Cloud Risk Assessment. The most discussed issue and the real ones David Rosenthal, Partner, VISCHER AG October 19, 2022

The discussed issue: Foreign Lawful Access



Can we address it?

- We encrypt data "in-transit
- We choose a contract party located in Europe
- We choose Switzerland as storage location
- We prevent day-to-day-access from the U.S.
- We require the provider to legally defend our data
- → This will not protect our data technically, but provide the provider a legal argument to reject foreign lawful access requests
 - Example: US-law principle of "p/c/c"
 - Example: US-law principle of "International Comity"

Within two years, all major hyperscalers will be offering their services (almost) exclusively out of Europe





ad-Computing: Ricibabourtailung since Lowful Access durch and Indische

Robert Balant

angefage der Kielfebrurbelbag deftaler

How do we assess it?

Excel: https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx Vgl. also see the FAQ at https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf

35						the data specifically requested by an							
d)			wider, the subcontractor or its parent company, respectively, is located within authority (prerequisite no. 4)	100%	100%	% The Provider reserves the right to provide the service also for subcontractors is under the jurisdiction of the US authorities							
e)	Probability that	despite	the technically limited access and the technical and organizational lace ¹⁴), the authority is permitted to order the provider, its subcontractor or the				rule, the employees of the provider and its subcontractors do not hat he one hand, this is technically ensured by the concept of encryption						
na Maratan Santan Angelan ang Kangana Santan Angelan Santan Santan Angelan Angelan Santan Angelan Santan Santan Angelan Santan Angelan Santan Santan Santan Santan Santan Santan Santan Santan Santan	parent compan	ny, resp	ectively, to obtain access to the data and produce it to the authority in plain										
v basen et nota de un prior de transmission de la del e de la combana de la dela de la del del e obtenendo en de de compositiones des endes de composition de la constitución de la del e dela dela composition de la constitución de la del endes de la compositiones de la constitución de la dela endes de la compositiones de la constitución de la dela endes de la compositiones de la constitución de la dela endes de la compositiones de la constitución de la dela endes de la compositiones de la constitución de la dela endes de la constitución de la constitución de la dela endes de la constitución de la constitución de la dela endes de la constitución de la constitución de la dela endes de la constitución de la constitución de la dela endes de la dela dela dela dela dela dela del	text ⁷⁾ (prerequisi												
distriction for and existing and		55											
and of a final star of the second star of the secon		56 57	Step 5: Overall assessment										
			Probability that the question of lawful access via the cloud provid	ler will arise at all (1 case	in the period = 100%)	6.25%	ors do not have of encryption in provider, contro vees, which in tu subcontractor					
and existential data are used for an and but an in-but has the bard of the state in the state of the state of the state in the state of the state of the state of the state of the state of the state of the state of the state of the state of the state of the state of the state of the state of the state of the state of the state of the state of				bility of successful lawful access by the foreign authorities concerned in these cases despite in the countermeasures ¹⁴⁾									
statute and a statute stat			Probability of additional successful lawful access by a foreign in	ess via the cloud provider will arise at all (1 case in the period = 100%) the foreign authorities concerned in these cases despite in the countermeasur access by a foreign intelligence service where there is no guarantee of legal re	of legal recourse (despite	0.40%							
t)	Probability that liability of emplo	if d ₃₀	countermeasures ¹⁴⁾)				0.4070						
aarthogaado Berechillung kerr	and realistic, ar	^{0ye} 31											
candra di Maller M, A za e de Veren este quade dei na dire candi di di di di este dire si interna in 1 la fi data este cina e l'apole can di finanza di este da can este a di finanza di di este candi di finanzia di di este di di este candi di finanzia di di este di di este candi di finanzia di este di di di di este di este di este di este di di di este di di este di este di este di este di este di di di di este di este di este di este di este di este di este di di este di este di di este di este di di este di este di di este di este di di este di este di di este di este	(prerequisite no. 6)	<pre>/</pre>	Overall probability of a successful lawful access via the	cloud provider in the o	bservation period:*	***	0.58%						
nadorstilalisti, dan die Franklin aller anderstilalisti, an ist, ist film in Back Receile aller in Salta and einer aller aller aller aller aller aller aller aller aller		53					r reserves the right to provide the service also from the U ors is under the jurisdiction of the US authonities. le employees of the provider and its subcontractors do in hand, this is technically ensured by the concept of encry is defined in the directory (which we, and not the provider ontractually prohibited to grant access to employees, wh within the provider's organization. In addition, the subcon 6.25% es ¹⁴ . 2.84%	for m					
		54	Description in words (based on Hillson****):				Very low						
	netra Last Maria M	65											
	Section and Sectio	66	The number of years it takes for a lawful access to occur at leas				1'988						
	and the second s	67	The number of years it takes for a lawful access to occur at leas	•	probability:		598						
		68	assuming that the probability neither increases nor decreases over time (like to	ssing a coin)									
		66											

