VISCHER

Outsourcing für Finanzinstitute.

Der Weg in die Cloud

Erfahrungen aus der Praxis

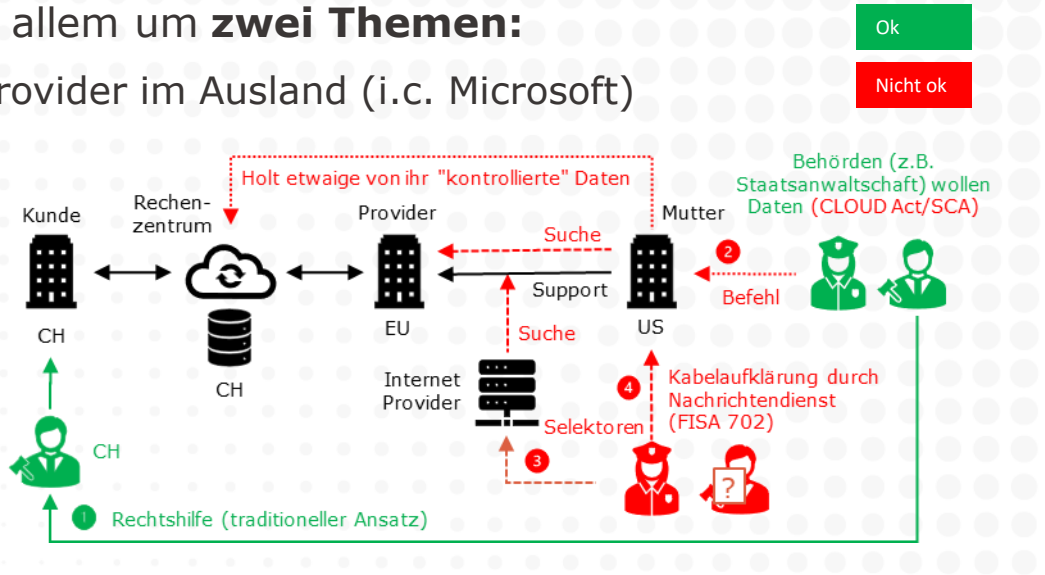
David Rosenthal, Partner, VISCHER AG
29. November 2023

Herausforderung?

- Was ist die Herausforderung für eine Schweizer Bank oder anderes Schweizer Finanzinstitut **beim Gang in die Cloud**?
  - Die grundsätzliche rechtliche Zulässigkeit und insbesondere das Risiko eines ausländischen Behördenzugriffs?
  - Die Akzeptanz seitens FINMA?
  - Die Verträge der Provider?
  - Anpassung der AGB?
  - **Heute nicht mehr …**

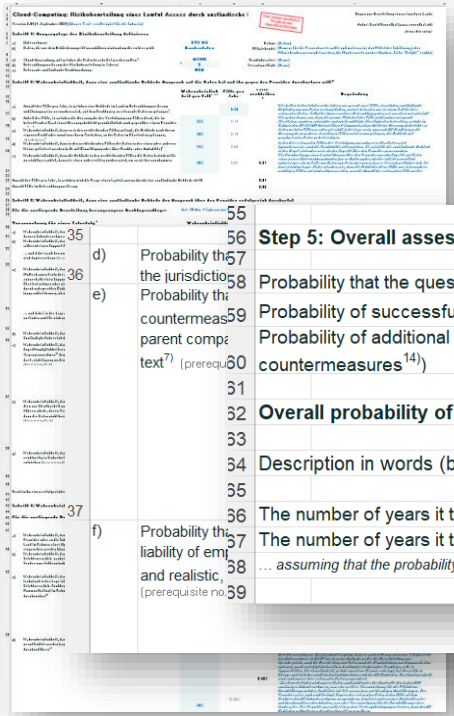
Mit Berufsgeheimnisdaten in die Cloud?

