VISCHER

Cloud in der öffentlichen Verwaltung.

Ein Prüfraster und Werkzeug für die Praxis

David Rosenthal, Partner, VISCHER AG
3. November 2022

Die Wogen gehen hoch bei der Cloud …

Quellen: Republik.ch, Inside-IT, Netzwoche

Öffnen wir den Blick …

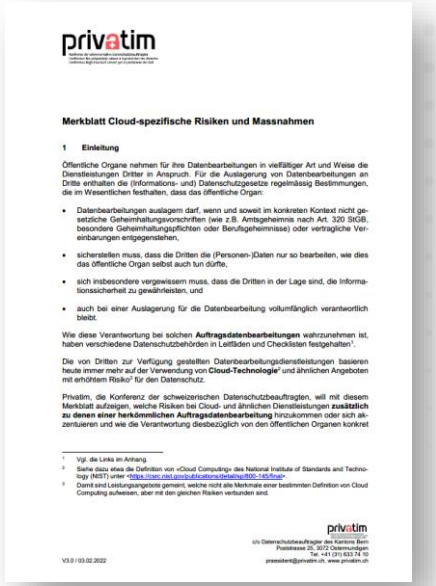
privatim hat im Februar 2022 ein «Merkblatt Cloud-spezifische Risiken und Massnahmen» publiziert, das den öffentlichen Organen insbesondere auch die Beurteilung des Einsatze M365 ermöglichen soll. Der Entscheid des Regierungsrates des Kantons Zürich bedeutet für die öffentlichen Organe grundsätzlich nicht, dass sie vom Inhalt und dem empfohlenen Vorgehen in diesem Me privatim si den Kanto

Richtig!

Beim ausländischen ***Lawful Access*** handelt es sich um einen kleinen Teilaspekt in der Risikoanalyse, der über die zu treffenden technischen und organisatorischen Massnahmen oder – sofern diese nicht genügen – einen Verzicht auf die Auslagerung entscheiden kann.

Auf jeden Fall können die Ausführungen zum ausländischen ***Lawful Access*** nicht die anfangs erwähnten Schritte wie Rechtsgrundlagenanalyse, Schutzbedarfsanalyse sowie Risikoanalyse mit den Restrisiken und den Massnahmenplan ersetzen.

Vorgaben des Datenschutzes …



privatim

Merkblatt Cloud-spezifische Risiken und Massnahmen

1 Einleitung

Öffentliche Organe nehmen für ihre Datenbearbeitungen in vielfältiger Art und Weise die Dienstleistungen Dritter in Anspruch. Für die Auslagerung von Datenbearbeitungen an Dritte enthalten die (Informations- und) Datenschutzgesetze regelmässig Bestimmungen, die im Wesentlichen festhalten, dass das öffentliche Organ:

- Datenbearbeitungen auslagern darf, wenn und soweit im konkreten Kontext nicht gesetzliche Geheimhaltungsvorschriften (wie z.B. Amtsgeheimnis nach Art. 320 StGB, besondere Geheimhaltungspflichten oder Berufsgeheimnisse) oder vertragliche Vereinbarungen entgegenstehen,
- sicherstellen muss, dass die Dritten die (Personen-)Daten nur so bearbeiten, wie dies das öffentliche Organ selbst auch tun dürfte,
- sich insbesondere vergewissern muss, dass die Dritten in der Lage sind, die Informationssicherheit zu gewährleisten, und
- auch bei einer Auslagerung für die Datenbearbeitung vollumfänglich verantwortlich bleibt.

Wie diese Verantwortung bei solchen **Auftragsdatenbearbeitungen** wahrzunehmen ist, haben verschiedene Datenschutzbehörden in Leitfäden und Checklisten festgehalten[1].

Die von Dritten zur Verfügung gestellten Datenbearbeitungsdienstleistungen basieren heute immer mehr auf der Verwendung von **Cloud-Technologie**[2] und ähnlichen Angeboten mit erhöhtem Risiko[3] für den Datenschutz.

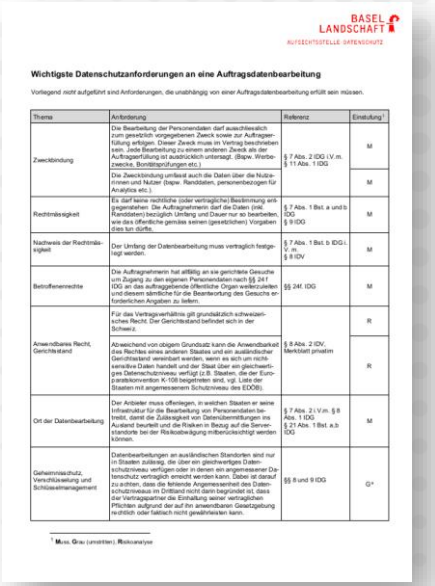
Privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, will mit diesem Merkblatt aufzeigen, welche Risiken bei Cloud- und ähnlichen Dienstleistungen **zusätzlich zu denen einer herkömmlichen Auftragsdatenbearbeitung** hinzukommen oder sich akzentuieren und wie die Verantwortung diesbezüglich von den öffentlichen Organen konkret

[1] Vgl. die Links im Anhang.
[2] Siehe dazu etwa die Definition von «Cloud Computing» des National Institute of Standards and Technology (NIST) unter <https://csrc.nist.gov/publications/detail/sp/800-145/final>.
[3] Damit sind Leistungsangebote gemeint, welche nicht alle Merkmale einer bestimmten Definition von Cloud Computing aufweisen, aber mit den gleichen Risiken verbunden sind.

privatim
c/o Datenschutzbeauftragter des Kantons Bern
Poststrasse 25, 3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

V3.0 / 03.02.2022

+



BASEL LANDSCHAFT
AUFSICHTSSTELLE DATENSCHUTZ

Wichtigste Datenschutzanforderungen an eine Auftragsdatenbearbeitung

Vorliegend *nicht* aufgeführt sind Anforderungen, die unabhängig von einer Auftragsdatenbearbeitung erfüllt sein müssen.

Thema	Anforderung	Referenz	Einstufung[1]
Zweckbindung	Die Bearbeitung der Personendaten darf ausschliesslich zum gesetzlich vorgegebenen Zweck sowie zur Auftragserfüllung erfolgen. Dieser Zweck muss im Vertrag beschrieben sein. Jede Bearbeitung zu einem anderen Zweck als der Auftragserfüllung ist ausdrücklich untersagt. (Bspw. Werbezwecke, Bonitätsprüfungen etc.)	§ 7 Abs. 2 IDG i.V.m. § 11 Abs. 1 IDG	M
	Die Zweckbindung umfasst auch die Daten über die Nutzerinnen und Nutzer (bspw. Randdaten, personenbezogen für Analytics etc.).		M
Rechtmässigkeit	Es darf keine rechtliche (oder vertragliche) Bestimmung entgegenstehen. Die Auftragnehmerin darf die Daten (inkl. Randdaten) bezüglich Umfang und Dauer nur so bearbeiten, wie das öffentliche gemäss seinen (gesetzlichen) Vorgaben dies tun dürfte.	§ 7 Abs. 1 Bst. a und b IDG § 9 IDG	M
Nachweis der Rechtmässigkeit	Der Umfang der Datenbearbeitung muss vertraglich festgelegt werden.	§ 7 Abs. 1 Bst. b IDG i. V. m. § 8 IDV	M
Betroffenenrechte	Die Auftragnehmerin hat allfällig an sie gerichtete Gesuche um Zugang zu den eigenen Personendaten nach §§ 24 f. IDG an das auftraggebende öffentliche Organ weiterzuleiten und diesem sämtliche für die Beantwortung des Gesuchs erforderlichen Angaben zu liefern.	§§ 24f. IDG	M
Anwendbares Recht, Gerichtsstand	Für das Vertragsverhältnis gilt grundsätzlich schweizerisches Recht. Der Gerichtsstand befindet sich in der Schweiz.	§ 8 Abs. 2 IDV, Merkblatt privatim	R
	Abweichend von obigem Grundsatz kann die Anwendbarkeit des Rechtes eines anderen Staates und ein ausländischer Gerichtsstand vereinbart werden, wenn es sich um nicht-sensitive Daten handelt und der Staat über ein gleichwertiges Datenschutzniveau verfügt (z.B. Staaten, die der Europaratskonvention K-108 beigetreten sind, vgl. Liste der Staaten mit angemessenem Schutzniveau des EDÖB).		R
Ort der Datenbearbeitung	Der Anbieter muss offenlegen, in welchen Staaten er seine Infrastruktur für die Bearbeitung von Personendaten betreibt, damit die Zulässigkeit von Datenübermittlungen ins Ausland beurteilt und die Risiken in Bezug auf die Serverstandorte bei der Risikoabwägung miteinbezogen werden können.	§ 7 Abs. 2 i.V.m. § 8 Abs. 1 IDG § 21 Abs. 1 Bst. a,b IDG	M
Geheimnisschutz, Verschlüsselung und Schlüsselmanagement	Datenbearbeitungen an ausländischen Standorten sind nur in Staaten zulässig, die über ein gleichwertiges Datenschutzniveau verfügen oder in denen ein angemessener Datenschutz vertraglich erreicht werden kann. Dabei ist darauf zu achten, dass die fehlende Angemessenheit des Datenschutzniveaus im Drittland nicht darin begründet ist, dass der Vertragspartner die Einhaltung seiner vertraglichen Pflichten aufgrund der auf ihn anwendbaren Gesetzgebung rechtlich oder faktisch nicht gewährleisten kann.	§§ 8 und 9 IDG	G*

[1] M=muss, G=soll (umsetzen), R=Risikoanalyse

+

weitere Aspekte ausserhalb des Datenschutzes

Cloud-Merkblatt privatim

z.B. Anforderungsliste DSB BL

Die derzeit wichtigsten Cloud-Themen

- **Abhängigkeit** und Geschäftsfortführung
- **Informationssicherheit**
- Modell der **"Shared Responsibility"**
- **Datenschutz** & **Berufsgeheimnis**
- Datenbearbeitung für **Zwecke des Providers**
- Ausländischer **Behördenzugriff** (Lawful Access)
- **Vertrag** mit dem Cloud-Provider
- **Überwachung** von Mitarbeitern
- **Rechtsgrundlagen** und Verhältnismässigkeit

Alles lösbar, aber es muss an alle wichtigen Punkte gedacht werden (und das ist für viele die erste Herausforderung)

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?

