VISCHER

CCRA-FI.

Eine Einführung in die Verwendung des Tools

David Rosenthal, Partner, VISCHER AG
24. April 2023

Ausgangslage

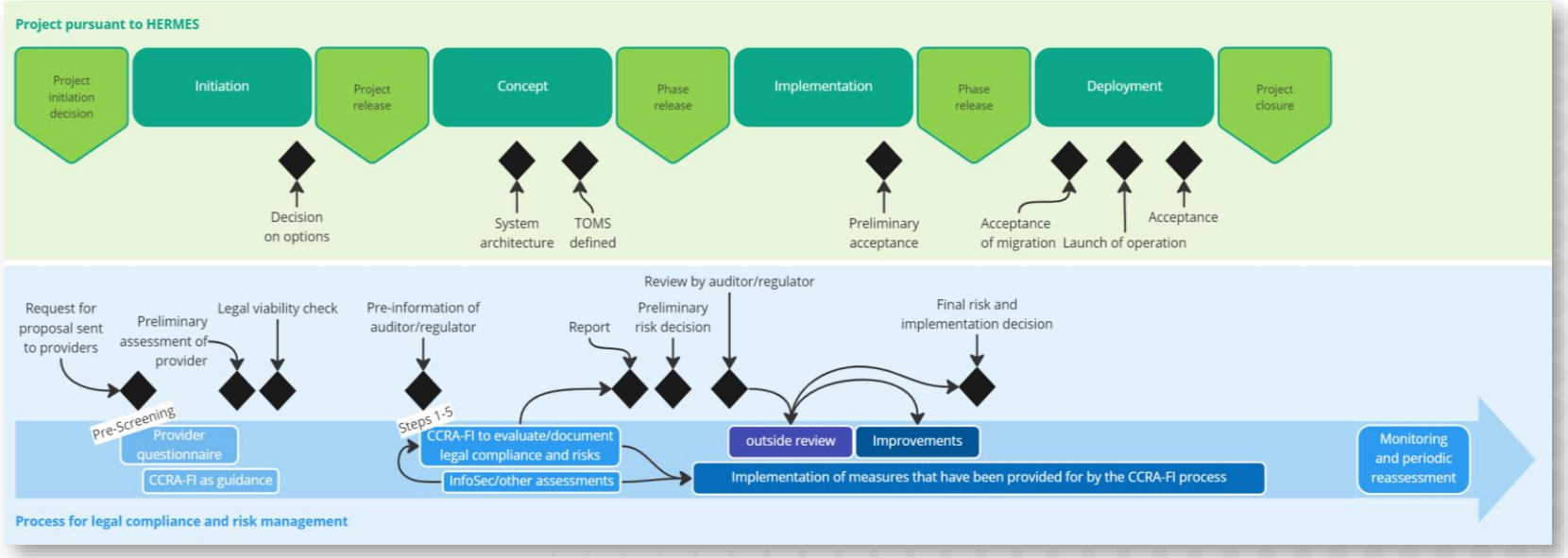
- **Vorgaben**
  - Datenschutzgesetz (ab 1. September 2023 revidiert)
  - Berufsgeheimnis
  - FINMA Rundschreiben 2018/3 Outsourcing
  - FINMA Rundschreiben 2023/1 Operationelle Risiken/Resilienz
  - Gute Cloud Praxis
- **Beurteilungs- und Informationsbedarf**
  - Einhaltung interner Vorgaben, Risikomanagement, IKS
  - Entscheidgrundlage für das Management
  - Prüfung durch die bankengesetzliche externe Prüfstelle, FINMA

Was ist zu tun?

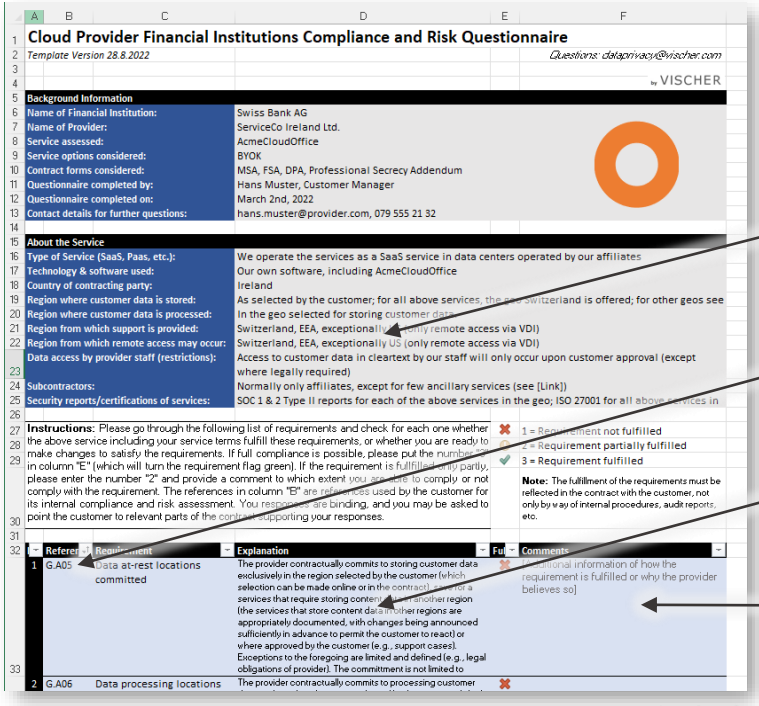
- **Provider evaluieren**
  - Leistungen und Verträge abfragen
- **Projekt definieren und ausarbeiten**
  - Worum es geht (M365 vs. Azure), warum und was geplant ist
  - Beschreibung aus Datensicht inkl. Schutzbedarfsanalyse
  - Massnahmen (inkl. Verträge) ausarbeiten und dokumentieren
  - Risikoanalysen durchführen (InfoSec, DSFA, Lawful Access)
- **Projekt auf Compliance und Gesamtrisiken prüfen**
  - Welche Rundschreiben kommen zur Anwendung?
  - Sind die rechtlichen Vorgaben erfüllt?
  - Welche Risiken bestehen für das Finanzinstitut

CCRA-FI

Zeitlicher Ablauf im Projekt



Vorbereitung: Provider evaluieren (optional)



Cloud Provider Financial Institutions Compliance and Risk Questionnaire

Template Version 28.8.2022 — *Questions: dataprivacy@vischer.com*

VISCHER

Background Information	
Name of Financial Institution:	Swiss Bank AG
Name of Provider:	ServiceCo Ireland Ltd.
Service assessed:	AcmeCloudOffice
Service options considered:	BYOK
Contract forms considered:	MSA, FSA, DPA, Professional Secrecy Addendum
Questionnaire completed by:	Hans Muster, Customer Manager
Questionnaire completed on:	March 2nd, 2022
Contact details for further questions:	hans.muster@provider.com, 079 555 21 32

