der Regulator innert nützlicher Frist in seinem Rechtsraum die Daten verfügbar hat und auf diese zugreifen kann	Güterkontrollgesetz
Produktedaten	Erhebung und Speicherung von Daten, welche die Erstellungs- Prozesse, die Komponenten und die durchgeführten Tests des Produkts beschrieben Aufbewahrungspflicht	PrSG

Daten-Art	Schweizerische Vorgaben	
Forschungsdaten	Erhebung und Speicherung von Daten, welche die Forschungs- inhalte, die Forschungsverfahren, die Beteiligten, die Ergebnisse sowie die durchgeführten Tests mit deren Ergebnissen beschreiben	FIFG
	Aufbewahrungspflicht, Auskunftspflicht und Sicherstellung, dass der Regulator innert nützlicher Frist in seinem Rechtsraum die Daten verfügbar hat und auf diese zugreifen kann	
IP Daten	Beschreibungen der Inhalte von IP und deren Registrierungen Angabe des Standortes und des Landes, in welchem das IP steuerlich alloziert ist	URG
Daten unter Amts- und Berufsgeheimnis	Daten, die der Staat verwaltet und die unter das Amtsgeheimnis fallen. Aufbewahrungspflicht und Auskunftspflicht sowie Löschpflichten.	StGB

Abbildung 2 – Wichtigste Daten-Compliance Vorgaben

Die Daten müssen auf deren Compliance-Anforderungen hin untersucht, entsprechend kategorisiert und mit den erforderlichen Massnahmen behandelt werden.

Da die Daten nun verschoben werden können, ergeben sich aus den obigen Ausführungen folgende Herausforderungen für die Compliance:

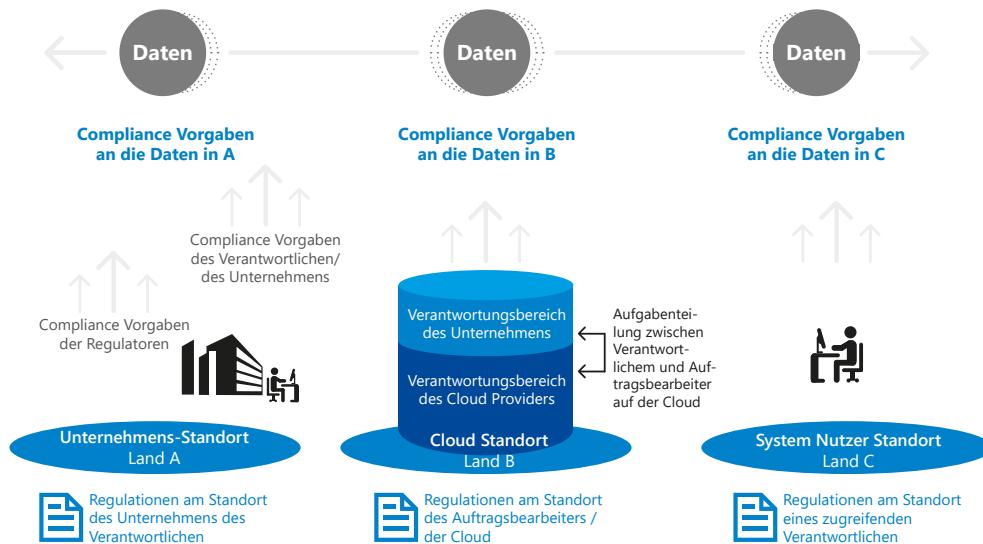


Abbildung 3 – Daten können an verschiedenen Standorten verschiedenen Compliance Vorgaben unterworfen sein und die Verantwortung für die Daten kann in verschiedenen Händen sein.

Zur Veranschaulichung und als Beispiel ein Schweizer Unternehmen, das besonders schützenswerte Personen-daten von Schweizer Bürgerinnen und Bürgern in die Cloud im EU-Raum, z.B. in die Niederlande verschiebt. Damit unterstehen die Daten dort einem adäquaten Schutzniveau wie in der Schweiz, nämlich der Europäischen Datenschutzgrundverordnung (DSGVO). Dennoch verschlüsselt das Unternehmen die Daten, um sicherzu-stellen, dass sie bei einem allfälligen Datenleck nicht gelesen werden können. Das Unternehmen übernimmt damit also die Verantwortung, seine Daten auf der Cloud verschlüsselt abzulegen, auf der Cloud einen Failover sicherzustellen und ein Back-up einzurichten. Der Cloud-Provider seinerseits übernimmt die Verantwortung für die Infrastruktur, den Cyber-Schutz der Systeme und die Aufrechterhaltung des Betriebs gemäss SLA.

Berechtigte Mitarbeiter des Unternehmens schliesslich können von überall her auf der Welt auf die Daten zugreifen. Dies setzt wiederum voraus, dass die Endgeräte dieser Nutzer ausreichend gesichert sind (End-point Protection). Ebenso müssen diese Nutzer durch Weisungen gehalten sein, nicht aus einem Land heraus auf die Daten zuzugreifen oder diese lokal herunterzuladen, wenn das betreffende Land keinen adäquaten Datenschutz bietet.

Transparenz ist wichtig

Das von den Sicherheits- und Compliance-Verantwortlichen des Kunden etablierte Design der Cloud-Lösung muss bei dessen Implementierung und während des anschliessenden Betriebs unbedingt dokumentiert werden. Auch anschliessend erfolgte Änderungen müssen zwingend nachgeführt werden. Ohne detaillierte Informationen über das Design der Cloud-Lösung und darüber, wie verschiedene Sicherheitskontrollen implementiert wurden, können die Risk-Management-Verantwortlichen keine Bewertung der Cloudsicherheit vornehmen. Microsoft bietet innerhalb ihrer Services die geforderte, detaillierte Transparenz über die den Compliance-Anforderungen entsprechende Datenhaltung und -verwaltung in der Cloud.

Datenstandort und geltendes Recht müssen sorgfältig gewählt werden

Besondere Bedeutung kommt dem Recht des jeweiligen Landes zu, in dem die Daten verwaltet werden. Das Cloud-Rechenzentrum kann sich in einem anderen Land befinden als der Hauptgeschäftssitz des Kunden und das geltende Recht kann sich daher vom lokal anwendbaren Recht des Kunden unterscheiden.

Bei den meisten Microsoft Azure-Diensten können die Kunden wählen, in welchem der Länder, in denen Microsoft seine Rechenzentren unterhält, die ruhenden Daten gespeichert werden sollen. Es ist wichtig, dass sich der Kunde darüber im Klaren ist, welches Recht auf den jeweiligen Vertrag anwendbar ist. Die Bewertung und Wahl des anwendbaren Rechts muss daher durch den Kunden stets vor der Nutzung von Cloud-Diensten vorgenommen werden.

Datenschutz-Folgeabschätzung vornehmen

Vorschriften wie die DSGVO / General Data Protection Regulation (GDPR) gewährleisten ein hohes Mass an Kontrolle über die Verarbeitung personenbezogener Daten von Einzelpersonen. Es ist äusserst wichtig, dass sowohl Datenverantwortliche als auch Datenverarbeiter diese Verordnung einhalten, um die sichere Verarbeitung personenbezogener Daten zu gewährleisten und die Privatsphäre der einzelnen Personen zu schützen.

Bei der Bewertung eines Cloud-Dienstes ist die Durchführung einer Datenschutz-Folgeabschätzung (Data Protection Impact Assessment, DPIA) ebenso unerlässlich wie die Sicherstellung, dass das System so eingerichtet ist, dass es die geforderte «Privacy by Design» bietet. Während einer Cloud-Risikobewertung empfehlen wir, mit der Lektüre dieser [vereinfachten DSGVO Anleitung](#) zu beginnen. Daneben bietet unser [Trust Center eine sehr ausführliche GDPR-Übersicht](#), eine Übersicht über die in jedem Microsoft-Produkt integrierten GDPR-Lösungen, eine GDPR-FAQ und eine Reihe von GDPR-Ressourcen wie Whitepapers und Videos.

Standardisierte Services und Verträge sind die Regel

Cloud-Plattformen leben von der Ausschöpfung grosser Synergiepotentiale. Diese können jedoch nur durch konsequente Standardisierung erreicht werden. Die meisten technischen Konzepte und Lösungen sowie die dazugehörigen Vertragsbedingungen liegen daher oft in konsequent standardisierter Form vor. Für Industrien mit besonderen Anforderungsprofilen gibt es zudem spezifische Vertragszusätze, beispielsweise das «Financial Services Amendment» oder das «Professional Secrecy Amendment».

Die Standardisierung der technischen Lösungen und Verträge unterscheidet Cloudservices-Verträge von traditionelleren Outsourcing-Verträgen, bei denen individuelle technische Konzepte eingebracht und die Verträge entsprechend individuell gestaltet werden können.

Integration von Legacy-Systemen

Die Integration von bestehenden Systemen in die Cloud bietet bei der Migration sowie auch beim Parallelbetrieb von On-Premise und Cloudlösungen einige Herausforderungen. Diese betreffen hauptsächlich die Regelung der Authentisierungs- und Zugriffsberechtigung sowie der Datenflüsse zwischen Cloud- und On-Premise-Umgebungen im Rahmen eines Parallelbetriebs (z.B. während der Transition).

Microsoft verfügt über die Erfahrung, Tools und Ressourcen, um Kunden bei der Ausarbeitung von Migrationszenarien zu unterstützen, die diesen Herausforderungen gerecht werden. Microsoft bietet für das Cloud Onboarding auch direkten Support durch «Microsoft FastTrack» und ihre Migrationspartner an. Diese Unterstützung hat sich in der Vergangenheit bei den Kunden als äusserst hilfreich erwiesen.

Ausarbeitung von Lösungen mit dem Risikomanagement

Beim Cloud Computing-Modell wird ein Teil der Kontrolle über die IT-Dienste und ihren Betrieb an den Cloud-Anbieter übertragen. Der Kunde soll prüfen, ob die vom Anbieter angebotenen Sicherheits- und Kontrollanforderungen den internen Vorgaben des Kunden entsprechen.

Aufgrund unterschiedlicher Ausgestaltung der Kontrollsysteme von Cloud-Anbietern und Kunden können unter Umständen Lücken auftreten. Dies führt dazu, dass ein Kunde alternative Szenarien zur Risikominimierung heranziehen oder auf einzelne, bisherige Massnahmen zur Mitigierung von Risiken verzichten muss.

Die Etablierung eines ausgereiften, firmeninternen Governance-Prozesses, der mit Risikoausnahmen umgehen kann, ist daher ein entscheidender Erfolgsfaktor. Ansonsten besteht die Gefahr, dass mangels einer sorgfältigen Due Diligence die Risiken des Cloud Computings falsch (zu hoch) bewertet und Vorhaben gestoppt werden. Der Cloud-Provider kann die vom Risk-Management des Kunden aufgebrachten Punkte aufnehmen und helfen, mit verschiedenen Massnahmen und Kontrollen dazu beizutragen, dass die als hoch erachteten Risiken abschliessend geklärt werden können.

Service-Ausfallsicherheit und Business Continuity Management

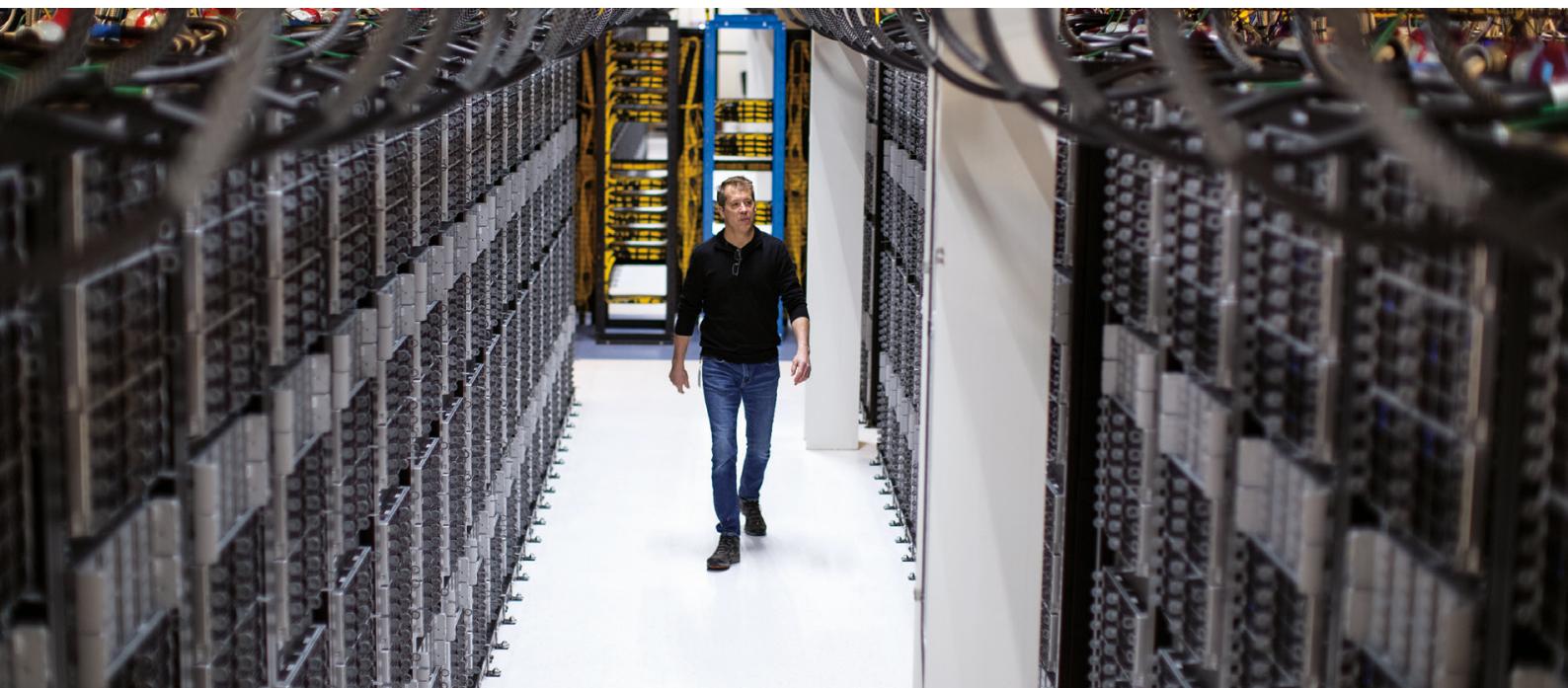
Mit der Auslagerung von Daten und Prozessen steigt sich die Komplexität eines Informationssystems erheblich, müssen doch verschiedene Akteure, welche für verschiedene Komponenten verantwortlich sind, zusammengebracht und koordiniert werden.