Was wir aus rechtlicher Sicht benötigen

- **Beschreibung**, was wir planen (auch aus Datensicht)
- Schutzbedarf beurteilen, Risiken der Informationssicherheit und des Datenschutzes einschätzen und **Massnahmen** definieren
  - "ISDS-Konzept", "DSFA", "FLARA"-Beurteilung, InfoSec-Analyse
  - Diverse weitere Konzepte (z.B. zu Einführung, IAM, Exit)
- Prüfung der **rechtlichen Anforderungen**
  - Rechtsgrundlagen-Analyse
  - Beurteilung Anforderungen Datenschutz, Berufsgeheimnis, spezialgesetzliche Vorgaben, "Gute Cloud-Praxis"
  - Vertragsprüfung
- Gesamthafte Beurteilung der **Restrisiken**

CCRA-PS

Tool für ein Cloud-Compliance- und Risk-Assessment im öffentlichen Sektor

CCRA-PS kurz zusammengefasst

- Standard-Prüfraster zur **Beurteilung von Cloud-Projekten** des öffentlichen Sektors aus Sicht von Recht und Risiko
  - Ca. 140 konkrete Anforderungen (inklusive Privatim und weitere)
  - Ca. 60 Risiken + Datenschutz-Folgenabschätzung (DSFA)
  - Gesamtheitliche Sicht, nicht nur Datenschutz und Amtsgeheimnis
  - Gibt es bisher nicht – oft fehlt auch die Erfahrung
- **Strukturierte Vorgehensweise** und **Dokumentation**
  - Technische Risikoanalyse (InfoSec) und Foreign Lawful Access-Beurteilung muss separat durchgeführt werden und fliesst ein
  - Grundlage für interne Risikoentscheide und externe Aufsicht
- **Jetzt downloaden:** https://bit.ly/3Uiz4v8 (www.rosenthal.ch)

Kooperationspartner:

INSELSPITAL
UNIVERSITÄTSSPITAL BERN
HÔPITAL UNIVERSITAIRE DE BERNE

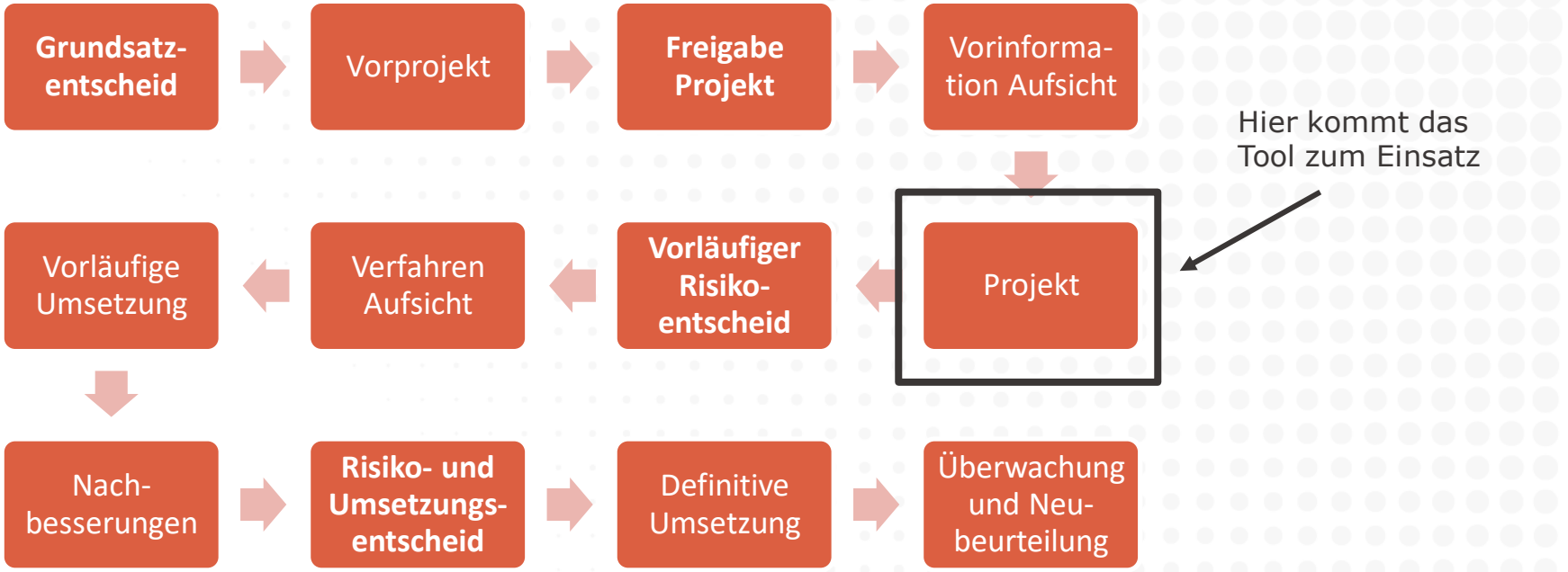
VGIch
Vereinigung Gesundheitsinformatik Schweiz

Luzerner Psychiatrie lups.ch
Luzern | Obwalden | Nidwalden

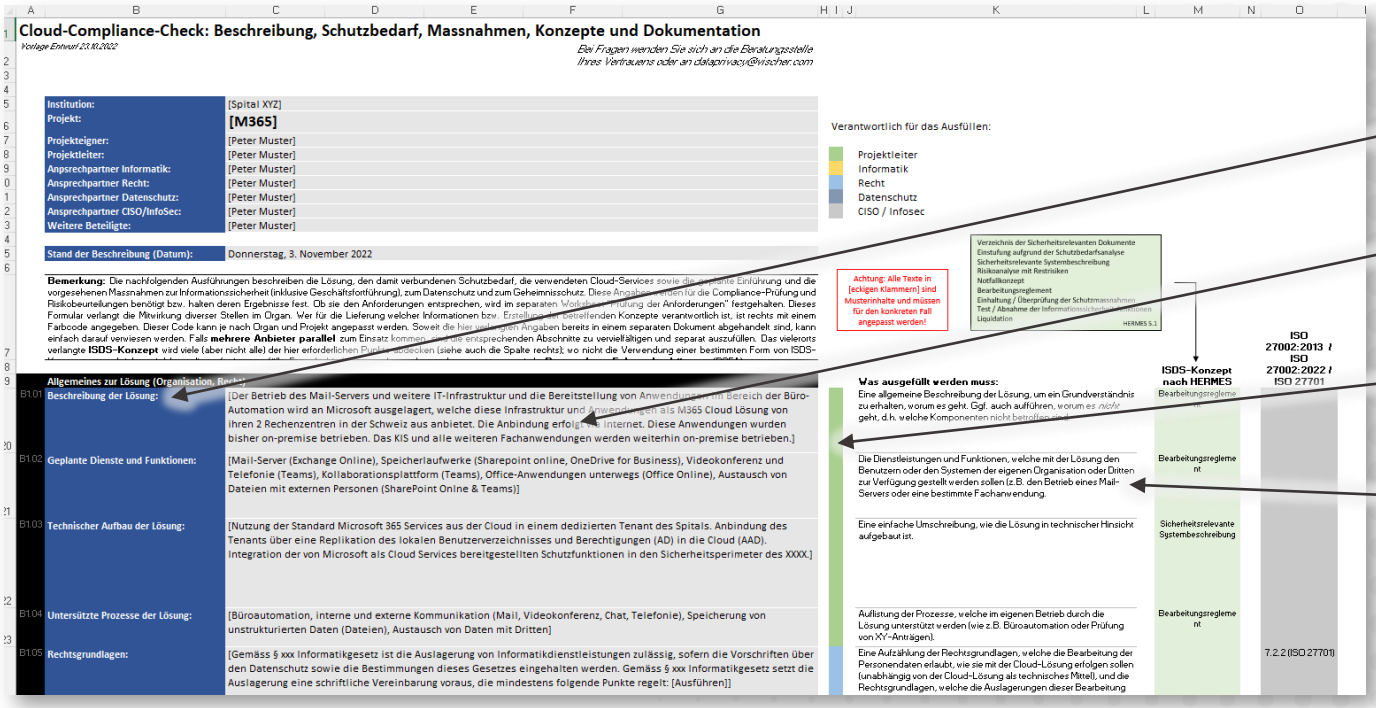
und weitere Institutionen

Entwurf for Public Comment

Ein typischer Ablauf eines Cloud-Projekts



Schritt 1: Beschreibung, Schuban, Massnahmen



Cloud-Compliance-Check: Beschreibung, Schutzbedarf, Massnahmen, Konzepte und Dokumentation

Vorlage Entwurf 23.10.2022

Bei Fragen wenden Sie sich an die Beratungsstelle Ihres Vertrauens oder an dataprivacy@vischer.com

Institution:	[Spital XYZ]
Projekt:	**[M365]**
Projekteigner:	[Peter Muster]
Projektleiter:	[Peter Muster]
Anpsrechpartner Informatik:	[Peter Muster]
Ansprechpartner Recht:	[Peter Muster]
Ansprechpartner Datenschutz:	[Peter Muster]
Ansprechpartner CISO/InfoSec:	[Peter Muster]
Weitere Beteiligte:	[Peter Muster]
Stand der Beschreibung (Datum):	Donnerstag, 3. November 2022

Verantwortlich für das Ausfüllen:
- Projektleiter
- Informatik
- Recht
- Datenschutz
- CISO / Infosec

Bemerkung: Die nachfolgenden Ausführungen beschreiben die Lösung, den damit verbundenen Schutzbedarf, die verwendeten Cloud-Services sowie die geplante Einführung und die vorgesehenen Massnahmen zur Informationssicherheit (inklusive Geschäftsfortführung), zum Datenschutz und zum Geheimnisschutz. Diese Angaben dienen für die Compliance-Prüfung und Risikobeurteilungen benötigt bzw. halten deren Ergebnisse fest. Ob sie den Anforderungen entsprechen, wird im separaten Workshop zur Prüfung der Anforderungen" festgehalten. Dieses Formular verlangt die Mitwirkung diverser Stellen im Organ. Wer für die Lieferung welcher Informationen bzw. Erstellung der betreffenden Konzepte verantwortlich ist, ist rechts mit einem Farbcode angegeben. Dieser Code kann je nach Organ und Projekt angepasst werden. Soweit die hier verlangten Angaben bereits in einem separaten Dokument abgehandelt sind, kann einfach darauf verwiesen werden. Falls **mehrere Anbieter parallel** zum Einsatz kommen, sind die entsprechenden Abschnitte zu vervielfältigen und separat auszufüllen. Das vielerorts verlangte **ISDS-Konzept** wird viele (aber nicht alle) der hier erforderlichen Punkte abdecken (siehe auch die Spalte rechts); wo nicht die Verwendung einer bestimmten Form von ISDS-

Achtung: Alle Texte in [eckigen Klammern] sind Musterinhalte und müssen für den konkreten Fall angepasst werden!