About the Service	
Type of Service (SaaS, Paas, etc.):	We operate the services as a SaaS service in data centers operated by our affiliates
Technology & software used:	Our own software, including AcmeCloudOffice
Country of contracting party:	Ireland
Region where customer data is stored:	As selected by the customer; for all above services, the geo Switzerland is offered; for other geos see
Region where customer data is processed:	In the geo selected for storing customer data
Region from which support is provided:	Switzerland, EEA, exceptionally [illegible] (only remote access via VDI)
Region from which remote access may occur:	Switzerland, EEA, exceptionally US (only remote access via VDI)
Data access by provider staff (restrictions):	Access to customer data in cleartext by our staff will only occur upon customer approval (except where legally required)
Subcontractors:	Normally only affiliates, except for few ancillary services (see [Link])
Security reports/certifications of services:	SOC 1 & 2 Type II reports for each of the above services in the geo; ISO 27001 for all above services in

Instructions: Please go through the following list of requirements and check for each one whether the above service including your service terms fulfill these requirements, or whether you are ready to make changes to satisfy the requirements. If full compliance is possible, please put the number "3" in column "E" (which will turn the requirement flag green). If the requirement is fulfilled only partly, please enter the number "2" and provide a comment to which extent you are able to comply or not comply with the requirement. The references in column "B" are references used by the customer for its internal compliance and risk assessment. You responses are binding, and you may be asked to point the customer to relevant parts of the contract supporting your responses.

✖ 1 = Requirement not fulfilled
[illegible] = Requirement partially fulfilled
✔ 3 = Requirement fulfilled

Note: The fulfillment of the requirements must be reflected in the contract with the customer, not only by way of internal procedures, audit reports, etc.

	Referen	Requirement	Explanation	Ful	Comments
1	G.A05	Data at-rest locations committed	The provider contractually commits to storing customer data exclusively in the region selected by the customer (which selection can be made online or in the contract), except in services that require storing content in another region (the services that store content data in other regions are appropriately documented, with changes being announced sufficiently in advance to permit the customer to react) or where approved by the customer (e.g., support cases). Exceptions to the foregoing are limited and defined (e.g., legal obligations of provider). The commitment is not limited to	✖	Additional information of how the requirement is fulfilled or why the provider believes so)
2	G.A06	Data processing locations	The provider contractually commits to processing customer	✖	

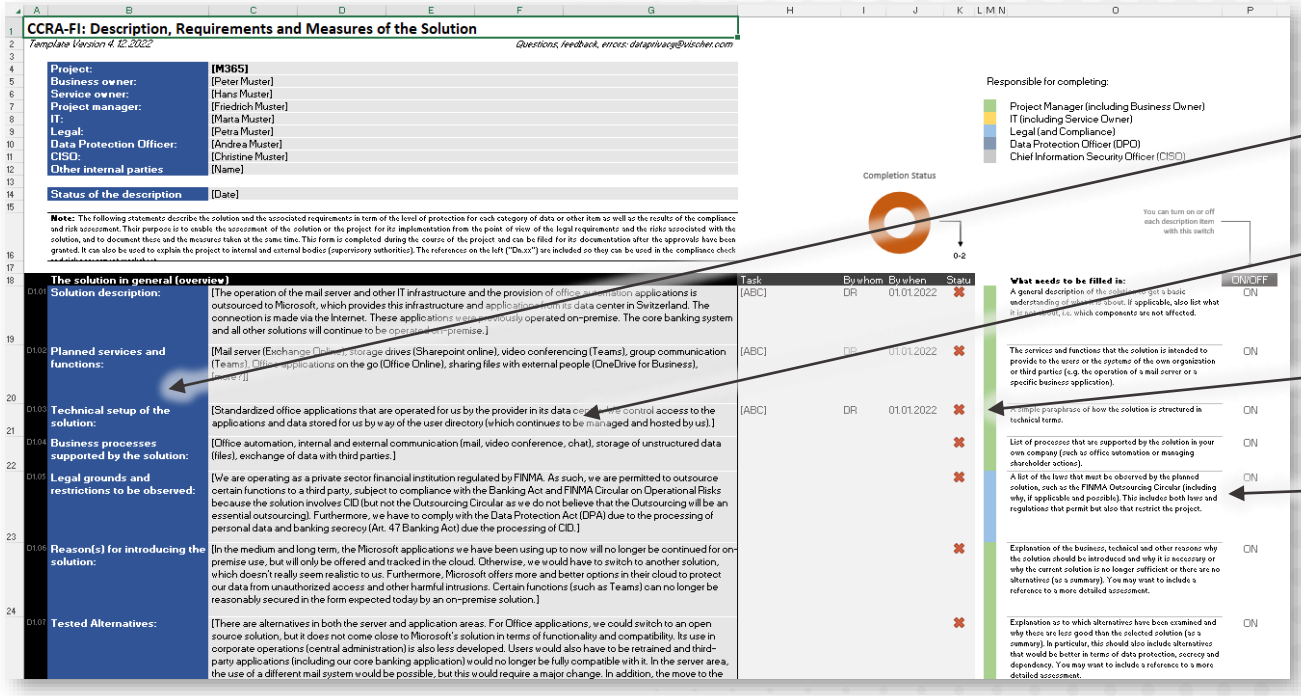
Angaben zum Service (des Providers)

Referenz auf Anforderung gemäss CCRA-FI-Methodik

Vorgabe an den Provider

Stellungnahme des Providers inkl. Fundstelle im Vertrag

Schritt 1: Beschreibung, Schuban, Massnahmen



Was es braucht

Inhalt oder Verweis auf Unterlagen

Wer es ausfüllen muss

Hilfestellung

Welche Konzepte und Unterlagen?

- **Konfigurationskonzept**
- **IAM**-Konzept (wer hat worauf Zugang)
- **BCM**-Konzept (inkl. Frage der Backups)
- **Exit**-Konzept
- **Weisungen**, Schulung
- **Datenschutzerklärung**
- **Personalplanung**, Einsatz externer **Dienstleister**
- **Verträge** (Service-Vereinbarung, AVV mit Schweizer Anpassungen, Professional Secrecy Addendum, Financial Services Addendum)

Welche Massnahmen treffen?

- **Berufsgeheimnis und Datenschutz**
  - Europäische Gegenpartei (z.B. Microsoft Ireland Operations Ltd.)
  - Datenhaltung in der Schweiz
  - Verschlüsselung von Daten (aber kein "bring-your-own-key")
  - 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)

Schritt 2: Spezifische Risikoanalysen

- **Analyse aus Sicht Informationssicherheit**
  - Ergebnis ist Risikoeinschätzung und Liste der TOMS
  - Insbesondere auch zur Konfiguration des Cloud-Service
- **Foreign Lawful Access Risk Assessment (FLARA)**
  - Risiko eines ausländischen Behörenzugriffs
- **Datenschutz-Folgenabschätzung (DSFA)**
  - Welche unerwünschten Nachteile für Betroffene hat das Projekt?
  - Welche Massnahmen treffen wir dagegen?

