VISCHER

Schweizer Banken in der Cloud.

Herausforderungen und Vorgehensweise

David Rosenthal, Partner, VISCHER AG
29. November 2023

Erste Schweizer Banken gehen den Weg …

Die Zürcher Kantonalbank hat angekündigt, dass sie 2022 mit der Verlagerung von Applikationen und Daten in die Public Cloud beginnt. Die Bank hat sich für die Microsoft Schweiz entschieden als deren erster Cloud Provider. Die Ver

Arbeitsplatz entsprechend entwickeln. Auch in der Bankenbranche hält diese moderne Arbeitsweise vermehrt Einzug. Als eine der ersten Arbeitgeberinnen hat sich die Raiffeisen Gruppe entschieden, auf Microsoft 365 und Teams zu setzen. «Unser Anspruch ist es, unseren Kollegin Arbeitsplatz zur Verfügung zu stellen – u Digital

Die Basellandschaftliche Kantonalbank (BLKB) gestaltet die Zukunft der Arbeit mit Microsoft 365 und Microsoft Teams aus Schweizer Rechenzentren

radicant baut Plattform auf Google Cloud

Zürich, 07.06.2022 – radicant ag, die erste nachhaltige, digitale und kollaborative Finanzdienstleisterin, die sich an den 17 Zielen für nachhaltige Entwicklung der UNO orientiert, wird die erste Bank in der Schweiz, die hauptsächlich auf Google Cloud basiert. Die

Mit M365 fängt es in der Regel an

Ist Zukunft Multivendor?

M365

Microsoft Azure

salesforce

AWS EC2

AWS S3

Snowflake

Google Cloud

Erwartete Herausforderungen

- **Datensicherheit** seitens des Cloud-Providers
- **Schweizer Vertragsklauseln** mit den Cloud-Providern
- Grundsätzliche Akzeptanz des **Regulators**
- Risiko eines ausländischen **Lawful Access** (z.B. CLOUD Act)

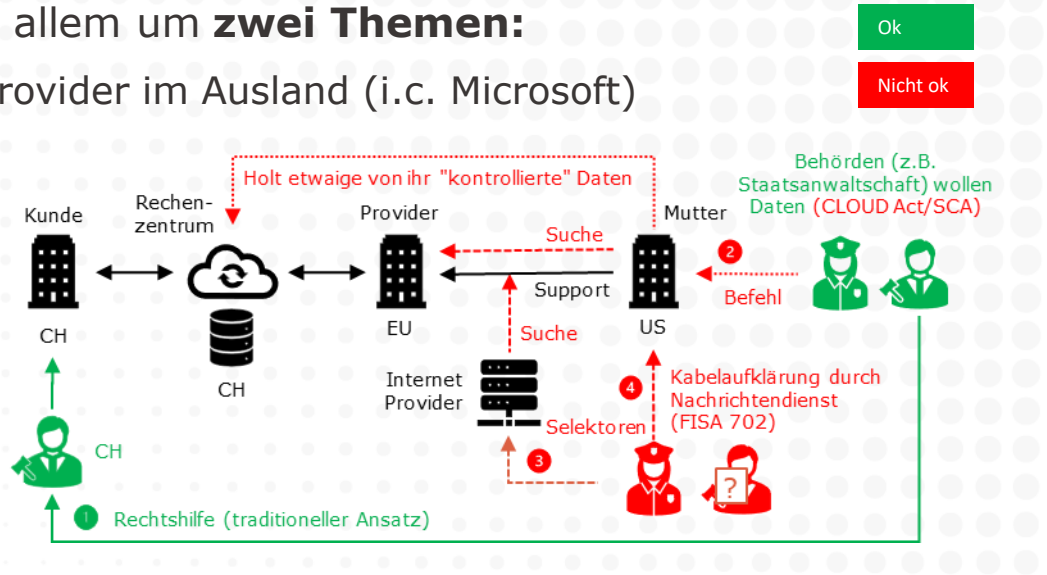
https://youtu.be/-sM34c59QOU

Das Unternehmen stellt sicher, dass es frühzeitig über den Beizug oder Wechsel von Unterakkordanten, die wesentliche Funktionen erbringen, informiert wird, und die Möglichkeit hat, das Outsourcing gemäss Rz 18.1 geordnet zu beenden. Werden solche Unterakkordanten beigezogen, sind ihnen die Pflichten und Zusicherungen des Dienstleisters, die zur Erfüllung dieses Rundschreibens erforderlich sind, zu überbinden.

Aus: FINMA Rundschreiben 2018/03 (Outsourcing), Rz. 33

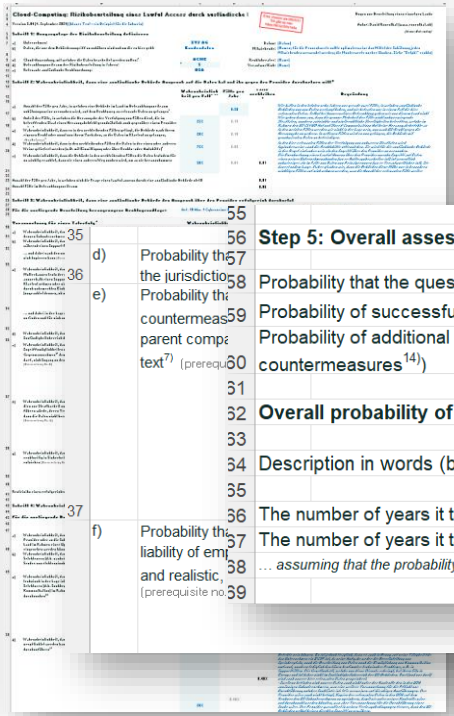
Mit Berufsgeheimnisdaten in die Cloud?

- **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")
- **Kein Thema mehr:** 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



55			
56	**Step 5: Overall assessment**		
57			
58	Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)		6.25%
59	Probability of successful lawful access by the foreign authorities concerned in these cases despite in the countermeasures[14)]		2.84%
60	Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures[14)])		0.40%
61			
62	**Overall probability of a successful lawful access via the cloud provider in the observation period:*** **		0.58%
63			
64	Description in words (based on Hillson****):	Very low	
65			
66	The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:		1'988
67	The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:		598
68	*… assuming that the probability neither increases nor decreases over time (like tossing a coin)*		
69			

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.