Verzeichnis der Sicherheitsrelevanten Dokumente
Einstufung aufgrund der Schutzbedarfsanalyse
Sicherheitsrelevante Systembeschreibung
Risikoanalyse mit Restrisiken
Notfallkonzept
Bearbeitungsreglement
Einhaltung / Überprüfung der Schutzmassnahmen
Test / Abnahme der Informatiksicherheitsmassnahmen
Liquidation
HERMES 5.1

	Allgemeines zur Lösung (Organisation, Rechtsgrundlagen, Technik)		Was ausgefüllt werden muss:	ISDS-Konzept nach HERMES	ISO 27002:2013 / ISO 27002:2022 / ISO 27701
B1.01	**Beschreibung der Lösung:**	[Der Betrieb des Mail-Servers und weitere IT-Infrastruktur und die Bereitstellung von Anwendungen im Bereich der Büro-Automation wird an Microsoft ausgelagert, welche diese Infrastruktur und Anwendungen als M365 Cloud Lösung von ihren 2 Rechenzentren in der Schweiz aus anbietet. Die Anbindung erfolgt via Internet. Diese Anwendungen wurden bisher on-premise betrieben. Das KIS und alle weiteren Fachanwendungen werden weiterhin on-premise betrieben.]	Eine allgemeine Beschreibung der Lösung, um ein Grundverständnis zu erhalten, worum es geht. Ggf. auch aufführen, worum es *nicht* geht, d.h. welche Komponenten nicht betroffen sind.	Bearbeitungsreglement	
B1.02	**Geplante Dienste und Funktionen:**	[Mail-Server (Exchange Online), Speicherlaufwerke (Sharepoint online, OneDrive for Business), Videokonferenz und Telefonie (Teams), Kollaborationsplattform (Teams), Office-Anwendungen unterwegs (Office Online), Austausch von Dateien mit externen Personen (SharePoint Online & Teams)]	Die Dienstleistungen und Funktionen, welche mit der Lösung den Benutzern oder den Systemen der eigenen Organisation oder Dritten zur Verfügung gestellt werden sollen (z.B. den Betrieb eines Mail-Servers oder eine bestimmte Fachanwendung.	Bearbeitungsreglement	
B1.03	**Technischer Aufbau der Lösung:**	[Nutzung der Standard Microsoft 365 Services aus der Cloud in einem dedizierten Tenant des Spitals. Anbindung des Tenants über eine Replikation des lokalen Benutzerverzeichnisses und Berechtigungen (AD) in die Cloud (AAD). Integration der von Microsoft als Cloud Services bereitgestellten Schutzfunktionen in den Sicherheitsperimeter des XXXX.]	Eine einfache Umschreibung, wie die Lösung in technischer Hinsicht aufgebaut ist.	Sicherheitsrelevante Systembeschreibung	
B1.04	**Untersützte Prozesse der Lösung:**	[Büroautomation, interne und externe Kommunikation (Mail, Videokonferenz, Chat, Telefonie), Speicherung von unstrukturierten Daten (Dateien), Austausch von Daten mit Dritten]	Auflistung der Prozesse, welche im eigenen Betrieb durch die Lösung unterstützt werden (wie z.B. Büroautomation oder Prüfung von XY-Anträgen).	Bearbeitungsreglement	
B1.05	**Rechtsgrundlagen:**	[Gemäss § xxx Informatikgesetz ist die Auslagerung von Informatikdienstleistungen zulässig, sofern die Vorschriften über den Datenschutz sowie die Bestimmungen dieses Gesetzes eingehalten werden. Gemäss § xxx Informatikgesetz setzt die Auslagerung eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt: [Ausführen]]	Eine Aufzählung der Rechtsgrundlagen, welche die Bearbeitung der Personendaten erlaubt, wie sie mit der Cloud-Lösung erfolgen sollen (unabhängig von der Cloud-Lösung als technisches Mittel), und die Rechtsgrundlagen, welche die Auslagerungen dieser Bearbeitung		7.2.2 (ISO 27701)

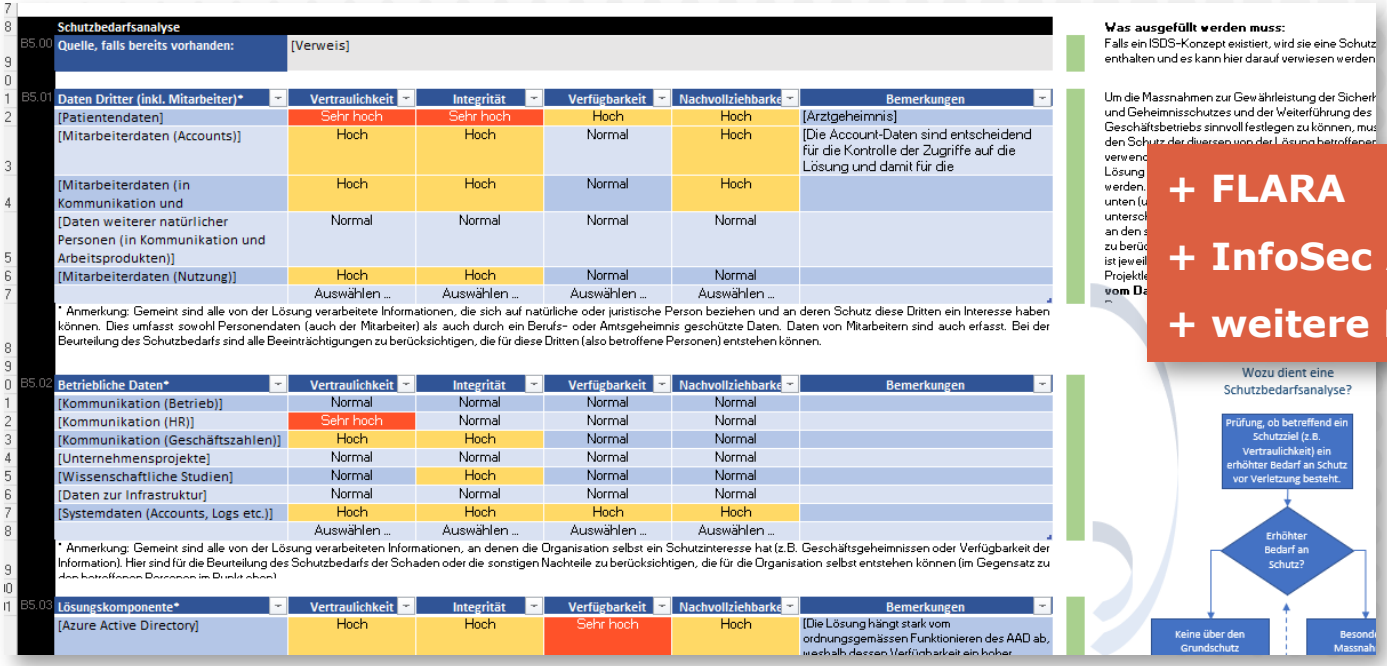
Was es braucht

Inhalt oder Verweis auf Unterlagen

Wer es ausfüllen muss

Hilfestellung

Schritt 1: Beschreibung, Schuban, Massnahmen



Schutzbedarfsanalyse

B5.00	Quelle, falls bereits vorhanden:	[Verweis]				
B5.01	Daten Dritter (inkl. Mitarbeiter)*	Vertraulichkeit	Integrität	Verfügbarkeit	Nachvollziehbarkeit	Bemerkungen
	[Patientendaten]	Sehr hoch	Sehr hoch	Hoch	Hoch	[Arztgeheimnis]
	[Mitarbeiterdaten (Accounts)]	Hoch	Hoch	Normal	Hoch	[Die Account-Daten sind entscheidend für die Kontrolle der Zugriffe auf die Lösung und damit für die
	[Mitarbeiterdaten (in Kommunikation und	Hoch	Hoch	Normal	Hoch	
	[Daten weiterer natürlicher Personen (in Kommunikation und Arbeitsprodukten)]	Normal	Normal	Normal	Normal	
	[Mitarbeiterdaten (Nutzung)]	Hoch	Hoch	Normal	Normal	
		Auswählen ...	Auswählen ...	Auswählen ...	Auswählen ...	

* Anmerkung: Gemeint sind alle von der Lösung verarbeitete Informationen, die sich auf natürliche oder juristische Person beziehen und an deren Schutz diese Dritten ein Interesse haben können. Dies umfasst sowohl Personendaten (auch der Mitarbeiter) als auch durch ein Berufs- oder Amtsgeheimnis geschützte Daten. Daten von Mitarbeitern sind auch erfasst. Bei der Beurteilung des Schutzbedarfs sind alle Beeinträchtigungen zu berücksichtigen, die für diese Dritten (also betroffene Personen) entstehen können.