Beurteilung ausländischer Lawful Access

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

Schritt 5: Gesamtbeurteilung		
Wahrscheinlichkeit, dass sich die Frage eines Lawful Access über den Cloud-Provider überhaupt stellt (1 Fall in der Periode = 100%)		6.25%
Wahrscheinlichkeit, dass es in diesen Fällen trotz der Gegenmassnahmen[14)] zu einem erfolgreichen Lawful Access durch die betreffenden ausländischen Behörden kommt		2.84%
Wahrscheinlichkeit, dass es zusätzlich zu einem erfolgreichen Lawful Access durch einen ausländischen Nachrichtendienst ohne Rechtsweggarantie kommt (trotz der Gegenmassnahmen[14)])		0.40%
Gesamtwahrscheinlichkeit eines erfolgreichen Lawful Access über den Cloud-Provider in der Betrachtungsperiode:* **		0.58%
Umschreibung in Worten (basierend auf Hillson****):	Sehr tief	
Soviele Jahre braucht es, damit es mit einer Wahrscheinlichkeit von **90 Prozent** mindestens ein Mal zu einem Lawful Access kommt:		1'988
Soviele Jahre braucht es, damit es mit einer Wahrscheinlichkeit von **50 Prozent** mindestens ein Mal zu einem Lawful Access kommt:		598
… unter der Annahme, dass die Wahrscheinlichkeit sich über Zeit weder erhöht noch reduziert (wie bei einem Münzwurf)		

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.
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 geheimnisgeschützten 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.

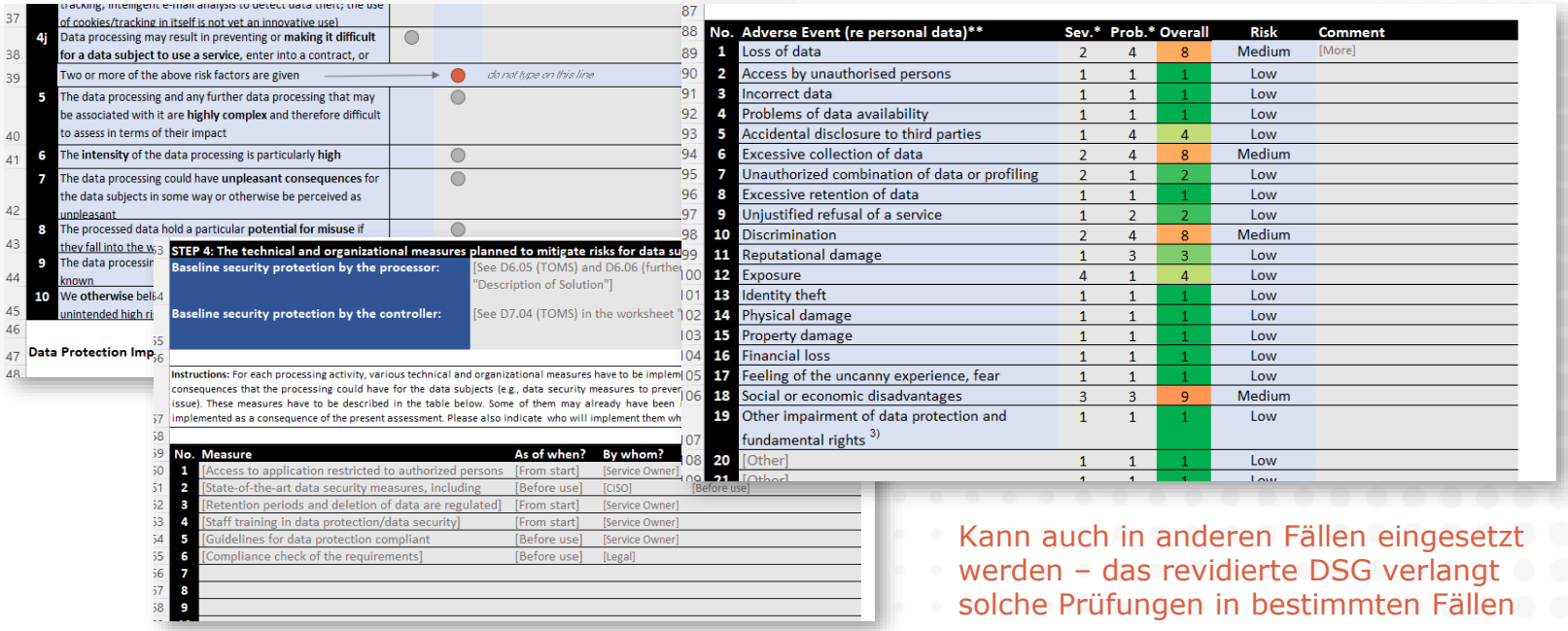
Bundeskanzlei: "Gute Praxis"

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

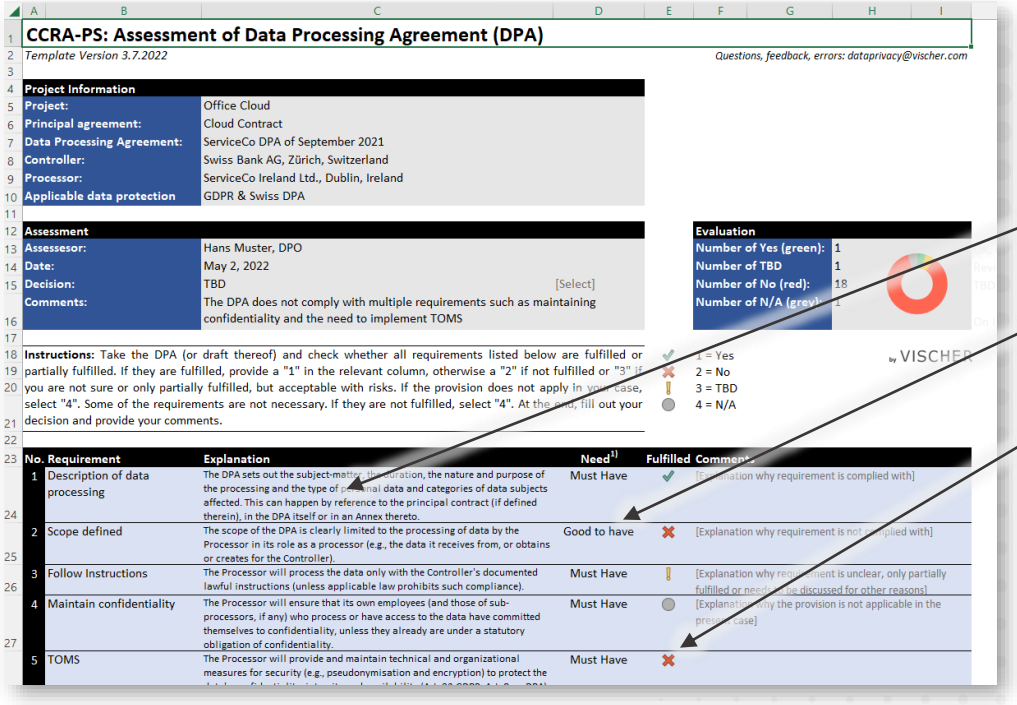
VISCHER

Datenschutz-Folgenabschätzung (DSFA)