Beurteilung ausländischer Lawful Access

dsb datenschutzbeauftragte des kantons zürich

Widerspricht herrschender Auffassung

Vgl. etwa https://datenrecht.ch/dsb-zuerich-taetigkeitsbericht-2022/

Bei Personendaten, die unter einem besonderen Amtsgeheimnis oder einem Berufsgeheimnis stehen, hält das Gesetz fest: Die verantwortliche Person macht sich strafbar, wenn sie Unberechtigten auch nur die Möglichkeit gibt, solche Daten zur Kenntnis zu nehmen. So ist die Entscheidung einfach. Daten unter einem besonderen Amtsgeheimnis oder einem Berufsgeheimnis können nur ausgelagert werden, wenn sie verschlüsselt sind und ausschliesslich die verantwortliche Person oder ihre Hilfspersonen den Schlüssel kennen.

Die gängigsten gesamtheitlichen Cloud-Lösungen stammen von US-amerikanischen Unternehmen. Sie unterstehen dem CLOUD Act. Der CLOUD Act ermöglicht amerikanischen Behörden, Zugriff auf die Daten zu verlangen, unabhängig davon, wo sie gespeichert sind. Damit werden die Abkommen zur Rechtshilfe umgangen. Das Vorgehen verstösst gegen die schweizerische Rechtsordnung. Vertragliche Absicherungen helfen nicht. Es steht dem US-amerikanischen Unternehmen nicht frei, wegen eines Vertrags das Gesetz der USA nicht einzuhalten.

Die Rechtsfrage kann nicht mit Wahrscheinlichkeitsrechnungen umgangen werden. Wenn ein Zugriff rechtswidrig ist, hilft es nicht, dass die Wahrscheinlichkeit eines solchen Zugriffs klein sein könnte. Ein öffentliches Organ hat sich immer rechtmäs-

Auszug aus: Tätigkeitsbericht 2022, DSB Zürich

Beim Berufsgeheimnis dürfen Informationen und Personendaten nur von der Geheimnisträgerin oder dem Geheimnisträger und ihren respektive seinen Hilfspersonen bearbeitet werden. Ausnahmen bestehen, wenn eine gesetzliche Bestimmung etwas anderes vorsieht, die betroffene Person im Einzelfall eingewilligt hat oder die vorgesetzte Behörde die Geheimnisträgerin oder den Geheimnisträger im Einzelfall von der Geheimnispflicht entbindet. Wenn die Mitarbeitenden des Cloud-Anbieters als Hilfspersonen qualifiziert werden können, besteht die Möglichkeit, auch Daten unter dem Berufsgeheimnis in die Cloud auszulagern. Bei Standardlösungen von internationalen Cloud-Anbietern sind ihre Mitarbeitenden in der Regel keine Hilfspersonen. Informationen und Personendaten unter dem Berufsgeheimnis können mit solchen Standardlösungen nur bearbeitet werden, wenn die Informationen verschlüsselt sind und das öffentliche Organ den Schlüssel behält oder wenn die Personendaten vorher anonymisiert oder pseudonymisiert wurden.

Nach herrschender Auffassung *sind* Cloud-Provider Hilfspersonen …

Problem gelöst?

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.

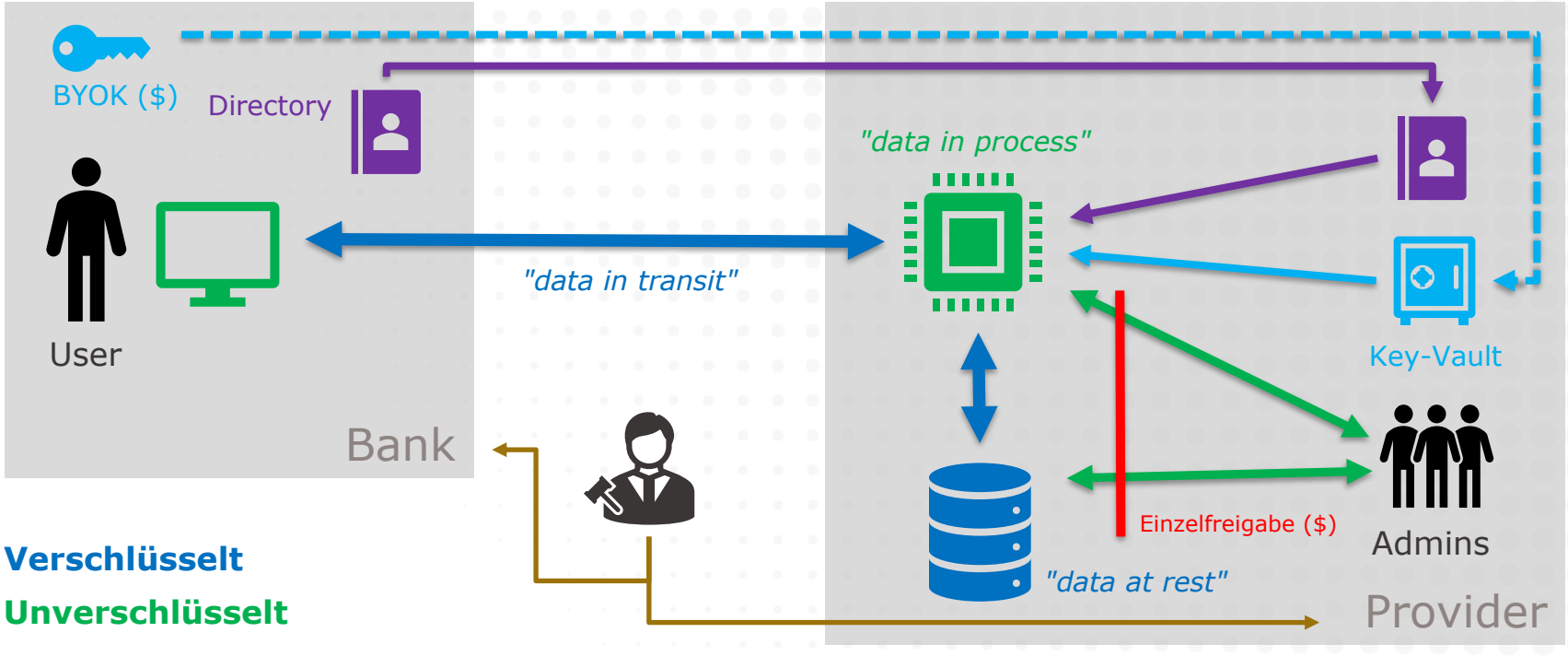
Risikobasierter Ansatz

Bundeskanzlei: "Gute Praxis"