B5.02	Betriebliche Daten*	Vertraulichkeit	Integrität	Verfügbarkeit	Nachvollziehbarkeit	Bemerkungen
	[Kommunikation (Betrieb)]	Normal	Normal	Normal	Normal	
	[Kommunikation (HR)]	Sehr hoch	Normal	Normal	Normal	
	[Kommunikation (Geschäftszahlen)]	Hoch	Hoch	Normal	Normal	
	[Unternehmensprojekte]	Normal	Normal	Normal	Normal	
	[Wissenschaftliche Studien]	Normal	Hoch	Normal	Normal	
	[Daten zur Infrastruktur]	Normal	Normal	Normal	Normal	
	[Systemdaten (Accounts, Logs etc.)]	Hoch	Hoch	Hoch	Hoch	
		Auswählen ...	Auswählen ...	Auswählen ...	Auswählen ...	

* Anmerkung: Gemeint sind alle von der Lösung verarbeiteten Informationen, an denen die Organisation selbst ein Schutzinteresse hat (z.B. Geschäftsgeheimnissen oder Verfügbarkeit der Information). Hier sind für die Beurteilung des Schutzbedarfs der Schaden oder die sonstigen Nachteile zu berücksichtigen, die für die Organisation selbst entstehen können (im Gegensatz zu

B5.03	Lösungskomponente*	Vertraulichkeit	Integrität	Verfügbarkeit	Nachvollziehbarkeit	Bemerkungen
	[Azure Active Directory]	Hoch	Hoch	Sehr hoch	Hoch	[Die Lösung hängt stark vom ordnungsgemässen Funktionieren des AAD ab, weshalb dessen Verfügbarkeit ein hoher

Was ausgefüllt werden muss:
Falls ein ISDS-Konzept existiert, wird sie eine Schutz
enthalten und es kann hier darauf verwiesen werden

Um die Massnahmen zur Gewährleistung der Sicherh
und Geheimnisschutzes und der Weiterführung des
Geschäftsbetriebs sinnvoll festlegen zu können, mus
den Schutz der diversen von der Lösung betroffenen
verwend
Lösung
werden.
unten (u
unterscl
an den
zu berü
ist jewei
Projekte
vom Da

+ FLARA

+ InfoSec Analyse

+ weitere Konzepte

Wozu dient eine Schutzbedarfsanalyse?

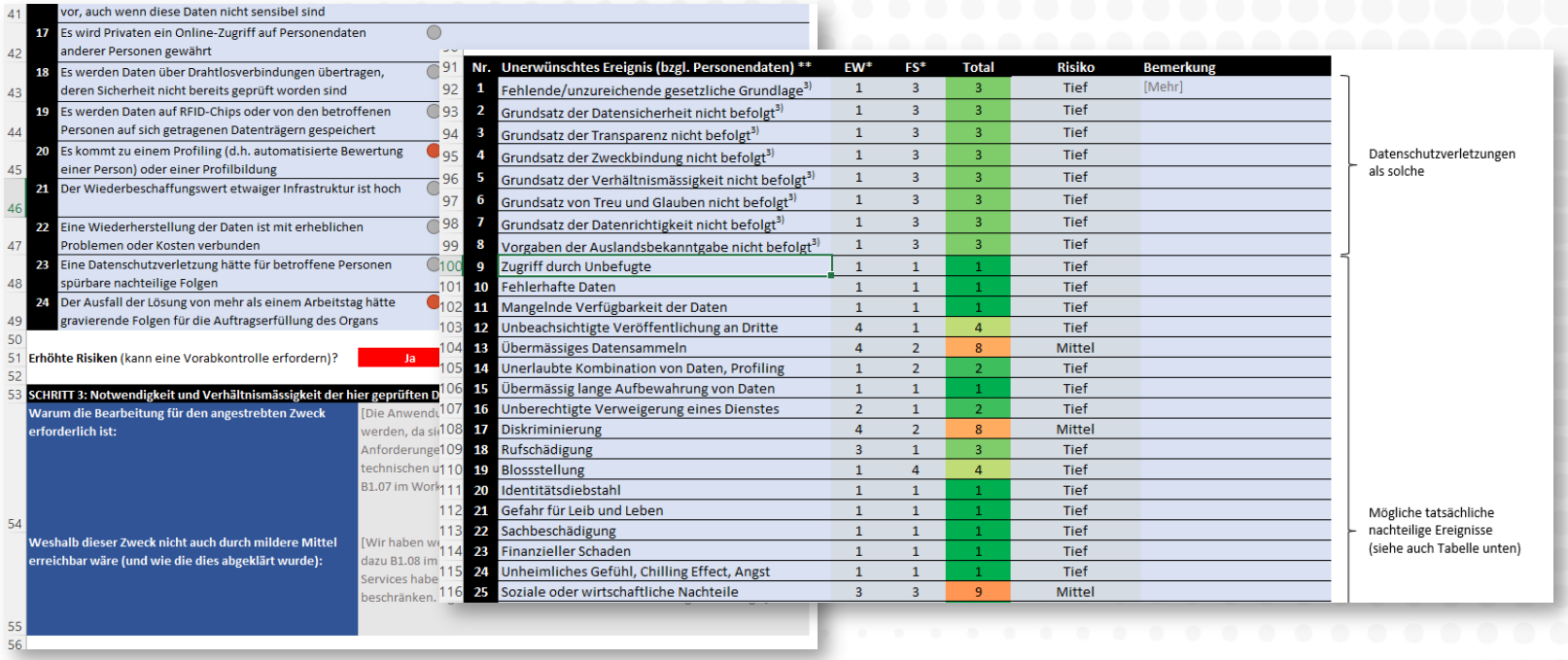
Prüfung, ob betreffend ein Schutzziel (z.B. Vertraulichkeit) ein erhöhter Bedarf an Schutz vor Verletzung besteht.

Erhöhter Bedarf an Schutz?

Keine über den Grundschutz

Besond
Massnah

Schritt 2: Datenschutz-Folgenabschätzung



17	Es wird Privaten ein Online-Zugriff auf Personendaten anderer Personen gewährt	
18	Es werden Daten über Drahtlosverbindungen übertragen, deren Sicherheit nicht bereits geprüft worden sind	
19	Es werden Daten auf RFID-Chips oder von den betroffenen Personen auf sich getragenen Datenträgern gespeichert	
20	Es kommt zu einem Profiling (d.h. automatisierte Bewertung einer Person) oder einer Profilbildung	
21	Der Wiederbeschaffungswert etwaiger Infrastruktur ist hoch	
22	Eine Wiederherstellung der Daten ist mit erheblichen Problemen oder Kosten verbunden	
23	Eine Datenschutzverletzung hätte für betroffene Personen spürbare nachteilige Folgen	
24	Der Ausfall der Lösung von mehr als einem Arbeitstag hätte gravierende Folgen für die Auftragserfüllung des Organs	

vor, auch wenn diese Daten nicht sensibel sind

Erhöhte Risiken (kann eine Vorabkontrolle erfordern)? Ja

SCHRITT 3: Notwendigkeit und Verhältnismässigkeit der hier geprüften D

Warum die Bearbeitung für den angestrebten Zweck erforderlich ist:

[Die Anwend… werden, da si… Anforderunge… technischen u… B1.07 im Work…

Weshalb dieser Zweck nicht auch durch mildere Mittel erreichbar wäre (und wie die dies abgeklärt wurde):

[Wir haben w… dazu B1.08 im … Services habe… beschränken.

Nr.	Unerwünschtes Ereignis (bzgl. Personendaten) **	EW*	FS*	Total	Risiko	Bemerkung
1	Fehlende/unzureichende gesetzliche Grundlage[3)]	1	3	3	Tief	[Mehr]
2	Grundsatz der Datensicherheit nicht befolgt[3)]	1	3	3	Tief	
3	Grundsatz der Transparenz nicht befolgt[3)]	1	3	3	Tief	
4	Grundsatz der Zweckbindung nicht befolgt[3)]	1	3	3	Tief	
5	Grundsatz der Verhältnismässigkeit nicht befolgt[3)]	1	3	3	Tief	
6	Grundsatz von Treu und Glauben nicht befolgt[3)]	1	3	3	Tief	
7	Grundsatz der Datenrichtigkeit nicht befolgt[3)]	1	3	3	Tief	
8	Vorgaben der Auslandsbekanntgabe nicht befolgt[3)]	1	3	3	Tief	
9	Zugriff durch Unbefugte	1	1	1	Tief	
10	Fehlerhafte Daten	1	1	1	Tief	
11	Mangelnde Verfügbarkeit der Daten	1	1	1	Tief	
12	Unbeachsichtigte Veröffentlichung an Dritte	4	1	4	Tief	
13	Übermässiges Datensammeln	4	2	8	Mittel	
14	Unerlaubte Kombination von Daten, Profiling	1	2	2	Tief	
15	Übermässig lange Aufbewahrung von Daten	1	1	1	Tief	
16	Unberechtigte Verweigerung eines Dienstes	2	1	2	Tief	
17	Diskriminierung	4	2	8	Mittel	
18	Rufschädigung	3	1	3	Tief	
19	Blossstellung	1	4	4	Tief	
20	Identitätsdiebstahl	1	1	1	Tief	
21	Gefahr für Leib und Leben	1	1	1	Tief	
22	Sachbeschädigung	1	1	1	Tief	
23	Finanzieller Schaden	1	1	1	Tief	
24	Unheimliches Gefühl, Chilling Effect, Angst	1	1	1	Tief	
25	Soziale oder wirtschaftliche Nachteile	3	3	9	Mittel	