Kann auch in anderen Fällen eingesetzt werden – das revidierte DSG verlangt solche Prüfungen in bestimmten Fällen

Schritt 3: Prüfung des AVV/DPA



CCRA-PS: Assessment of Data Processing Agreement (DPA)

Template Version 3.7.2022 — *Questions, feedback, errors: dataprivacy@vischer.com*

Project Information	
Project:	Office Cloud
Principal agreement:	Cloud Contract
Data Processing Agreement:	ServiceCo DPA of September 2021
Controller:	Swiss Bank AG, Zürich, Switzerland
Processor:	ServiceCo Ireland Ltd., Dublin, Ireland
Applicable data protection	GDPR & Swiss DPA

Assessment		
Assessesor:	Hans Muster, DPO	
Date:	May 2, 2022	
Decision:	TBD	[Select]
Comments:	The DPA does not comply with multiple requirements such as maintaining confidentiality and the need to implement TOMS	

Evaluation	
Number of Yes (green):	1
Number of TBD	1
Number of No (red):	18
Number of N/A (grey)	1

Instructions: Take the DPA (or draft thereof) and check whether all requirements listed below are fulfilled or partially fulfilled. If they are fulfilled, provide a "1" in the relevant column, otherwise a "2" if not fulfilled or "3" if you are not sure or only partially fulfilled, but acceptable with risks. If the provision does not apply in your case, select "4". Some of the requirements are not necessary. If they are not fulfilled, select "4". At the end, fill out your decision and provide your comments.

1 = Yes
2 = No
3 = TBD
4 = N/A

by VISCHER

No.	Requirement	Explanation	Need[1]	Fulfilled	Comment
1	Description of data processing	The DPA sets out the subject-matter, the duration, the nature and purpose of the processing and the type of personal data and categories of data subjects affected. This can happen by reference to the principal contract (if defined therein), in the DPA itself or in an Annex thereto.	Must Have	✓	[Explanation why requirement is complied with]
2	Scope defined	The scope of the DPA is clearly limited to the processing of data by the Processor in its role as a processor (e.g., the data it receives from, or obtains or creates for the Controller).	Good to have	✗	[Explanation why requirement is not complied with]
3	Follow Instructions	The Processor will process the data only with the Controller's documented lawful instructions (unless applicable law prohibits such compliance).	Must Have	!	[Explanation why requirement is unclear, only partially fulfilled or need to be discussed for other reasons]
4	Maintain confidentiality	The Processor will ensure that its own employees (and those of sub-processors, if any) who process or have access to the data have committed themselves to confidentiality, unless they already are under a statutory obligation of confidentiality.	Must Have	○	[Explanation why the provision is not applicable in the present case]
5	TOMS	The Processor will provide and maintain technical and organizational measures for security (e.g., pseudonymisation and encryption) to protect the	Must Have	✗	

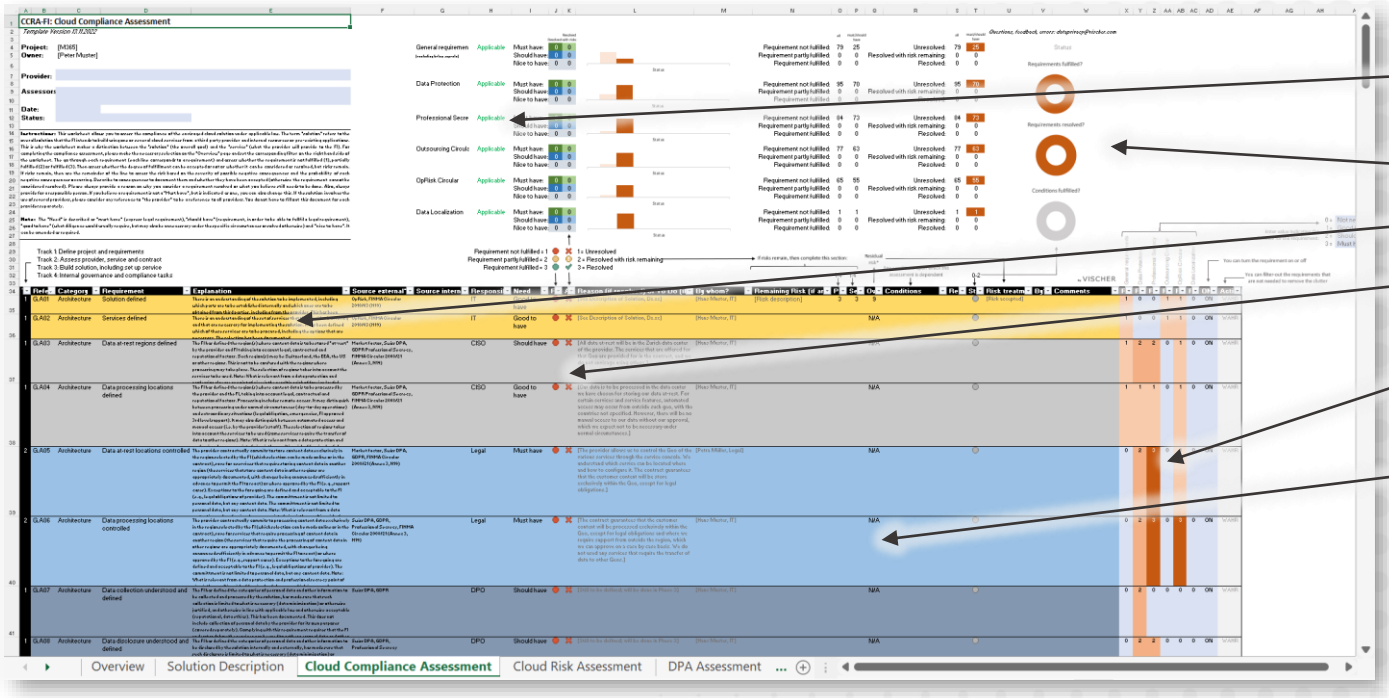
Anforderung

Zwingend oder nicht

Erfüllungsgrad

Kann auch in anderen Fällen eingesetzt werden – das revidierte DSG stellt fehlende AVV unter Strafe

Schritt 4: Prüfung der Anforderungen



Welche Vorgaben sollen gelten?