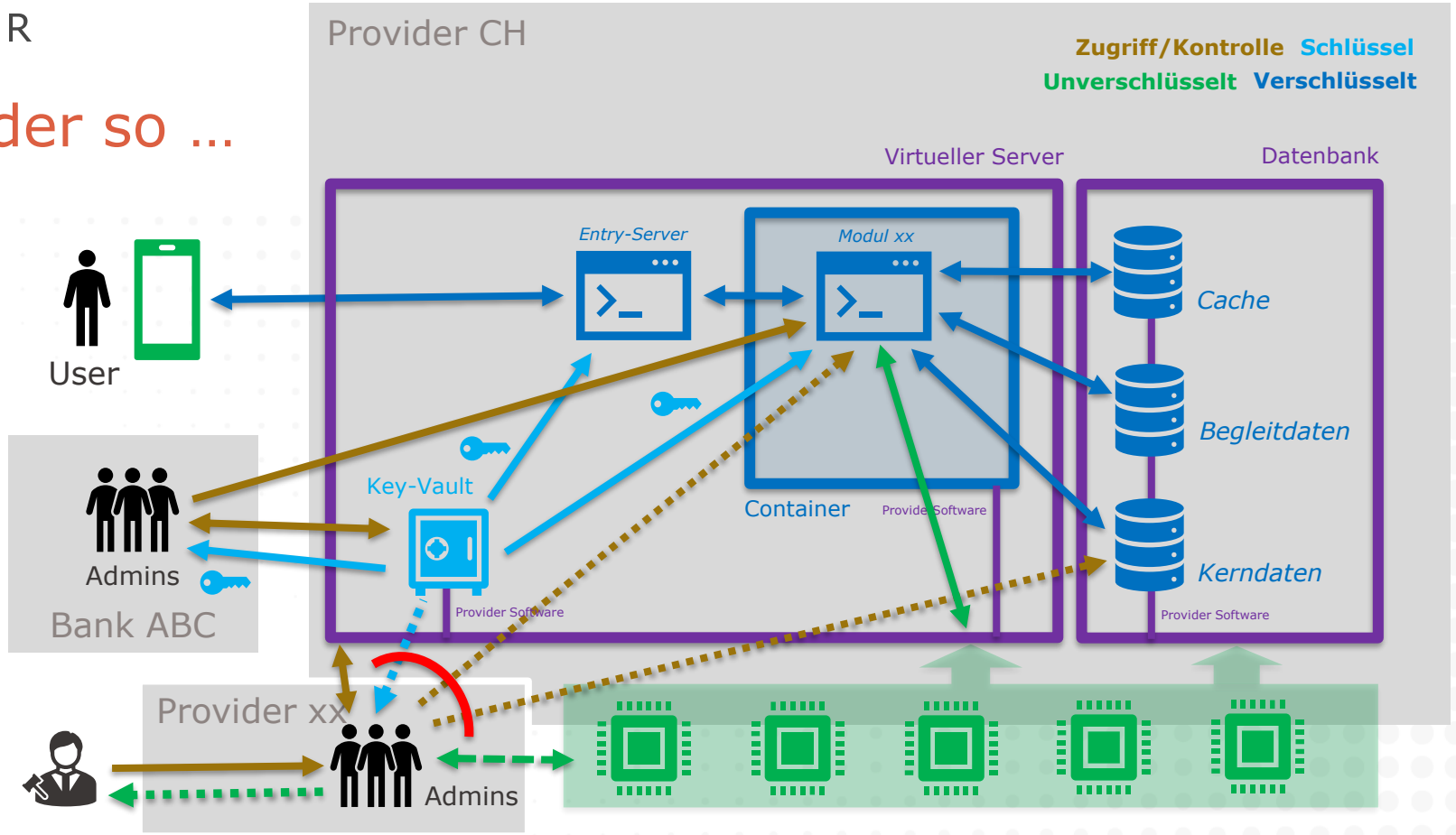
Kanton Zürich: "Standard"

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



Oder so …


Provider CH
Zugriff/Kontrolle
Schlüssel
Unverschlüsselt
Verschlüsselt
Virtueller Server
Datenbank
Entry-Server
Modul xx
Cache
Begleitdaten
Kerndaten
User
Key-Vault
Container
Provider Software
Admins
Bank ABC
Provider Software
Provider Software
Provider xx
Admins

Welche Massnahmen treffen?

- **Berufsgeheimnis und Datenschutz**
  - Europäische Gegenpartei (z.B. Microsoft Ireland Operations Ltd.)
  - Datenhaltung in der Schweiz
  - Verschlüsselung von Daten (MPIP, aber nicht BYOK oder DKE)
  - Manuelle Provider-Zugriffe einschränken (z.B. "Lockbox" – teuer)
  - 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 (US CLOUD Act)