Kunden müssen nachweisen können, dass ihre Dienste und Prozesse im Falle von Betriebsausfällen oder Katastrophen in Übereinstimmung mit ihren Policy-Vorgaben funktionsfähig bleiben. Kundeneigene Disaster-Recovery- und Prozesse der Geschäftskontinuität müssen neu sowohl die eigene IT als auch den Cloud-Provider berücksichtigen.

Entsprechend muss das Business Continuity Management (BCM) des Kunden bei Konzeption und Testing seiner Massnahmen den Cloud-Anbieter mitberücksichtigen und darüber hinaus nachweisen, dass eventuelle Exit-Strategien funktionieren. Um diese BCM Assessments und Lösungen zu unterstützen und dem Kunden laufend entsprechende Nachweise der BCM Fähigkeiten zu liefern, kann sich der Kunde im Microsoft «Service Trust Portal» stets transparent über die erfolgten Microsoft BCM-Tests und deren Ergebnisse informieren und diese in sein Compliance Reporting integrieren.

Erweiterte Lieferketten (Chain Outsourcing)

Die meisten Cloud-Anbieter verlassen sich bei der Erbringung ihrer Dienste auf weitere Drittparteien. Diesbezüglich verpflichtet sich Microsoft explizit, vollständig transparent darzustellen, wie und auf welche Art und Weise bei dem Betrieb und der Verwaltung von Cloud-Diensten Drittparteien einbezogen werden. Aus Sicht des Kunden kann die Auslagerung an grosse Cloud-Anbieter wie Microsoft indirekt erfolgen. Zum Beispiel bietet der «Azure Marketplace» hunderte von Drittanbieter-Diensten, die auf «Azure» laufen. Die Herausforderung für den Kunden besteht nun darin, die kontinuierliche Sicherheit und Sichtbarkeit des End-to-End-Services über eine möglicherweise umfangreiche Service-Lieferkette zu gewährleisten, damit die Services weiterhin den internen Compliance-Anforderungen gerecht werden. Solche stark verketteten Services mit mehreren Unterakordanten sind im Outsourcingbereich nicht neu. Im Bereich Cloud kommen solche Lieferketten aber häufiger vor.



3 DIE RISIKOSICHERUNG (RISK ASSURANCE)

Viele Firmen und Organisationen sehen in der Adoption von Cloud-Lösungen die Chance für erhebliche Kostensenkungen, dynamische Verbesserung der Leistung und eine Erhöhung der Skalierbarkeit. Dies nicht zuletzt, weil künftig ein substanzialer Teil der bisher innerhalb des Unternehmens verwalteten Ressourcen extern betrieben werden soll.

Oftmals zeigt sich, dass Kunden die anvisierten Cloudprojekte mit den bereits bekannten, klassischen Outsourcing Ansätzen angehen. Obwohl es Parallelen gibt, müssen bei cloudbasierten Auslagerungsvorhaben aber einige grundlegende Aspekte besonders berücksichtigt werden.

Da Cloud-Computing auf eine grosse Skalierung (Hyperscale) setzt, sind viele Aspekte standardisiert geregelt. Es ist deshalb wichtig, dass sich Kunden vorab mit den Regelungen in den Verträgen vertraut machen und allfällige Unklarheiten oder Bedenken im offenen Austausch klären.

In der Praxis zeigt sich, dass die Evaluation einer Cloud-Plattform eine gute Möglichkeit bietet, insbesondere Fragen der Datensicherheit zu überdenken. Die traditionelle Perimeter-Verteidigung ist überholt, und die Firmen sind gefordert, eine deutlich heterogene Angriffsfläche gegen kriminelle Gruppen oder gar staatlich geförderte Cyberspionage zu schützen.

Es ist deshalb von zentraler Bedeutung, dass Unternehmen die Chancen und Risiken der Cloud ganzheitlich identifizieren und umfassend bewerten. Dies erfordert einen formalisierten Ansatz zum Verständnis und zur Adressierung von Risiken einer Cloud-basierten Betriebsumgebung. Die Erfahrung zeigt, nichts tun stellt ein deutlich höheres Risiko dar und zieht oft hohe Kosten nach sich.

Auch bei geteilten Zuständigkeiten bleibt die Kontrolle beim Kunden

Cloud-Lösungen können als Infrastructure as a Service (IaaS), Platform as a Service (PaaS) oder als Software as a Service (SaaS) realisiert werden. Abhängig vom gewählten Cloud Service-Modell verschiebt sich der Zuständigkeitsbereich zwischen dem Cloud-Serviceprovider und dem Kunden. Je stärker der Serviceanteil einer Lösung ist, desto mehr Verantwortungen können an den Cloud-Provider delegiert werden. Es ist aber zu beachten, dass die Verantwortung immer zwischen beiden Parteien aufgeteilt bleibt (geteilte Zuständigkeit) und auch bei SaaS Lösungen (z.B. Microsoft 365 oder Dynamics 365) ein Teil der Kontrollen beim Kunden verbleibt.



Abbildung 4 – Geteilte Zuständigkeiten

Die Erfolgsfaktoren für ein Cloud Projekt

Damit ein Cloud-Projekt erfolgreich umgesetzt werden kann, sind die folgenden Elemente von zentraler Bedeutung:

- **Entscheidungsprozess** mit eindeutig definiertem Ablauf und klar zugewiesenen Personen aus der obersten Managementstufe
- **Dedizierter Sponsor** aus der obersten Managementstufe, welcher in der Lage ist, aufgrund vorliegender Risiken verbindliche Entscheide zu fällen und die Prozesse voranzutreiben
- **Interdisziplinäres Team**, welches sich holistisch um alle Themen der Einführung von Clouddiensten kümmert. Diesem Team sollen Vertreter aus Business Management, User, System- und Data Owners, IT, IT Security, Legal, Risk & Compliance, Data Protection- sowie Procurement angehören. Das Team muss gemeinsam die für das konkrete Projekt anstehenden Risiken beurteilen und Lösungen vorschlagen, welche dann vom Management abgenommen werden

Diese Bausteine sind für den erfolgreichen Verlauf eines Cloud-Projekts entscheidend. Sind sie nicht vorhanden, kann es im Prozessverlauf zu Missverständnissen, fehlender Abstimmung und kostspieligen Verzögerungen kommen. Besonders wichtig ist, dass eine klare Sicht auf die angestrebten Zielvorgaben gewährleistet ist.

Interne Stakeholder

Ein Cloud-Projekt involviert unterschiedliche Interessengruppen. Deshalb müssen die entsprechenden Funktionen frühzeitig identifiziert und ein einheitliches Verständnis über deren Aufgaben formuliert werden. Im Folgenden sind einige der Rollen beschrieben, wobei diese – je nach Organisation und Projekt – variieren können:

Provider Management

- Definition von Rollen und Verantwortlichkeiten im Zusammenhang mit den verschiedenen Aufgaben, die es in der Interaktion mit dem Cloud-Provider zu erledigen gilt
- Überwachung der Services des Cloud-Providers (SLA Monitoring)
- Operatives Management des Vertrags

Legal & Compliance

- Vertragsgestaltung
- Management des Datenschutzes
- Integration in das Risk Management und in das firmeninterne Control Framework sowie in das Compliance Monitoring und in das Compliance Reporting

Interne IT

- Vorbereitung der Applikationen für den Cloud Betrieb (z.B. Containerization, Anpassung an das Betriebssystem, etc.)
- Integration der Cloud ins eigene IT-Service Management (Helpdesk, Incident-, Problem-, Change- und Release-Management) und Anpassung der herkömmlichen Prozesse an die neu in der Cloud erforderlichen DevOps Prozesse
- Technisches Life Cycle Management der in der Cloud laufenden Funktionen
- Management der Schnittstelle zur eigenen IT, welche mit den Cloud-Systemen arbeitet
- Cloud-Anbindung mittels eines geeigneten, möglichst redundanten Netzwerks
- Aufbau und regelmässiges Testen der Business Continuity und Disaster Recovery Massnahmen in Zusammenarbeit mit dem CISO

CISO

- Design eines «End to End» IT-Security Konzeptes mit Einbezug des Cloud-Anbieters
- Definieren der Cloud Security Features
- Definition und Aufbau des operativen IT Security Managements unter Einbezug aller Komponenten (Cloud und on-premise)
- Integration in ein vorhandenes Identity & Access Management
- Analyse und Klärung von potentiellen Sicherheitslücken beim Parallelbetrieb von Lösungen bei der Transition oder im operativen Betrieb z.B. einer Hybrid Cloud
- Spezifikation des Business Continuity und Disaster Recovery Designs
- Überprüfung von Business Continuity und Disaster Recovery Tests
- Regelmässige Überprüfung und Nachführung der IT-Sicherheit

Business Applikationsverantwortliche

- Spezifikation der funktionalen Anforderungen
- Mitwirkung bei der Ideensammlung und Neugestaltung von Prozessen oder beim Aufbau neuer, durch Cloud-Computing möglich gewordener Services
- Spezifikation der erforderlichen Service Levels
- Feedback bezüglich der Zufriedenheit und SLA Einhaltung (z.B. melden von Ausfällen)

CFO

- Berechnen von Cloud Business Cases
- Festlegung von Budgetvorgaben und Budgetverantwortlichen für Cloud-Services
- Controlling der Cloud-Kosten in Zusammenarbeit mit dem Business und Einkauf
- Überprüfung der Business Cases

Verwaltungsrat/CEO

- Strategische Integration von Cloud Computing als mögliches Element zur Umsetzung oder Erweiterung der Unternehmensstrategie
- Initiierung und Durchsetzung von verbesserten oder neuen Geschäftsprozessen, welche mittels Cloud-Technologie erreicht werden sollen
- Vorgaben an die Evaluationskriterien und Festlegung der umzusetzenden Cloud-basierten Projekte
- Sicherstellung der Ressourcen und Innovationsbudgets
- Wo notwendig: Fällen von risikobasierten Entscheidungen bezüglich Risiken der Cloud oder der Transition
- Etablieren von Kontrollen über die laufenden Cloud-Programme

Microsoft Assurance Framework

Damit die Risiken eines Cloudprojektes adressiert und ein effektives Kontrollsysteum aufgebaut werden können, muss ein gutes Verständnis der geltenden Vertragskonditionen, technischen und organisatorischen Massnahmen, Zertifizierungen sowie Auditberichte der Microsoft Cloud-Services vorhanden sein. Hierzu bietet das «Microsoft Assurance Framework» einen strukturierten Überblick. Dieses kann gleichzeitig als Orientierungshilfe darüber verstanden werden, wie eine Risikoabschätzung orchestriert werden kann und was es zu beachten gilt.

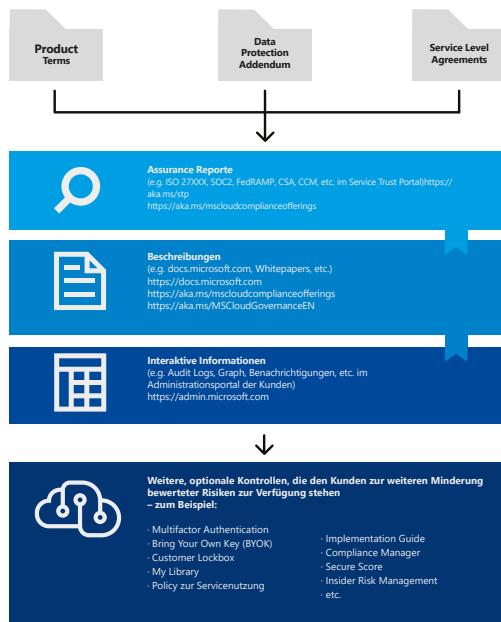


Abbildung 5 – Microsoft Assurance Framework

1. Die oberste Ebene des Microsoft Assurance Frameworks bilden die vertraglichen Vereinbarungen. Dazu gehören die Product Terms, die Datenverarbeitungsvereinbarung für Microsoft Cloud-Services («Data Protection Addendum») und die Cloud-Service Level Agreements. Diese Dokumente regeln wichtige Themen wie den Ort der Datenverarbeitung, den Speicherort, die Zugriffs- und Zugangsbestimmungen sowie die Zusammenarbeit mit Unterauftragsnehmern oder die Datenlöschung. Sie stellen gleichzeitig die Instruktionen des Auftraggebers an Microsoft dar.