Datenschutzverletzungen als solche

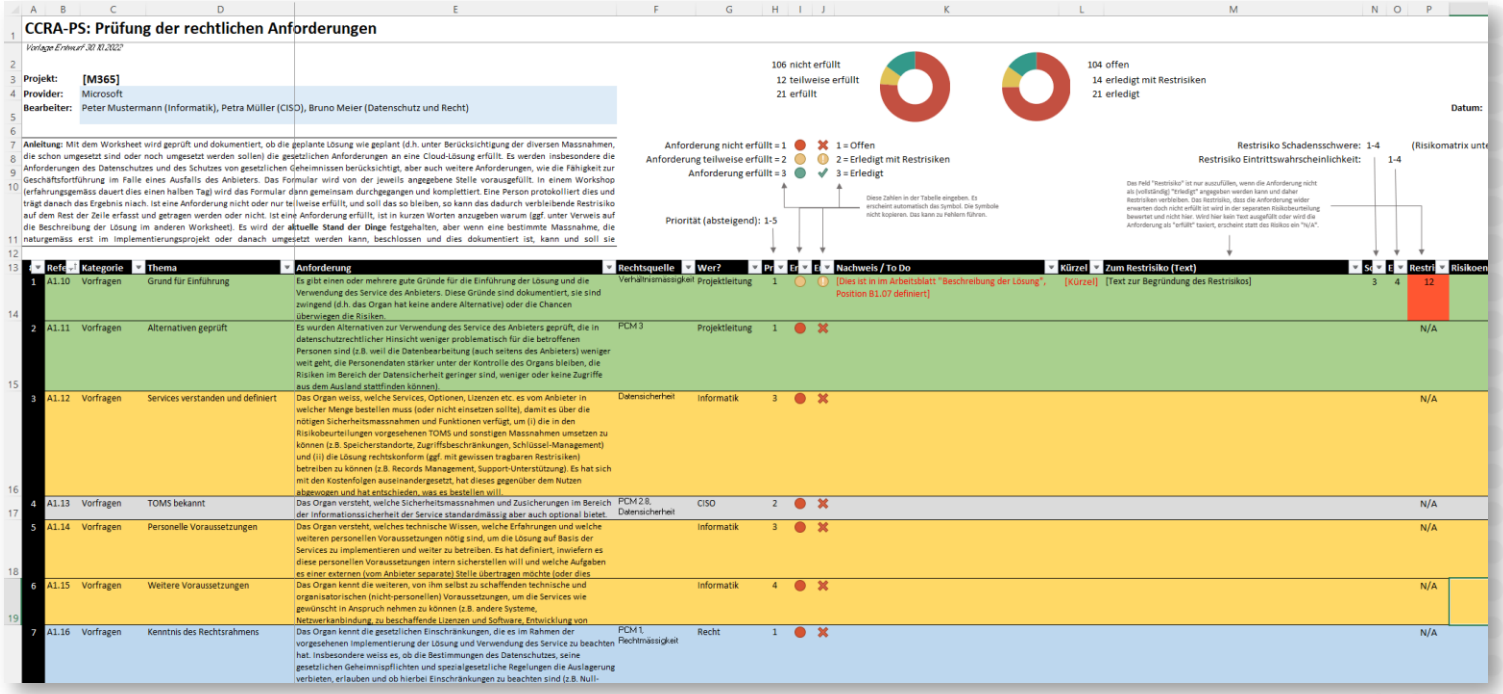
Mögliche tatsächliche nachteilige Ereignisse (siehe auch Tabelle unten)

Schritt 2: Datenschutz-Folgenabschätzung

Ursache		Folge betreffend die Personendaten		Folge für die betroffene Person
Mangelhafte Sicherheit seitens des Anbieters …	führt / führen zu	… Datenverlust …	und schliesslich zu	… einer unrechtmässigen Verweigerung/Gewährung eines Dienstes
Mangelhafte Sicherheit seitens der Institution …		… Zugriff durch unbefugte Mitarbeiter des Anbieters auf die Daten …		… einer Diskriminierung der betroffenen Person
Eine Fehlkonfiguration seitens des Anbieters …		… Zugriff durch unbefugte eigene Mitarbeiter auf die Daten …		… einem Identitätsdiebstahl
Eine Fehlmanipulation des Anbieters …		… Zugriff durch Dritte auf die Daten …		… einem Rufschaden der betroffenen Person
Eine Fehlmanipulation eigener Mitarbeitender …		… unberechtigter Bekanntgabe der Daten ins Ausland …		… einer Blossstellung der betroffenen Person
Eine Fehlkonfiguration eigener Mitarbeitender …		… unbeabsichtigter Veröffentlichung der Daten …		… einem finanziellen Schaden der betroffenen Person
Die Verletzung des Vertrages durch den Anbieter …		… mangelnde Verfügbarkeit der Daten …		… einem Schaden an Leib und Leben der betroffenen Person
Die Missachtung von Weisungen durch den Anbieter …		… fehlerhaften Daten …		… einem Schaden an Eigentum der betroffenen Person
Mangelhafte Weisungen gegenüber dem Anbieter …		… übermässigem Datensammeln …		… sozialen Nachteilen der betroffenen Person
Wirtschaftliche Probleme des Anbieters …		… unerlaubter Kombination von Daten …		… wirtschaftlichen/beruflichen Nachteilen der betroffenen Person
Rechtliche Probleme des Anbieters …		… übermässig langem Aufbewahren der Daten …		… politischen Nachteilen der betroffenen Person
Das wirtschaftliche Interesse des Anbieters …		… Profiling …		… einem unheimlichen Gefühl/Angst bei der betroffenen Person
Ein Rechtsverfahren im Ausland …		… Verwendung der Daten für Zwecke des Anbieters …		… psychologischen Folgen bei der betroffenen Person
Ein untreuer Mitarbeitender …		… einer Zweckentfremdung der Daten …		… einer unangebrachten Beeinflussung der betroffenen Person

Ursachen und mögliche Folgen …

Schritt 3: Prüfung der Anforderungen



CCRA-PS: Prüfung der rechtlichen Anforderungen

Vorlage Entwurf 30.10.2022

Projekt: [M365]
Provider: Microsoft
Bearbeiter: Peter Mustermann (Informatik), Petra Müller (CISO), Bruno Meier (Datenschutz und Recht)

106 nicht erfüllt
12 teilweise erfüllt
21 erfüllt

104 offen
14 erledigt mit Restrisiken
21 erledigt

Datum:

Anleitung: Mit dem Worksheet wird geprüft und dokumentiert, ob die geplante Lösung wie geplant (d.h. unter Berücksichtigung der diversen Massnahmen, die schon umgesetzt sind oder noch umgesetzt werden sollen) die gesetzlichen Anforderungen an eine Cloud-Lösung erfüllt. Es werden insbesondere die Anforderungen des Datenschutzes und des Schutzes von gesetzlichen Geheimnissen berücksichtigt, aber auch weitere Anforderungen, wie die Fähigkeit zur Geschäftsfortführung im Falle eines Ausfalls des Anbieters. Das Formular wird von der jeweils angegebene Stelle vorausgefüllt. In einem Workshop (erfahrungsgemäss dauert dies einen halben Tag) wird das Formular dann gemeinsam durchgegangen und komplettiert. Eine Person protokolliert dies und trägt danach das Ergebnis nach. Ist eine Anforderung nicht oder nur teilweise erfüllt, und soll das so bleiben, so kann das dadurch verbleibende Restrisiko auf dem Rest der Zeile erfasst und getragen werden oder nicht. Ist eine Anforderung erfüllt, ist in kurzen Worten anzugeben warum (ggf. unter Verweis auf die Beschreibung der Lösung im anderen Worksheet). Es wird der **aktuelle Stand der Dinge** festgehalten, aber wenn eine bestimmte Massnahme, die naturgemäss erst im Implementierungsprojekt oder danach umgesetzt werden kann, beschlossen und dies dokumentiert ist, kann und soll sie

Anforderung nicht erfüllt = 1 — 1 = Offen
Anforderung teilweise erfüllt = 2 — 2 = Erledigt mit Restrisiken
Anforderung erfüllt = 3 — 3 = Erledigt

Diese Zahlen in der Tabelle eingeben. Es erscheint automatisch das Symbol. Die Symbole nicht kopieren. Das kann zu Fehlern führen.

Priorität (absteigend): 1-5

Restrisiko Schadensschwere: 1-4 (Risikomatrix unte
Restrisiko Eintrittswahrscheinlichkeit: 1-4

Das Feld "Restrisiko" ist nur auszufüllen, wenn die Anforderung nicht als (vollständig) "Erledigt" angegeben werden kann und daher Restrisiken verbleiben. Das Restrisiko, dass die Anforderung wider erwarten doch nicht erfüllt ist wird in der separaten Risikobeurteilung bewertet und nicht hier. Wird hier kein Text ausgefüllt oder wird die Anforderung als "erfüllt" taxiert, erscheint statt des Risikos ein "N/A".