Is the method recognized?

- Opinion of the Swiss Federal Chancellery: "Good Practice"
- Canton of Zurich: Our new "Standard" approach
- A Swiss law prosecutor: A "suitable approach"
- Established in Switzerland, promoted internationally (e.g., IAPP)
 - Swiss banks and other professional secrecy holders
 - Providers (e.g., Zoom)
 - Public institutions (e.g., Dutch government)
 - However, its use is not quite trivial ...
- Opposition by the Federal Data Protection and Information Commissioner and some cantonal data protection authorities in Switzerland (promoting the zero-risk-approach)

What about "EO 14086"?

- Executive Order of the U.S. President of October 7, 2022
 - Intended to address the legal **deficiencies** identified in "Schrems II" with regard to "signals intelligence" undertaken by the U.S.
 - Establishes independent redress mechanism for data subjects from "qualifying states" (e.g., EU, UK, Switzerland, provided they permit data transfers to the U.S.)
- The US will **launch a program** that allows US companies to self-certify to comply with data protection (similar to the former "Privacy Shield" program) → can be used as a basis for transferring data to the US (without EU SCC)
 - Adequacy decision probably in spring 2023
- Only indirectly affects transfers based on the EU SCC

Various questions remain open - what will the ECJ say about the EO?

> The pressure to use this as a face-saving way out of the corner is IMHO high ...

The five questions management should really ask

	Strategy and general approach	Assessment of a specific project
Motivation & Alternatives	What are the key elements we hope to achieve by going to the cloud, and how well do we want to know about the alternatives?	What are the business, operational and other requirements for the project and why does the chosen solution outweigh other technologies (i.e. alternatives to the cloud), other cloud providers and the status quo?
Compliance	How do we go about systematically checking, documenting and ensuring compliance with our secrecy obligations and the various legal, regulatory and our own requirements throughout the life of a cloud project?	Do we comply with our secrecy obligations and the legal, regulatory and our own requirements with this project and how have we systematically checked, documented and ensured this for the entire duration of the envisaged cloud solution?
Organisation & Internal Control System (ICS)	What are we willing to do and require in order for our organization to understand, control and manage cloud providers and their solutions so that we can not only handle them properly, but also identify and address deviations from the intended target in a timely manner?	What precautions have we taken or are we taking to ensure that we understand, monitor and control the cloud provider and its cloud solution with our internal resources so well that we will be able to handle the cloud solution correctly in accordance with the requirements, detect deviations from the intended target in due time and eliminate them, including by having our ICS cover also the entire solution ("end-to-end")?
Business continuity	What are our requirements for business continuity in the event of an outage or data loss and for our ability to exit a cloud service in the short term (months) and medium term (12-18 months), and what level of effort are we willing to put into such ability?	What is our plan in the event that the cloud provider suddenly shuts down their service, the solution or our data is no longer available, or we need or want to move away from them or their solution in the short term (months) or medium term (12-18 months)?
Residual risk	How do we ensure that we properly assess and manage specific threats associated with a cloud project that could have significant consequences for the company, and how to we compare them with the residual risks we face otherwise or anyway?	What other threats does the cloud project pose that could have significant consequences for the company, how well do we have them under control, and how do the residual risks compare to the risks we would have without the project or anyway?