2. Die Ebene «Assurance Reports» dient zur Überprüfung, wie Microsoft die vertraglichen Zusicherungen in organisatorische und technische Kontrollen übersetzt. Die Berichte, welche von unabhängigen Drittparteien erstellt werden, bestätigen gleichzeitig die Effektivität der relevanten Kontrollen. Über das Portal <https://servicetrust.microsoft.com> stehen die unredigierten Prüfberichte der unabhängigen Auditoren, Standard Compliance-Zertifikate, Security Optimization

Assessment (SOA) zur Verfügung.

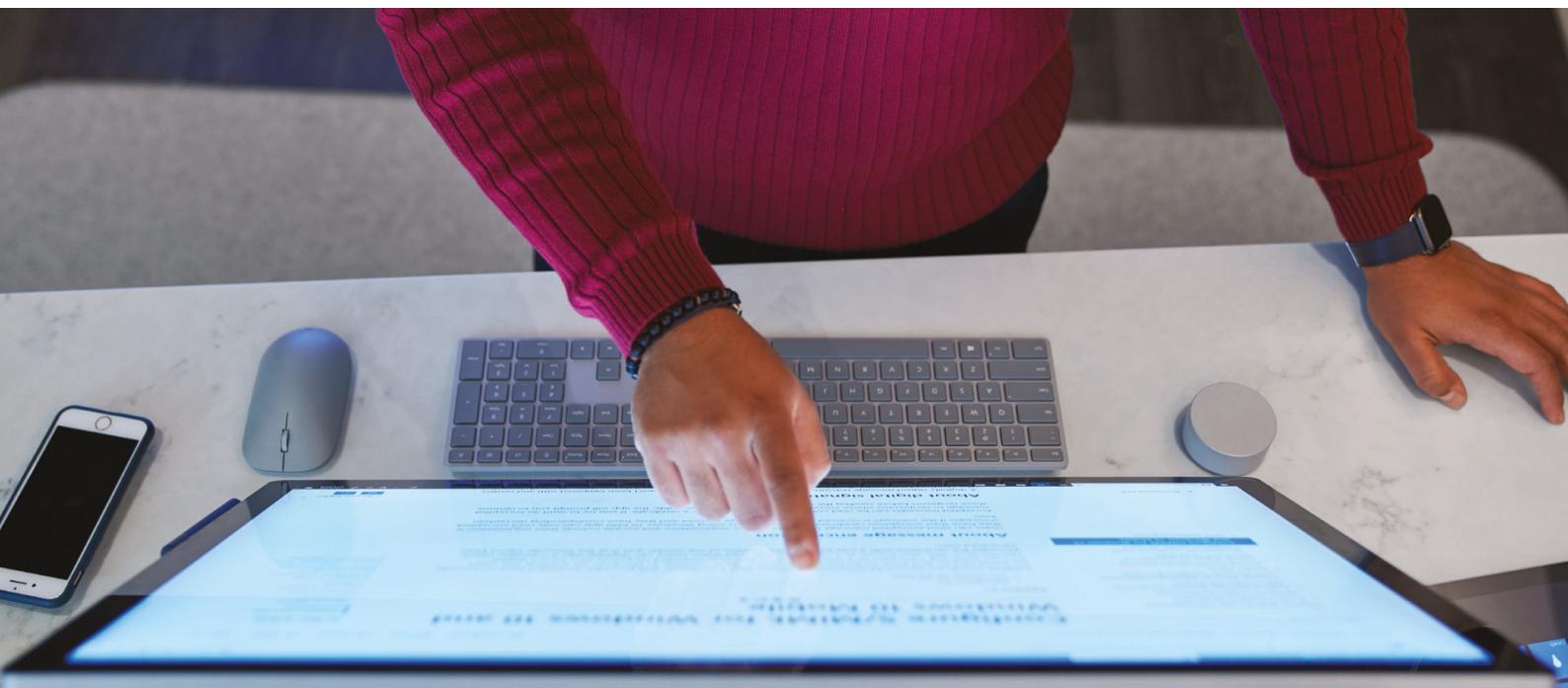
3. Das dritte Element bilden die unterschiedlichen Dokumentationen und Leitfäden. Darunter fallen umfassende Beschreibungen bestimmter Funktionen, Features, Prozesse und dergleichen. Das Spektrum reicht dabei von allgemeinen Whitepapers bis zu detaillierten technischen Dokumentationen.
4. Der Bereich «Interaktive Information» schliesslich stellt dem Kunden fortlaufende Dokumentationen und Informationen zu Microsoft Cloud-Services zur Verfügung. Der Zugriff erfolgt über das individuelle Cloud-Service Management-Portal.

Für alle vier Stufen des Assurance Frameworks gibt es eine Vielzahl von zusätzlichen Funktionen, Diensten und Prozessen, welche die Kunden individuell implementieren können. Mit Hilfe dieser zusätzlichen Kontrollen können identifizierte Risiken weiter abgemildert werden. Die obige Grafik zeigt einige der meistgenutzten Kontrollen in der untersten Box.

Das Microsoft Assurance Framework spielt eine kritische Rolle bei der Etablierung des Government Prozesses.

Datentypen

Die Microsoft Cloud-Verträge beinhalten eine Reihe von Definitionen zu Datentypen, die es zu verstehen gilt, wenn Daten in der Cloud gespeichert werden. Die Definitionen zu den Datenkategorien sind im Kapitel «Definitionen» des Microsoft Products and Services Data Protection Addendum aufgeführt.



4 DER RISIKOBEURTEILUNGSPROZESS

Häufig wird Risiko als etwas wahrgenommen, das es zu eliminieren gilt, da sich Risiko in seiner Definition auf die Wahrscheinlichkeit eines negativen Ergebnisses bezieht. Das Eingehen «kontrollierbarer» Risiken ist jedoch für das Wachstum einer Organisation von grundlegender Bedeutung. Wenn eine Organisation einen ausgewogenen, risikobasierten Ansatz verfolgt, kann ein Gleichgewicht zwischen den Chancen einer bestimmten Aktivität und deren Risiken mittels eines richtigen Masses an Risikomanagement gefunden werden. Der sogenannte risikobasierte Ansatz ist auch als grundlegendes Prinzip in relevanten Rahmenbedingungen enthalten, wie zum Beispiel in der Datenschutzgrundverordnung der EU. Zudem hat die Europäische Kommission bei den neuen Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer (sog. SCC, für «Standard Contractual Clauses») im Juni 2021 ebenfalls einen risikobasierten Ansatz gewählt. Eine akkurate Risikobeurteilung und saubere Dokumentation seitens Kunde sind also entscheidende Faktoren.

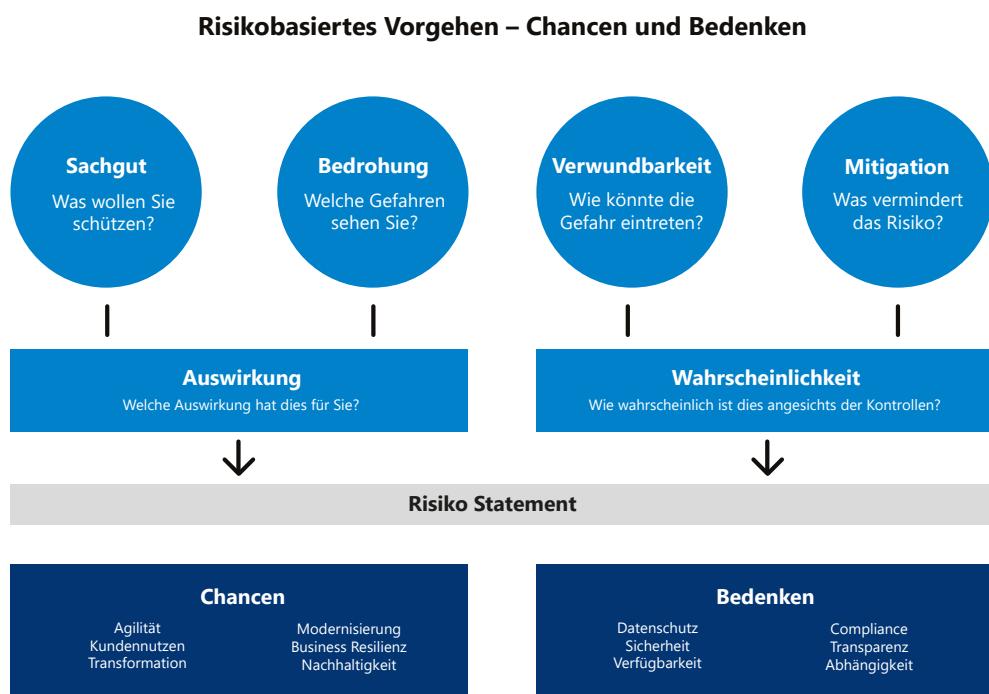


Abbildung 6 – Beurteilung und Bewertung der Risiken

Jede Datenverarbeitung birgt Risiken, unabhängig von der Architektur, dem Bereitstellungsmodell usw. Das Ziel einer entsprechenden Risikobewertung ist es daher nicht, Risiken zu eliminieren, sondern die Risiken zu bewerten, zu minimieren und fortlaufend zu verwalten. Ein solides Risikomanagement unterstützt die Interessen des Unternehmens / der Organisation sowie der Endkunden. Insbesondere was die Cloud betrifft, werden die meisten Organisationen durch kontinuierliche Risikobewertungen stete Verbesserungen in ihrem Risikomanagement sehen. Dies insbesondere, wenn sie aktuelle On-Premise-Lösungen mit Hyperscale-Lösungen vergleichen. Es ist also entscheidend, nicht nur den potentiellen Cloud Einsatz zu bewerten, sondern auch den Vergleich zur jetzigen Situation in die Gesamtbetrachtung einzubeziehen.

Der ISO 31000 Risikomanagement Standard

Die Integration des Risikomanagements in die Organisation und über deren Cloud-Provider hinweg ist ein dynamischer Prozess, der fortlaufend an die Ziele und Abläufe des Unternehmens angepasst werden muss. Der Risikobeurteilungsprozess nach ISO 31000 erfolgt über die in der folgenden Darstellung gezeigten sechs Stufen.

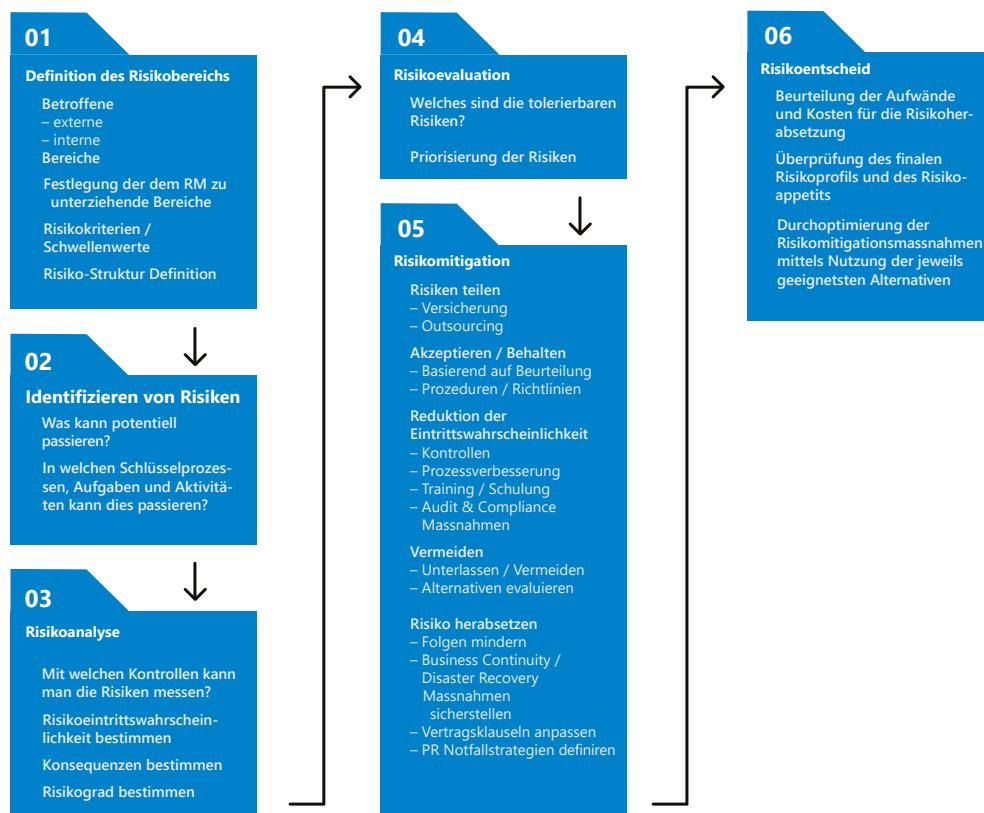


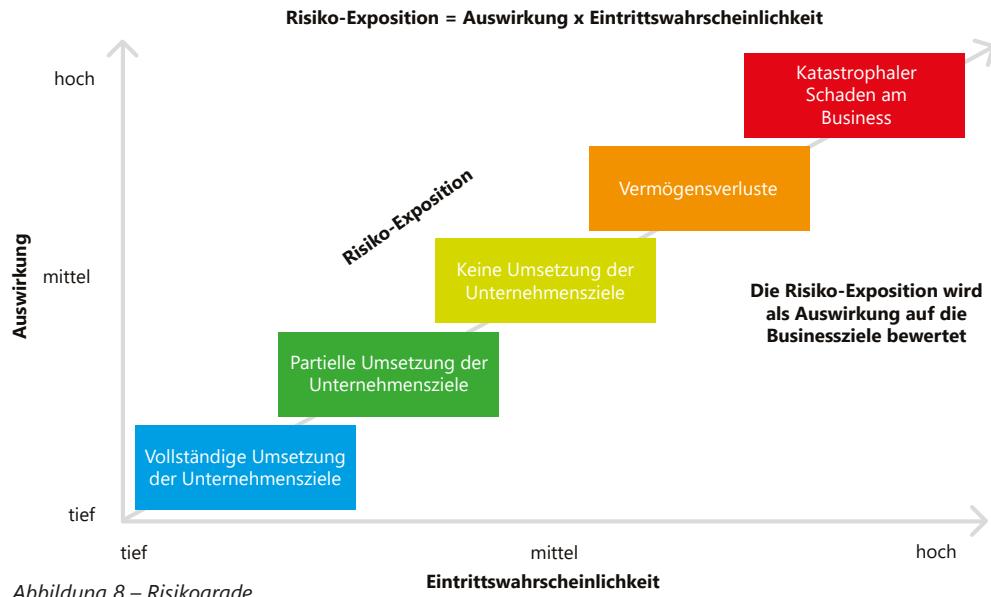
Abbildung 7 – 6 Stufen des Risikomanagement Prozesses nach ISO Norm 31000