	Refe	Kategorie	Thema	Anforderung	Rechtsquelle	Wer?	Pr	Er	E	Nachweis / To Do	Kürzel	Zum Restrisiko (Text)	S	E	Restri	Risikoen
1	A1.10	Vorfragen	Grund für Einführung	Es gibt einen oder mehrere gute Gründe für die Einführung der Lösung und die Verwendung des Service des Anbieters. Diese Gründe sind dokumentiert, sie sind zwingend (d.h. das Organ hat keine andere Alternative) oder die Chancen überwiegen die Risiken.	Verhältnismässigkeit	Projektleitung	1			[Dies ist in im Arbeitsblatt "Beschreibung der Lösung", Position B1.07 definiert]	[Kürzel]	[Text zur Begründung des Restrisikos]	3	4	12	
2	A1.11	Vorfragen	Alternativen geprüft	Es wurden Alternativen zur Verwendung des Service des Anbieters geprüft, die in datenschutzrechtlicher Hinsicht weniger problematisch für die betroffenen Personen sind (z.B. weil die Datenbearbeitung (auch seitens des Anbieters) weniger weit geht, die Personendaten stärker unter der Kontrolle des Organs bleiben, die Risiken im Bereich der Datensicherheit geringer sind, weniger oder keine Zugriffe aus dem Ausland stattfinden können).	PCM 3	Projektleitung	1								N/A	
3	A1.12	Vorfragen	Services verstanden und definiert	Das Organ weiss, welche Services, Optionen, Lizenzen etc. es vom Anbieter in welcher Menge bestellen muss (oder nicht einsetzen sollte), damit es über die nötigen Sicherheitsmassnahmen und Funktionen verfügt, um (i) die in den Risikobeurteilungen vorgesehenen TOMS und sonstigen Massnahmen umsetzen zu können (z.B. Speicherstandorte, Zugriffsbeschränkungen, Schlüssel-Management) und (ii) die Lösung rechtskonform (ggf. mit gewissen tragbaren Restrisiken) betreiben zu können (z.B. Records Management, Support-Unterstützung). Es hat sich mit den Kostenfolgen auseinandergesetzt, hat dieses gegenüber dem Nutzen abgewogen und hat entschieden, was es bestellen will.	Datensicherheit	Informatik	3								N/A	
4	A1.13	Vorfragen	TOMS bekannt	Das Organ versteht, welche Sicherheitsmassnahmen und Zusicherungen im Bereich der Informationssicherheit der Service standardmässig aber auch optional bietet.	PCM 2.8, Datensicherheit	CISO	2								N/A	
5	A1.14	Vorfragen	Personelle Voraussetzungen	Das Organ versteht, welches technische Wissen, welche Erfahrungen und welche weiteren personellen Voraussetzungen nötig sind, um die Lösung auf Basis der Services zu implementieren und weiter zu betreiben. Es hat definiert, inwiefern es diese personellen Voraussetzungen intern sicherstellen will und welche Aufgaben es einer externen (vom Anbieter separate) Stelle übertragen möchte (oder dies		Informatik	3								N/A	
6	A1.15	Vorfragen	Weitere Voraussetzungen	Das Organ kennt die weiteren, von ihm selbst zu schaffenden technische und organisatorischen (nicht-personellen) Voraussetzungen, um die Services wie gewünscht in Anspruch nehmen zu können (z.B. andere Systeme, Netzwerkanbindung, zu beschaffende Lizenzen und Software, Entwicklung von		Informatik	4								N/A	
7	A1.16	Vorfragen	Kenntnis des Rechtsrahmens	Das Organ kennt die gesetzlichen Einschränkungen, die es im Rahmen der vorgesehenen Implementierung der Lösung und Verwendung des Service zu beachten hat. Insbesondere weiss es, ob die Bestimmungen des Datenschutzes, seine gesetzlichen Geheimnispflichten und spezialgesetzliche Regelungen die Auslagerung verbieten, erlauben und ob hierbei Einschränkungen zu beachten sind (z.B. Null-	PCM 1, Rechtmässigkeit	Recht	1								N/A	

Ca. 140

Schritt 3: Prüfung der Anforderungen

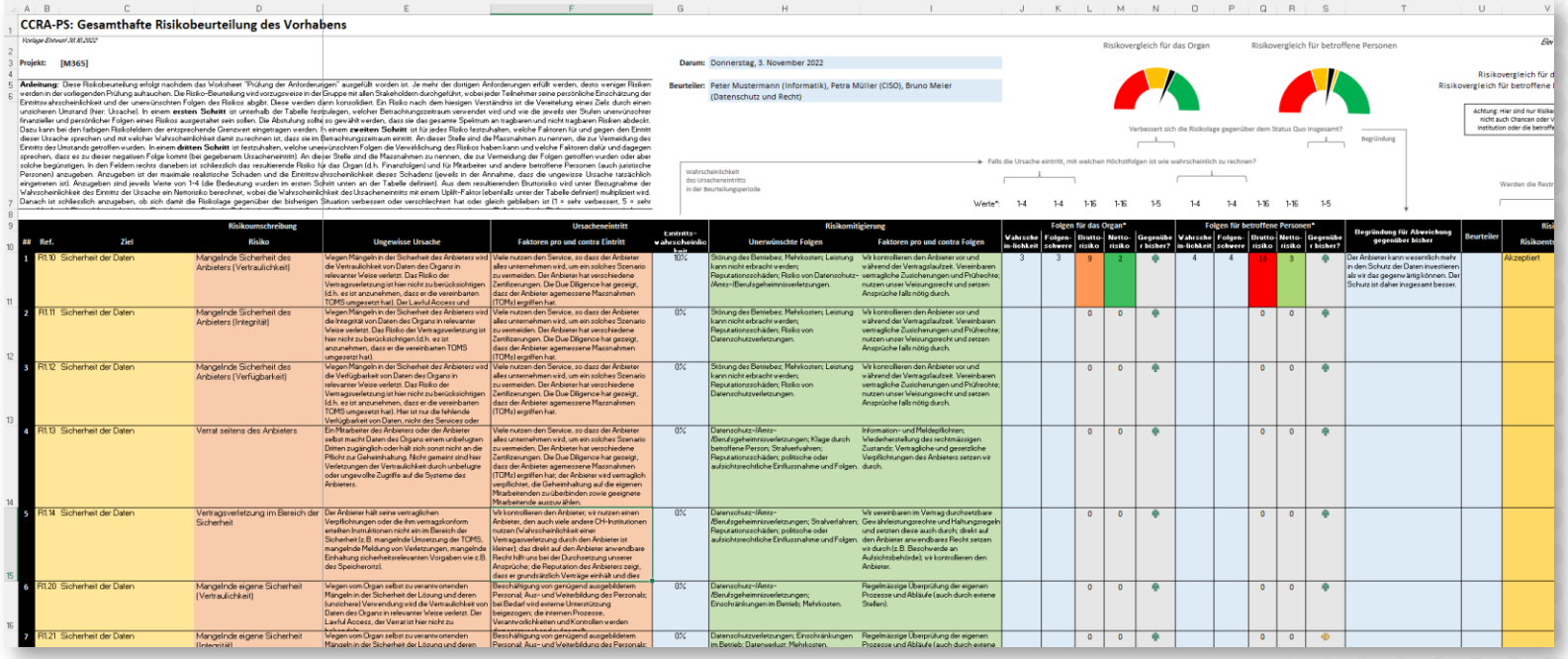
			Bearbeitung von Daten zu eigenen Zwecken des Bearbeiters umfassen.		
4	A2.21	Vertrag	Beizug von Unterauftragnehmern	Der Anbieter muss dem Organ den Beizug von Unterauftragsbearbeitern und anderen wesentlichen Unterauftragnehmern (insb. solche mit Zugang zu Inhalten) innert einer definierten Frist ankündigen, dem Organ deren Angaben offenlegen und ihnen die für sie relevanten Pflichten aus dem Vertrag überbinden (inklusive betr. Datenschutz und Geheimhaltung). Der Anbieter muss für das Verhalten der Unterauftragnehmer haften wie für sein eigenes Verhalten. Das Organ muss dem Beizug zustimmen oder hat das Recht, den Vertrag vorzeitig zu kündigen, falls ihm der Beizug als untragbar erscheint.	PCM 2.5

"Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern" sowie Anlagen 1 und 2 DPA; Ziff. 3 und 6 Anlage A CTM DPA. Eine Haftung des Anbieters für das Verhalten von Unterauftragnehmer "wie für sein eigenes" ist aber nicht vertraglich vereinbart. Damit ist nicht klar, ob in allen Fällen eines Fehlverhalten des Unterauftragnehmers auch zur Haftung von Microsoft führt.	AB	Microsoft haftet selbst für Vertragsverletzungen. Es kann bei einem Fall, den Microsoft selbst nicht zu verantworten hat, wohl aber ein Unterauftragnehmer eine Diskussion darüber geben, ob Microsoft haftet. Allerdings ist die Haftung von Microsoft ohnehin stark begrenzt. Ein besonderes Zusatzrisiko sehen wir hier nicht.	2	2	4
"Datenübermittlungen und Speicherstelle" und	VISCHER				N/A

Schritt 3: Prüfung der Anforderungen

121	A5.10	Überwachung	Überwachung Konfiguration	Das Organ überprüft regelmässig (z.B. quartalsweise) oder aus konkretem Anlass, ob die Konfiguration und Parametrisierung der Services des Anbieters noch dem Konfigurationsschema entspricht, ob Konfigurationselemente hinzugekommen oder weggefallen sind. Gibt es relevante Änderungen, werden die nötigen Massnahmen getroffen.	
122	A5.11	Überwachung	Providerseitige Anpassungen	Das Organ überprüft regelmässig (z.B. quartalsweise), ob seitens des Anbieters (i)	
102	A4.30	ISDS-Konzept	Datenminimierung	Es ist definiert, welche Funktionen ein- oder auszuschalten sind, damit es nicht zu einer unnötigen oder oder unerwünschten Erhebung oder sonstigen Bearbeitung von Personendaten kommt (z.B. Gesprächsaufzeichnungen, automatische Analysen). Soweit festgelegt werden kann, welche Personendaten erhoben werden sollen, ist dies zu definieren. Die zu erhebenden Personendaten ist so weit wie möglich einzuschränken. Die Anforderung der Pseudonymisierung wird aber nicht hier abgehandelt.	ISO 27701 7.4 Zweckbindung Verhältnismäs
103	A4.31	ISDS-Konzept	Pseudonymisierung und Anonymisierung	Personendaten und alle Inhalte, die einer gesetzlichen Geheimhaltungspflicht unterliegen, werden soweit und so rasch wie es der Anwendungszweck es erlaubt pseudonymisiert oder sogar anonymisiert. Wir haben diesbezüglich geprüft, was seitens der Services bzw. der Lösung vernünftigerweise möglich ist und dies entsprechend vorgesehen.	ISO 27701 7.4 Zweckbindung Verhältnismäs
104	A4.32	ISDS-Konzept	Aufbewahrungsfristen	Soweit eingestellt werden kann, wie lange Personendaten zugänglich gemacht oder aufbewahrt werden, ist festgelegt, wie lange dies sein soll (standardmässig, maximal). Dasselbe ist auch für andere Kategorien von Informationen festzulegen. Soweit eine Archivierungspflicht besteht, ist dies bei der technischen Konzeption der Lösung berücksichtigt. Die Aufbewahrungsfrist soll auf das Nötige bzw. (soweit geregelt) das	Verhältnismäs

