Anhang C: Übersicht Risiken und Massnahmen[1]

Dieser Anhang soll einen groben Überblick über die Risiken und die jeweiligen Mitigierungsmassnahmen bieten. Für Cloud-Outsourcings im Rahmen von WTO 20007 wird ein Minimalstandard mit den Rahmenverträgen gewährleistet (vgl. Ziff. Teil 1, Ziff. 5 im Bericht).[2] Welche weiteren Massnahmen nötig sind, ist für ein konkretes Vorhaben anhand einer Risikoanalyse festzulegen. Nicht alle Massnahmen müssen in jedem Fall umgesetzt werden, namentlich dann nicht, wenn es sich weder um Personendaten noch um klassifizierte Daten bzw. Daten mit besonderem Schutzbedarf handelt.
Der Entscheid, ob und welche Cloud-Leistungen von einer Verwaltungseinheit bezogen werden, obliegt der Verwaltungseinheit. BK-DTI stellt Instrumente zur Verfügung, welche beim Entscheid helfen und vor diesem zu berücksichtigen sind.

Kategorien (vgl. Teil 1 Ziff. 3.1 im Bericht)

- C, Compliance-Risiken (rechtliche Risiken im engeren Sinne): Datenschutzverletzungen, Amtsgeheimnisverletzungen, Verletzung Informationsschutz (z.B. durch Zugriffe von Unberechtigten).
- BC, Business-Continuity-Risiken: Verfügbarkeit des Zugriffs auf eigene Daten, Verfügbarkeit der Netzwerke, Integrität der Daten.
- P, Politische Risiken: Rechtliches Umfeld im Ausland, z.B. Einschränkungen des freien Datenverkehrs; Behördenzugriffe nach ausländischem Recht ("legal access"); nachrichtendienstliche Ausspähung
- T: Technisches Risiko

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
1	Auftragnehmer und Unterauftragnehmer sind ungenügend instruiert und kontrolliert	C	Die verantwortlichen Bundesorgane müssen zwingend sicherstellen, dass insb. datenschutzrechtliche Anforderungen (einschliesslich Datensicherheit) eingehalten werden.	Vertragliche Massnahmen: • Regelung der Pflichten des CSP und deren Unterauftragnehmer. • Regelung der Voraussetzungen zum Beizug von Unterauftragnehmern durch den CSP, Widerspruchsrecht gegen Beizug von Subunternehmern, die wesentliche Teile der Leistung erbringen. • Kontrollbefugnisse des Auftraggebers vorsehen, z.B. Zugang zu Auditberichten, direkte Kontrollen.

[1] Quellen (Neben den im Bericht angeführten): David Rosenthal, Genügt eine Cloud-Lösung den Anforderungen einer Schweizer Bank; Dokumentation Microsoft Public Sector Cloud Design, Version 1.4
[2] Es sei daran erinnert, dass die Beschaffung WTO20007 Public Cloud hat zum Ziel hat, ein bestehendes Marktangebot abzuholen.

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
			Das verantwortliche Bundesorgan hat im Falle eines Cloud-Outsourcings Kontrollpflichten. Von CSP angebotene Standardvertragskonditionen reichen unter Umständen nicht aus, für ein rechtskonformes Cloud-Outsourcing. Werden die rechtlichen Vorgaben nicht eingehalten bzw. umgesetzt, drohen Haftungs- und Reputationsrisiken. Ebenso können betroffene Personen Klage wegen Grundrechtsverletzung einreichen.	• Kontrollaufgaben müssen tatsächlich durchgeführt werden. • Informationspflichten des CSP bei sicherheitsrelevanten Vorkommnissen vorsehen (vgl. auch Risiko Nr. 18) Organisatorische Massnahmen: • Vorgängige Klärung der konkreten Umsetzung der allgemeinen und bereichsspezifischen rechtlichen Anforderungen im Rahmen von Cloud-Sourcing-Projekten[3]. Vgl. Teil 2, Ziff. 1.5.3 im Bericht
2	Datenbekanntgabe in ausländische Staaten ohne angemessene Datenschutzgesetzgebung	C	Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet (Art. 16 Abs. 1 nDSG). Sollen Daten in Staaten übermittelt werden, die nicht über einen angemessenen Datenschutz verfügen, so sind besondere Schutzmechanismen nötig. Diese können vertraglicher oder auch technischer Art sein (Art. 16 Abs. 2 nDSG).	Vertragliche Massnahmen: • Bei der Nutzung von Cloud-Lösungen muss gewährleistet sein, dass Daten nur in einem bestimmten ausländischen Staat oder in bestimmten ausländischen Staaten bearbeitet und gespeichert werden und das ein angemessenes Datenschutzniveau gewährleistet ist. • Verpflichtung des CSP zum Abschluss von Standardvertragsklauseln mit Unterauftragnehmern, die aus Staaten ohne angemessene Datenschutzgesetzgebung auf Personendaten zugreifen. Technische Massnahmen:

[3] Verfügbare Hilfsmittel verwenden, insb. Schutzbedarfsanalyse (Schuban; https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/beurteilung-schutzbedarf.html) ; Informationsscherheits- und Datenschutzkonzept (ISDS; https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/erhoehter-schutz.html).

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
				• Verschlüsselung der Daten, welche den Zugriff auf den personenbezogenen Dateninhalt durch den (ausländischen) Auftragsdatenbearbeiter weitgehend ausschliesst (insb. für *data at rest*). • Prüfen, ob Vorgaben für *data in transit* möglich sind, z.B. betreffend das Routing. Vgl. Teil 2, Ziff. 1.2 im Bericht
3	Rechtsverletzungen aufgrund von Anwendbarkeit ausländischen Rechts	C	Gegebenenfalls stellt sich die Frage, ob die Rechtsordnung in einem Zielland generell besondere Risiken beinhaltet, etwa, weil Behörden des betreffenden Staates möglicherweise ohne Kenntnis des Cloud-Nutzers Zugang zu Daten verlangen können (oder zumindest ohne, dass er die Möglichkeit hat, sich dagegen zur Wehr zu setzen) oder auf Hardware zugreifen können (Beschlagnahmung)	Vertragliche Massnahmen: • Verpflichtung des CSP, sich an das einschlägige schweizerische Recht zu halten (insb. Datenschutzgesetz, ggf. auch Spezialgesetze); als Gerichtsstand ist grundsätzlich die Schweiz zu vereinbaren. • Vereinbarungen darüber, wie der Cloud-Anbieter auf Anfragen von Behörden oder Verfahren im Zusammenhang mit der Übergabe oder Übertragung geschützter Informationen vorgeht. • Soweit gesetzlich zulässig (Vgl. Teil 2, 1.6 im Bericht), sollten geschützte Informationen nur an ausländische Behörden übermittelt werden • mit schriftlicher Zustimmung des Cloud-Nutzer oder • aufgrund eines Urteils eines zuständigen Schweizerischen Gerichts oder • Bewilligung durch eine Schweizer Behörde. • Wo es das Gesetz erlaubt, bzw. eine behördliche Anordnung erlaubt, sollte der Cloud-Anbieter • den Cloud-Kunden rechtzeitig informieren, wenn er von einer ausländischen Behörde mit der Anordnung um Übertragung oder Offenlegung seiner in der Cloud gespeicherten Daten konfrontiert wird.. • dem Cloud-Nutzer das Recht einräumen, das Verfahren zu führen und bei der Bearbeitung von Ersuchen ausländischer Behörden mitzuwirken