Dashboard

Anforderung

Erfüllungsgrad

Relevanz betr. die gewählten Vorgaben

Ggf. Restrisiko

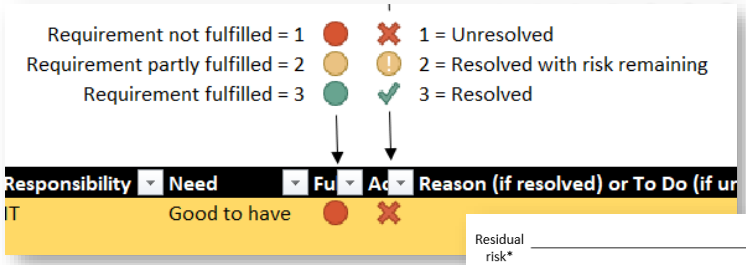
148

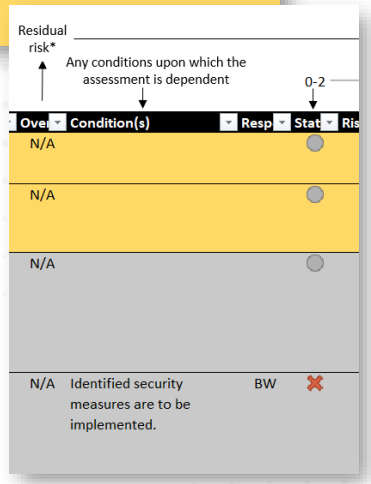
Schritt 4: Prüfung der Anforderungen

	be achieved by use of backups, but also mirrors.	
Provider has adequate BCM measures in place	The provider has commited to BCM measures that ensure an ongoing service delivery and service restoration in the event of a disaster and other extraordinary circumstances. They have been reviewed by the FI and they meet the FI's needs and have been aligned with FI's own BCM measures. If the BCM measures are optional, the FI will select these options. For the purpose of disaster recovery, the FI has also made sure that any backup data center is geographically sufficiently separated from the "normal" data center.	FINMA Circular 2018/03 (N25), FINMA Circular 2008/21 (N135.11, N136)
Continuation of business ensured in	It is ensured that in the event of a failure of the solution or parts of it (whether	FINMA Circular 2018/03 (N25),

Should have	Microsoft has and will maintain for the duration of the Enrollment adequate business continuity and disaster recovery plans intended to restore normal operations and the proper provision of the Online Services in the event of an emergency and in accordance with applicable laws and regulations. (clause 7(e) M453)	VISCI
Must have		

Schritt 4: Prüfung der Anforderungen

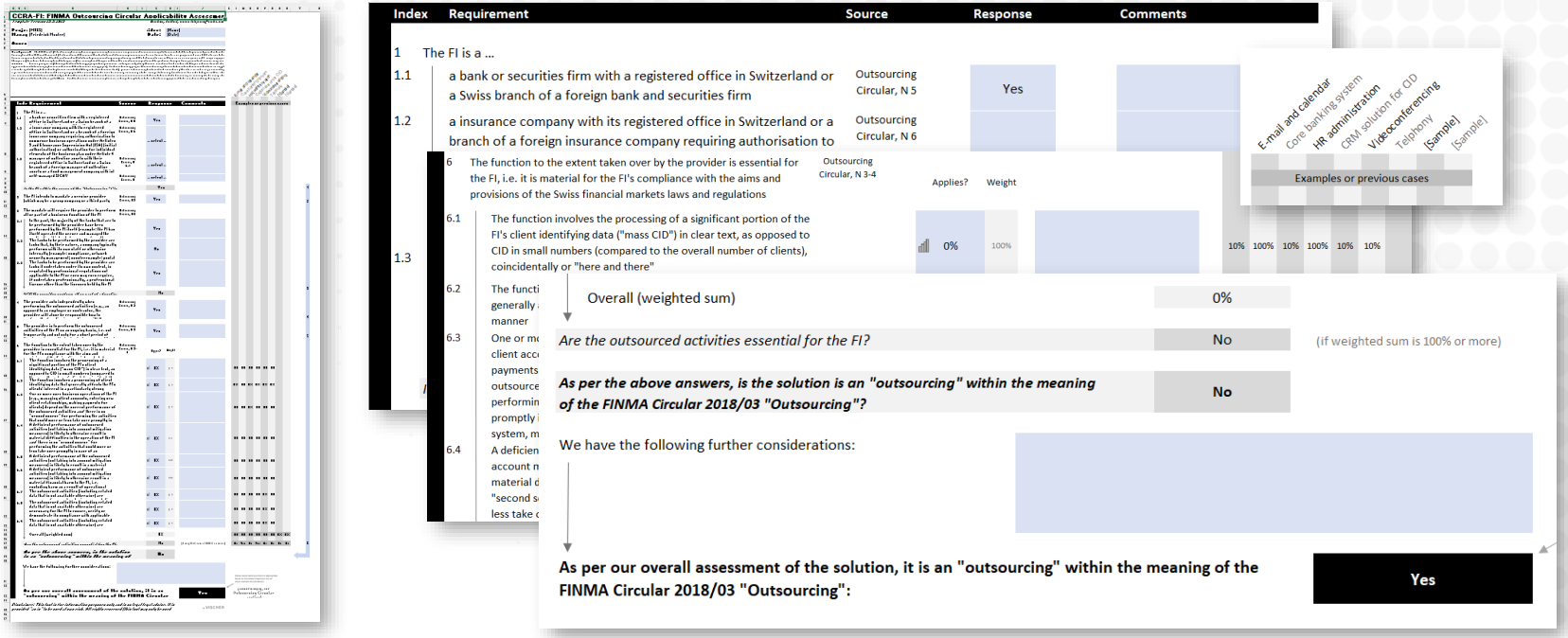




Alle Anforderungen werden im Hinblick auf die Erfüllung der definierten Massnahmen beurteilt.