Zur Risikobeurteilung wird in diesem Kapitel unter anderem auf die ISO Norm 31000:2018 «Risikomanagement» abgestützt. Die Norm unterstützt die Entwicklung einer Risikomanagementstrategie und einer Risikomanagementkultur, mittels derer Risiken rasch und effektiv identifiziert werden. Durch geeignete technische, organisatorische und/oder juristische Massnahmen können diese abgeschwächt werden. Damit erhöht sich die Wahrscheinlichkeit, dass eine Organisation ihre Ziele erreicht und ihre Vermögenswerte schützen kann.

Nachfolgend werden lediglich diejenigen Elemente der Norm verwendet, welche für Cloud-Computing wesentlich sind.

Was ist ein «Risiko»?

Ein Risiko ist definiert als «Auswirkung von Unsicherheit auf Ziele». Eine Auswirkung stellt dabei eine Abweichung entweder in positiver, negativer oder auch in beide Richtungen dar. Das Risiko wird anhand der Risikoursache, der potenziellen Ereignisse, ihrer Auswirkungen und ihrer Wahrscheinlichkeit dargestellt.



Definition des Risikobereichs

In dieser ersten Phase geht es um die Eingrenzung des Bereichs, innerhalb dessen man die Risikobeurteilung vornehmen möchte. Hierbei soll bestimmt werden, welche IT-Systeme und Funktionalitäten vom Projekt betroffen sind. Als externen Kontext gilt es zu definieren, welche regulatorischen Vorgaben relevant sind. Der interne Kontext wiederum gibt vor, welche firmenbezogenen Regelwerke zu beachten sind und wie in der Organisation mit den angegangenen Themen (z.B. Innovation, Einführung neuer Technologien) umgegangen werden soll. Zudem gilt es die Stakeholder des Projekts zu definieren und aktiv miteinzubeziehen.

Identifizieren von Risiken

Um den Prozess der Risikozuordnung zu beschleunigen, enthält dieses Dokument eine Vorlage möglicher auftretender Geschäftsrisiken, die mit typischen Cloud Vorhaben einhergehen können. Die statuierten Risiken richten sich weitgehend nach der «Cloud Security Alliance» und deren «Cloud Controls Matrix 2». Einige Risiken sind spezifisch für bestimmte Branchen. Diese sind möglicherweise nicht in dieser Vorlage enthalten und müssten der zu verwendenden Risikoliste zugefügt werden.

Risiko-Art	Risiken
Compliance Risiken	Inadäquater Aufbau der Governance und des Risikomanagements für eine Cloud-Nutzung Unsichere Situation bez. der Compliance mit bestehenden, regulatorischen Anforderungen nach Verlagerung in die Cloud (z.B. FINMA Rundschreiben, besonders schützenswerte Personendaten, Exportkontrollen, etc.) Offene rechtliche Fragen: Verträge mit Cloud Providern, Profiling oder kritische Datenregister, Beendigung von bestehenden Verträgen mit bisherigen Partnern und Lieferanten Nicht geregelte / Mangelhafte Incident Response Kapazität Mangelnde Transparenz bez. gespeicherter Daten in den verschiedenen Jurisdiktionen Für Clouds nicht vorhandenes Compliance und Audit-Management Datenschutz-Risiken aufgrund länderspezifischer Vorgaben Bereinigung, Haltung, Archivierung und Löschung sensibler Daten Nicht-Verfügbarkeit von Audits oder Zertifizierungen beim Cloud Provider und dessen Unterakkordanten Fehlende / ungeeignete Compliance Controls für die Cloud

Strategische Risiken	Fehlende(s) /Mangelhafte(s) Informationsmanagement / Datensicherheit Interoperabilität und Portabilität Auswahl ungeeigneter Anbieter Fehlende Bereitschaft der Organisation Fehlende Anbieter-Redundanz Lock-in Fehlende / unvollständige Datenklassifizierung Datenmigration von On-Premise in die Cloud (Public, Private oder Hybrid)
Migrations-Risiken	Fehlende Ausbildung und Fähigkeiten der Mitarbeiter Fehlende Datentransfersicherheit in die Cloud - Sicherstellung des vollständigen Datenbestands am Zielort Systemausfälle bei gescheitertem Onboarding Interferenzen beim Parallelbetrieb von Systemen On-Premise und in der Cloud während der Transition Fehlende Fallback Lösungen bei Scheitern der Transition Fehlende IT Security während der Projektphase Fehlendes Nachführen bislang gehaltener Zertifikate wie z.B. ISO 27001, ISO 9001. Fehlende Zusammenarbeit mit dem Auditor für die Transition. Fehlende Audit Statements oder rote Audit Statements nach der Betriebsübergabe.
Operationelle Risiken	Fehlende Anpassung des Rechenzentrumsbetriebs sowie fehlende Integration der Cloud Services in die Operations. Insbesondere fehlende Anpassung des IT Service Managements und hierbei Regeln des Miteinanders der klassischen ITIL Prozesse im eigenen Data Center und der DevOps-Prozesse für die Cloud Datenhaltung und Interferenzen beim Zusammenspiel von Systemen On-Premise und in der Cloud und mangelhafte Integration in bestehende Geschäftslösungen Fehlende Ausbildung der Mitarbeitenden im Cloud Betrieb Ausfall von Logging & Tracing Kapazitäten Fehlendes «end to end» Security Konzept und Ausfall des IT-Schutzdispositives Backup-Ausfall Mangelhaftes Informationsmanagement und dadurch mangelhafte Datensicherheit mit Datenverlust und in der Folge Verletzung des Datenschutzes Ungeeignete interne Betriebsabläufe Mutwillige oder ungewollt schädliche Mitarbeiteraktivitäten Fehlendes Management der Betriebsabläufe Zwangsverfügungen der Behörden inklusive sog. «Fishing»- Aktionen um mittels e-Discovery Zugang auf Firmen- und Kundeninformationen in der Cloud zu kriegen Unbefugter Zugang zu Räumlichkeiten Diebstahl von IT-Ausrüstung Fehlende Endpoint Security auf Endgeräten (Laptops, PCs, Smartphones, etc.) von denen aus der Cloud-Dienst in Anspruch genommen wird. Limitierte HR Ressourcen Naturkatastrophen Lizenzierungs-Risiken Cyber Attacken mit Datenverlust mangels Anpassung der vorherigen Cybersicherheits-, Business Continuity und Disaster Recovery Kapazitäten Reputationsverlust Kündigung oder Ausfall von Diensten
Marktrisiken / finanzielle Risiken	Beschlagnahmung von Daten oder Systemen durch die Behörden Fehlendes Kapazitätsmanagement Fehlende Agilität der Betriebsumgebung und damit ungenügende «Time to Market» Falsche oder zu träge Reaktion auf Vorfälle

Abbildung 9 – Liste potentieller Risiken bei Cloud Migration und Betrieb

Risikoanalyse vornehmen

Aufgrund der Liste potentieller Risiken ist nun festzuhalten, welche von diesen bei der konkreten strategischen Initiative berücksichtigt werden müssen. Das interdisziplinäre Team hat jetzt die Aufgabe, die Risiken eines Vorhabens sequentiell und in ihrem Zusammenwirken zu bewerten.

Wichtig dabei ist die Definition, wie Risiken gemessen werden. Ein Risiko soll gemäss seiner Kritikalität auf einer Skala positioniert und anderen Risiken gegenübergestellt werden. Später soll eine Kontrolle erkennen, ob sich ein Risiko über die Zeit auf der Skala bewegt hat.

Auswirkungen eines Ereignisses

Kategorie	Ereignisfolgen	Auswirkung			
		Dauer	Operative Reichweite	Reputationsverlust	Rechtliche- und Compliance-Folgen
Katastrophal	Sehr schwere bis vollständige Vernichtung von Vermögenswerten oder schwere Reputationsschädigung, nach aussen hin breit sichtbar und mit substantiellen Auswirkungen auf den Betrieb und das Vertrauen in der Öffentlichkeit, insbesondere dasjenige der Kunden und Geschäftspartner. Massive Kosten zur Bereinigung des Schadens und dessen Folgen sowie Ausfälle oder massive Minderungen der Aufträge und in der Folge der Umsätze und Gewinne.				
Gravierend	Schwerwiegender, aber nicht vollständige Schädigung des Vermögens oder der Reputation. Nach aussen hin zum Teil gut sichtbar und den Betrieb und das Vertrauen der Öffentlichkeit, der Kunden und Geschäftspartner beeinträchtigend. Erhebliche Kosten zur Bereinigung des Schadens und dessen Folgen sowie mehrere Ausfälle oder wesentliche Minderungen der Aufträge und in der Folge eine wesentliche Minderung der Umsätze und Gewinne.				
Schwer	Mässiger Schaden oder Verlust, z. B. beeinträchtigt den internen Betrieb, verursacht eine Erhöhung der Betriebskosten oder eine Verringerung der Betriebsleistung. Spürbare Auswirkung auf die Produktivität und die Kosten zur Bereinigung des Schadens und dessen Folgen. Die Auswirkung auf das Betriebsergebnis sind teilweise sichtbar, aber gut verdaubar.				
Mässig	Geringe Schäden oder Verluste, z. B. Auswirkungen auf interne Abläufe. Der Kostenanstieg ist nicht messbar. Keine messbaren Auswirkungen, geringer Anstieg der Support- oder Infrastruktukrkosten.				
Gering	Geringfügige oder keine Änderung im operativen Geschäft. Wird durch den normalen Geschäftsbetrieb absorbiert. Keine messbaren Auswirkungen auf Supportkosten, Produktivität oder geschäftliche Verpflichtungen.				