+ Nutzungsrichtlinien

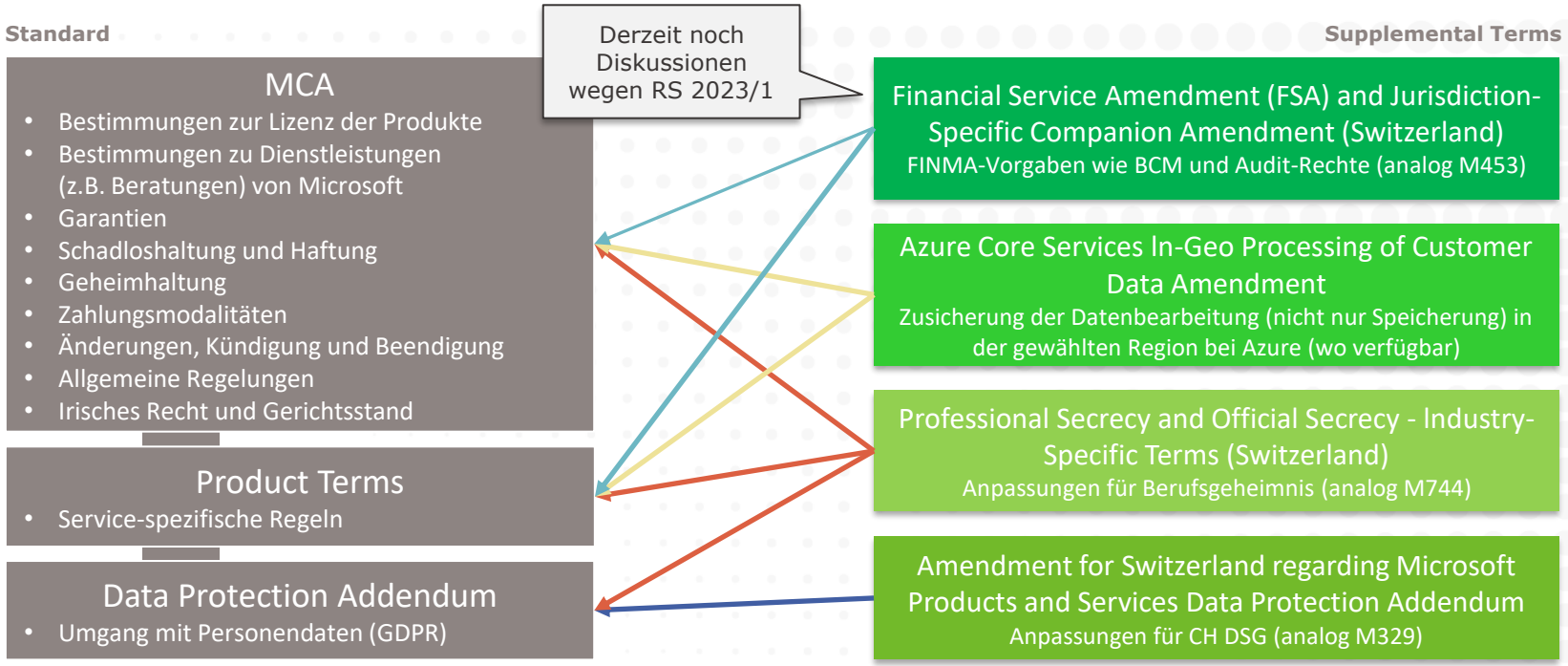
Anforderung FINMA

- **Rundschreiben Outsourcing 2018/3**
  - 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**
  - 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)

Verträge

- Die **Basisverträge** der Hyperscaler genügen nicht
  - Ergänzungen sind nötig betreffend Berufsgeheimnis, Schweizer Datenschutz und Vorgaben der FINMA, ggf. Haftung
- **Microsoft**
  - Von uns für diverse Banken verhandelt; jetzt in einen Standard überführt, der heute für alle CH-Finanzinstitute verfügbar ist
- **Amazon Web Services (AWS)**
  - Verhandlungen von uns für Schweizer Finanzinstitute laufen; wir streben (wie bei Microsoft) Standard-Vertragsergänzungen an
- **Google**
  - Anpassungen für Schweizer Recht erfolgen bisher jeweils in individuellen Verhandlungen

Übersicht MCA und Supplemental Terms



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

Die weiteren Cloud-Themen


Too big to fail

Article Talk

From Wikipedia, the free encyclopedia

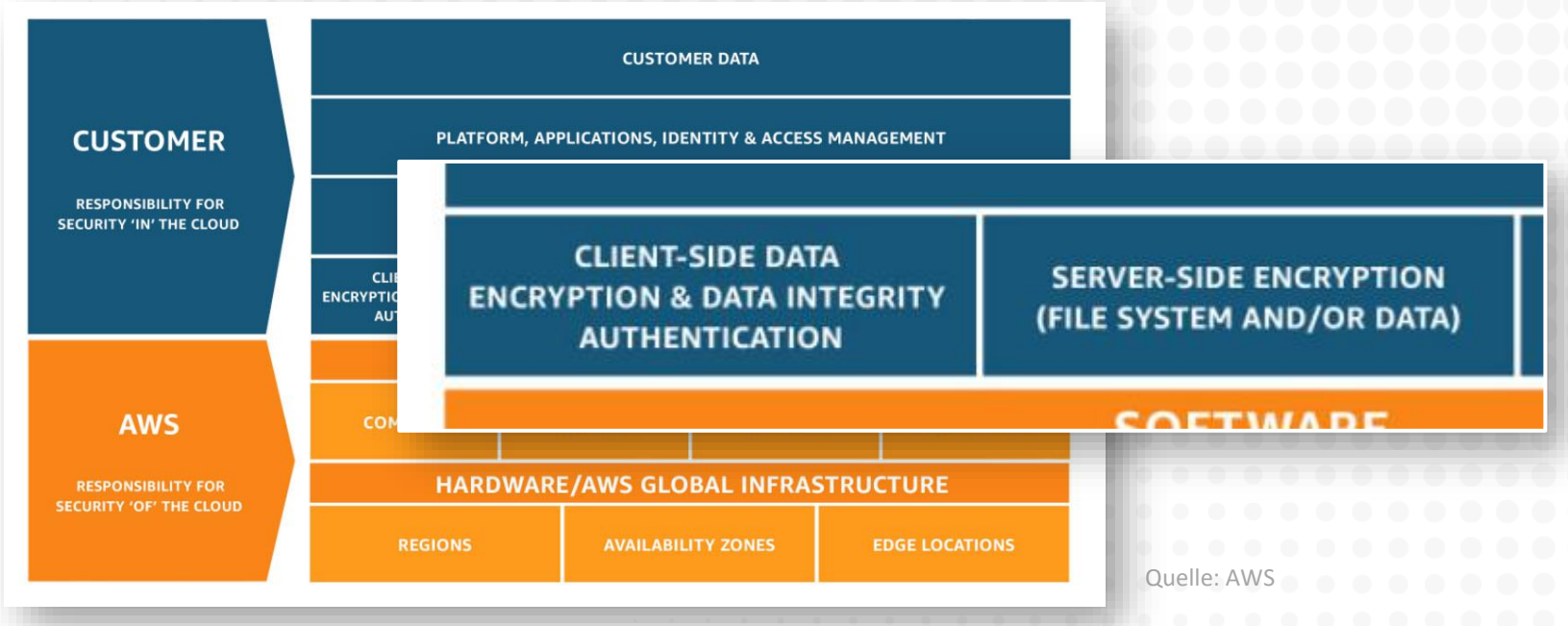
This article is about a theory in economics. For the legal designation, see Systemically impor
see Too Big to Fail (book). For the film, see Too Big to Fail (film).