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
				• Wenn der Anbieter aufgrund zwingenden Rechts nicht in der Lage ist, den Cloud-Nutzer im Voraus über die Übermittlung oder Offenlegung geschützter Informationen an ausländische Behörden oder andere Parteien im Ausland zu informieren, muss der Cloud-Anbieter im Rahmen der getroffenen Vereinbarung und im Interesse des Cloud-Nutzer die geeigneten rechts- oder sicherungsrechtlichen Massnahmen ergreifen. Festlegen von Berichtspflichten des CSP und Zugang zu Auditergebnissen. Organisatorische Massnahmen: • Der Cloud-Anbieter bietet ausreichenden Einblick in seine Abläufe und Richtlinien bezüglich des staatlichen Zugriffs auf Daten, der dem Cloud-Nutzer eine informierte Entscheidung zu diesem Thema ermöglicht. Technische Massnahmen: • Verschlüsselung, insb. von *data at rest* und *data in transit*. • Management des Schlüssels durch Auftraggeber (Bundesorgan) oder allenfalls Drittanbieter. Der Auftraggeber autorisiert Benutzer, Prozesse und kann Berechtigungen überwachen. • Kollisionen (z.B. im Falle der Beschlagnahmung von Hardware im Rahmen eines Strafverfahrens im Ausland, die auch Daten eines Bundesorgans umfassen) können nicht vollständig ausgeschlossen werden. Vgl. Ziff. Teil 2, Ziff. 1.2 und 1.6 im Bericht
4	Veränderung des Rechtsrahmens aufgrund von Änderun-	C	Vgl. Nr. 2 und 3	Vertragliche Massnahmen: • Jederzeitige Transparenz über Standorte; wenn möglich Verpflichtung des CSP auf bestimmte Standorte

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
	gen des Standortes von Rechenzentren		Unzulässige Datenbearbeitung an dem Auftraggeber unbekannten Standorten	Vgl. Teil 2, Ziff. 1.6 im Bericht
5	Sicherheitsvorfälle werden dem Auftraggeber Bund nicht kommuniziert, es werden durch die Cloud-Dienstleister keine genügenden Massnahmen getroffen	C	Im Falle von schweren Sicherheitsvorfällen muss der Auftraggeber analysieren können, was geschehen ist, wie Angreifer vorgegangen sind, welche Bereiche betroffen sind und diese ggf. schnellstmöglich isolieren. Der Auftraggeber muss Massnahmen definieren können, um ähnliche Vorfälle zu verhindern. Der Auftraggeber muss die Kontrolle über das Sicherheitsmanagement behalten können.	Vertragliche Massnahmen: • Regelung der Verteidigung bei Angriffen gegen auf der Cloud betriebene Applikationen des Bundes. • Festlegen von Berichtspflichten des CSP und Zugang zu Auditergebnissen. • Regelung der Unterstützung der zuständigen Stellen des Bundes (insb. CSIRT/BIT; NCSC) durch CSP (ggf. Mitwirkungspflicht vorsehen). Organisatorische Massnahmen: • Verantwortlichkeiten beim Security Incident Management festlegen.
6	Mangelnde Sicherheitsmassnahmen	T	Es muss sichergestellt werden, dass der CSP mindestens das gleiche Sicherheitsniveau gewährleistet wie der Auftraggeber. Die zu ergreifenden Sicherheitsmassnahmen richten sich insb. nach der Art der bearbeiteten Daten und nach dem Bedarf ein ungemessenes Datenschutzniveau zu kompensieren (Ergebnis Schutzbedarfsanalyse).	Vertragliche Massnahmen: • Weitergehende Verpflichtungen des CSP (insb. beim Beizug von Subunternehmern) vereinbaren. • CSP muss Prüfberichte vorweisen, welche die Datensicherheit dokumentieren (der Nachweis einer Zertifizierung oder eine Prüfbestätigung genügt nicht). • Verpflichtung des CSP zur Meldung von schwerwiegenden Cyberangriffen mit Auswirkungen auf Daten des Bundes und vom Bund bezogene Dienstleistungen. Organisatorische Massnahmen: • Standardkonditionen des CSP prüfen. • Zugriffskonzept erstellen.