Abbildung 10 – Risiko-Auswirkung - Tabelle zur Beurteilung

Eintrittswahrscheinlichkeit eines Ereignisses

Kategorie	Erwägung	Eintrittswahrscheinlichkeit	Häufigkeit
Erwartet	Es ist praktisch sicher, dass dieses Risikoereignis oder der Sachverhalt eintritt oder es ist effektiv in den letzten 6 Monaten bereits eingetreten	90–100%	Ca. alle 3 Mt
Sehr wahrscheinlich	Es ist sehr wahrscheinlich, dass das Risikoereignis 70–90% oder der Sachverhalt eintreten		Jährlich
Wahrscheinlich	Es ist wahrscheinlicher, dass das Risikoereignis oder der Sachverhalt eintreten als nicht	50–70%	Alle 2-3 Jahre
Wenig wahrscheinlich	Es ist möglich, dass das Risikoereignis oder der Sachverhalt eintreten	10–50%	Alle 4-6 Jahre
Unwahrscheinlich	Dass das Risikoereignis oder der Sachverhalt eintreten, ist nur sehr im Entfernten denkbar	<10%	Alle 7 Jahre und mehr

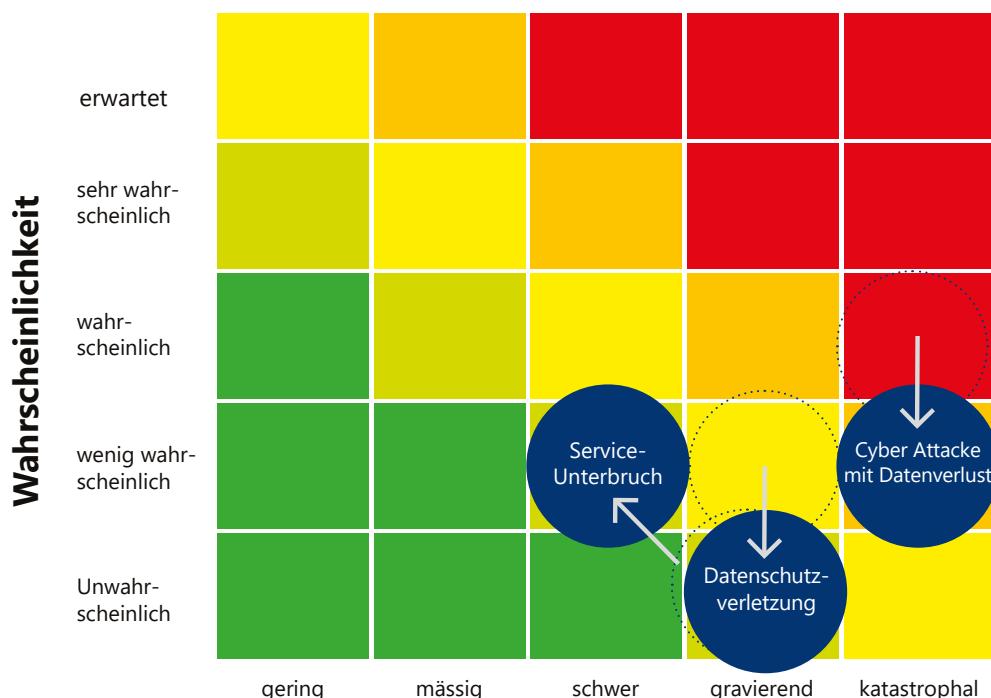
Abbildung 11 – Eintrittswahrscheinlichkeit von Risiken: Tabelle zur Beurteilung

Risikoevaluation

Die eruierten Risiken müssen nun nach den beiden Dimensionen beurteilt und die Ergebnisse in der Risikomatrix eingesetzt werden. Damit ergibt sich in einer einfachen Übersicht die Kritikalität und daraus abgeleitet die Priorisierung der Risiken. Wie eingangs erwähnt, ist ein Null-Risiko Ansatz nicht das Ziel. Restrisiken werden fast immer vorhanden sein und sollten bewusst akzeptiert, verwaltet und für zukünftige Änderungen überwacht werden.

In der Praxis zeigt sich häufig, dass eine erste Cloud-Risikobeurteilung im Verlauf der internen Abstimmungen angepasst wird – insbesondere falls der Vergleich gemacht wird mit bestehenden On-Premise Lösungen, welche selbstverständlich auch Risiken ausgesetzt sind z.B. in den Bereichen Cyber-Security oder Service-Unterbruch.

Bei der Festlegung und der Beurteilung der Risiken sollten die Risiken sinnvoll gruppiert werden. Es sollten nicht zu viele kleine Einzelrisiken festgelegt werden.



Auswirkung

Abbildung 12 – Beispiel einer Risikobeurteilungsmatrix

Risikomitigation: Wie können Risiken eingedämmt werden?

Um das Gesamtrisiko zu reduzieren, können Massnahmen ergriffen werden, die entweder einen oder beide Faktoren betreffend Auswirkung und Wahrscheinlichkeit senken. Zum Beispiel kann ein identifiziertes Risiko, dass personenbezogene Daten durch den physischen Verlust des digitalen Geräts eines Mitarbeiters in die Hände eines unerwünschten Dritten fallen, sowohl in der Wahrscheinlichkeit als auch in der Auswirkung von 3 bis 5 auf 2-3 gesenkt werden, wenn zusätzliche Massnahmen wie ein starker Passwortschutz, Multifaktor-Authentifizierung oder Ähnliches implementiert werden. Und durch eine vollständige Geräteverschlüsselung sowie die Möglichkeit zur Fernlöschung eines Geräts, könnten beide Faktoren auf einen Wert von 1 herabgesetzt werden. Dadurch kommt das Risiko auf den niedrigsten Punkt und somit in den häufigsten Fällen auf ein akzeptables Niveau. Welche dieser Massnahmen für eine bestimmte Organisation angemessen sind und im Verhältnis zum tatsächlichen Risiko stehen, hängt von der jeweiligen Risikobewertung der Daten, der anwendbaren Szenarien usw. ab. Jede Datenverantwortliche und jeder Datenverantwortliche ist letztlich für die Durchführung der Bewertung und Dokumentation der Angemessenheit und Akzeptanz des Restrisikos verantwortlich.

Prinzipien der Risikomitigation

Know-how Aufbau

Eine effektive Risikobewertung setzt gute Kenntnisse der bisherigen und neuen Risiken voraus und muss mit einem interdisziplinären Team ausgearbeitet und permanent überprüft werden. Das Team muss die entsprechenden Kompetenzen mitbringen und sich gegenseitig verstehen, was angesichts der Breite der Materie eine Herausforderung sein kann.

Als erstes empfiehlt sich eine Schulung zu den Themen, was das Betriebsmodell einer Cloud ausmacht und wie es sich vom bekannten Outsourcing unterscheidet, was es mit den Daten und dem Datenschutz auf sich hat und wie die Compliance funktionieren muss, damit die Risiken unter Kontrolle gebracht werden können.

Versachlichung der Risiken

Im interdisziplinären Team, welches die Risiken evaluiert, werden zum gleichen Risiko häufig mehrere Sichtweisen und Meinungen vorgebracht. Dies ist normal und notwendig, denn je nach Bereich kann etwas anderes wichtig sein und jeder der Beteiligten ist in seiner Rolle z.B. als Benutzer, Datenschützer, Unternehmensjurist oder CISO dazu angehalten, sein Fachgebiet zu vertreten.

Kompromisse suchen

Die Lösung ist deshalb nicht immer ein Konsens, sondern oft ein Kompromiss zwischen den Involvierten. Dies muss bei Start allen klar sein. Der Risikobeurteilungsprozess sollte darum sorgfältig orchestriert und eventuell mit externer Hilfe kompetent begleitet werden. Ansonsten kann die Diskussion ins Stocken kommen, sich im Endlosen drehen und damit umsonst massiven Aufwand generieren. Bei einem Dissens im Team werden risikobasierte Entscheide benötigt, welche nur vom Management vorgenommen werden können. Das Management muss sich dessen bewusst sein und entsprechend einbringen. Bei einer Cloud-Transformation handelt es sich unter dem Strich um ein Change- Management-Projekt, welches entsprechend orchestriert werden sollte.

Fakten Check

Die Versachlichung der Risiken ist für die Diskussion das Allerwichtigste, denn es existiert viel Halbwissen was Cloud-Risiken betrifft. Dabei erleichtert die Geschwindigkeit der technischen Entwicklung die Versachlichung der Diskussion nicht immer, nicht zuletzt, weil einige der in der Vergangenheit oft aufgebrachten Befürchtungen durchaus ihre Berechtigung hatten. Dank der technischen Entwicklung wurden diese aber komplett bereinigt und bestehen nicht mehr.

Eine entscheidende Frage kann sein: «Ist dieses Risiko ein bestehendes und wenn ja, wie oft ist es in der Vergangenheit effektiv eingetreten?». Im Rahmen der «US CLOUD Act»-Diskussion kann man zum Beispiel fragen: Wie oft hat in den letzten Jahren das US-Amerikanische Department of Justice im Zusammenhang mit einer strafrechtlichen Verfolgung die Herausgabe von Personendaten vom angestrebten Cloud-Provider oder vom Kunden selbst eingefordert? Durch die so versachlichte Betrachtung der konkreten Fälle wird transparent, wie viel Risiko effektiv in einem bestimmten Bereich besteht.

Vergleich von Heute mit der Zukunft

Wie erwähnt gibt es keine IT ganz ohne Risiken. Eine derzeitige «On-Premise-Lösung» hat bereits Risiken, welche identisch oder häufig gar grösser als diejenigen der Cloud sind. So ist es beispielsweise fast nicht möglich, im eigenen Unternehmen aus eigener Kraft eine Cyber Security aufzubauen, welche derjenigen einer Cloud auch nur annähernd gleichkommt.

Die Beurteilung des Risikos muss also zwischen dem aktuellen Zustand und der angestrebten Cloud- Lösung abgewogen werden, wobei natürlich immer das Ziel sein soll, dass die Summe der bewerteten Risiken mit der Nutzung der Cloud kleiner wird.

Umfang des Risikomitigationskonzepts

Das oft geforderte Erarbeiten eines holistischen und unternehmensweiten Gesamtkonzepts, welches jede Art von Risiken des Cloud Onboardings mitigt, funktioniert in der Praxis nicht. Die Komplexität der Materie sowie die Dynamik der technischen Entwicklung und Gesetzgebung ist schlicht zu hoch, um in einem einzigen «Konzept für jeden Fall» Platz zu finden.

Häufig ist es deshalb zielführender, aus im Einzelfall gefundenen, guten Lösungen später generelle Regeln festzulegen. So lernt man aus ersten Proof-of-Concepts und Pilotprojekten und sammelt die Erfahrungen für künftige Projekte. Dieses «Bottom-up-Verfahren» ist schneller, effizienter und auch anpassungsfähiger.

Arten von Mitigationsmassnahmen

Juristische Massnahmen

Hierunter versteht man vertragliche Massnahmen, um Cloud-Risiken abzusichern. Dazu gehört ein vertraglicher Rahmen mit dem Cloud-Provider, welcher z.B. die Datenspeicherorte oder Zugriffsmöglichkeiten seitens Cloud-Provider abdeckt. Juristische Massnahmen können auch interne rechtliche Abklärungen beinhalten. So können durch die Organisation zulässige Kontrollen der Mitarbeiter bezüglich missbräuchlicher Datenabflüsse geregelt werden.

Organisatorische Massnahmen

Hierzu gehört z.B. die Festlegung von Rollen und Verantwortlichkeiten, um die Cloud zu betreiben, die Kosten und die SLA-Einhaltung zu kontrollieren, Berechtigungen zu erteilen, die Cloud zu konfigurieren und die Business Continuity im Notfall zu aktivieren und sicherzustellen. Weitere Beispiele sind Weisungen bezüglich den Zugriffsberechtigungen auf Daten in der Cloud oder Weisungen, die vorgeben, welche Daten in der Cloud gespeichert werden dürfen.

Technische Massnahmen

Darunter versteht man z.B. das Verschlüsseln von Daten in der Cloud, die Zweifaktor-Authentisierung der Benutzer oder die Blockierung von fahrlässig oder mutwillig beabsichtigten, die Compliance-Regeln verletzenden Datenexporten zu unerlaubten Empfängern mittels sogenannten «Data Leakage Prevention Tools».

Etablieren von Kontrollen

Allein die Implementierung von Massnahmen genügt für die Risikomitigierung nicht. Die Massnahmen müssen über die Zeit hinweg auch greifen. Hierzu etabliert man Kontrollen und es wird eine entsprechende Governance erstellt.

Kontrollen sind Aktivitäten, die die Wahrscheinlichkeit oder die Auswirkungen eines Risikos reduzieren, falls es sich manifestiert. Kontrollen helfen also, die Risiken weiter zu senken. Eine Kontrolle muss drei Kriterien genügen:

1. Sie muss effektiv sein, also möglichst genau messen, was ein Risiko bestimmt und dieses maximal reduzieren.
2. Sie muss regelmässig in sinnvollen Abständen durchgeführt und dokumentiert werden.
3. Basierend auf dem Kontroll-Ergebnis müssen bei einer Non-Compliance korrigierende Massnahmen erfolgen.

Ein Beispiel für eine Kontrolle ist, ob alle an einer Cloud-Applikation Berechtigten auch tatsächlich noch bei der Firma arbeiten und ob sie aufgrund ihrer aktuellen Rolle noch zugriffsberechtigt sein dürfen. Die Wirksamkeit der Kontrolle kann man damit sicherstellen, indem man aus dem HR System die Liste der aktuell angestellten Mitarbeitenden exportiert und diese mit denjenigen der Zugriffsberechtigten vergleicht. Zudem kann man zusammen mit den Application Owners prüfen, welche Rolle die Mitarbeitenden aktuell haben und ob sie mit der Rolle im Zugriffssystem übereinstimmen. Diese Kontrolle sollte idealerweise in sehr hoher Frequenz (sogar z.B. durch einen Real Time Abgleich von HR und Zugriffsberechtigungsregister) durchgeführt werden, um sicherzustellen, dass ehemalige Mitarbeitende nicht auf das System zugreifen und sich unbemerkt Daten herunterladen können.

Jede Kontrolle wird anschliessend einem Control-Owner zugeteilt, welcher sicherstellen muss, dass die Kontrolle eingehalten und regelmässig geprüft wird. Für das Management und die Sicherstellung, dass die Kontrollen hochgehalten werden, ist die Compliance Funktion zuständig. Wenn Compliance die Kontrolle prüft und es eine Beanstandung gibt, muss aus der Beschreibung der Kontrolle hervorgehen, wo dies zu melden ist und wer sich um die Wiederherstellung des Soll-Zustandes kümmern hat. Weiter können auch interne oder externe Audits eine Kontrolle prüfen.