- **Es kommt darauf an …**
  - Vor allem ob die Vertraulichkeit gewahrt bleibt
- Umstritten sind bzw. waren vor allem um **zwei Themen:**
  - Offenlegung gegenüber dem Provider im Ausland (i.c. Microsoft)
  - Provider muss Behörden im Ausland allenfalls auf die Daten Zugriff gewähren ("Foreign Lawful Access")
- **Weniger umstritten:** Datensicherheit zum Schutz vor Angriffen durch Dritte
  - z.B. Cyber-Kriminelle



Beurteilung ausländischer Lawful Access

Input: Bisherige Erfahrungen mit Anfragen ausländischer Behörden, technische und organisatorische Massnahmen



Step 5: Overall assessment		
Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)		6.25%
Probability of successful lawful access by the foreign authorities concerned in these cases despite in the countermeasures[14]		2.84%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures[14])		0.40%
Overall probability of a successful lawful access via the cloud provider in the observation period:* **		0.58%
Description in words (based on Hillson****):	Very low	
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:		1'988
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:		598
… assuming that the probability neither increases nor decreases over time (like tossing a coin)		

Excel: https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx
Vgl. auch den Beitrag unter https://bit.ly/2HaEet5 und Anhang unter https://bit.ly/2H8MyZY und die FAQ: https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf

Beurteilung ausländischer Lawful Access

Staatsanwaltschaft des Kantons Basel-Stadt

- Die Bedenken bezüglich einer strafrechtlichen Verantwortlichkeit beschränkt sich mit Blick auf das geplante Outsourcing in die Microsoft Cloud, gemäss Ihren Angaben, auf die Frage des "Lawful Access" ausländischer Behörden auf die geheimnisgesch Daten. Im Vordergrund steht dabei die Gefahr eines Zugriffs US-amerikanischer Behörden auf Grundlage des US Cloud Acts. Dieser Einschätzung kann aus Sicht der Staatsanwaltschaft zugestimmt werden.

- Die Berechnung des Risikos eines ausländischen "Lawful Access" erscheint nach Ansicht der Staatsanwaltschaft grundsätzlich ein geeignetes Kriterium, um die Vertretbarkeit der Auslagerung auch vor einem strafrechtlichen Hintergrund zu beurteilen. Eine Überprüfung des Ergebnisses im konkreten Fall ist der Staatsanwaltschaft indes nicht möglich, da dieses letztlich von den Einschätzungen der einzelnen Berechnungsfaktoren abhängt. Diese können von aussen nicht überprüft werden.