"Too big to fail" (**TBTF**) is a theory in banking and finance that asserts that certain corporations, particularly financial institutions, are so large and so interconnected that their failure would be disastrous to the greater economic system, and therefore should be supported by government when they face potential failure.[1] The colloquial term "too big to fail" was

... wie werden wir geschützt?

- Das **"Shared Responsibility Model"**
  - Der Kunde muss sagen, was er wie haben will
  - Der Kunde ist für Steuerung und Kontrolle verantwortlich
  - Komplexität von Cloud-Umgebungen nimmt zu
  - Schäden können auch Benutzerseitig verursacht werden
- Die **Cloud verändert** sich **ständig** und ist **nicht transparent**
  - Auch die Verträge; erfordert viel Wissen, Arbeit, Aufmerksamkeit
- **Abhängigkeit** führt zu Risiken (z.B. Geschäftsfortführung)
  - Gibt es eine Alternative? Was wäre, wenn Microsoft seinen Dienst plötzlich abstellt? Backups? Ausstieg möglich? Zu welchem Preis?
- **Kontrolle** und **Überblick** behalten? **Risikomanagement**?

Shared Responsibility Model?



Quelle: AWS

Eine neue Welt auch für uns Juristen …

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

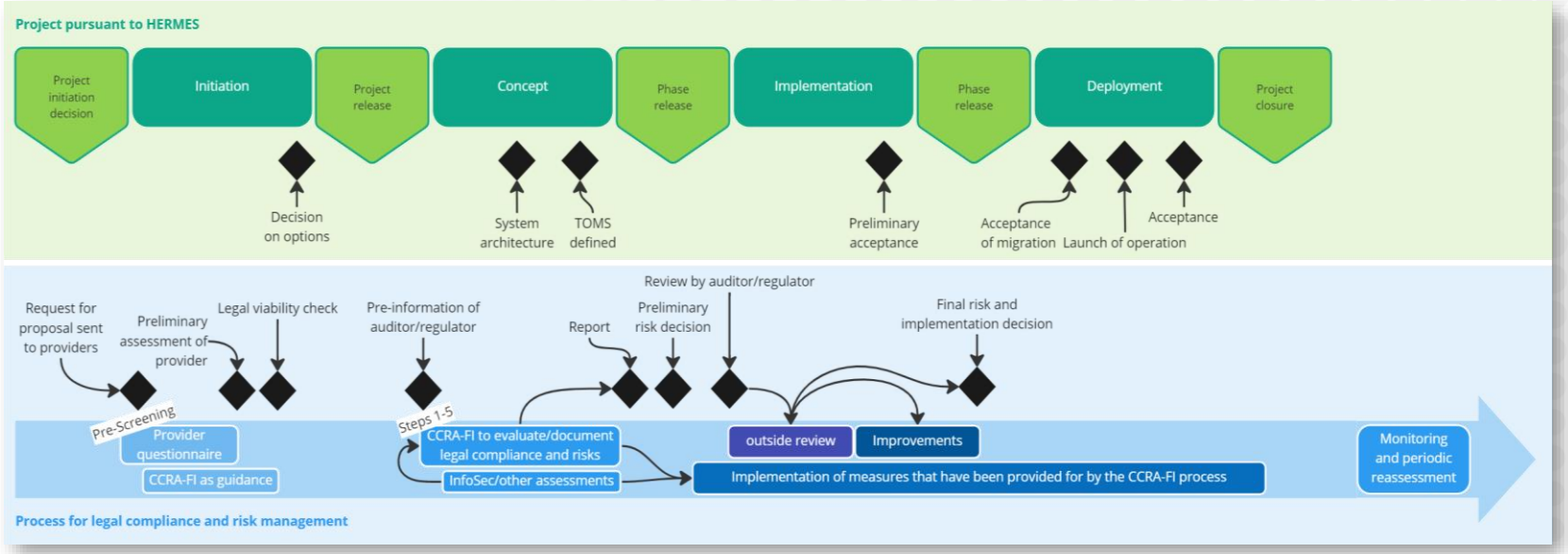
Current scope is detailed in the audit report and summarized in the Microsoft Trust Center.

Microsoft

Die fünf Cloud-Fragen der Leitung einer Bank …

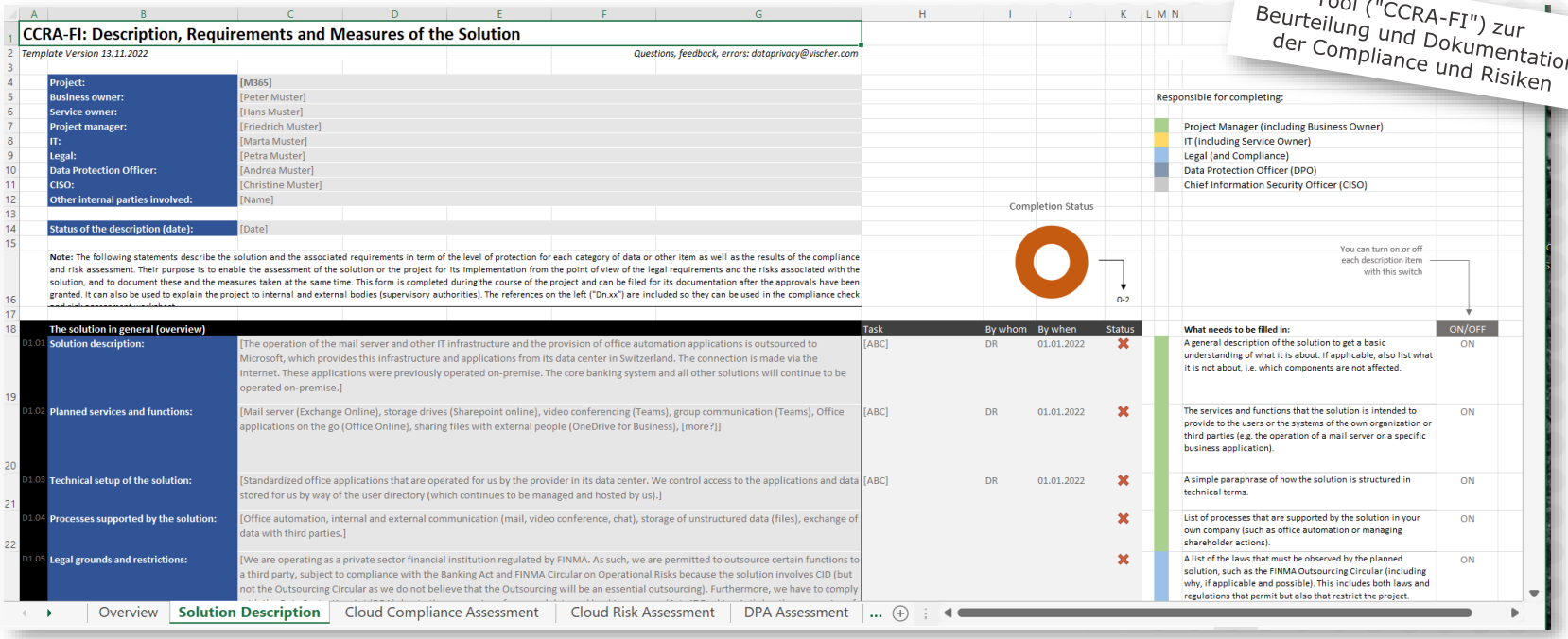
	Strategie und Vorgehensweise	Beurteilung eines konkreten Vorhabens
Motive & Alternativen	Welche Dinge erhoffen wir uns vom Gang in die Cloud und wie gut wollen wir die Alternativen kennen?	Was sind die geschäftlichen, operationellen und anderen Anforderungen an das Vorhaben und wieso überwiegt die gewählte 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?