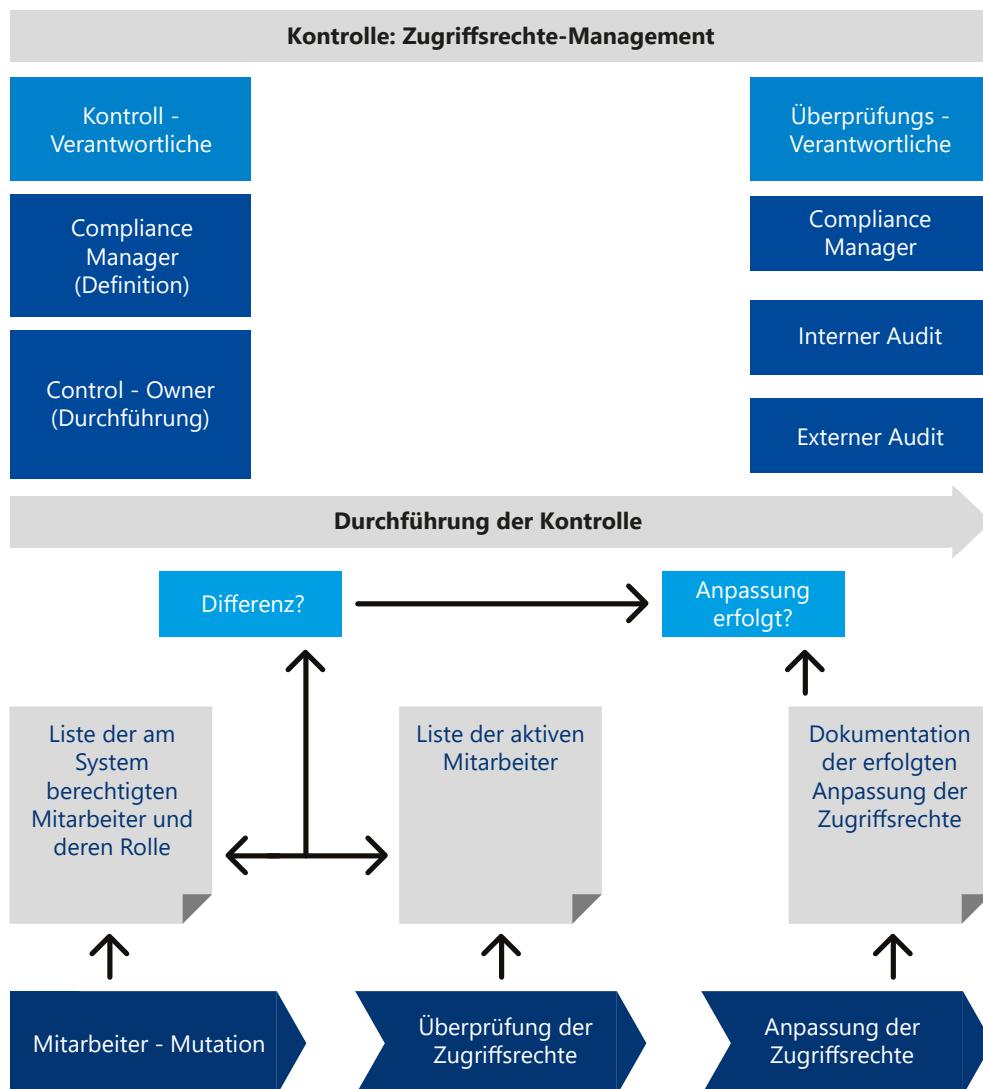


Abbildung 13 – Beispiel einer Kontrolle für das Nutzerberechtigungsmanagement

End to End Compliance mittels Einbindung der Cloud-Provider-Kontrollen

Sinn und Zweck von Compliance ist es, die Vernetzung der eigenen Organisation mit der Cloud entsprechend den regulatorischen Vorgaben sicherzustellen. Entsprechend müssen die internen Kontrollen mit den Kontrollen synchronisiert sein, welche Cloud-seitig vom Cloud-Provider implementiert sind. Damit nicht jeder Cloud-Kunde mit dem Cloud-Provider einzelne Kontrollen definieren und etablieren muss, bieten die meisten Cloud-Provider eine Auswahl von Standardkontrollen an, welche die Unternehmen in ihr eigenes Kontrollsyste einbinden können.

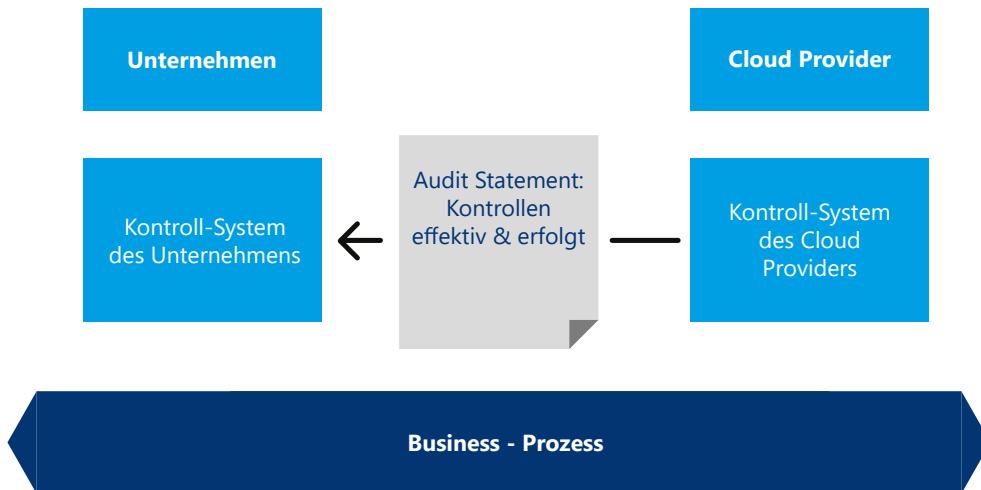


Abbildung 14 – Einbindung der Kontrollen des Cloud Providers

Damit der Cloud-Provider gegenüber den Kunden den Nachweis erbringen kann, dass er alle Kontrollen auch effektiv etabliert, durchführt und einhält, werden externe Auditoren eingesetzt. Diese bestätigen in regelmässigen Audit Statements, dass die Kontrollen ordnungsgemäss und korrekt implementiert und geprüft wurden. Mit diesem Konzept können die Kunden ihrer Sorgfaltspflicht nachkommen und sicherstellen, dass ihr Prozess «end to end» konform ist.

Um Unternehmen und Organisationen bei der Definition der erforderlichen Cloud-Anforderungen zu unterstützen, hat die [«Cloud Security Alliance»](#) ein Set von Kontrollen entwickelt, welche öffentlich bereitgestellt werden und frei verfügbar sind. Microsoft selbst hat hierzu den «Compliance Manager» etabliert, ein Tool, welches drei Arten von Kontrollen etabliert und jeweils deren Status überprüft:

1. Von Microsoft verwaltete und verantwortete Kontrollen
2. Kontrollen des Kunden
3. Gemeinsam genutzte Kontrollen, für deren Implementierung und Durchführung sowohl der Kunde als auch Microsoft gemeinsam verantwortlich sind

Regelung geteilter Zuständigkeiten

Die Verantwortlichkeit für die Compliance kann nicht allein dem Cloud-Provider zugewiesen werden, auch wenn dieser alles tut, um seine Angebote den Compliance Anforderungen regelmässig anzupassen. So kann beispielsweise der Cloud-Provider nicht bestimmen, wer seitens des Kunden auf die Daten Zugriff erhält. Auch kann er nicht dafür verantwortlich gemacht werden, was im Netzwerk des Anbieters passiert, welches zu ihm führt.

Je nach Cloud-Service-Modell (IaaS, PaaS, SaaS) verschiebt sich aber die Verantwortung für die Einhaltung der Compliance und die daraus abgeleiteten Sicherheitskontrollen für einen bestimmten Service zwischen dem Cloud-Provider und den Kunden, wie bereits früher im Dokument darauf eingegangen wurde.

Selbst bei SaaS-Lösungen wie Microsoft 365 und Dynamics 365 verbleibt ein Teil der Verantwortung beim Kunden. Um das geforderte Compliance-Niveau einer Cloud-basierten Lösung sicherzustellen, kann abhängig von der Wahl der Cloud-Servicelizenz aus einer langen Liste von Sicherheits- und Compliance-Funktionen ausgewählt werden.

Die Sicherheits- und Compliance-Verantwortlichen des Kunden müssen das Sicherheitsdispositiv selbst festlegen und die richtigen Optionen für ihr Vorhaben auswählen. Das ermöglicht ihnen, ihre Cloud-Lösung im Kontext ihrer eignen Situation so konfigurieren, dass sie jederzeit die «End-to-End» Kontrolle haben. Der Cloud-Provider seinerseits muss sicherstellen, dass die von ihm bereitgestellten Funktionen die Compliance-Anforderungen des Kunden jederzeit zu erfüllen vermögen.

Cloud Adoption Framework

Microsoft bietet mit dem sogenannten [Cloud Adoption Framework \(CAF\)](#) eine Grundlage für die Reise in die Cloud. Ein Teil des CAF widmet sich dem Thema der Governancekontrolle für materielle Risiken. Die entsprechende Dokumentation mit Vorlagen finden Sie [hier](#).

Der Umgang mit Risiken

Die Entscheidung über den Umgang mit Risiken basiert nicht nur auf der Gesamtbewertung des Risikos, sondern auch auf der Bewertung der Kosten zur Risikoverminderung. Entscheide, wie mit Risiken umzugehen ist, müssen vom Management abgesegnet, schriftlich begründet und langfristig festgehalten werden.

Es gibt vier Optionen für den Umgang mit Risiken:

Risikominderung oder -beseitigung

Mittels Risikominderungsstrategien können die Wahrscheinlichkeiten und die Auswirkungen von Risiken reduziert werden. Zum Beispiel kann man durch redundanten Aufbau des Betriebs das Ausfallrisiko minimieren.

Risiko-Akzeptanz

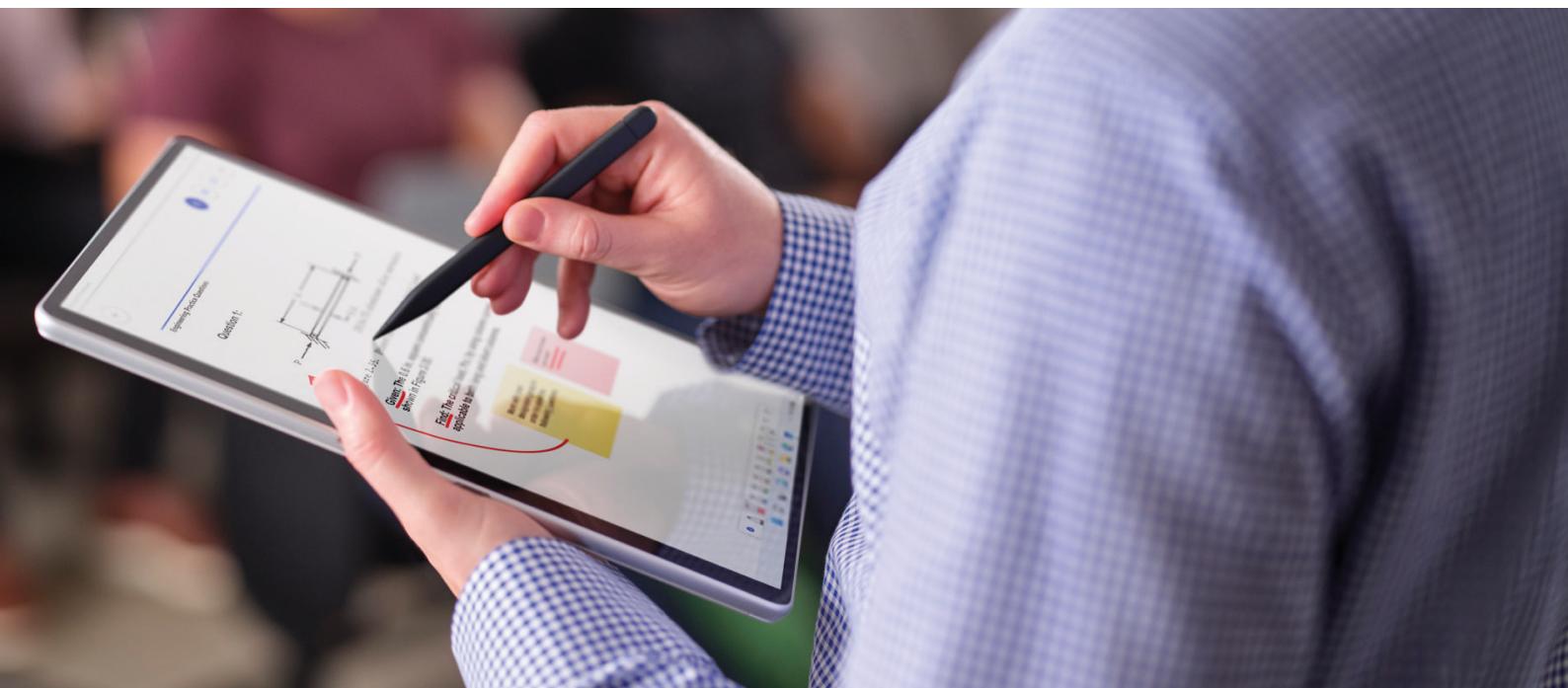
Das Unternehmen kann festlegen, ob es ein durch die Cloud-Lösung hervorgerufenes Risiko tolerieren kann und will. Dies ist abhängig vom sogenannten Risikoappetit der Firma, also der Risikobereitschaft.