Swiss law is not applicable. Instead, the FI will have to raise claims under Irish law and before Irish courts. This will make it more difficult to and costly pursue claims. Also, an Irish court may offer less protection than a Swiss one. But legal action remains reasonably possible.	2	3	6	N/A

Anwendbarkeit Outsourcing-Rundschreiben



Operator Access und Geo Restrictions

CCRA-FI: Assessment of Cloud Provider Access and Geo Restrictions

Template Version 29.3.2023

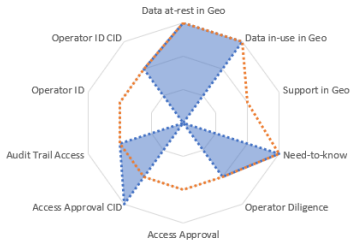
Questions, feedback, errors: dataprivacy@vischer.com

Project:

Provider:

Assessor:

Date:



Comments:

Instructions: When evaluating a cloud service provider, the location of the FI's data as well as access to such data is a critical risk and compliance factor. However, the various forms of access, processing locations and logging of such processing are to be carefully distinguished. The following table provides for the requirements that apply based on the obligations a FI may have under professional secrecy (e.g., bank secrecy), under the FINMA Circular 2023/1 on operational risks and resilience for banks and as per the FI's own general terms & conditions (GTC). Please complete the last column ("**Degree of Fulfillment**") by selecting the appropriate response in view of the provider, contract and services under consideration. The chart on the left will give you an overview on the situation and may help you to compare different scenarios and providers. You can enter your own minimum requirements in the column with the heading "**Min.**".

Requirement	Description	Legal Reason	Min. (0-3)	Degree of Fullfillment (0-3)
Data at-rest in Geo	Customer content is stored only in the selected geo, unless approved otherwise by customer to to comply with a lawful access request.	Professional secrecy,[1] Circular 2023/1 (N79),[2] pot.	3	3 - committed
Data in-use in Geo	Customer content is processed only in the selected geo, unless approved otherwise by customer or to comply with a lawful access request.[4]	Professional secrecy,[1] Circular 2023/1 (N79),[2] pot.	3	3 - committed
Support in Geo	All provider support that requires access to customer content in clear-text is available on-site or at least in geo.	Professional secrecy,[1] Circular 2023/1 (N79),[2] pot.	2	0 - not committed
Need-to-know	Operator access to customer content is only permitted on a strict need-to-know and least-privilege basis and privileges are verified regularly.	Professional secrecy,[1] Circular 2023/1 (N78, N79)[2]	3	3 - committed
Operator Diligence	Operators with access to customer content are carefully selected, monitored and trained (commensurate to their privileges).[5]	Professional secrecy,[1] Circular 2023/1 (N72, N76,	2	2 - committed, with the measures remaining unclear
Access Approval	No operator access to customer content (with privileges to impact availability) occurs without customer approval or a lawful access request.	Circular 2023/1 (N72, N76, N78, N80)[2],[6]	2	0 - not committed
Access Approval CID	No operator access to customer content in clear-text (with read or change privileges) occurs without customer approval or a lawful access request.	Professional secrecy,[1] Circular 2023/1 (N72, N76, N78, N80)[2],[6]	2	3 - committed
Audit Trail Access	Any operator access to customer content is logged by audit trails available to the customer, except where prohibited by law.	Professional secrecy,[1] Circular 2023/1 (N80,	2	2 - committed, except in BCM cases
Operator ID	Operators with access to customer content (with privileges to impact availability) are identified towards the FI.	Circular 2023/1 (N80)[2],[8]	2	0 - not committed
Operator ID CID	Operators with acess to customer data in clear-text (with read or change privileges = confidentiality, integrity) are identified towards the FI.	Circular 2023/1 (N80)[2],[8]	2	2 - committed, only by way of an audit request

[1] This requirement is for compliance with professional secrecy obligations, as it has an impact on the probability of a successful foreign lawful access to client data (to be considered in a foreign lawful access risk

[2] For the present purposes, we assume that customer content contains "critical data" in the meaning of the FINMA Circular 2023/1.

[3] This includes remote access for support or other purposes (i.e. any remote access from outside the geo, even if only for an automated process, is a violation of this requirement).

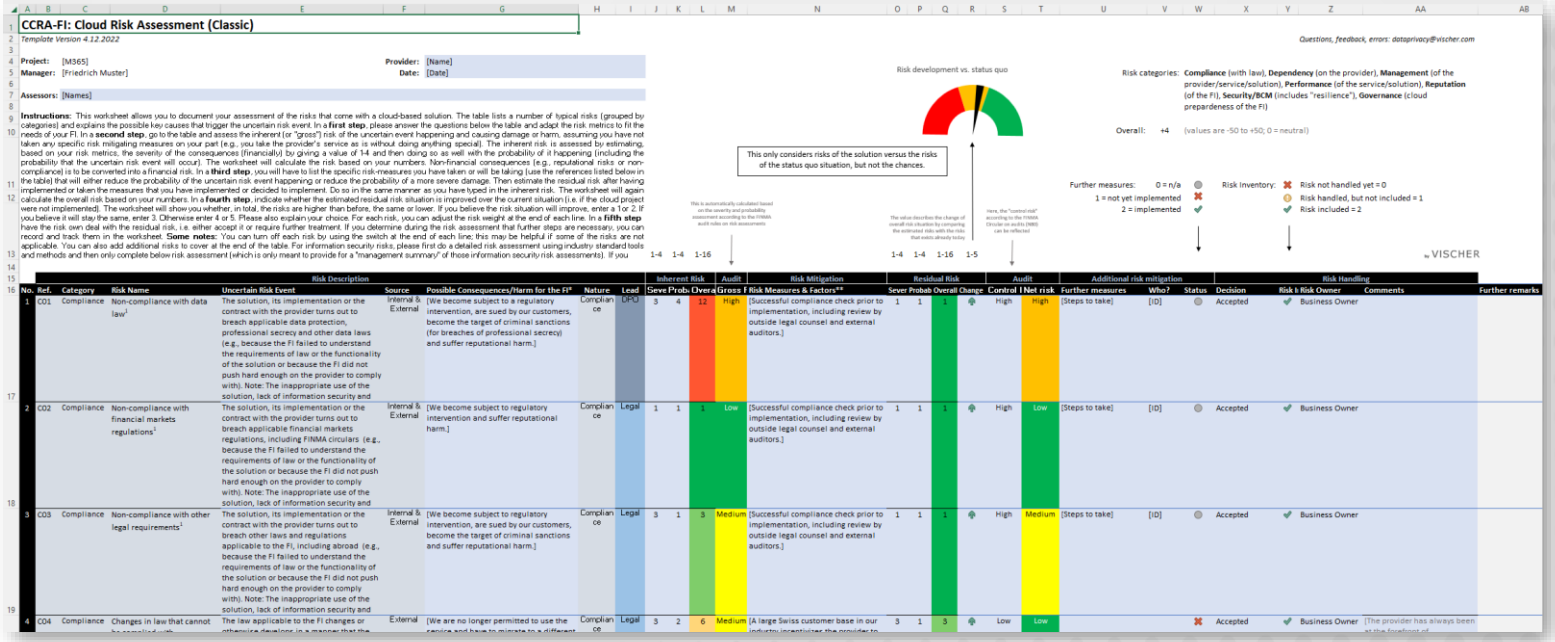
[4] This requirement is relevant if the GTC of the FI were to promise that no data will be passed on to the service provider that can identify the client.