Prozess aus Sicht Legal & Risk



Cloud-Risiko- und Compliance-Beurteilung

Tool ("CCRA-FI") zur Beurteilung und Dokumentation der Compliance und Risiken



CCRA-FI: Description, Requirements and Measures of the Solution

Template Version 13.11.2022 — *Questions, feedback, errors: dataprivacy@vischer.com*

Project:	[M365]
Business owner:	[Peter Muster]
Service owner:	[Hans Muster]
Project manager:	[Friedrich Muster]
IT:	[Marta Muster]
Legal:	[Petra Muster]
Data Protection Officer:	[Andrea Muster]
CISO:	[Christine Muster]
Other internal parties involved:	[Name]
Status of the description (date):	[Date]

Responsible for completing:
- Project Manager (including Business Owner)
- IT (including Service Owner)
- Legal (and Compliance)
- Data Protection Officer (DPO)
- Chief Information Security Officer (CISO)

Completion Status: 0-2

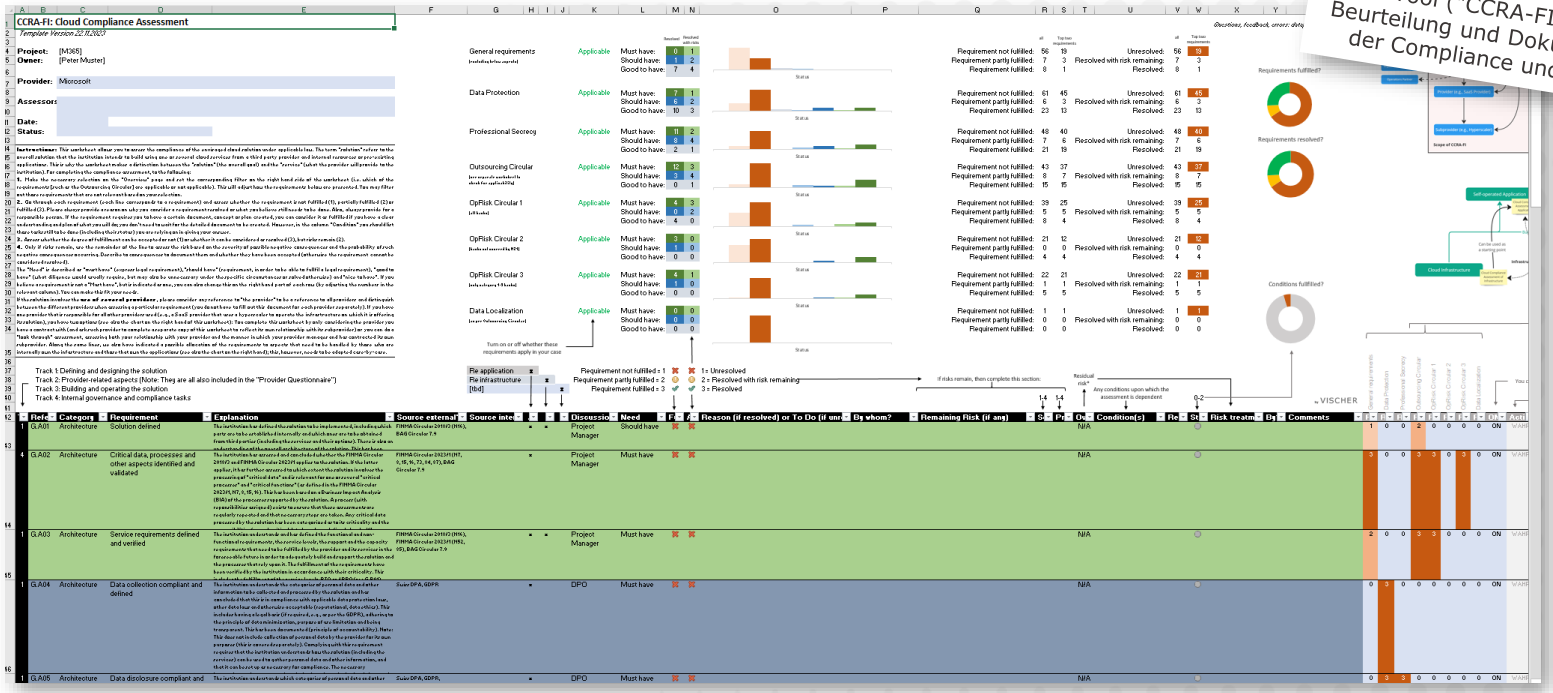
You can turn on or off each description item with this switch

Note: The following statements describe the solution and the associated requirements in term of the level of protection for each category of data or other item as well as the results of the compliance and risk assessment. Their purpose is to enable the assessment of the solution or the project for its implementation from the point of view of the legal requirements and the risks associated with the solution, and to document these and the measures taken at the same time. This form is completed during the course of the project and can be filed for its documentation after the approvals have been granted. It can also be used to explain the project to internal and external bodies (supervisory authorities). The references on the left ("Dn.xx") are included so they can be used in the compliance check