Risikovermeidung

Das Unternehmen kann ein Risiko als zu hoch bewerten und sich entscheiden, gewisse Datenarten zumindest momentan nicht in die Cloud zu überführen. Dadurch wird das Risiko vermieden.

Risikoübertragung

Das Unternehmen kann Dritte suchen, welche bereit sind, Teile oder gar die gesamten Risiken zu übernehmen, beispielsweise Versicherungen.



Risikoentscheid

Am Ende dieses Prozesses hat das Team Optionen zur Risikominderung gebildet. Die Optionen zur Risikomitigierung sollten basierend auf den Ergebnissen der Risikobewertung, der erwarteten Kosten für die Mitigierungsmassnahmen (z.B. Kontrollen) und des erwarteten Nutzens beurteilt werden.

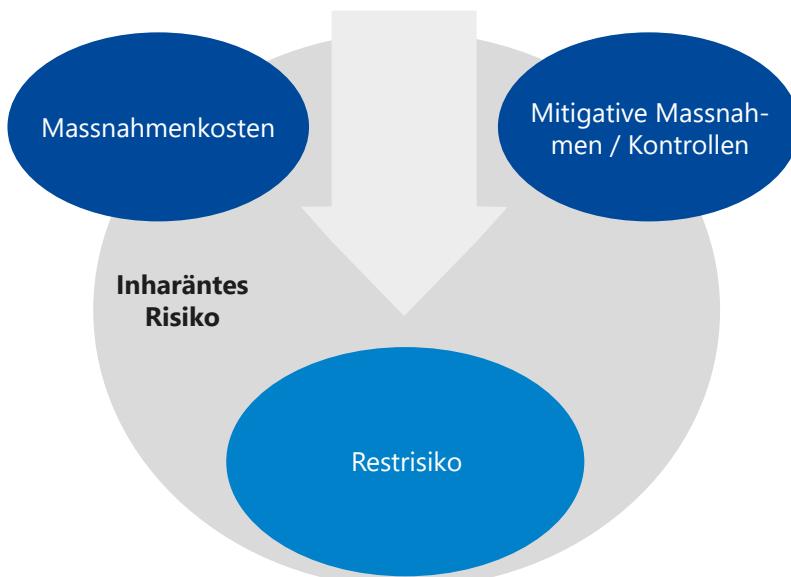


Abbildung 15 – Elemente einer ausgearbeiteten Risiko-Option

Die Wahl des idealen Mix aus technischen, organisatorischen und juristischen Massnahmen, welche das Risiko für den individuellen Risikoappetit des Unternehmens abzufedern vermögen, ergibt das zu etablierende Risikomanagement-Konzept.

Hierbei ist der Fokus darauf zu legen, dass man Innovationen und vernünftige Transformationen ermöglicht und nicht verhindert. Voraussetzung, um den optimalen Cocktail aus den drei Massnahmenbereichen zu finden, ist eine gewisse Flexibilität aller Beteiligten.

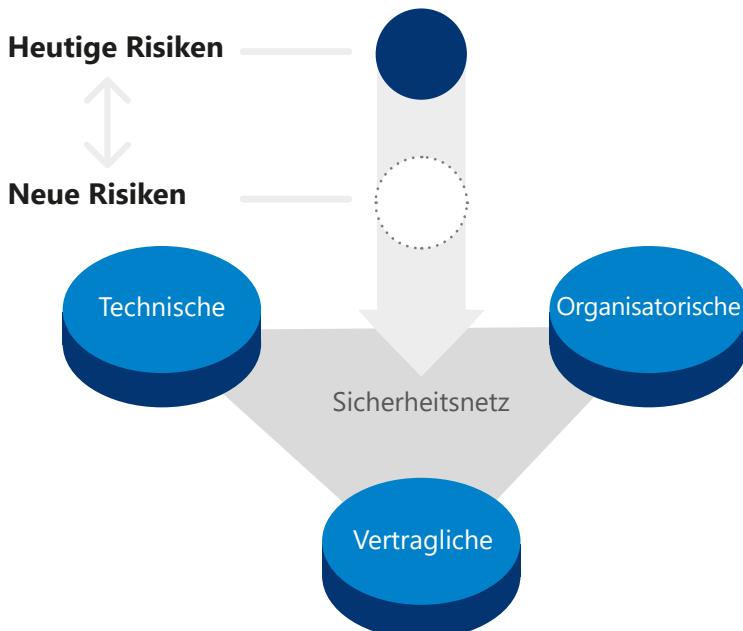


Abbildung 15b – Optimaler Mix aus juristischen, technischen und organisatorischen Massnahmen

Wie das Risikomanagement auch immer formuliert wird, ein Restrisiko bleibt stets bestehen. Dieses Restrisiko muss von der Spalte des Managements akzeptiert oder verworfen werden. Diskussionen zur Formulierung des optimalen Risiko-Mixes können langwierig sein und hängen wesentlich davon ab, wie gut das Team die Risiken aufarbeitet, wie präzis die mitigierende Massnahmen definiert werden und wie entscheidungsfreudig das Management ist.

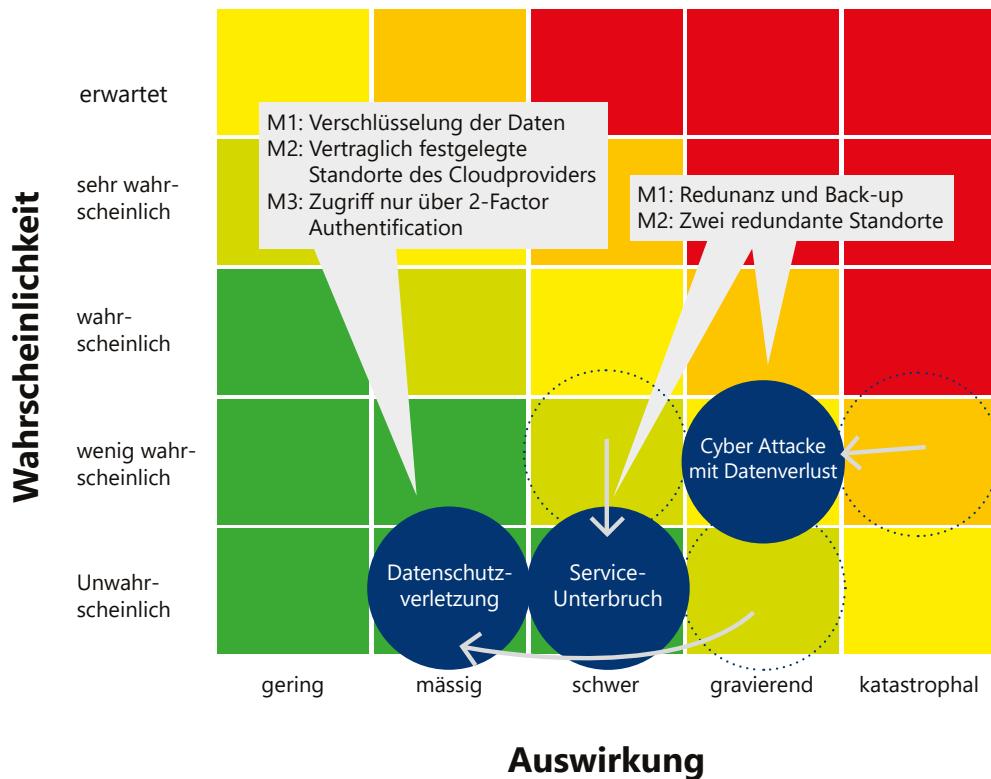


Abbildung 16 – Beurteilte Risiken, vor und nach mitigierenden Massnahmenpaketen

5 CLOUD-GOVERNANCE

Die Art und Weise, wie eine Compliance- und Risikoanalyse durchgeführt wird, ist je nach Organisation punktuell unterschiedlich. Im Wesentlichen – wie auch in den vorgehenden Kapiteln beschrieben – basiert sie immer auf nachfolgender Methodik:

Anforderungsdefinition

1. Prüfung der Cloud-Provider-Bereitstellungseigenschaften (vertraglich, technisch, organisatorisch)
2. Identifikation von Risiken
3. Bewerten der Risiken
4. Festlegen von Massnahmen zur Risikominimierung/Kontrollmechanismen
5. Re-Validierung der Compliance

Die Wiederholung der einzelnen Prozessschritte ist erforderlich, damit die Organisation kontinuierlich konform bleibt und den bestmöglichen Datenschutz sowie operative Sicherheit bieten kann. Wenn sich einer der Faktoren ändert (z. B. eine neue potenzielle Bedrohung, Änderungen an der Menge oder die Sensitivität der erhobenen, gespeicherten und/oder verarbeiteten personenbezogenen Daten ändert, usw.), muss der Prozess neu gestartet werden. Dies nicht jeweils von Grund auf, es gilt vielmehr die geänderten Elemente zu prüfen und die Zusicherungen, Kontrollen und Prozesse (technische und organisatorische Massnahmen) neu zu bewerten, um den Änderungen Rechnung zu tragen.

Ziel dieses Prozesses ist die Etablierung einer optimalen Cloud-Governance innerhalb der Organisation.

Die Cloud-Governance definiert, wie Risiken und Cloud-Nutzung kontinuierlich überwacht und verwaltet werden können. Dabei geht es nicht nur darum, laufend zu beurteilen, welche Sicherheits-, Datenschutz- und Compliance-Kontrollen und -Aktivitäten zu einem bestimmten Zeitpunkt erforderlich sind, sondern auch darum, die zuständige Organisation und die notwendigen Prozesse sowie die Verantwortlichkeiten zu etablieren und operativ zu verankern.

Die gesamte Governance lässt sich dabei in zwei Dimensionen unterteilen:

- Regulatorische Cloud-Governance
- Cloud-Operation Governance/Online Service Management

Die Kontrolle des Kunden über seine Daten und der entsprechenden Cloud-Nutzung ergeben sich aus dem Zusammenspiel zwischen regulatorischer Cloud-Governance und Cloud-Operation-Governance. Dabei sollten die Kunden sicherstellen, dass diese Prozesse immer in ihrer eigenen Kontrolle liegen.

Regulatorische Cloud-Governance

Microsoft stellt seine Hyperscale Cloud-Computing-Dienste in standardisierter Form technisch, organisatorisch und vertraglich zur Verfügung, hat aber keine Kenntnis über die Art der Daten, die im Auftrag des Kunden verarbeitet werden und wird auch keine Beurteilung der kundenspezifischen Umgebung durchführen. Entsprechend ist es für die Etablierung der regulatorischen Governance und Compliance zentral, dass sich jeder Kunde mit den von Microsoft bereitgestellten Rahmenbedingungen auf Basis des Microsoft Assurance Frameworks auseinandersetzt und dessen Kompatibilität, bzw. Einfluss auf die eigenen Vorgaben regelmäßig überprüft und versteht. Das Microsoft Assurance Framework wurde früher im Dokument vor gestellt.

Berücksichtigung aller Entitäten im Unternehmen

In der Regel sind die relevanten Vorgaben und Rahmenbedingungen seitens Kunden nicht nur an zentraler Stelle (IT), sondern unter Einbezug aller Einheiten wie Fachabteilungen oder Industriezweige innerhalb der Organisation zu prüfen. Die IT-Abteilung kann hier als zentrale Drehscheibe und Projektlead agieren, inhaltlich sind jedoch meist die verschiedenen Entitäten in der Verantwortung, die für sie relevanten Grundlagen zu erarbeiten, welche später für die Etablierung der Governance notwendig sind.

Cloud-Operation Governance/Online-Service-Management

Die Cloud-Operation-Governance ist eine IT-bezogene Aufgabe. Hier steht die kontinuierliche Sicherstellung des konformen operativen Betriebes im Fokus. Aspekte, die hier festgelegt werden müssen, sind u.a.

- Engineering- und Betriebsverantwortung
- Architekturmanagement
- Wissensmanagement
- Release- und Lifecycle Management
- Sicherheits- und Compliance Management
- Kostenmanagement
- etc.

Microsoft stellt den Kunden ein umfangreiches Set an verschiedenen Cloud-Service-Management Portalen zur Verfügung, welche in den verschiedenen Disziplinen wertvolle Unterstützung zur Aufgabenerfüllung bieten (z.B. Compliance Center, Security Center, Monitoring, etc.)

Um die kontinuierliche Risikobewertung durch den Kunden / Datenverantwortlichen auf vereinfachte Weise sicherzustellen, können Konfigurationen basierend auf etablierten Frameworks gewählt werden (z.B. ISO 27001, etc.).

Vorgehensweise zur Erarbeitung einer Cloud-Governance

Es ist davon auszugehen, dass in jedem Unternehmen bereits Governanceprozesse etabliert sind und somit entsprechend adaptiert werden können. Nachfolgende Darstellung gibt einen Überblick, wie die entsprechenden Mechanismen seitens Kunde mit denen des Cloud-Providers in Einklang gebracht werden können.