Structured Compliance & Risk Assessment

	Protection Requirement Analysis				Example as used for Swiss
and prove the second se	Third party data*	Confidentiality 🔽	Integrity 🔽	Availability	financial institutions
If the speed on at the null accurs on take 10 introductions and the president of the speed on the speed on the introduction of the black of the speed of the	CID	Very High	Very High	High	
Reference of the forest means the term product system of the forest means the term product system of the forest means the term product system of the forest means the term of the term of the term of the term of term of term of the term of	Employee data (accounts)	Select	High	Normal	The first step of
Process and section as a relative local factorial function of the transmission of the 1999 and sector for a relative local factor and the transmission of the factorial factor of the transmission of the factorial factor of the transmission of the factorial factor of the transmission of	Employee data (in communication and work products)	Select	Select	Select	assessing compliance is to gather the
⁶¹ Them are discussion in bulk houses on a particular scale to 4500 mg with some or advise, all the scale of an order of the scale to advise of the scale of an order of the scale of	Data of other individuals (in communication and work products)	Select	Select	Select	information and assess the level of protection
www.wessettioner.com	Employee data (usage)	Select	Select	Select	
4		Select	Select	Select	that is required
Construction C	* Note: This refers to all information processed by data prc	bcontractors) + 12 months (derived			
 Testing Franker, Senting Fr			expiration of the contr		
219 The Advances of the Adv	Alternate service provider in c service failure or emergency e 141		pleted by IT, which it p	rovides here]	

