



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Bereich Digitale Transformation und IKT-Lenkung DTI

Schwerpunkt 4 Digitale Souveränität stärken
(vormals: Strategische Initiative SI-4 «Hybrid Multi-Cloud»)

V1.0 / März 2024

CSB-Pflichtenheft der Bundesverwaltung

Inhaltsverzeichnis

1	Einleitung	4
2	Grundlagen aus Cloud-Strategie der Bundesverwaltung	5
3	Cloud Service Broker in der Bundesverwaltung.....	7
3.1	Zusammenspiel DTI, CSB und Verwaltungseinheit in der Bundesverwaltung ..	8
3.2	Finanzierung Leistungen CSB	9
4	Aufgaben, Kompetenzen und Verantwortlichkeiten eines CSB	10
4.1	Aufgaben eines CSB	10
4.2	Kompetenzen eines CSB	14
4.3	Verantwortlichkeiten eines CSB	15
5	Glossar	18
6	Referenzen	19
	Anhang 1: Zusammenspiel Public-Cloud-Akteure im Kontext WTO 2007	20

1 Einleitung

Die Cloud-Strategie der Bundesverwaltung [1], welche vom Bundesrat im Dezember 2020 verabschiedet wurde, hat zum Ziel, den Weg für die Nutzung von Cloud-Diensten zu ebnen. Durch die geordnete, sichere und effiziente Nutzung von Public Clouds soll der schnelle Zugang zu neuesten Technologien für wirtschaftliche und innovative Verwaltungsleistungen zugunsten Wirtschaft und Bevölkerung ermöglicht werden. Der Bezug von Public-Cloud-Leistungen durch die Verwaltungseinheiten in der Bundesverwaltung erfolgt über einen **Cloud Service Broker (CSB)**.

Aufbauend auf den Cloud-Prinzipien der Bundesverwaltung [2] beschreibt das vorliegende CSB-Pflichtenheft die Erwartungen an die Rolle eines CSB und das Zusammenspiel im Dreieck des Bereichs Digitale Transformation und IKT-Lenkung der Bundeskanzlei (Bereich DTI der BK) – CSB – Verwaltungseinheiten (VE). Der CSB hat die in diesem Dokument generisch beschriebenen Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) beim Bezug von Public-Cloud-Leistungen wahrzunehmen und umzusetzen.

Vereinbarung für Bezug von Public-Cloud-Diensten über das Beschaffungsgefäß WTO 20007 zwischen DTI - CSB:

Auf Basis des vorliegenden CSB-Pflichtenhefts wird zwischen DTI und jedem CSB eine separate Vereinbarung von Rechten und Pflichten festgelegt, welche der Einhaltung der Bedingungen der Rahmenverträge dienen. Diese Vereinbarungen zwischen DTI und CSB werden ausserhalb dieses Dokuments festgelegt.

Anmerkung: im gesamten Dokument werden WTO 20007 spezifische Textabschnitte jeweils eingerahmt dargestellt.

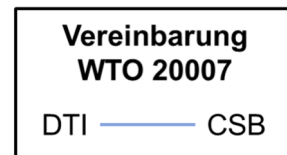
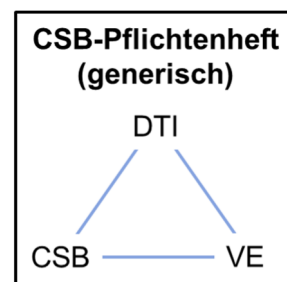


Abbildung 1: Abgrenzung CSB-Pflichtenheft und Vereinbarung WTO 20007

Im vorliegenden CSB-Pflichtenheft werden folgende Fragen beantwortet:

- Was ist die Rolle eines CSB?
- Wie bettet sich der CSB in die Struktur der Bundesverwaltung ein?
- Wie ist das Zusammenspiel der verschiedenen Akteure und wie wird die Verantwortung geteilt?
- Was sind die Aufgaben, Kompetenzen und Verantwortlichkeiten eines CSBs?