	The solution in general (overview)		Task	By whom	By when	Status	What needs to be filled in:	ON/OFF
D1.01	Solution description:	[The operation of the mail server and other IT infrastructure and the provision of office automation applications is outsourced to Microsoft, which provides this infrastructure and applications from its data center in Switzerland. The connection is made via the Internet. These applications were previously operated on-premise. The core banking system and all other solutions will continue to be operated on-premise.]	[ABC]	DR	01.01.2022	✖	A general description of the solution to get a basic understanding of what it is about. If applicable, also list what it is not about, i.e. which components are not affected.	ON
D1.02	Planned services and functions:	[Mail server (Exchange Online), storage drives (Sharepoint online), video conferencing (Teams), group communication (Teams), Office applications on the go (Office Online), sharing files with external people (OneDrive for Business), [more?]]	[ABC]	DR	01.01.2022	✖	The services and functions that the solution is intended to provide to the users or the systems of the own organization or third parties (e.g. the operation of a mail server or a specific business application).	ON
D1.03	Technical setup of the solution:	[Standardized office applications that are operated for us by the provider in its data center. We control access to the applications and data stored for us by way of the user directory (which continues to be managed and hosted by us).]	[ABC]	DR	01.01.2022	✖	A simple paraphrase of how the solution is structured in technical terms.	ON
D1.04	Processes supported by the solution:	[Office automation, internal and external communication (mail, video conference, chat), storage of unstructured data (files), exchange of data with third parties.]				✖	List of processes that are supported by the solution in your own company (such as office automation or managing shareholder actions).	ON
D1.05	Legal grounds and restrictions:	[We are operating as a private sector financial institution regulated by FINMA. As such, we are permitted to outsource certain functions to a third party, subject to compliance with the Banking Act and FINMA Circular on Operational Risks because the solution involves CID (but not the Outsourcing Circular as we do not believe that the Outsourcing will be an essential outsourcing). Furthermore, we have to comply				✖	A list of the laws that must be observed by the planned solution, such as the FINMA Outsourcing Circular (including why, if applicable and possible). This includes both laws and regulations that permit but also that restrict the project.	ON

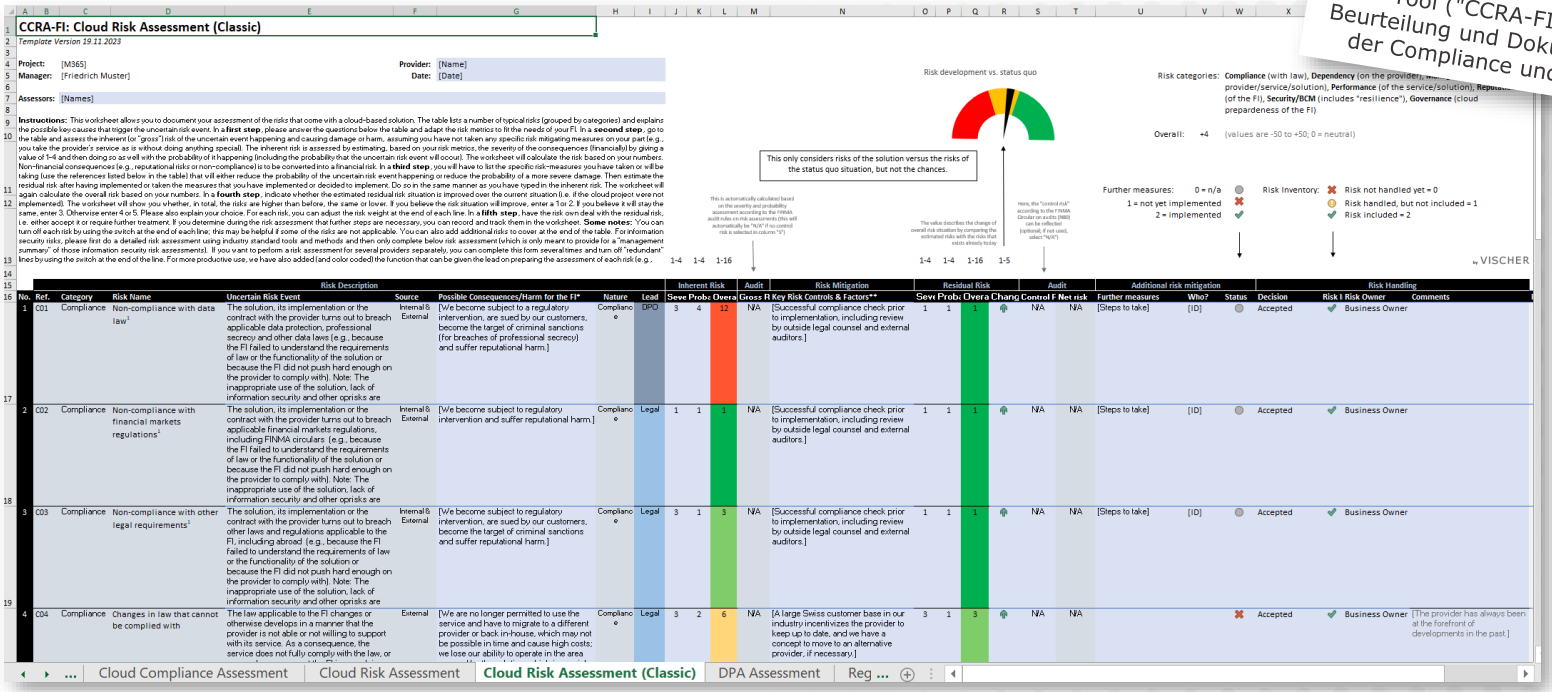
Overview | Solution Description | Cloud Compliance Assessment | Cloud Risk Assessment | DPA Assessment

Cloud-Risiko- und Compliance-Beurteilung



Cloud-Risiko- und Compliance-Beurteilung

Tool ("CCRA-FI") zur Beurteilung und Dokumentation der Compliance und Risiken



CCRA-FI: Cloud Risk Assessment (Classic)

Template Version 19.11.2023

Project: [M365] Provider: [Name]
Manager: [Friedrich Muster] Date: [Date]

Assessors: [Names]