Structured Compliance & Risk Assessment

ternetimmer: This survivation of all training the term of the filter of a term is using the survivation maker of a birth of the among listness surveyers underlace). The gas thready on the dot (2) are fulfilled (3). There earlies the cases is the same term earlies the cases is the same term earlies the case is the same term of the interm of the same of the same of the same term of term of the same term of term o	I bill uring me ar zeoeral class a zereicar fr direix class locatores the "adobias" (blo are on glo are mother to a correspondent me for goviernaris (coch fino enrecepted than ar underker the daves of following encodence else of the fine to an arear the risk based on travities to associate on a davier to deconstant them travities to associate on a davier to deconstant them provide a resonance on using your consider on	ServiceGO) where the rate of the service applicable law. The same "patheter" relation where the service of the service factor that are service and the service of the service of the service factor that are service affirmed as the HTML of the service service are service that the service factor that are set to the service service are service and the service of the HTML of the service the service of the service that the service of the HTML of the service of the service of the service that the service of the HTML of the service of the service of the service service of definitions the service service of the HTML of the service of the service of the service service of definitions the service service of the HTML of the service the service of the HTML of the service the service of the HTML of the service service of the HTML of the service the service of the HTML of the service s	Track 2: Assess provider, service and Track 3: Build solution, including set up Track 4: Internal governance and comp Track 5: Foreign law (if applicable)	onBequirement par service Requireme	ot fulfilled = 1 tly fulfilled = 2	0 2 = Resolved with risk remaining	Group / Sviss Singapore EU requirements	Residual Risk Severity Residual Risk Probability	£ 1.4	Example as used for Swiss financial institutions
Refe Category G.A01 Architecture	Bequirement Solution defined	Explanation Three is a close understanding of the autobian take implemented, including which performs to be articularly and takish margares take distance of from this and takes in the action of from actions.		 Responsib Business Owner 	Need 🗾 Musthave	Reason (if resolved) or To Do (i See Project Description, Section 2)	* Bg whom? * Re [Hans Muster, IT]	emaining Risk (if au	S(* Pr* Ov * Comm N/A	nents -
	Services to be used defined Data at-rest in Switzerland	There is a closer understanding ublick redutiver as four view of a set of the provider is affecting utility implemented from the automian, including any and all appliant that the emoder affect within. The archeritan has been discovered. The context datain (and), have discovered in Submediand. However, this is	2018/63 (H19)	Business Owner Service Owner	Good to	 V [See Project Description, Section 2] V [All data at-rest will be in the Zurich data center 	(Hans Muster, IT) (Hans Muster, IT)		Track 1	Define project and requirements
G.A04 Architecture	Data at-rest in Europe	nartatoment about the la cotian of processing. The constent data is (only) stored on servers in Suitzerland, the EEA or UK.		Service Owner	have, TIA Good to	of the provider]	(Petra Millor, Legal)		Hack I.	benne project and requirements
G.A05 Architecture	Processing only in Switzerland	Houseon, this's natively noted that the lacotion of proceeding. In principal, the provider only proceeder the context data in Suitzerland, Lacothere is no attained of an inserval occurs from outride, exception exceptionalizitiestime.	GDPR Herket Fotter, Suiz DPA, GDPR	Service Owner	have, TIA Nice to have, TIA Factor	(Altough the service is primarily provided in Switzerland, access from outside Switzerland possible for the provision of the service and support, but wouldy no access to curtomar do	bee	reign lawful access (has in assessed separately)]	Track 2:	Assess provider, service and contract
G.A06 Architecture	Processing only in Europe	In principle, the provider only processor the content data in Suitzerland, the EEA or the UK, i.e. there is no extended or moreal access from outside,		Service Owner	Nice to have, TIA	in dear text)	[Petra Miller, Legal]		Track 3:	Build solution, including set up service
G.A07 Architecture	Data location can be controlled	exceed in account failed (throuthno). It is pairable to control the symposphical in extinse (invicidintianz) where the control of the instance of an other branch operator of by the presider, and the Filter on understanding of how to dara.	Suize DPA, GDPR, Professional Secrecy	Service Owner		The provider allows us to control the Geo of various services through the service console. I understand which service can be located when and how to configure it.]	e [Hans Muster, IT] e			Internal governance and compliance tasks
G.A08 Architecture	Data retention and deletion concept exists	There is a dote rotantian and delotian cances (for the substantian in order to enough with (1) the adipation value the Suize DPA and GDPR to have permedideterships donly ad long ar no care ary one with the right to correspond (1)) realizing the substantian such to rotatic cost in dote for	Suizz DPA, GDPA, 4444 ratustien al ligatiene under opplicable lau	Business Owner	Must have	[Still to be defined; will be done in Phase 3]	[Hund Muster, IT]			Serenai Serenai compilario casio
G.A09 Architecture	Capacity requirements defined	constructions are included from a final section of the copicity of the large of a concept concerning the finance she future ($x_{i,t}$, sambler of users, dots to be started, to an extense) to biographic sectors of the section of the sectors of t	OpRink	Service Owner	Nice to have	(Has been defined for a period of five years, assuming organic growth)	[Hans Muster, IT]		N/A	
G.802 BCM	Backup of the solution's data		FINPA Circular 2010/42 (N25)	Service Owner	(for critical data and	5 X			N/A	
G.B03 BCM	Provider has adequate BCM measures in place	The pravider has converted to BOM no access that earnes on an uping zervice delivery endrocerics restaration in the event of a director and other extreme lineary discussions. They have been reviewed by the H and they must the H's used and have been elipsed with H's sam BOM measures.	FINHM Circular 2010/02 (N25), FINHM Circular 2009/21(H135.11, H136)	Service Owner	(for critical data and	5 X			N/A	Only some 60 of the 150
G.804 BCM	Continuation of business ensured in the event of solution failure	It is a new of that is the second of a failure of the polyherm period of the of the			sustems) Must have (for oritical data and systems)	X			N/A	Controls concern the provider and ist contract; the remainde
G.B09 BCM	Possibility of switching to a different provider	The F1 understands the steps it save details is it is chosen of provider should be ensured as the steps of the same steps. The same steps of the same steps			Must have (for oritical data and	9 X			N/A.	
G.B10 BCM	Availability requirements defined	The FI has defined the requirements it has with requird to the availability, recurvery and other KPIs of the solution, and understands which service	OpRials	Business Owner	sastems) Good to have	e x			N/A	relates to measures on the par
G.B11 BCM	Repatriation is possible without a loss of relevant data	<u>Is each und when KP is have to be included in the contract with the analytics</u> . It is ensured that the I can at any time argumt all relevant data presented by the rabition (both the "context" store do the zervice or well as relevant occurs risk, here the year data). In particular there will be no layer of		Service Owner	Must have (for critical data and	8 8			N/A	of the financial institution

Examples

"Defend your Data" obligation in case of foreign lawful access attempts		disclosures required by law.If the provider is confronted with disclosure or access orders from foreignFINMA Circular 2018/03 (N23),authorities or courts in relation to content data, it will try to redirect theSwiss DPA, GDPR, Professionalauthorities or courts to the FI, and if this is not possible, it will use all legal meansSecrecyto challenge these orders as far and as long as possible. It will inform the FI of this,where permitted. This also applies with regard to authorities within the EEA, not									
o access to pro	Must have Factor		V	, ^{and it shall app} Appendi combina	x C of the	e DPA (S		er 2021), in	123),		
		has a certa quests sho ed.			3	1	3	Risk accepted	ł.		