Schritt 4: Risikobeurteilung



CCRA-PS: Gesamthafte Risikobeurteilung des Vorhabens

Vorlage Entwurf 30.10.2022

Projekt: [M365]

Anleitung: Diese Risikobeurteilung erfolgt nachdem das Worksheet "Prüfung der Anforderungen" ausgefüllt worden ist. Je mehr der dortigen Anforderungen erfüllt werden, desto weniger Risiken werden in der vorliegenden Prüfung auftauchen. Die Risiko-Beurteilung wird vorzugsweise in der Gruppe mit allen Stakeholdern durchgeführt, wobei jeder Teilnehmer seine persönliche Einschätzung der Eintrittswahrscheinlichkeit und der unerwünschten Folgen des Risikos abgibt. Diese werden dann konsolidiert. Ein Risiko nach dem hiesigen Verständnis ist die Vereinbarung eines Ziels durch einen unsicheren Umstand (hier: Ursache). In einem **ersten Schritt** ist unterhalb der Tabelle festzulegen, welcher Betrachtungszeitraum verwendet wird und wie die jeweils vier Stufen unerwünschter finanzieller und persönlicher Folgen eines Risikos ausgestaltet sein sollen. Die Abstufung sollte so gewählt werden, dass sie das gesamte Spektrum an tragbaren und nicht tragbaren Risiken abdeckt. Dazu kann bei den farbigen Risikofeldern der entsprechende Grenzwert eingetragen werden. In einem **zweiten Schritt** ist für jedes Risiko festzuhalten, welche Faktoren für und gegen den Eintritt dieser Ursache sprechen und mit welcher Wahrscheinlichkeit damit zu rechnen ist, dass sie im Betrachtungszeitraum eintritt. An dieser Stelle sind die Massnahmen zu nennen, die zur Vermeidung des Eintritts des Umstands getroffen wurden. In einem **dritten Schritt** ist festzuhalten, welche unerwünschten Folgen die Verwirklichung des Risikos haben kann und welche Faktoren dafür und dagegen sprechen, dass es zu dieser negativen Folge kommt (bei gegebenem Ursachereintritt). An dieser Stelle sind die Massnahmen zu nennen, die zur Vermeidung der Folgen getroffen wurden oder aber solche begünstigen. In den Feldern rechts daneben ist schliesslich das resultierende Risiko für das Organ (d.h. Finanzfolgen) und für Mitarbeiter und andere betroffene Personen (auch juristische Personen) anzugeben. Anzugeben ist der maximale realistische Schaden und die Eintrittswahrscheinlichkeit dieser Schadens (jeweils in der Annahme, dass die ungewisse Ursache tatsächlich eingetreten ist). Anzugeben sind jeweils Werte von 1-4 (die Bedeutung wurden im ersten Schritt unten an der Tabelle definiert). Aus dem resultierenden Bruttorisiko wird unter Berücksichtigung der Massnahme der Wahrscheinlichkeit des Eintritts der Ursache ein Nettorisiko berechnet, wobei die Wahrscheinlichkeit des Ursachereintritts mit einem Uplift-Faktor (ebenfalls unter der Tabelle definiert) multipliziert wird. Danach ist schliesslich anzugeben, ob sich damit die Risikolage gegenüber der bisherigen Situation verbessert oder verschlechtert hat oder gleich geblieben ist (1 = sehr verbessert, 5 = sehr

Datum: Donnerstag, 3. November 2022

Beurteiler: Peter Mustermann (Informatik), Petra Müller (CISO), Bruno Meier (Datenschutz und Recht)

Risikovergleich für das Organ

Risikovergleich für betroffene Personen

Verbessert sich die Risikolage gegenüber dem Status Quo insgesamt?

Begründung

Falls die Ursache eintritt, mit welchen Höchstfolgen ist wie wahrscheinlich zu rechnen?

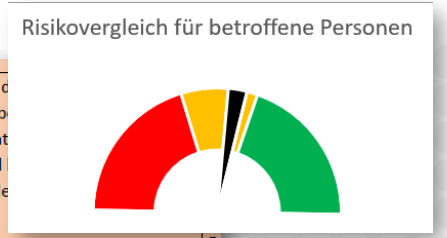
Wahrscheinlichkeit des Ursachereintritts in der Beurteilungsperiode

Werte*: 1-4 1-4 1-16 1-16 1-5 1-4 1-4 1-16 1-16 1-5

##	Ref.	Ziel	Risikoumschreibung: Risiko	Ungewisse Ursache	Ursacheneintritt: Faktoren pro und contra Eintritt	Eintritts-wahrscheinlichkeit	Risikomitigierung: Unerwünschte Folgen	Faktoren pro und contra Folgen	Folgen für das Organ*: Wahrscheinlichkeit	Folgenschwere	Bruttorisiko	Nettorisiko	Gegenüber bisher?	Folgen für betroffene Personen*: Wahrscheinlichkeit	Folgenschwere	Bruttorisiko	Nettorisiko	Gegenüber bisher?	Begründung für Abweichung gegenüber bisher	Beurteiler	Risikoentscheid
1	R1.10	Sicherheit der Daten	Mangelnde Sicherheit des Anbieters (Vertraulichkeit)	Wegen Mängeln in der Sicherheit des Anbieters wird die Vertraulichkeit von Daten des Organs in relevanter Weise verletzt. Das Risiko der Vertragsverletzung ist hier nicht zu berücksichtigen (d.h. es ist anzunehmen, dass er die vereinbarten TOMS umgesetzt hat). Der Lawful Access und	10%	Störung des Betriebes; Mehrkosten; Leistung kann nicht erbracht werden; Reputationsschäden; Risiko von Datenschutz-/Amts-/Berufsgeheimnisverletzungen.	Wir kontrollieren den Anbieter vor und während der Vertragslaufzeit. Vereinbaren vertragliche Zusicherungen und Prüfrechte; nutzen unser Weisungsrecht und setzen Ansprüche falls nötig durch.	3	3	9	2		4	4	16	3		Der Anbieter kann wesentlich mehr in den Schutz der Daten investieren als wir das gegenwärtig können. Der Schutz ist daher insgesamt besser.		Akzeptiert
2	R1.11	Sicherheit der Daten	Mangelnde Sicherheit des Anbieters (Integrität)	Wegen Mängeln in der Sicherheit des Anbieters wird die Integrität von Daten des Organs in relevanter Weise verletzt. Das Risiko der Vertragsverletzung ist hier nicht zu berücksichtigen (d.h. es ist anzunehmen, dass er die vereinbarten TOMS umgesetzt hat).	0%	Störung des Betriebes; Mehrkosten; Leistung kann nicht erbracht werden; Reputationsschäden; Risiko von Datenschutzverletzungen.	Wir kontrollieren den Anbieter vor und während der Vertragslaufzeit. Vereinbaren vertragliche Zusicherungen und Prüfrechte; nutzen unser Weisungsrecht und setzen Ansprüche falls nötig durch.			0	0				0	0				
3	R1.12	Sicherheit der Daten	Mangelnde Sicherheit des Anbieters (Verfügbarkeit)	Wegen Mängeln in der Sicherheit des Anbieters wird die Verfügbarkeit von Daten des Organs in relevanter Weise verletzt. Das Risiko der Vertragsverletzung ist hier nicht zu berücksichtigen (d.h. es ist anzunehmen, dass er die vereinbarten TOMS umgesetzt hat). Hier ist nur die fehlende Verfügbarkeit von Daten, nicht des Services oder	0%	Störung des Betriebes; Mehrkosten; Leistung kann nicht erbracht werden; Reputationsschäden; Risiko von Datenschutzverletzungen.	Wir kontrollieren den Anbieter vor und während der Vertragslaufzeit. Vereinbaren vertragliche Zusicherungen und Prüfrechte; nutzen unser Weisungsrecht und setzen Ansprüche falls nötig durch.			0	0				0	0				
4	R1.13	Sicherheit der Daten	Verrat seitens des Anbieters	Ein Mitarbeiter des Anbieters oder der Anbieter selbst macht Daten des Organs einem unbefugten Dritten zugänglich oder hält sich sonst nicht an die Pflicht zur Geheimhaltung. Nicht gemeint sind hier Verletzungen der Vertraulichkeit durch unbefugte oder ungewollte Zugriffe auf die Systeme des Anbieters.	0%	Datenschutz-/Amts-/Berufsgeheimnisverletzungen; Klage durch betroffene Person; Strafverfahren; Reputationsschäden; politische oder aufsichtsrechtliche Einflussnahme und Folgen.	Information- und Meldepflichten; Wiederherstellung des rechtmässigen Zustands; Vertragliche und gesetzliche Verpflichtungen des Anbieters setzen wir durch.			0	0				0	0				
5	R1.14	Sicherheit der Daten	Vertragsverletzung im Bereich der Sicherheit	Der Anbieter hält seine vertraglichen Verpflichtungen oder die ihm vertragskonform erteilten Instruktionen nicht ein im Bereich der Sicherheit (z.B. mangelnde Umsetzung der TOMS, mangelnde Meldung von Verletzungen, mangelnde Einhaltung sicherheitsrelevanten Vorgaben wie z.B. des Speicherorts).	0%	Datenschutz-/Amts-/Berufsgeheimnisverletzungen; Strafverfahren; Reputationsschäden; politische oder aufsichtsrechtliche Einflussnahme und Folgen.	Wir vereinbaren im Vertrag durchsetzbare Gewährleistungsrechte und Haftungsregeln und setzen diese auch durch; direkt auf den Anbieter anwendbares Recht setzen wir durch (z.B. Beschwerde an Aufsichtsbehörde); wir kontrollieren den Anbieter.			0	0				0	0				
6	R1.20	Sicherheit der Daten	Mangelnde eigene Sicherheit (Vertraulichkeit)	Wegen vom Organ selbst zu verantwortenden Mängeln in der Sicherheit der Lösung und deren (unsicherer) Verwendung wird die Vertraulichkeit von Daten des Organs in relevanter Weise verletzt. Der Lawful Access, der Verrat ist hier nicht zu	0%	Beschäftigung von genügend ausgebildetem Personal; Aus- und Weiterbildung des Personals; bei Bedarf wird externe Unterstützung beigezogen; die internen Prozesse, Verantwortlichkeiten und Kontrollen werden	Regelmässige Überprüfung der eigenen Prozesse und Abläufe (auch durch externe Stellen).			0	0				0	0				
7	R1.21	Sicherheit der Daten	Mangelnde eigene Sicherheit (Integrität)	Wegen vom Organ selbst zu verantwortenden Mängeln in der Sicherheit der Lösung und deren	0%	Beschäftigung von genügend ausgebildetem Personal; Aus- und Weiterbildung des Personals;	Datenschutzverletzungen; Einschränkungen im Betrieb; Datenverlust; Mehrkosten;	Regelmässige Überprüfung der eigenen Prozesse und Abläufe (auch durch externe			0	0				0	0				