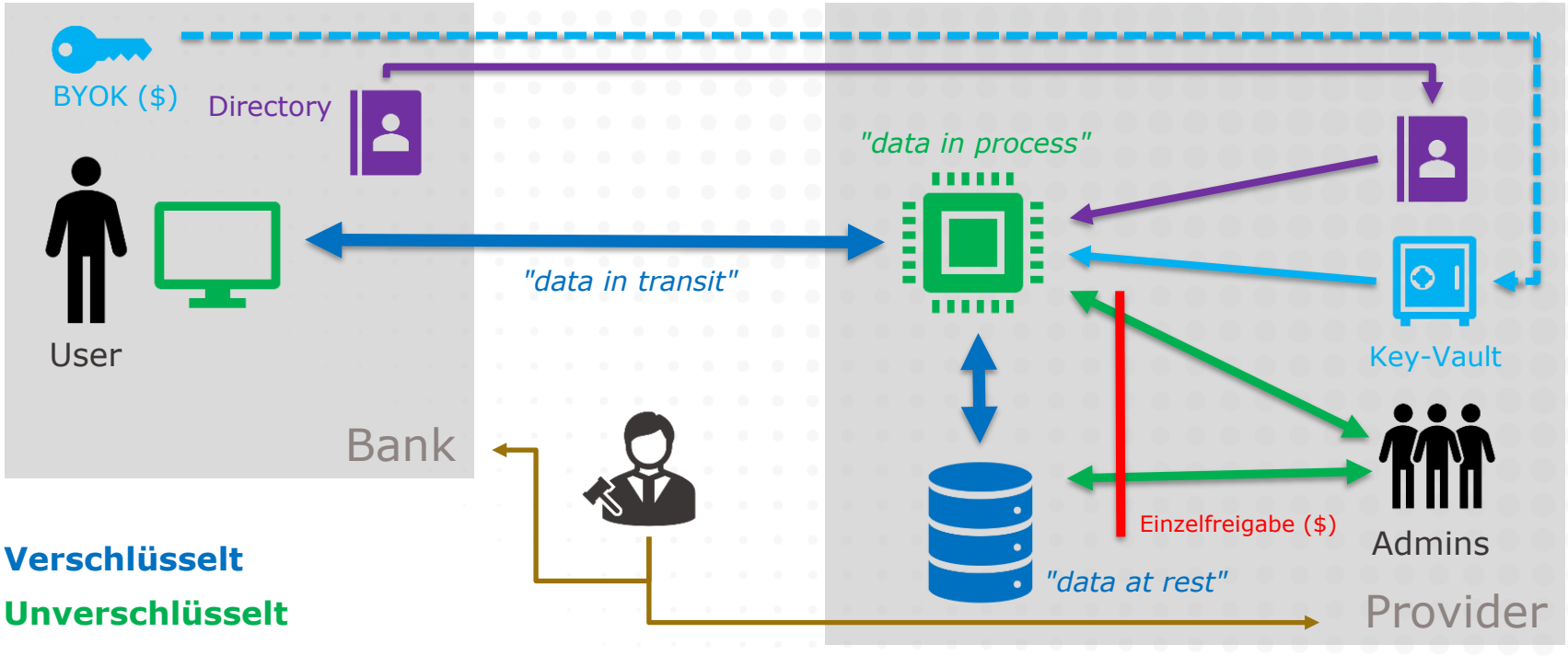
Risikobasierter Ansatz

Bundeskanzlei: "Gute Praxis"

Kanton Zürich: "Standard"

Auszug aus: Schreiben der Staatsanwaltschaft Basel-Stadt nach einem Workshop zur Berechnung des Risikos eines ausländischen Behördenzugriffs im Kontext eines Cloud-Projekts des Basler USB/UKBB

Wie Daten in der Cloud geschützt werden



Welche Massnahmen treffen?

- **Berufsgeheimnis und Datenschutz**
  - Europäische Gegenpartei (z.B. Microsoft Ireland Operations Ltd.)
  - Datenhaltung in der Schweiz
  - Verschlüsselung von Daten (z.B. MPIP, nicht BYOK oder DKE)
  - Manueller Providerzugriff beschränken (z.B. "Customer Lockbox")
  - Vertraulichkeitsverpflichtung, Defend-your-data-Klausel
  - Schutzmassnahmen für Personendaten gelten für alle Inhalte
  - Einschränkung der Bearbeitung für eigene Providerzwecke
- **Weitere Massnahmen**
  - Konfiguration und Steuerung, Prüfrechte & Einbindung ins IKS, Backups/BCM, Exit-Konzept, ggf. Schweizer Recht/Gerichtsstand

Massnahmen gegen Lawful Access aus dem Ausland (z.B. US CLOUD Act)

+ Nutzungsrichtlinien

Anforderungen FINMA

- **Rundschreiben Outsourcing 2018/3** Lösbar
  - Prüfrechte, auch für FINMA und externe Prüfstelle
  - Regelung für den Beizug wesentlicher Subunternehmer
  - Möglichkeit zur geordneten Rückführung, Geschäftsfortführung
  - Direkte Kontrollrechte für regulierte Institute
- **Rundschreiben Operationelle Risiken/Resilienz 2023/1** Lösbar
  - Informationssicherheit, Geschäftsfortführung
  - Management der IKT- und Cyber-Risiken (z.B. Entdecken und Notifizieren von Cyber-Vorfällen innert 24 Stunden)
  - Management der Risiken kritischer Daten (z.B. Mitarbeiter mit privilegiertem Zugang)