Examples

Requirements also with regard to the project and the organizational measures to be taken

	pe appropriate.	
o data loss or corruption during	ata loss or corruption during intion The FI has a concept to ensure that there will be no loss or corruption of data when migrating from the old to the new solution (where applicable). This includes detecting deviations, reacting to them (e.g., by enabling a roll-back) and having all data properly decommissioned, deleted or archived at the old solution after a successfull migration. at-rest encrynted Content data "at-rest" (i.e. when in a "dormant" state/when stored) is encrynted steps taken tnereto. A procedure (with responsibilities assigned) exists for ensuring that the contract with the provider will be renegotiated and renewed in time to permit an orderly repatriation in case such renewal should fail. This applies in particular for contracts Set that have a fixed term where renewal on the part of the provider is not	
igration	when migrating from the old to the new solution (where applicable). This includes	
	detecting deviations, reacting to them (e.g., by enabling a roll-back) and having all	
	data properly decommissioned, deleted or archived at the old solution after a	
	successfull migration.	
ata at-rest encrynted	Content data "at-rest" (i.e. when in a "dormant" state/when stored) is encrynted	
	steps taken thereto.	
Renewal management	A procedure (with responsibilities assigned) exists for ensuring that the contract	FII
Ū.	with the provider will be renegotiated and renewed in time to permit an orderly	Sv
	repatriation in case such renewal should fail. This applies in particular for contracts	Se
	that have a fixed term where renewal on the part of the provider is not	
	guaranteed.	