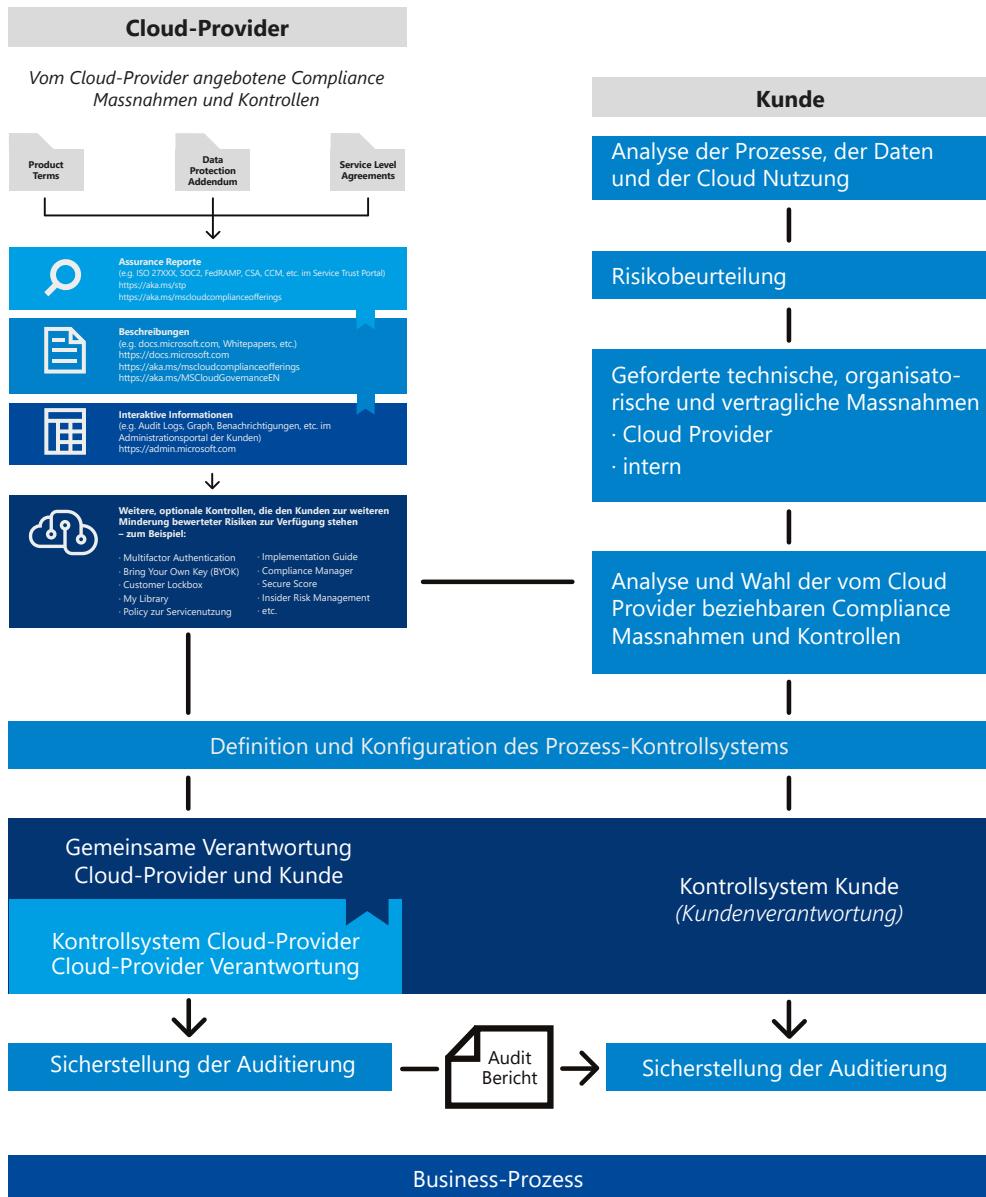


Abbildung 17 – Homogenisierung der Governance Struktur zwischen Kunde und Cloudprovider

Unter Berücksichtigung der dynamischen Entwicklung von Hyperscale Cloud-Services ist im Hinblick auf die initiale Erarbeitung von Governance Strukturen ebenfalls ein iterativer Ansatz zu wählen. Damit wird sichergestellt, dass die erarbeiteten Rahmenbedingungen zeitnah an die zur Nutzung vorgesehenen Workloads/Dienste angepasst und weiterentwickelt werden. Hierzu bietet sich ein Minimum Viable Product (MVP)-Ansatz an, welcher in den ersten Projekten zur Anwendung kommen sollte. Innert kürzester Zeit soll eine erste Version der Governance Strukturen etabliert sein, ohne jedoch Anspruch auf Vollständigkeit zu haben. Im Rahmen eines agilen Vorgehens sind Schritt für Schritt die weiteren Eckpunkte der zukünftigen Governance zu erarbeiten und festzulegen. So kann sichergestellt werden, dass Projektvorhaben zeitlich nicht verzögert werden. Ziel ist, den Governance Maturitätsgrad mit zunehmender Adoption von Cloud-Services zu erhöhen.

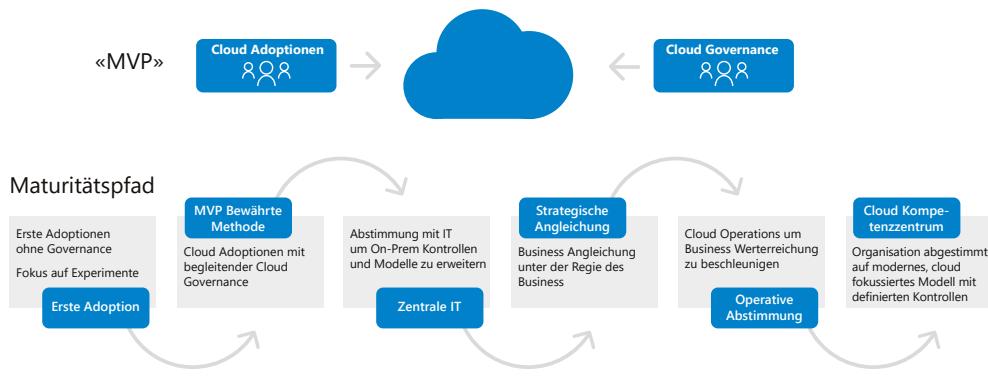


Abbildung 18 – MVP-Ansatz für die Erarbeitung der Cloud-Governance

Daten Governance

Die Relevanz von Daten ist unbestritten. Damit diese Daten jedoch für die Wertschöpfung zur Anwendung kommen können und geschäftsrelevanten Charakter erhalten, müssen sie minimal folgende Eigenschaften aufweisen:

- Sie müssen auffindbar sein
- Sie müssen formal definiert/strukturiert sein
- Sie müssen vertrauenswürdig sein
- Sie müssen geschützt sein

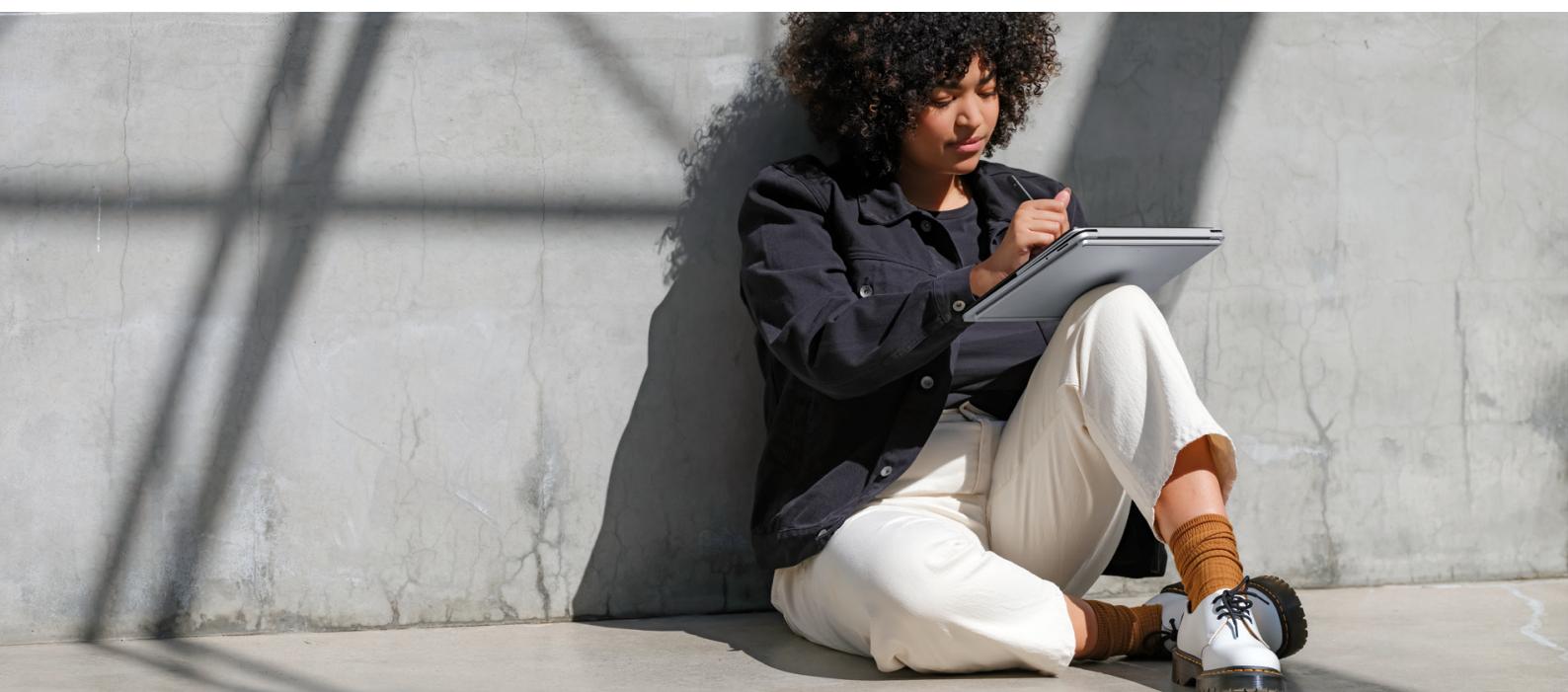
Damit diese Eigenschaften sichergestellt werden können, sind folgende Aspekte im Rahmen der notwendigen Daten-Governance zu berücksichtigen:

- Festlegung der Verantwortlichen für das Vorhaben
- Analyse und Dokumentation des Business Prozesses, seiner geographischen Ausdehnung und der Standorte der im Prozess involvierten internen und externen Parteien
- Analyse und Dokumentation der Systeme und Applikationen, welche diesen Business Prozess unterstützen
- Analyse und Dokumentation der Daten und Datentypen, welche für diesen Business Prozess verwendet werden
- Dokumentation der Standorte, an denen die verschiedenen Datentypen physisch gespeichert sind
- Analyse, Festlegung und Dokumentation der geltenden gesetzlichen und internen Compliance-Regeln, welche auf diese Daten in den verschiedenen Lokationen / Rechtsräumen anwendbar sind
- Analyse und Dokumentation der Risiken, welche mit der Verwendung dieser Daten an den verschiedenen Standorten einhergehen
- Festlegung adäquater Mitigationsmaßnahmen technischer, organisatorischer und/oder vertraglicher Art gegenüber intern, extern und dem Cloud-Provider entsprechend der bestehenden Risikobereitschaft
- Analyse, ob der Cloud-Provider die von ihm geforderten Mitigationsmaßnahmen anbietet kann
- Entscheid, ob die Cloud unter den gegebenen Umständen benutzt werden kann und welche Mitigationsmaßnahmen aus der Cloud bezogen werden müssen
- Design eines adäquaten Kontrollsystems für die Daten, beinhaltend die vom Cloud-Provider beigestellten Mitigationsmaßnahmen und Kontrollen
- Sicherstellung des operativen Betriebs und der Auditierbarkeit des Kontrollsystems

Schlussbemerkung

Dass die Cloud-Technologie grossen und kleineren Unternehmen, Organisationen und Verwaltungen schon heute viele Möglichkeiten bietet, ist unbestritten. Dies insbesondere auch deshalb, weil die Datensicherheit entscheidend verbessert wurde. Noch ist aber das wirkliche Potential der Cloud-Technologie nicht wirklich erfasst, geschweige denn ausgereizt. Auch aus diesem Grund ist es sinnvoll, sich heute ernsthaft mit einem Einstieg in die Cloud-Technologie zu befassen und auf ein nachhaltig funktionierendes Fundament zu stellen. Häufig wird nämlich der Fehler gemacht, die Risikobeurteilung zu stark auf den Einzelfall zu fokussieren. Damit vergibt man sich aber die Chance der Replizierbarkeit. Und genau diese ist wichtig, will man mittelfristig in den Modus der industrialisierten Cloud Adoption kommen.

In den allermeisten Fällen ist es sinnvoll, den Weg in die Cloud mit einem Partner anzugehen, welcher andere Organisationen bereits erfolgreich in die Cloud brachte. Microsoft ist mit über 30 Jahren Erfahrung in der Schweiz und einem Netzwerk von über 4'600 lokal verankerten Partnerfirmen bestens aufgestellt und steht auch im dauernden Kontakt mit Regulatoren und Aufsichtsbehörden. Zudem kann Microsoft eigene Cloud-Services aus Datenzentren in der Schweiz anbieten und die ruhenden Daten spezifischer Services innerhalb des Landes lagern, was bezüglich Datensicherheit ein nicht zu unterschätzender Vorteil ist.





Danke
Merci
Grazie
Engraziel