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
			U.u. sind spezifische Massnahmen vorgeschrieben, die das Bundesorgan ergreifen muss (z.B. bezüglich Protokollierung, Datenhaltung). Sicherheitsfragen kann insb. der Einsatz von (privaten) Mobilgeräten aufwerfen (Zugriff via Apps).	• Vereinbarung betr. Kontrollen vor Ort. Technische Massnahmen: • Vorkehrungen zum Schutz der Integrität und Verfügbarkeit der Daten • Zugriff von Mobilgeräten aus erfolgt nur via sandboxed App Vgl. Teil 2, Ziff. 1.2.2 im Bericht
7	Beschlagnahmung von Hardware mit Daten des Bundes durch Behörden im Ausland	C	Werden Datenträger im Ausland beschlagnahmt, kann es aufgrund gemeinsamer Nutzung der Hardware-Infrastruktur zu Offenlegung von Daten kommen, die nicht Gegenstand des Herausgabebegehrens waren.	Vertragliche Massnahmen: • Vgl. Nr. 3 oben. Organisatorische Massnahmen: • Cloud-Nutzung auf geteilter Infrastruktur für bestimmte Daten vermeiden (Nutzung Private Cloud). Technische Massnahmen: • Verschlüsselung; Management des Schlüssels durch Auftraggeber (Bundesorgan) • logische Trennung von Daten (eigene Tenants/Mandanten) Vgl. Teil 2, Ziff. 1.2 im Bericht
8	Nichteinhaltung von rechtlichen Vorgaben im Bereich des Datenschutzes oder des Geheimnisschutzes	C	Der Auftraggeber muss sicherstellen, dass mindestens die Vorgaben des DSG (oder der DSGVO) sowie allfällige spezialgesetzliche Vorgaben im jeweiligen Aufgabenbereich eingehalten werden. Soweit Daten in Staaten bearbeitet werden, die über kein angemessenes Datenschutzniveau verfügen, ist zu prüfen, wo	Vertragliche Massnahmen: • Verpflichtungen des CSP klar formulieren. • CSP darf nicht für eigene Zwecke auf Daten zugreifen. Organisatorische Massnahmen: • Service-Spezifikationen des CSP prüfen. • Zugriffskonzept festlegen. Technische Massnahmen:

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
			zusätzliche Vereinbarungen mit dem CSP nötig sind. Der Umfang der Verantwortung des CSP ist auch abhängig vom Cloud-Modell. Insb. unklare Regelungen von Zugriffen können zu Datenschutzverletzungen oder Verletzungen des Geheimnisschutzes führen.	• Verschlüsselung und Schlüsselmanagement • Zugriffe nur mit Multifaktor-Authentisierung Vgl. Teil 2, Ziff. 1.2 im Bericht Vgl. auch Risiko Nr. 6
9	Politischer Druck auf Provider zur Kooperation mit ausländischen Behörden zum Schaden des Bundes (Datenherausgabe, Blockierung von Daten)	P	Die rechtlichen und politischen Rahmenbedingungen in den Ländern, in denen Daten gehostet und/oder bearbeitet werden, sind dynamisch und können sich im Zeitablauf ändern.	Vertragliche Massnahmen: • Vereinbarung von Bearbeitungsstandorten, die rechtlich und politisch stabil sind. • Vereinbarung von Exit-Klauseln Organisatorische Massnahmen: • Regelmässige Prüfung des rechtlichen und politischen Umfeldes • Regelmässige Prüfung der Länderliste Technische Massnahmen: • Verschlüsselung; Management des Schlüssels durch Auftraggeber (Bundesorgan) Vgl. Teil 2, Ziff. 1.2 im Bericht
10	Mangel an erforderlichen personellen Ressourcen mit adäquatem Fachwissen	BC	Kein Cloud-spezifisches Risiko. Der Cloud-Nutzer muss Zugang zu adäquaten Ressourcen für den Betrieb von hybriden Systemlandschaften haben.	Organisatorische Massnahmen: • Sicherstellung des Zugangs zu den nötigen fachlichen Ressourcen • Angemessene Planung und Vorbereitung des Vorhabens • Unterstützung bei der Einführung durch CSP • Austausch von «best practices» innerhalb der Bundesverwaltung