[5] Careful selection includes appropriate vetting (e.g., background checks); monitoring includes audit trails, review of logs, four-eye-principle, etc. (see FINMA Circular 2023/1, footnote 20).

[6] The FI may wish to restrict access to customer content if (i) this is necessary pursuant to its security standards, or (ii) the provider is not able to provide a list of operators or not provide audit trails of each operator

[7] As per FINMA Circular 2023/1, N82, the "service providers must be monitored and checked periodically as part of the institution's internal control system".

Schritt 5: Risikobeurteilung



CCRA-FI: Cloud Risk Assessment (Classic)

Template Version 4.12.2022

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 1or 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

Questions, feedback, errors: dataprivacy@vischer.com

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), **Management** (of the provider/service/solution), **Performance** (of the service/solution), **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

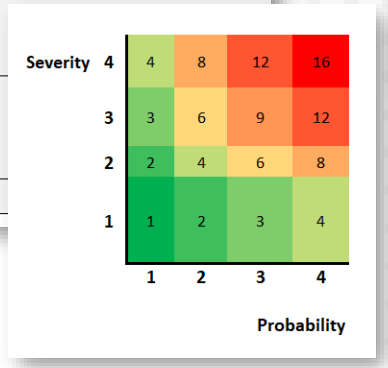
1-4 1-4 1-16 1-4 1-4 1-16 1-5

VISCHER

No.	Ref.	Category	Risk Name	Uncertain Risk Event	Source	Possible Consequences/Harm for the FI*	Nature	Lead	Inherent Risk: Severity	Inherent Risk: Probability	Inherent Risk: Overall	Inherent Risk: Gross Risk	Risk Mitigation: Risk Measures & Factors**	Residual Risk: Severity	Residual Risk: Probability	Residual Risk: Overall	Audit: Change	Audit: Control Level	Audit: Net risk	Additional risk mitigation: Further measures	Additional risk mitigation: Who?	Additional risk mitigation: Status	Risk Handling: Decision	Risk Handling: Risk Owner	Risk Handling: Comments	Further remarks
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	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	High	[Successful compliance check prior to implementation, including review by outside legal counsel and external auditors.]	1	1	1		High	High	[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	Internal & External	[We become subject to regulatory intervention and suffer reputational harm.]	Compliance	Legal	1	1	1	Low	[Successful compliance check prior to implementation, including review by outside legal counsel and external auditors.]	1	1	1		High	Low	[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	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	Medium	[Successful compliance check prior to implementation, including review by outside legal counsel and external auditors.]	1	1	1		High	Medium	[Steps to take]	[ID]		Accepted	Business Owner		
4	C04	Compliance	Changes in law that cannot	The law applicable to the FI changes or	External	[We are no longer permitted to use the	Compliance	Legal	3	2	6	Medium	[A large Swiss customer base in our	3	1	3		Low	Low				Accepted	Business Owner	[The provider has always been	

Schritt 5: Risikobeurteilung

Question	Answer
What are the financial, legal and reputational consequences if the customer data to be stored or otherwise processed by the solution is disclosed to an unauthorized third party?	
What action can the regulator take against the FI in case of non-compliance with applicable law?	
What is the reputation of the provider in terms of stability, long-term product development and compliance with law and contractual obligations?	
What are the financial, legal and reputational consequences to the FI if the solution or key functionality is no longer available for a medium term period (with no replacement available)?	
What are the financial, legal and reputational consequences to the FI if the solution or key functionality is no longer available for a long term period (with no replacement available)?	
What does "medium" and "long" term mean?	



Probability of these consequence	Level	FINMA
Very rare event (once every 100+ years)	1	Low
Rare even (once every 25-100 years)	2	Medium
Possible (once every 5-25 years)	3	High
Frequent (once every 1-5 years)	4	Very high

Severity of consequences for the FI	Level	FINMA
Non-material consequences for the FI (financial damage under CHF 500k or immaterial reputational damage or legal consequences)	1	Low
Material consequences for the FI (financial damage under CHF 10m or material reputational damage or legal consequences)	2	Medium
Material consequences for the FI (financial damage under CHF 10m or material reputational damage or legal consequences)	3	High
Catastrophic consequences for the FI (financial damage beyond 100m or catastrophic reputational damage or legal consequences)	4	Very high

Severity	Probability	Inherent risk	Gross risk
4	4	16	Very high
4	3	12	Very high
4	2	8	High
4	1	4	High
3	4	12	High
3	3	9	High
3	2	6	Medium
3	1	3	Medium
2	4	8	Medium
2	3	6	Medium
2	2	4	Medium
2	1	2	Low
1	4	4	Low
1	3	3	Low
1	2	2	Low
1	1	1	Low

Risk table according to FINMA Circular 2013/3 (Audits), N23

Betrachtungszeitraum
i.d.R. fünf Jahre.

Schritt 5: Risikobeurteilung

Risk Description						Inherent Risk			Audit
Risk Name	**Uncertain Risk Event**	**Source**	**Possible Consequences/Harm for the FI***	**Nature**	**Lead**	**Severit**	**Probabi**	**Overall**	**Gross Risk**
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 covered elsewhere.	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	High

Risk Mitigation	Residual Risk				Audit		Additional risk mitigation			Risk Handling		
Risk Measures & Factors**	**Sever**	**Probab**	**Overall**	**Change**	**Control Risk**	**Net risk**	**Further measures**	**Who?**	**Status**	**Decision**	**Risk Ir**	**Risk Owner**	**Comments**
[Successful compliance check prior to implementation, including review by outside legal counsel and external auditors.]	1	1	1	↑	High	High	[Steps to take]	[ID]		Accepted	✓	Business Owner	

Hoch: Die Prüfgesellschaft hat bisher keine Prüfungshandlungen zum Vorhandensein und Funktionieren von Kontrollen durchgeführt oder hat keine Klarheit, dass Kontrollen bestehen oder hat die Kontrollen als nicht wirksam beurteilt oder es gibt Hinweise, dass das Kontrollsystem seit der letzten Intervention wesentlich angepasst wurde.

Schritt 5: Risikobeurteilung

Net risk amounts (k):

	Sum	Max	Damage Category
Overall:	**1**	**1**	
Group A:	-	-	Migration costs
Group B:	1	1	
Group C:	-	-	
Group D:	-	-	

s can be changed.