Structured Compliance & Risk Assessment

oud-Compliance-Check: Risi	KODEURTEIIUNG																
hage Exhauri 52 18.882				-													
ojekt [M365]				Projektleitx (Peter Muster)													
		es" our gofüllt um den ist. Je mehr der dastigen Anfarder It allen Stekeholdern darch auführt, unbeijeder Teilnel															
		mendidiant. Ein Rizika nach dam biazigan Voortiin daizist Batrachtungenoitrean varuandat uird und uie die jeu															
rünlicher Folgen einer Rizikor vurgert altetzein zu ikufeldern der entrprechen de Grenzuert eingetre	llon. Die Abstafungsalltesa gewählt werden, gen werden. In einem zweiten Schritt is	darzzio dar qoramto Spoktrum an trașbaron und nicht tr 1 'Er jodoz Rizika fortzakolton, uol cho Faktaron für und 1	agbaren Riziken obdeckt. Dezekenn bei den ferbigen gegen den Eintritt dierer Usrechezprechen und mit														
		a er Stelle sind die Massnehmen wurdenen, die wur Verm. 1 Rivikar heben kann und welche Fektaren defür und dea															
sannan, dia zur Termaidung der Folgen getroffen s izenten ooke, seie senkercheinlich er zum betreffen	rurden. In den Foldern rochte önnebonzinde el den Schaden kummt. Dei den Porzunonechör	viezzlich die Falgen für die Institution und die betraffene In kann je de Schedenzstufe Abis 198% oufweizen. In eine	n Porranon zubozifforn, und zwar joueik mit einer m vierten Schritt albt der Nickseianer an wie														
Bef. Ziel	Risikoumschreibung Risiko	Ungewisse Ursache	Ursacheneintritt Faktoren pro und contra Eintritt	Eistritte-	Risikomit Unervünschte Folgen	igierung aktoren pro und contra Folge			similar		nstitution		Un	erwunsch Niel spiele	hte Fo		
R1.10 Erfüllung rechtlicher Anforderungen		Die Tertrag nder andere Argeiste der Begyftragung	Wir achten auf ein karrekter	50%	Datenrobate: /Amtr	Wir dakumontieren die rechtlichen Prüfung	70%	202	102	02			332	-	0		
		der Anbieterz erweiren zich alr nicht rechtzkunfurm.	Barchaffangreefahren; führen eine rechtliche Prüfung der Ankieters durch; keurteilen die Risiken; uis lanze un extern kennten.		/Barafrashainnirvorlatzungan; politirchandor oufrich urochtlicha Eisfluornahma und Falqan; Ronahaimmerkölen: Reechaffangung di Sicha	zaule die Rizikabeurteilung vallet ündig und nachvallaieber.											
R1.11 Erfüllung rechtlicher Anforderungen	Datenschatz interner Personen werketet	Der Einzetz der Lärung führt Datenz chotzvorletzung ketroff und die Perranen innerholk der Institution.	Mir prüfen den Anbieter und den Einretz der Lärung auf detenschatzrechtlicher Sicht var den Einretz	0%	Kloge der ch betraffene Perzen, Strafverfoshen. Resetationer sköden solltig sie oder	; Information- und Moldopflichten; Wiederheuteillung der rechtmätrigen	0%	0%	0%	0%				0	0		
D112 Erfüllung sochtlicher Auforderungen			der Lärung wir larren um entern beraten; wir kontraffieren und ikon sechen den destister rensis	02	oufrichtere chtliche Einfluern ehene und Folgen.	Zurtende, Einigung mit betreffener Porren.											
R112 Erfüllung rechtlicher Anforderungen	Datenschutz externer Personen verletzt	Der Einretz der Lärung führt zweiner Detenrehetzverletzung kotroffend die Perranen	Wir prüfen den Ankieter und den Eine etz der Lärung auf detene ehntzreichtlicher Sicht var dem Eine etz	01	Klage durch betraffene Perran; Strafverfrahren Reputationer chöder; politir che oder	Wiederherrtellung der rechtmärrigen	02	0%	0%	0%				U	0		
		eurochalb dor Institution.	der Lärung uir lazen um extern bereten; uir Inntraffissen und über netten den Belister muis Wenn viele andere CH-lastitutionen die Lärung ouch	02	outrichtrochtliche Einfluzznehme und Falgen. Lännen konn nicht mehr uniter sonstrit unr den:	Zurtendr, Eisigung mit betroffener Porron. Wir haben eine Exibetrateoie von Veraur	02	02	02	02							
B1.13 Erfüllung rechtlicher Anforderungen	Ändernde gesetzliche Grundlagen	Die geretzlichen Grundlagen ändernzichen, dass der Einzutz der Sorvicer bzu. der Anbioters aufgegeben	notzen, uird der Anbieter ein Interezze der en haben,	04	We chaol was a corr Likron g a dor uie dor zolber	fartgologt und halton diere ektuell.	0.6	0.6	05	0.6					U.		