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
			Es muss gewährleistet werden können, dass die mit Cloud-Outsourcing verbundenen Risiken umfassend eingeschätzt und nur angemessene Risiken eingegangen werden. Die Einführung von Cloud-Lösungen bedingt einen Prozess, der die betroffenen Applikationen umfassend darauf ausrichtet und insb. die Mitarbeitenden ausreichende vorbereitet.	• Ausbildung der Mitarbeitenden, die mit der Cloud-Applikation arbeiten.
13	Mängel in der Zusammenarbeit zwischen Bund und CSP, dadurch unvorhergesehener Service-Stop oder Serviceänderung, Betriebsunterbrüche	BC	Services können aus verschiedenen Gründen nicht mehr oder nur unter veränderten Bedingungen zugänglich sein: CSP ändert Standardkonditionen Schadensereignisse Angriffe Wie weit solche Risiken tragbar sind, ist von den business-continuity-Anforderungen an die betreffenden Anwendungen abhängig.	Vertragliche Massnahmen: • Wesentliche Serviceänderungen sind mit ausreichendem zeitlichen Vorlauf durch den CSP mitzuteilen. • Exit-Option bei Änderung der Konditionen. • Regelung der Zusammenarbeit mit dem CSP für Wiederherstellungsverfahren, forensische Analysen, illegaler oder missbräuchlicher Nutzung der Ressourcen. • Finanzielle Kompensation bzw. Konventionalstrafen für besonders kritische Arten von unvorhergesehenen Serviceunterbrechungen. Organisatorische Massnahmen: • Überwachung der Tätigkeiten der CSP und Subunternehmer. • Alternativplanungen für Service-Ausfälle (BC). Technische Massnahmen: • Sicherstellen, dass Daten (allenfalls innerhalb der Schweiz) unabhängig von der Cloud-Anwendung verfügbar sind (Backups oder Mirrors)

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
				• Wiederherstellungsverfahren implementieren Vgl. Teil 2, Ziff. 1.2 im Bericht Vgl. auch Risiko Nr. 16
14	Angriffe durch böswillige Mitarbeitende, Innentäter	BC	Kein Cloud-spezifisches Risiko, es verschärft sich aber möglicherweise im Cloud-Umfeld. Cloud-Computing-Architekturen erfordern hochprivilegierte Zugänge und Berechtigungen. Innentäter haben u.U. die Möglichkeit, Daten zu manipulieren, an Unberechtigte weiterzugeben oder die Verfügbarkeit eines Dienstes zu stören. Das Risiko ist in einem Outsourcing-Szenario höher als bei on-premises Bearbeitung, insb. weil der Cloud-Nutzer Sicherheitskontrollen nicht selber durchführen kann. Das Risiko ist abhängig vom jeweiligen Cloud-Modell.	Vertragliche Massnahmen: • Klare Regelung der Befugnisse von Administratoren (auf beiden Seiten) • Vertragliche Regelung der anzuwendenden Sicherheitsverfahren (ggf. auch gestützt auf allgemeine Geschäftsbedingungen). • Ggf. Sicherheitsverfahren und -kontrollen für die Mitarbeitenden des CSP vertraglich regeln bzw. entsprechende Optionen vereinbaren (z.B. Advanced Secure Support) Organisatorische Massnahmen: • Rollenmodelle auf Cloud-Anwendung ausrichten, • Zugriffskonzepte definieren. Technische Massnahmen: • Protokollierung • Strikte Umsetzung des Need-to-know-Prinzips
15	Risiken, welche durch die gemeinsame Nutzung von Infrastruktur entstehen (Multi-tenacity, shared technologie issues);	T	Beim Public-Cloud-Modell werden typischerweise Ressourcen auf der Seite des CSP mit anderen Kunden geteilt. Die Isolierung von Daten kann dabei fehlerhaft sein; eine logische Trennung ist aus heutiger Sicht weniger sicher, als eine physische Trennung von Daten.	Technische Massnahmen: • Verschlüsselung • Gesicherte Bearbeitung • Besondere, gesicherte VM-Architekturen