Ca. 60

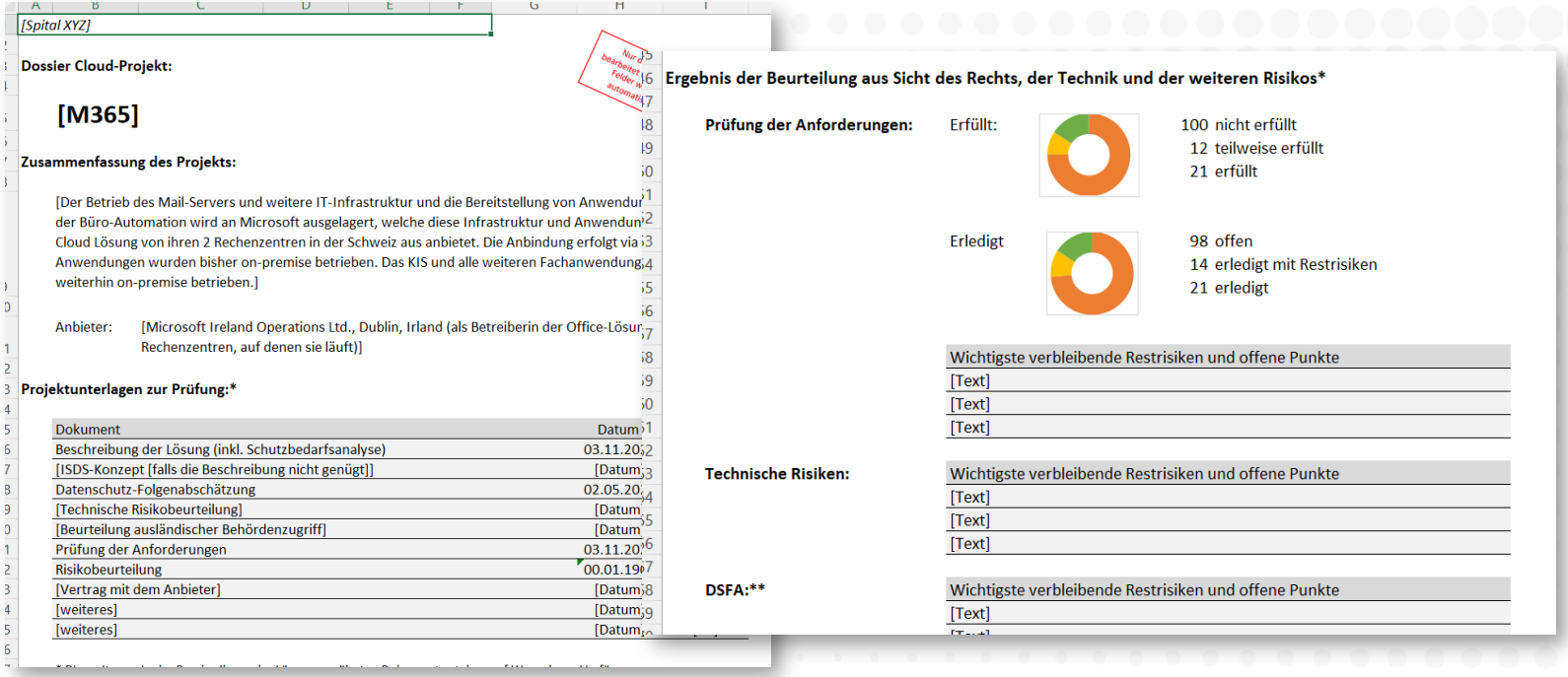
Schritt 4: Risikobeurteilung



			zu behandeln.	
4	R1.13 Sicherheit der Daten	Verrat seitens des Anbieters	Ein Mitarbeiter des Anbieters oder macht Daten des Organs einem unb zugänglich oder hält sich sonst nicht Geheimhaltung. Nicht gemeint sind Vertraulichkeit durch unbefugte ode auf die Systeme des Anbieters.	G üb
5	R1.14 Sicherheit der Daten	Vertragsverletzung im Bereich der Sicherheit	Der Anbieter hält seine vertraglichen Verpflichtungen oder die ihm vertragskonform erteilten Instruktionen nicht ein im	W Ar

Folgen für das Organ*					Folgen für betroffene Personen*					Begründung für Abweichung gegenüber bisher
Wahrscheinlichkeit	Folgenschwere	Bruttorisiko	Nettorisiko	Gegenüber bisher?	Wahrscheinlichkeit	Folgenschwere	Bruttorisiko	Nettorisiko	Gegenüber bisher?	
3	3	9	2	↑	4	4	16	3	↑	Der Anbieter kann wesentlich mehr in den Schutz der Daten investieren als wir das gegenwärtig können. Der Schutz ist daher insgesamt besser.

Schritt 5: Zusammenfassung



[Spital XYZ]

Dossier Cloud-Projekt:

[M365]

Zusammenfassung des Projekts:

[Der Betrieb des Mail-Servers und weitere IT-Infrastruktur und die Bereitstellung von Anwendur der Büro-Automation wird an Microsoft ausgelagert, welche diese Infrastruktur und Anwendun Cloud Lösung von ihren 2 Rechenzentren in der Schweiz aus anbietet. Die Anbindung erfolgt via Anwendungen wurden bisher on-premise betrieben. Das KIS und alle weiteren Fachanwendung weiterhin on-premise betrieben.]

Anbieter: [Microsoft Ireland Operations Ltd., Dublin, Irland (als Betreiberin der Office-Lösur Rechenzentren, auf denen sie läuft)]

Projektunterlagen zur Prüfung:*

Dokument	Datum
Beschreibung der Lösung (inkl. Schutzbedarfsanalyse)	03.11.20
[ISDS-Konzept [falls die Beschreibung nicht genügt]]	[Datum
Datenschutz-Folgenabschätzung	02.05.20
[Technische Risikobeurteilung]	[Datum
[Beurteilung ausländischer Behördenzugriff]	[Datum
Prüfung der Anforderungen	03.11.20
Risikobeurteilung	00.01.19
[Vertrag mit dem Anbieter]	[Datum
[weiteres]	[Datum
[weiteres]	[Datum

Ergebnis der Beurteilung aus Sicht des Rechts, der Technik und der weiteren Risikos*

Prüfung der Anforderungen:

Erfüllt:

100 nicht erfüllt
12 teilweise erfüllt
21 erfüllt

Erledigt

98 offen
14 erledigt mit Restrisiken
21 erledigt

Wichtigste verbleibende Restrisiken und offene Punkte
[Text]
[Text]
[Text]

Technische Risiken:

Wichtigste verbleibende Restrisiken und offene Punkte
[Text]
[Text]
[Text]

DSFA:**

Wichtigste verbleibende Restrisiken und offene Punkte
[Text]

Wie weiter?

Mit der nötigen Unterstützung machen wir auch eine französische Version

- Ab sofort **kostenlos** auf Deutsch zum Download verfügbar
  - https://www.rosenthal.ch/downloads/Rosenthal_CCRA-PS.xlsx
  - Es kann und soll jeder seine eigenen Berater verwenden
- Es ist ein Entwurf **"for public comment"**
  - Von uns bereits in diversen Pilotanwendungen von öffentlichen Organen des kantonalen Rechts und des Bundesrechts im Einsatz
  - Jetzt sollen es auch andere in Anwendungen testweise benutzen, um es kritisch zu prüfen und es besser zu machen helfen
- Wunderbar wäre, wenn unsere Initiative nicht nur Orientierung bietet, sondern auch den **Austausch an Know-how** fördert
  - Beispielsweise über Muster-Inhalte, Templates für Konzepte etc.

VISCHER

Vielen Dank für Ihre Aufmerksamkeit!

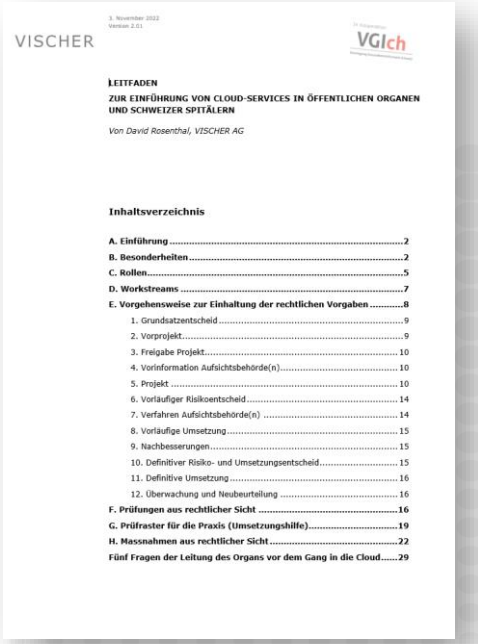
Fragen & Feedback: drosenthal@vischer.com

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


VISCHER

VGIch

LEITFADEN
ZUR EINFÜHRUNG VON CLOUD-SERVICES IN ÖFFENTLICHEN ORGANEN UND SCHWEIZER SPITÄLERN

Von David Rosenthal, VISCHER AG

Inhaltsverzeichnis

Cloud-Leitfaden für öffentliche Organe und Spitäler
https://bit.ly/3DOBwo4