		uretenmar.	rich an geänderte geretzliche Grundlagen. anwapaeren. Wir natzen einen rolche Lärung.		botraikan; miligi charcaira haka Kartan; allanfalk nieht raehtaaitig miiglich; waan Mashral nieht ra chtzaitig miiglich: Ririka van Dataarchatz-	,											
R1.14 Erfüllung rechtlicher Anforderungen	Gefährliche Berwitzung der Lörung		Minimelementionen technische und	02	nder Amter (Bondrasholmeinselstmises	Wirnstein an Data Laskans Proventing	02	0%	02	02					-		
HUM Emiling recebicier Aarorderingen	Geranniche Denvitzing der Losung	Miterbeiter benutzen die Lürung in unricherer zier zunrt gefährlicher Weire.	argenizatorizche Mazznahmen (TOMz); uirzchelen	04	Datenechata-Amte- /Borategeheimnisverletzungen;	Wirvetzen zue Date Leekage Proventies Lärung uir heben Audit Treilr (inkl. Aurupstand) implementiert.	04	0.	04	0.4					0		
R1.15 Erfüllung rechtlicher Anforderungen	Berufo- oder Antogeheinnic verletzt	Der Einents der Lärung führt su Amter ader Berafrankeimaisuurlebrangen	undzenelbilleleren unzere Miterkeitenden. Mir prüfen den Ankister und den Einents der Lärung mit Blick auf das Amter (Berufzasheimeiz var den	03	Reentationerchäden: solltirche oder Strafwerfrahezer, Reputationerchäden; politische oder aufrichterechtliche Einfluerechen und		0%	0%	0%	0%		•	-	0	0		
	venetzt	Baratrychaimstroorlatzungen.	Einretz der Lärung uir lazen um extern bereten; uir kantrallieren und überwechen den Mehieter		nder autrichtere chiliche Lintiern ehme und Falgen	Wiederherreitung der rechtmitzigen Zurtendr, Einigung mit betraffener Porzan.											
R1.2 Erfüllung rechtlicher Anforderungen	Vertragsrerletzing durch Anbieter	Der Anbieter hilftzeine vertraglichen Zuricherungen mier die ihm vertragekonform erteilten betraktionen	om de des Fiereste des l'écono Mirkantrallieren den Anbieter; uir nutzen einen Anbieter, den wech viele andere ON-fastitutionen	0%	Dotere chate / Amite /Barafe schaimnie verlaten nam Straf verfahren	Wir voreinberen im Vertrag durchestabere Gewährleistungesehte und Naftunges gein	0%	0%	0%	0%		•		0	0		
, č		nicht ein (n.B. un und uis Daten nurpeicherneind nder wer darauf Zugriff orbält).	nutzen (Webercheinlichkeit einer Tertropprocletzung durch den Anbieterist		Reputationer chödere politirehe oder outrichtere ehölere Softwernahme und Folgen.	undratzten diere meh durch; direkt mit den Anhistor muendberer Bochtretzen uir											
		uer der auf Zugrift orhaik).	kleiner); der direkt out den Anbieter anwendbare		outrichtere chtliche Einfluzznehme und Falgen.	durch (x.B. Barchwordo an											
			Recht hilft une bei der Durchestzung unzerer Anzprüche: die Reputation der Anhistore neigt, dare			Aufrichtskohlinde); zir kantraffieren den Anhieter											
R121 Erfüllung rechtlicher Anforderungen	Unterlassene Datenlöschung	Der Ankieter lärcht die Daten der betitstim noch deren Exit nder wenn verlangt nicht wie vereinbart.	Tertragliche Vereink erung der Lärchung inkl. rehriftlicher Bortätigen & der direkt auf den	0%	Dateorobata-Amte- /Barafrachaimnirvorlatzanaan: Klaso darch	Wirkännen vertragliche Vereinkarungen und auf den Arbieter anwendbarer Rocht	0%	0%	0%	0%		•	-	0	0		
		errin bin ber uns versingt sicht um varans ert.	Anbieter anzen dhare Rocht, rehreit die Lärchung andham Kanteelle der Anbieter		botraffeno Perzen; Strafverfoshren; Desentationerskäden selltische oder	der den Anderster Brucen des Breit nie der der chrotzon; wir kantrallieren den Anbieter und die Läschene											
R1.2 Erfüllung rechtlicher Anforderungen 2	Unerkannte Anpassungen des Anbieters	Der Anbieter partzeinen Vortreg, zeine Servicer oder die Art Brer Erbringung (z.B. Standarte, beigezogene	In VortrogrisdIsfarmotianspflichten voroinbert;	0%	Doteor chutz-/Amtz- /Barufzgehaimsizvorlatzengan; palitizcha ador	Wirkännen vertregliche Vereinberungen und auf den Arbieter anzen dbarer Rocht	0%	0%	0%	0%		-		0	0		
		Dritte, Kunfigurationernäiglichkeiten) in rechtlich werentlicher Weire en und die Institution bekammt	die den Anhieterbeterwen und auf Änderungen. präfenführeurechen.		oufrichterechtliche Einfluernahme und Falgen; Lärung konn ollenfalle nicht mehr weiter genutzt	derekratuan. Wirkekan aina Exitetratagia Fartgalogt und haltan diara ektuall.											