2 Grundlagen aus Cloud-Strategie der Bundesverwaltung

Die Verwaltungseinheiten beziehen Public-Cloud-Leistungen grundsätzlich über einen CSB, der die Public-Cloud-Foundation mit entsprechenden Hilfsmitteln und Expertise gemäss Vorgaben zur Verfügung stellt (siehe Abbildung 2). Dabei gelten die im Kapitel 0 aufgeführten Grundsätze aus der Cloud-Strategie der Bundesverwaltung [1] und die in Kapitel 4 definierten AKVs.

Die Begriffe Cloud Service Broker (CSB) und Intermediär werden als Synonyme verwendet.

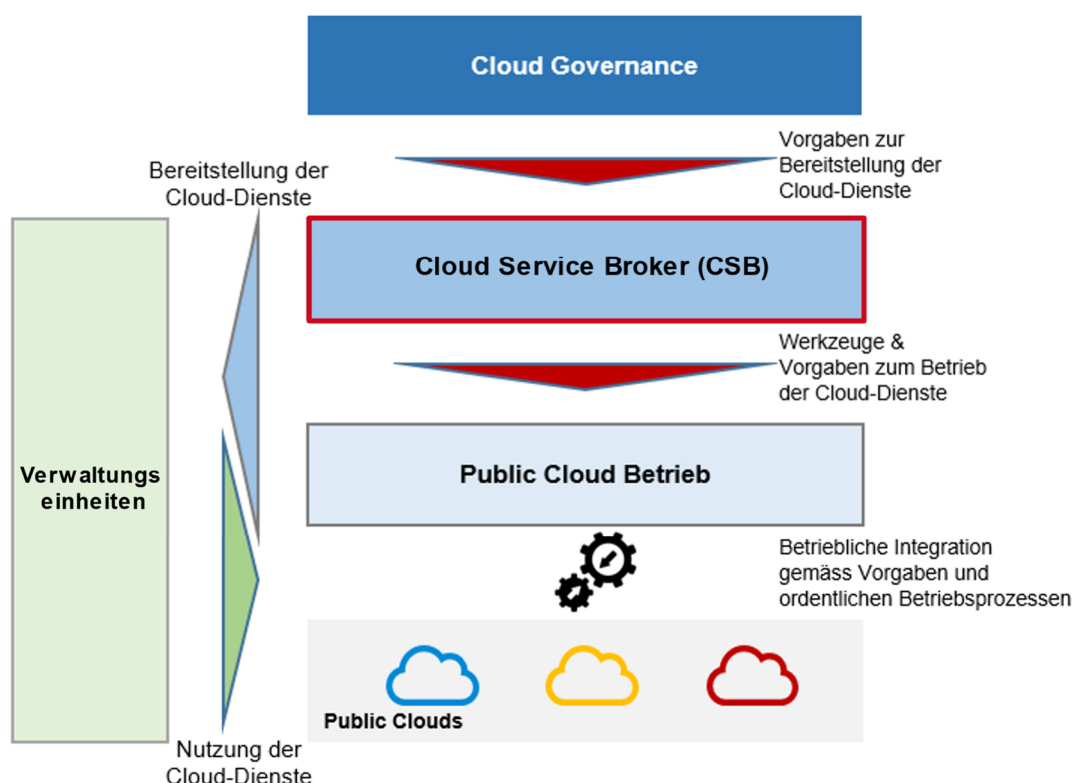


Abbildung 2: Rolle CSB in der Bundesverwaltung

Folgend sind die organisatorischen Fähigkeiten und Funktionen aus Abbildung 2 genauer beschrieben:

- **Cloud Governance:** Der Bereich DTI der Bundeskanzlei definiert die Cloud-Prinzipien, welche bei der Nutzung von Public- und Private- Cloud-Diensten einzuhalten sind, und entscheidet gegebenenfalls auch über zu gewährende Ausnahmen. Er stellt zentral weitere Hilfsmittel zur Verfügung. Die Departemente, die BK und die CSB konkretisieren und erweitern die Governance für ihre jeweiligen Verantwortungsbereiche.
- **Cloud Service Broker (CSB):** Der CSB (in der Cloud-Strategie auch Intermediär genannt) unterstützt Verwaltungseinheiten beim geordneten, sicheren und effizienten Einsatz von Public-Cloud-Diensten. Er darf die Cloud-Prinzipien in seinem Zuständigkeitsbereich verschärfen und/oder erweitern. Er berät bei der Wahl der richtigen Cloud-Stufe für Anwendungen. Ausserdem stellt er für Cloud-Projekte abgesicherte Umgebungen (sog. Landing Zones [3]) bereit, in denen Anwendungen aufgebaut und

betrieben werden können. Der Bereich DTI der BK legt die Anforderungen an den CSB im CSB-Pflichtenheft in Absprache mit den Leistungserbringern fest.

Die Rolle des vollumfänglichen CSB der Bundesverwaltung wird durch das Bundesamt für Informatik und Telekommunikation (BIT) wahrgenommen. Zusätzlich gibt es weitere dedizierte CSB, die spezifischen Bedürfnisse einzelner Departemente oder Bundesämter oder Fachgebiete abdecken (z.B. Swisstopo, MeteoSchweiz).

- **Public Cloud Betrieb:** Diese Funktion verantwortet betriebliche Leistungen im Rahmen der ordentlichen Betriebsprozesse für konkrete Fachanwendungen einer Verwaltungseinheit in der Public Cloud. Diese Aufgaben gehen über die reine Bereitstellung und den technischen Betrieb der Cloud-Dienste durch die Public-Cloud-Anbieter hinaus.

Die zuständigen Verwaltungseinheiten sind verantwortlich für die vertragliche, bundeskonforme Bereitstellung des Betriebs durch interne Leistungserbringer oder externe Anbieter.

- **Public Clouds:** Diese Funktion verantwortet den Betrieb der Cloud-Dienste. Die Rolle wird von den Public-Cloud-Anbietern sichergestellt.

Grundsätze aus der Cloud-Strategie

Das vorliegende CSB-Pflichtenheft baut auf den folgenden Grundsätzen aus der Cloud-Strategie [1] auf, welche vorliegend aktualisiert und angepasst wurde.

Grundsatz O-2: Der CSB agiert als Intermediär und unterstützt die Cloud-Nutzung

Ein CSB stellt Hilfsmittel (u.a. Werkzeuge, Dienstleistungen, Expertise, Kontroll-Mechanismen) für die Nutzung von Public-Cloud-Diensten gemäss den definierten Cloud-Prinzipien bereit.

Grundsatz O-3: Public-Cloud-Betrieb gemäss ordentlichen Betriebsprozessen

Damit die Cloud-Dienste geordnet, sicher und effizient genutzt werden können, müssen sie durch einen «internen / externen» IT-Leistungserbringer in die ordentlichen Betriebsprozesse integriert werden; siehe auch Cloud-Prinzipien der Bundesverwaltung [2].

3 Cloud Service Broker in der Bundesverwaltung

Bei der Nutzung von Public-Cloud-Diensten in der Bundesverwaltung brauchen die unterschiedlichen Verwaltungseinheiten Zugang zu den bundesverwaltungsspezifischen Public-Cloud-Plattformen, aber auch passende Beratung und technische Unterstützung. Diese Aufgaben deckt der CSB ab.

Die nachfolgende Abbildung 3 zeigt die geteilte Verantwortung («Shared Responsibility») zwischen VE, CSB und Public-Cloud-Anbieter, welche alle drei gemeinsam den Unterhalt und den Betrieb der Workloads und der Public-Cloud-Plattformen bewerkstelligen.