Instructions: This worksheet allows you to document your assessment of the risks that come with a cloud-based solution. The table lists a number of typical risks (grouped by categories) and explains the possible key causes that trigger the uncertain risk event. In a **first step**, please answer the questions below the table and adapt the risk metrics to fit the needs of your FI. In a **second step**, go to the table and assess the inherent (or "gross") risk of the uncertain event happening and causing damage or harm, assuming you have not taken any specific risk mitigating measures on your part (e.g., you take the provider's service as is without doing anything special). The inherent risk is assessed by estimating, based on your risk metrics, the severity of the consequences (financially) by giving a value of 1–4 and then doing so as well with the probability of it happening (including the probability that the uncertain risk event will occur). The worksheet will calculate the risk based on your numbers. Non-financial consequences (e.g., reputational risks or non-compliance) is to be converted into a financial risk. In a **third step**, you will have to list the specific risk-measures you have taken or will be taking (use the references listed below in the table) that will either reduce the probability of the uncertain risk event happening or reduce the probability of a more severe damage. Then estimate the residual risk after having implemented or taken the measures that you have implemented or decided to implement. Do so in the same manner as you have typed in the inherent risk. The worksheet will again calculate the overall risk based on your numbers. In a **fourth step**, indicate whether the estimated residual risk situation is improved over the current situation (i.e. if the cloud project were not implemented). The worksheet will show you whether, in total, the risks are higher than before, the same or lower. If you believe the risk situation will improve, enter a 1 or 2. If you believe it will stay the same, enter 3. Otherwise enter 4 or 5. Please also explain your choice. For each risk, you can adjust the risk weight at the end of each line. In a **fifth step**, have the risk own deal with the residual risk, i.e. either accept it or require further treatment. If you determine during the risk assessment that further steps are necessary, you can record and track them in the worksheet. **Some notes:** You can turn off each risk by using the switch at the end of each line; this may be helpful if some of the risks are not applicable. You can also add additional risks to cover at the end of the table. For information security risks, please first do a detailed risk assessment using industry standard tools and methods and then only complete below risk assessment (which is only meant to provide for a "management summary" of those information security risk assessments). If you want to perform a risk assessment for several providers separately, you can complete this form several times and turn off "redundant" lines by using the switch at the end of the line. For more productive use, we have also added (and color coded) the function that can be given the lead on preparing the assessment of each risk (e.g.,

Risk development vs. status quo

This only considers risks of the solution versus the risks of the status quo situation, but not the chances.

Risk categories: **Compliance** (with law), **Dependency** (on the provider), **Reputation** (of the FI), **Security/BCM** (includes "resilience"), **Governance** (cloud preparedness of the FI)

Overall: +4 (values are -50 to +50; 0 = neutral)

Further measures: 0 = n/a; 1 = not yet implemented; 2 = implemented

Risk Inventory: Risk not handled yet = 0; Risk handled, but not included = 1; Risk included = 2

by VISCHER

								Risk Description				Inherent Risk				Audit	Risk Mitigation	Residual Risk				Audit	Additional risk mitigation			Risk Handling		
No.	Ref.	Category	Risk Name	Uncertain Risk Event	Source	Possible Consequences/Harm for the FI*	Nature	Lead	Seve	Probs	Overa	Gross R	Key Risk Controls & Factors**	Sevi	Probs	Overa	Chang	Control F	Net risk	Further measures	Who?	Status	Decision	Risk I	Risk Owner	Comments
1	C01	Compliance	Non-compliance with data law[1]	The solution, its implementation or the contract with the provider turns out to breach applicable data protection, professional secrecy and other data laws (e.g., because the FI failed to understand the requirements of law or the functionality of the solution or because the FI did not push hard enough on the provider to comply with). Note: The inappropriate use of the solution, lack of information security and other oprisks are	Internal & External	[We become subject to a regulatory intervention, are sued by our customers, become the target of criminal sanctions (for breaches of professional secrecy) and suffer reputational harm.]	Compliance	DPO	3	4	12	N/A	[Successful compliance check prior to implementation, including review by outside legal counsel and external auditors.]	1	1	1		N/A	N/A	[Steps to take]	[ID]		Accepted		Business Owner	
2	C02	Compliance	Non-compliance with financial markets regulations[1]	The solution, its implementation or the contract with the provider turns out to breach applicable financial markets regulations, including FINMA circulars (e.g., because the FI failed to understand the requirements of law or the functionality of the solution or because the FI did not push hard enough on the provider to comply with). Note: The inappropriate use of the solution, lack of information security and other oprisks are	Internal & External	[We become subject to regulatory intervention and suffer reputational harm.]	Compliance	Legal	1	1	1	N/A	[Successful compliance check prior to implementation, including review by outside legal counsel and external auditors.]	1	1	1		N/A	N/A	[Steps to take]	[ID]		Accepted		Business Owner	
3	C03	Compliance	Non-compliance with other legal requirements[1]	The solution, its implementation or the contract with the provider turns out to breach other laws and regulations applicable to the FI, including abroad (e.g., because the FI failed to understand the requirements of law or the functionality of the solution or because the FI did not push hard enough on the provider to comply with). Note: The inappropriate use of the solution, lack of information security and other oprisks are	Internal & External	[We become subject to regulatory intervention, are sued by our customers, become the target of criminal sanctions and suffer reputational harm.]	Compliance	Legal	3	1	3	N/A	[Successful compliance check prior to implementation, including review by outside legal counsel and external auditors.]	1	1	1		N/A	N/A	[Steps to take]	[ID]		Accepted		Business Owner	
4	C04	Compliance	Changes in law that cannot be complied with	The law applicable to the FI changes or otherwise develops in a manner that the provider is not able or not willing to support with its service. As a consequence, the service does not fully comply with the law, or	External	[We are no longer permitted to use the service and have to migrate to a different provider or back in-house, which may not be possible in time and cause high costs; we lose our ability to operate in the area	Compliance	Legal	3	2	6	N/A	[A large Swiss customer base in our industry incentivizes the provider to keep up to date, and we have a concept to move to an alternative provider, if necessary.]	3	1	3		N/A	N/A				Accepted		Business Owner	[The provider has always been at the forefront of developments in the past.]

Cloud Compliance Assessment | Cloud Risk Assessment | Cloud Risk Assessment (Classic) | DPA Assessment | Reg ...

VISCHER

Diskussion!

Fragen: drosenthal@vischer.com

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

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

www.vischer.com