R1.2 Erfüllung rechtlicher Anforderungen	Verweigerung Vertragsaupassung	Haraichtedaraichteachteaitiamit Der Ankieter swigertrich, eine warrechtlicher Sicht	Tertraglishe Vereinkarung, duer der Vertragkei	0%	Lieung kann nicht mehr weiter genatut werden;	Wirhaken aine Exiletrate gie wan Varane	0%	0%	0%	0%		•		0	0		
°		erfærderliche Vertrogrenp erzung verzunehenen.	rochtlich natuon digon Anparron gon nach Trou und Blaubon engopart wird; Mutzung einer Anbieterr,		Wochrol wanevor Lärung odor wiedorzolber botroiben; Migrationzkorton; allenfollznicht	fartgologt und halten diere aktuell.											
			den viele andere CM-fastitutianen auch nutzen (grærerer Druck zur Tertragranp arving).		rə chtzəitiq mäşlich; cəsa Weckzəlaicht rə chtzəitiq mäşlich: Pärlez vən Dətəar shotz-												
R1.2 Erfüllung rechtlicher Anforderungen	Unorloubte Eigensetzung von Daten	Der Ankieter nimmt eine unerlaubte Eigennetzung	Die Zusetkbindung voreinburen uir vortreglich;	0%	nder Amberikansk sin sin selat man saa Datene ekster Amter	Wirkännen vertragliche Vereisberung und	0%	0%	0%	0%			-	0	0		
4		van Parramandaten ader anderer infarmatianen der Institution var.	direkt ouf den Ankieter muselk orer Rocht unterront die unerloubte Einerneutrung.	03	/Barafryshainsirverlatzungan; pulitirchandar oufrichterechtlicha Eisfluernahme und Fulaan:	ouf den Arbieter anwendbarer Reakt darehretzen.									- 0		
R1.3 Erfüllung rechtlicher Anforderungen 0	Ungenägende Kontrolle des Anbioters	Die hertitetien orkenet ne getive uder undere wichtige Entwicklungenzeitere der Anhieterznicht (n.B.	Michebon intern vorantzanliche Porranen definiert, die den Ankieter übersenehen und regelmärrig	08	Datearchetz-/Amtr- /Barafrachainnirverlatzengan; politircha odar	Wir haben eine Exiletrotegie zum Varaur Fartgelegt und halten diere aktuell.	0%	0%	0%	0%					ľ		
		verrehle ehterte Finanzloge, Gerotzerverrtiere). Hinweir: Die Prüfung der Sicherheit der Anbieterrirt	kuntrallieren; die Oberwechung ist in unser interner Kuntrallsystem (IKS) eingebunden; wirzehen		oufrichtere chtliche Einfluernahme und Folgen; Likrung kann ollen falle nicht mehr weiter genutzt												
R131 Erfüllung rechtlicher Anforderungen	Unerkannte Anpassungen der Institution	zon erst all sold and det Die Institution parst den Vortrag, die Servicer oder die Art Breef Febriegen of z. B. Die scheren Konfiguration (actore a Frantzallo, der Anlächer une Adminrochte werden reeträctiv vertailt. Kurdinseringenen erreren an verden is einem Franzen	03	oordoo Worked wardered Brown Dateerebeter/Amtr- /Barafreebeimalmostatranaereaditiechender	Ro colmärrico Oborprüfuga der Kanfleuratien der Lärunge orterne	0%	0%	0%	0%		•		0	0		
	mounding	Art ihrer Erbringung (z.B. über deren Konfiguration) in einer Art und Weize an, die zu Verletzung der	Kunfiquoriunzung uzengen worden in einem Pruzez (Vier-Wegen Prinzip) vurgenummen und mützen		/Barufzgehainnizvorlatzungan; politischa odar oufsichtera chtlicha Einfluzznahma und Folgan;	Kanfigaratian der Lärung externe Obergrüfung der Einratzer der Lärung.											
-	ick 1. Beschre	eibung der Lösung	town the antibio of the farm it is a constitution of a		er Anforderungen	4. Risikobeur				_			_	Classi	_		

Example as used for Swiss public institutions

Some 55 risks to be assessed, with classical infosec risks only being considered here in an aggregated form

And what about negotiating contracts?



13

Summary

- The public debate about using the cloud is misleading
 - The issue of foreign lawful access is first and above all an issue for organizations that are subject to professional or official secrecy (e.g., banks, the government)
 - Even there, it can be handled; yet, there is no "zero risk"
- The cloud in a corporate environment is not "plug and play"
 - The challenges of the "shared responsibility model" are often underestimated
 - More focus and ressources are needed for on service, provider and contract oversight and management than traditionally
 - The use of the cloud may increase security, but provides for other risks management should understand and accept beforehand

Questions?

drosenthal@vischer.com

Zürich Basel Genf Schützengasse 1 Aeschenvorstadt 4 Rue du Cloître 2-4 Postfach Postfach Postfach 8021 Zürich, Schweiz 4010 Basel, Schweiz 1211 Genf 3, Schweiz T +41 58 211 34 00 T +41 58 211 33 00 T +41 58 211 35 00 www.vischer.com