Provider-Verträge

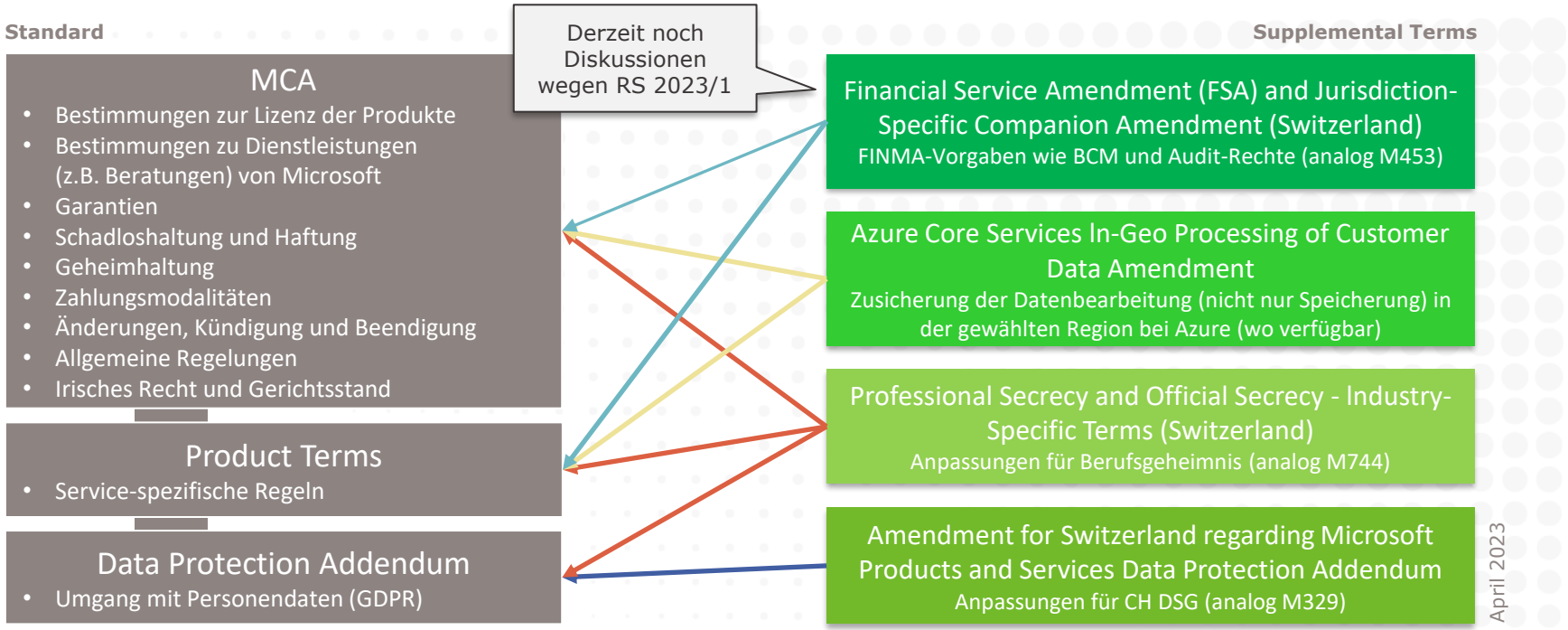
- Die **Basisverträge** der Hyperscaler genügen nicht
  - Ergänzungen sind nötig betreffend Berufsgeheimnis, Schweizer Datenschutz und Vorgaben der FINMA, ggf. Haftung

Derzeit noch Diskussionen wegen RS 2023/1

- **Microsoft**
  - Von uns für diverse Banken verhandelt; wurde in einen Standard überführt, der heute für alle CH-Finanzinstitute verfügbar ist
- **Amazon Web Services (AWS)**
  - Verhandlungen für Schweizer Finanzinstitute laufen; hoffentlich führt dies (wie bei Microsoft) zu Standard-Vertragsergänzungen
- **Google**
  - Anpassungen für Schweizer Recht erfolgen bisher jeweils in individuellen Verhandlungen