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
	Isolationsversagen insb. im Angriffsfall		Das Risiko kann durch technische Massnahmen gesenkt, aber nicht vollständig eliminiert werden.	Vgl. Teil 2, Ziff. 1.2 im Bericht
16	Abhängigkeit vom Anbieter (vendor lock-in), beschränkte Datenportabilität	BC	Ein späterer Wechsel des Anbieters kann sich technologisch und wirtschaftlich schwierig gestalten. Er kann aber schon nur aus beschaffungsrechtlichen Gründen nötig sein[4]. Unter Umständen bieten CSP nur sehr beschränkte Unterstützung, wenn Daten aus der Cloud zu einem anderen Provider oder zurück auf eine eigene «on-premise» Umgebung migriert werden. Allenfalls kann ein CSP solche Migrationen aktiv oder passiv erschweren. Eine Migration kann grössere organisatorische oder technische Anpassungen nötig machen.	Vertragliche Massnahmen: • Exit-Szenario (Opt-Out) vereinbaren. • Datenexport und Migration regeln (z.B. APIs). Berücksichtigen, dass Daten ohne die zugehörige Business-Logik u.U. wenig nützen (z.B. bei SaaS). Organisatorische Massnahmen: • BC-Planung für Anbieterwechsel oder Rückführung Bei Projektstart Exit-Strategie festlegen. Technische Massnahmen: • Wählen einer Architektur (Abstraktionslayer), welche den Betrieb unabhängig vom darunterliegenden Cloud-Modell bzw. –Anbieter ermöglicht. • Zurverfügungstellung von APIs für Migration • Klären, ob die proprietären Datenstrukturen der CSP dokumentiert und für Auftraggeber zugänglich sind. • Dokumentation von Exportformaten. • Importroutinen (Mapping) definieren. • Sicherstellen, dass Daten (allenfalls innerhalb der Schweiz) unabhängig von der Cloud-Anwendung verfügbar sind (Backups oder Mirrors)

[4] Bei Cloud-Outsourcings im Rahmen der mit WTO 20007 beschafften Dienstleistungen ist zu beachten, dass die Laufzeit der Rahmenverträge 5 Jahre ab Mitte 2021 (Datum des Zuschlags) beträgt (eine Verlängerung ist derzeit in Prüfung).

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
17	Unzureichendes Schlüsselmanagement	BC, T	Risiken können sich einerseits dadurch ergeben, dass der CSP oder Unterauftragnehmer auf Schlüssel zugreifen können, wenn diese in der Cloud gespeichert werden müssen und daher logisch und physisch unter der Kontrolle des CSP stehen. Andererseits besteht bei unzureichender Organisation des Schlüsselmanagements das Risiko von Datenverlusten. Schliesslich ist zu gewährleisten, dass notwendigenfalls die Löschung von Schlüsseln auch umgesetzt wird, insb. wen Hosting Provider beigezogen werden.	Organisatorische Massnahmen: • Klären (ggf. vertraglich festlegen) an welcher Stelle (beim CSP oder bei beigezogenen Dritten) die Verschlüsselung stattfindet, wer welche Schlüssel zur Entschlüsselung generiert und wo diese Schlüssel physisch gespeichert sind (jeweils für die verschiedenen Bearbeitungsstadien). • Rollenkonzept definieren, Verantwortlichkeiten klären (Bearbeitungsreglement) • Best practices anwenden Technische Massnahmen: • Detektion einer nicht autorisierten Schlüsselverwendung Vgl. Teil 2, Ziff. 1.2 im Bericht
18	Kompromittierte Software, kompromittierte Hardware-Komponenten (backdoors)	T	Dieses Risiko hat verschiedene Ausprägungen: - Verschlüsselung (Generalschlüssel/Nachschlüssel) - Sicherheitslücken («zero days»), die nicht offengelegt und z.B. nachrichtendienstlich verwendet werden - Hardware-backdoors, Spychips Das Risiko kann gesenkt, aber nicht vollständig eliminiert werden.	Dieses Risiko besteht zu erheblichen Teilen auch bei on-premises-Lösungen. Vertragliche Massnahmen: • Zusicherung, dass Begehren um Zugriff auf Daten durch ausländische Behörden nur in den jeweils vorgesehenen Rechtsverfahren behandelt und der CSP die verfügbaren rechtlichen Mittel ergreift. • Verpflichtung des CSP zur Einhaltung von ISO-Standards. • Informationspflichten bei Sicherheitsvorfällen und bei (erfolgreichen und nicht erfolgreichen Angriffen auf Daten des Bundes. • Zugang der verantwortlichen Bundesstelle zu Audit-Ergebnissen.