If the uncertain risk event occurs, then we need to understand the probability of damage

Enter the probability of damage for each range (combined = 100%)

that exists already today

1-5

ce	Risk Consequences		Financial consequence for FI despite mitigation (residu						
Probability	**Possible Consequences/Harm for the FI***	**Mitigation Measures & Factors****	**100 k**	**1 000 k**	**25 000 k**	**1 000 000 k**	**Gross (k)**	**Net (k)**	**Change**
25%	[We become subject to regulatory intervention and suffer reputational harm. If a violation of data law or a data breach occurs, the responsible individuals may be subject to criminal sanctions for not having provided for the necessary contractual provisions. Affected third parties may sue us.]	[M14, M20; Successful compliance check prior to implementation, including review by outside legal counsel and external auditors.]	50%	40%	10%	0%	3	1	
10%	[We become subject to regulatory intervention and	[M14, M20; Successful compliance check prior to	0%	0%	0%	0%	0	0	

Bei der "Weighted Average Risk"-Methode wird zuerst die Eintretens-wahrscheinlichkeit der ungewissen Ursache beurteilt (unter 100%) und dann die Wahrscheinlichkeiten der verschiedenen Schadensklassen (100%)

Finanzrisiko (Brutto, Netto)

Veränderung gegenüber bisher

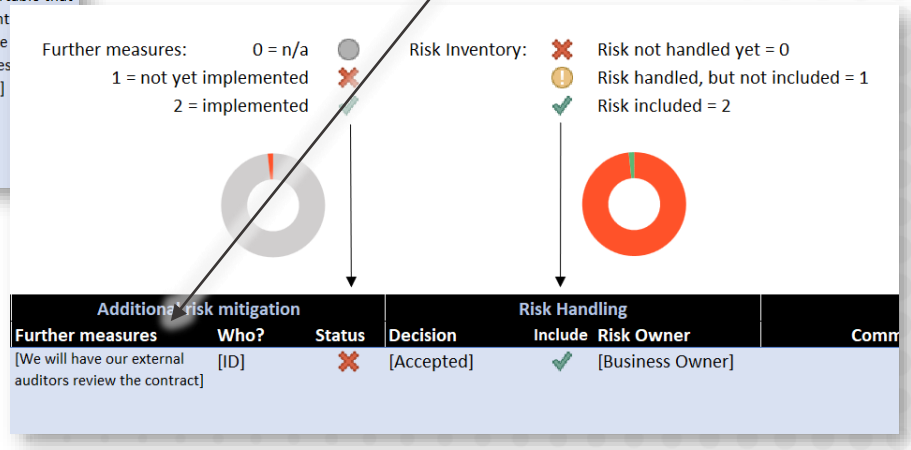
Schritt 5: Risikobeurteilung

Assess the probability of a serious regulatory sanction or criminal sanction in case of the uncertain risk event occurring

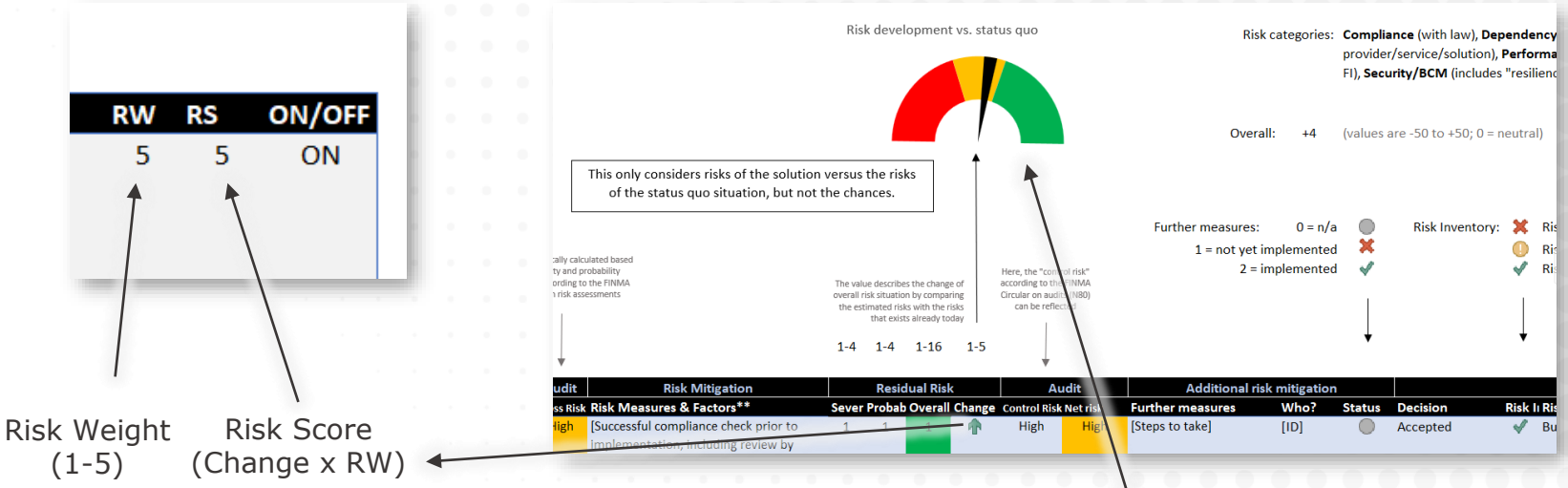
Serious Regulatory Sanctions			Criminal Sanctions for FI		
Gross (%)	Net (%)	Comments	Gross (%)	Net (%)	Comments
10%	3%	[We don't expect a situation that we cannot cure.]	10%	1%	[We are comfortable that at least the cont provides for the provisions neces protecting CID.]

Nicht finanzielle Risiken

Weitere Massnahmen, die während der Risikobeurteilung ermittelt wurden



Schritt 5: Risikobeurteilung



Abschluss

Tracking der ausstehenden Arbeiten durch das Projektmanagement

- **Cover-Memo**
  - Überblick
  - Wichtigste Erkenntnisse aus spezifischen und genereller Risikobeurteilung (z.B. die drei grössten Risiken)
  - Wichtigste Erkenntnisse aus Compliance-Beurteilung
  - Wichtigste bzw. teuerste offene Massnahmen
- **Beilagen**
  - CCRA-FI als PDF (vorher nicht benötigten Blätter löschen)
  - Risikobeurteilung Informationssicherheit
  - FLARA
  - Massnahmen, die umgesetzt werden müssen

Die fünf Fragen, die gestellt werden sollten …

	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 Berufs- und Amtsgeheimnisses 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 Berufs- und Amtsgeheimnis 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 das Organ haben können, richtig einschätzen, steuern und in Bezug zu den Restrisiken stellen, die wir sonst bzw. sowieso haben?	Welche weiteren Bedrohungen, welche für das Organ 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

Fragen & Diskussion

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