Heikler sind mitunter Drittanbieter, welche die Cloud nutzen

Beispiel Microsoft: MCA und Supplemental Terms



April 2023

AGB / Waiver

12. Auslagerung (Outsourcing)

Die Bank kann Bereiche und Funktionen (z. B. Wertschriftenverwaltung, Zahlungsverkehr, Druck & Versand, Kundenservice, IT) inklusive Bankkundendaten ganz oder teilweise an Dienstleister im In- und Ausland auslagern. Diese können Bankkundendaten wiederum Dritten bekanntgeben, soweit die Dritten sie benötigen oder zur Vertraulichkeit verpflichtet sind.

13. Datenschutz / Bankkundengeheimnis

Die Bank sorgt mit angemessenen Massnahmen für die Einhaltung des Datenschutzes und des Bankkundengeheimnisses. Der Kunde entbindet die Bank von ihrer Geheimhaltungspflicht, soweit:

a) dies zur Wahrung berechtigter Interessen der Bank nötig ist, insbesondere (i) bei

c) Daten im Rahmen einer Auslagerung gemäss Ziffer 12 dieser Bedingungen bekanntgegeben werden. Details betreffend Bekanntgabe von Daten ins Ausland im Zusammenhang mit Auslagerungen (Outsourcings) gemäss Ziffer 12 dieser Bedingungen sind in der Datenschutzerklärung enthalten (www.raiffeisen.ch/rechtliches oder auf Nachfrage bei der Bank erhältlich);

d) Daten in der Raiffeisen Gruppe im Rahmen deren Geschäftstätigkeit ausgetauscht werden;

e) dies im Zusammenhang mit der nachfolgend beschriebenen Bekanntgabe von Daten an Kooperationspartner im In- und Ausland erfolgt;

f) der Kunde Software oder Applikationen herunterlädt, installiert und / oder benutzt und dabei Daten Dritten (z.B. App-Anbieter bzw. -Entwickler, Netzbetreiber) bekannt werden und dadurch insbesondere die Bankbeziehung offengelegt wird.

Im Rahmen der Geschäftstätigkeit der Bank dürfen Daten, welche die Geschäftsbeziehung mit dem Kunden betreffen auch gegenüber Kooperationspartnern bekanntgegeben werden

deren Kooperationspartnern. Für Marketing und Werbezwecke werden jedoch Profile und personenbezogene Daten nur mit Zustimmung des Kunden an Kooperationspartner weitergegeben. Der Kunde kann der Profilbildung zu Marketing und Werbezwecken und Werbezusendungen aber jederzeit widersprechen.

Angaben dazu, zu den wichtigsten aktuellen Kooperationspartnern und auch sonst zur Datenbearbeitung und anderen Rechten betroffener Personen sind in der jeweils geltenden Datenschutzerklärung (www.raiffeisen.ch/rechtliches oder auf Nachfrage) enthalten. Der Kunde wird der Bank Daten von Dritten nur mitteilen, wenn er dazu berechtigt ist und die Dritten über die Bearbeitung der Daten ausreichend informiert hat.

Der Kunde nimmt zur Kenntnis, dass Daten im Ausland nicht dem Schutz des Schweizer Rechts unterstehen. Eine ausländische Behörde wie beispielsweise ein Gericht oder andere Dritte können gegebenenfalls nach dem ausländischen Recht die Herausgabe anordnen oder auf Daten zugreifen.