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
				Technische Massnahmen: • Einsatz von Trusted Platform Modules • Verschlüsselung; Management des Schlüssels durch Auftraggeber (Bundesorgan)
19	Systemintegrität und Kompromittierte Management-Interfaces beim Zugriff via Internet	T	Bei der Nutzung von Cloud-Diensten via Internet können sich Unbefugte durch Angriff auf die Management-Interfaces Zugang zu Anwendungen und Daten verschaffen.	Vertragliche Massnahmen: • Information der verantwortlichen Bundesstelle über Angriffe festlegen. • Vertragliche Zusicherungen betr. Detektion von Schwachstellen durch den Provider. • Vorgaben betr. Personensicherheit beim CSP und Unterauftragnehmern Organisatorische Massnahmen: • Zusammenarbeit der Administratoren auf Seiten CSP und Bund klären • Berechtigungs- und Zugriffsmanagement klar definieren Technische Massnahmen: • Allenfalls Penetration-Testing durch die Bundesverwaltung, bei sehr sensiblen Systemen. • Zugriffsbeschränkungen auf autorisierte Kunden IP Adressbereiche
20	Unsichere oder unvollständige Datenlöschung	C, T	Sichere und vollständige Datenlöschung ist in insb. in folgenden Szenarien nötig: - Im Falle eines Anbieterwechsels; - Gesetzliche Maximalfristen, insb. für die Aufbewahrung von Perso-	Die Prozesse beim CSP betr. Datenlöschung sind vorab zu klären. Vertragliche Massnahmen: • Zugang zu Auditergebnissen sicherstellen, welche die Einhaltung von Prozessen zertifizieren. • Information/Bestätigung von Löschungen vorsehen. • Unbefristete Geheimhaltungsverpflichtung des CSP (und von Unterauftragnehmern) vereinbaren.

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
			nendaten (insb. auch von Randdaten) - Umsetzung von Löschungsbegehren bei Personendaten.	Organisatorische Massnahmen: • Verantwortlichkeiten für die Löschung von Daten dokumentieren. Technische Massnahmen: • Verschlüsselung; Management des Schlüssels durch Auftraggeber (Bundesorgan)
21	Ungenügende Netzwerkkapazitäten	T	Kein Cloud-spezifisches Risiko. Die Verfügbarkeit der Cloud-Dienste hängt aber besonders von der Verfügbarkeit der Netzwerke ab, die für den Datenaustausch benutzt werden. Ungenügende Bandbreite kann dazu führen, dass die Verfügbarkeit der Cloud-Dienste nicht im notwendigen Umfang gegeben ist. Ausmass des Risikos hängt auch davon ab, wie hoch die Verfügbarkeit des betreffenden Dienstes bzw. der betreffenden Anwendung sein muss.	Vertragliche Massnahmen: • Zusagen (vom CSP oder ggf. einem dritten Netzbetreiber) betr. Verfügbarkeit verlangen (Einhaltung von Standards/best practices) • Konventionalstrafen vereinbaren, die fällig werden, wenn bestimmte Verfügbarkeitsziele nicht eingehalten werden. Organisatorische Massnahmen: • Alarmierung durch den CSP klären • BC-Massnahmen für den Ausfall des Dienstes definieren Technische Massnahmen: • Redundanzen vorsehen • Anbindung der BVerw an Public Cloud Anbieter über Cloud Exchange Provider (CXP). • Nutzung künftiger Standarddienst Datenkommunikation (DAKO).
22	Nichteinhaltung von vertraglichen Verpflichtungen durch CSP	C	Der CSP muss Gewähr bieten für die vertragstreue Umsetzung seiner Verpflichtungen.	Vertragliche Massnahmen: Ausschluss von einseitigen Vertragsänderungen. Alternativ: Informationsmöglichkeit über Vertragsänderungen mit genügend Vorlauf. Kündigungsrechte bei Vertragsänderungen

Nr.	Risiko	Kategorie	Risikobeschreibung	Mögliche Massnahmen
				Angemessene Haftung für Vertragsverletzungen durch CSP und Unterauftragnehmer, kein Ausschluss bei grober Fahrlässigkeit oder Vorsatz (dort, wo das ausländische Recht dies zulässt).