Quelle: Raiffeisen.ch

Herausforderung der "Cloud"

Bild von Pexels (Pixabay)

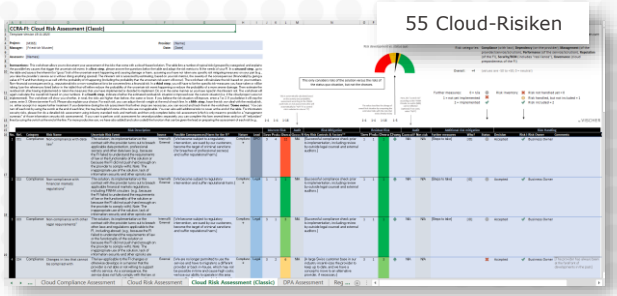
Sorgen Sie für:

- Klarheit
- Koordination
- Kontrolle

Für Klarheit sorgen

- Worum geht es bei einem **Cloud-Projekt**?
  - Was soll eingeführt werden? Wie spielt all dies zusammen? Welche Einstellungsoptionen gibt es?
  - Was passiert seitens des Providers (z.B. im Falle der Verschlüsselung von Daten)?
- Was sind die **Risiken**?
  - Blick öffnen (z.B. BCM, Kosten, interne Risiken)
  - Strukturierte Vorgehensweise und Beurteilung in der Gruppe sorgt für höhere Ergebnisqualität
  - Dokumentieren und mit Status-quo vergleichen
  - Aber: Risikobeurteilungen bleiben subjektiv

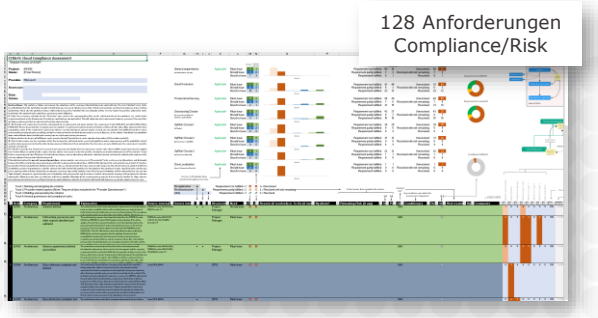
Quelle:
https://pro.jumpto365.com/@/hexatown.com/PTO365



https://www.rosenthal.ch/downloads/VISCHER-CCRA-FI-Info.PDF

Für Koordination sorgen

- Cloud-Projekte sind **nicht (nur) Projekte der IT**
  - Regulatory, Rechtsdienst, Datenschutzstelle, CISO, Risk, Business Owner, Projektmanager, Operations, Procurement, Internal/External Audit
  - Für die meisten sind Cloud-Projekte Neuland



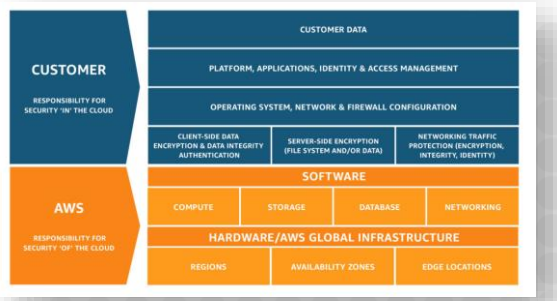
CCRA-FI

- **Bewährt:** Zuteilung von "Hausaufgaben", aber gemeinsame Erörterung ihrer Ergebnisse und der verbleibenden Risiken
  - Braucht es z.B. nebst dem Zielsystem eine Notlösung? Wie schnell muss eine solche realisiert werden können und was ist machbar? Hängt dies auch vom Vertrag mit dem Provider ab?
  - Welche Funktionen sind betroffen, wenn z.B. das E-Mail-System nicht mehr funktioniert? Bsp. die Bankomatenversorgung?

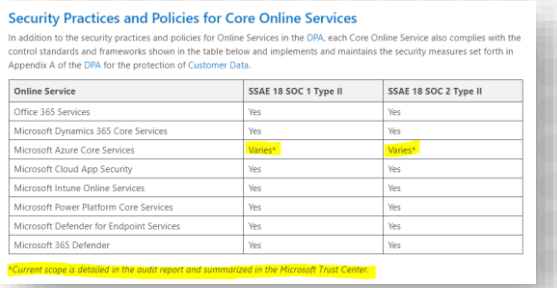
Erfordert eine interdisziplinäre Diskussion

Für Kontrolle sorgen

- Tücken des **"Shared Responsibility Model"**
  - Es liegt viel mehr Verantwortung und Arbeit beim Finanzinstitut als beim klassischen Outsourcing
  - Komplexität und interne Risiken mitunter höher
- Cloud **ändert** sich laufend und ist **intransparent**
  - Gilt auch für die Verträge der Hyperscaler
- **Kontinuierliche Kontrolle** des Providers, der eigenen Organisation und der Restrisiken
  - Das Cloud-Compliance- und Risiko-Assessment endet nicht mit dem Projekt
  - Oft fehlen noch die nötigen Prozesse/Ressourcen



Quelle: AWS



Security Practices and Policies for Core Online Services

In addition to the security practices and policies for Online Services in the DPA, each Core Online Service also complies with the control standards and frameworks shown in the table below and implements and maintains the security measures set forth in Appendix A of the DPA for the protection of Customer Data.

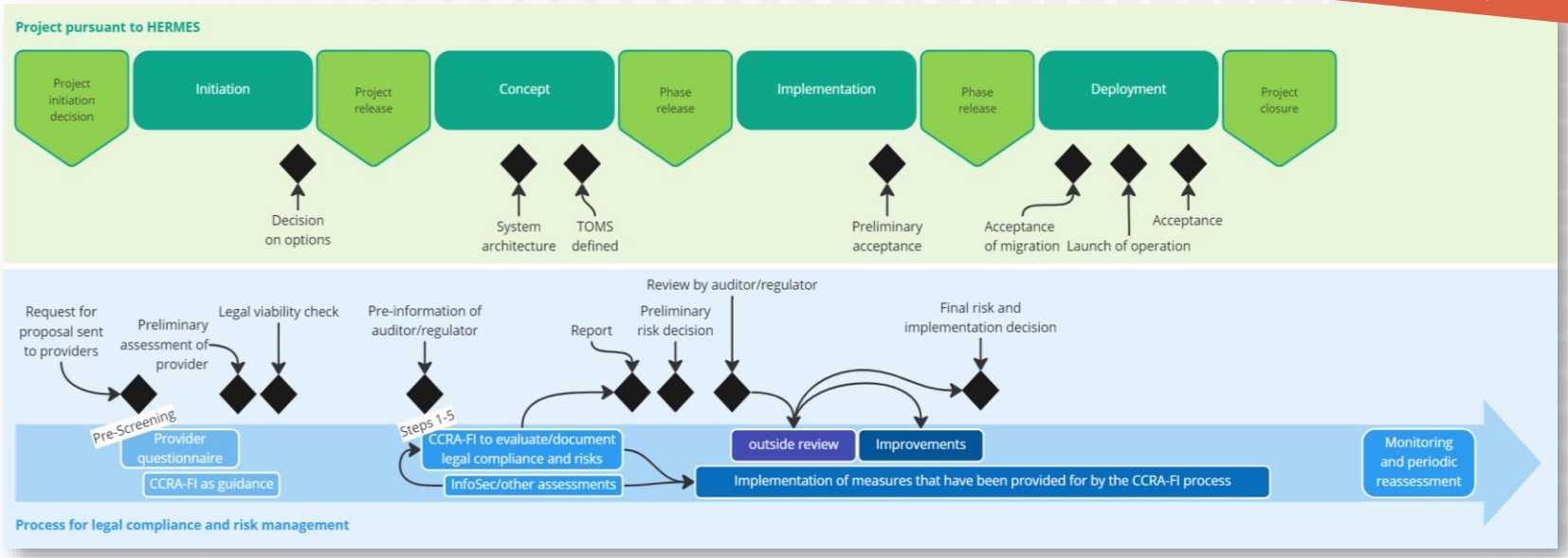
Online Service	SSAE 18 SOC 1 Type II	SSAE 18 SOC 2 Type II
Office 365 Services	Yes	Yes
Microsoft Dynamics 365 Core Services	Yes	Yes
Microsoft Azure Core Services	Varies*	Varies*
Microsoft Cloud App Security	Yes	Yes
Microsoft Intune Online Services	Yes	Yes
Microsoft Power Platform Core Services	Yes	Yes
Microsoft Defender for Endpoint Services	Yes	Yes
Microsoft 365 Defender	Yes	Yes

*Current scope is detailed in the audit report and summarized in the Microsoft Trust Center.

Quelle: Microsoft

Prozess aus Sicht Compliance & Risk

Nutzen Sie ein erstes Projekt, um Erfahrungen zu sammeln



Quelle: CCRA-FI

Die fünf Cloud-Fragen der Leitung eines Instituts

	Strategie und Vorgehensweise	Beurteilung eines konkreten Vorhabens
Motive & Alternativen	Welche Dinge erhoffen wir uns vom Gang in die Cloud und wie gut wollen wir die Alternativen kennen?	Was sind die geschäftlichen, operationellen und anderen Anforderungen an das Vorhaben und wieso überwiegt die gewählte Lösung gegenüber anderen Techniken (d.h. Alternativen zur Cloud), anderen Cloud-Providern und dem Status quo?
Compliance	Wie gehen wir vor, um die Einhaltung des Bankgeheimnisses und der diversen gesetzlichen, regulatorischen wie auch eigenen Vorgaben systematisch zu prüfen, zu dokumentieren und während der ganzen Laufzeit der Cloud-Vorhaben sicherzustellen?	Halten wir mit dem Vorhaben das Bankgeheimnis und die gesetzlichen, regulatorischen wie auch die eigenen Vorgaben ein und wie haben wir dies systematisch geprüft, dokumentiert und für die ganze Laufzeit des Cloud-Vorhabens sichergestellt?
Organisation & Internes Kontrollsystem (IKS)	Was sind wir bereit zu tun und zu verlangen, damit unsere Organisation Cloud-Provider und deren Lösungen verstehen, kontrollieren und steuern können, so dass wir sie nicht nur richtig handhaben können, sondern auch Abweichungen vom Soll rechtzeitig erkennen und beseitigen können?	Welche Vorkehrungen haben wir getroffen oder treffen wir, damit wir den Provider und seinen Cloud-Lösung mit unseren internen Mitteln so gut verstehen, kontrollieren und steuern können, dass wir die Cloud-Lösung gemäss den Anforderungen richtig handhaben, Abweichungen vom Soll rechtzeitig erkennen und sie beseitigen können werden, inklusive seiner bzw. ihrer "end-to-end" Einbindung in unser IKS?
Geschäftsfortführung	Welche Anforderungen stellen wir an die Sicherstellung der Geschäftsfortführung bei einem Ausfall oder Datenverlust und unsere Fähigkeit für einen kurzfristigen (Monate) und mittelfristigen (12-18 Monate) Ausstieg aus einem Cloud-Service und welchen Aufwand sind wir bereit dafür zu betreiben?	Was ist unser Plan für den Fall, dass der Cloud-Provider seinen Service plötzlich abstellt, die Lösung oder unsere Daten nicht mehr verfügbar sind oder wir kurzfristig (Monate) und mittelfristig (12-18 Monate) von ihm oder seiner Lösung weg müssen oder wollen?
Restrisiken	Wie stellen wir sicher, dass wir konkrete Bedrohungen, die mit einem Cloud-Vorhaben einhergehen und gewichtige Folgen für die Bank haben können, richtig einschätzen, steuern und in Bezug zu den Restrisiken stellen, die wir sonst bzw. sowieso haben?	Welche weiteren Bedrohungen, welche für die Bank gewichtige Folgen haben können, bringt das Cloud-Vorhaben mit sich, wie gut haben wir diese im Griff und wie stehen die Restrisiken zu jenen Risiken, die wir ohne das Vorhaben bzw. sowieso hätten?

VISCHER

Danke für Ihre Aufmerksamkeit!

Fragen: drosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

www.vischer.com

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00