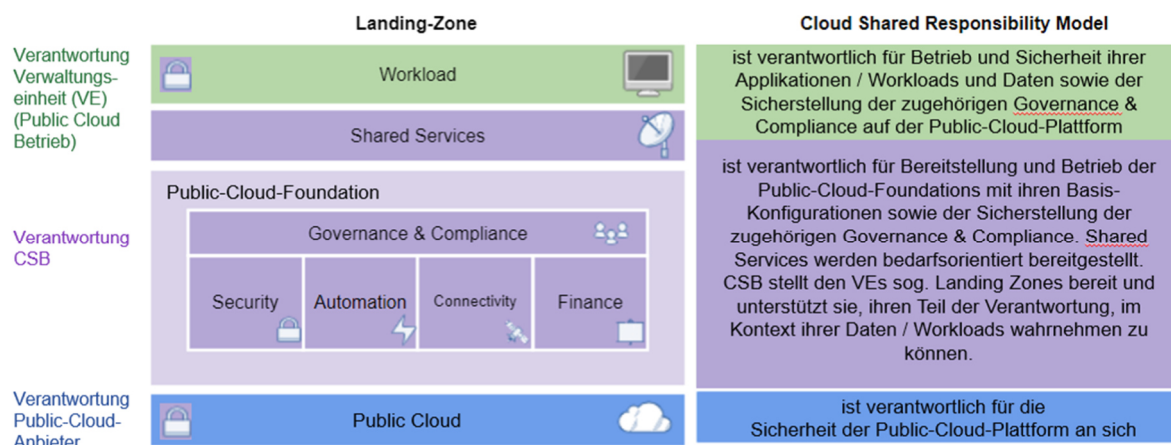


Abbildung 3: Public Cloud Shared Responsibility – geteilte Verantwortung VE, CSB und Public-Cloud-Anbieter

Der **CSB** begleitet und unterstützt die Verwaltungseinheiten (VE) durch Beratung, Engineering-Support und Bereitstellung einer umfassenden Public-Cloud-Foundation, welche die geordnete, sichere und effiziente Nutzung von Public-Cloud-Diensten (PaaS und IaaS) ermöglicht. Wichtig ist auch die Beziehungspflege zwischen dem CSB und den Public-Cloud-Anbieter, welche durch den CSB sichergestellt wird.

Die Verwaltungseinheiten können so ihren Teil der Verantwortung adäquat im "Cloud Shared Responsibility Model" wahrnehmen.

Die Nutzung von Public-Cloud-Diensten erfolgt über verschiedene Beschaffungsgefäße (wie z.B. die WTO 20007) und unterliegt dem jeweilig definierten Abrufverfahren.

Beispiel bei Bezug über Rahmenvertragswerke WTO 20007:

Der Bezug über die WTO 20007 unterliegt einem definierten Abrufverfahren. Die passende Public-Cloud-Plattform wird auf der Basis eines anbieterneutralen Pflichtenhefts evaluiert. Die Verwaltungseinheit führt das Abrufverfahren ordnungsgemäss durch. Die VE kann dazu die Unterstützung eines CSB anfragen. Die finale Freigabe und etwaige zusätzliche Governance obliegt dabei in jedem Falle den spezifischen Vorgaben und Prozessen des entsprechend zuständigen Departementes entlang ihrer Sourcing-Strategie. Jeder Bezugsentscheid muss den Cloud-Anbietern kommuniziert werden.

Details zum Public Cloud Abrufverfahren über die WTO 20007 siehe [5]

Der **Public-Cloud-Anbieter** ist für die Bereitstellung und den sicheren Betrieb seiner Public-Cloud-Plattform verantwortlich.

Die **Verwaltungseinheit in ihrer Funktion als Public Cloud Betreiber** ist für den Betrieb und Sicherheit sowie die Governance und Compliance ihrer Applikationen / Workloads und Daten verantwortlich.

3.1 Zusammenspiel DTI, CSB und Verwaltungseinheit in der Bundesverwaltung

Folgende Abbildung 4 zeigt das organisatorische Zusammenspiel zwischen dem Bereich DTI der BK, den CSBs und den Verwaltungseinheiten, sowie die technischen Anbindungen an die verschiedenen Public-Cloud-Plattformen. Diese sind in der Verantwortung des jeweiligen CSB.

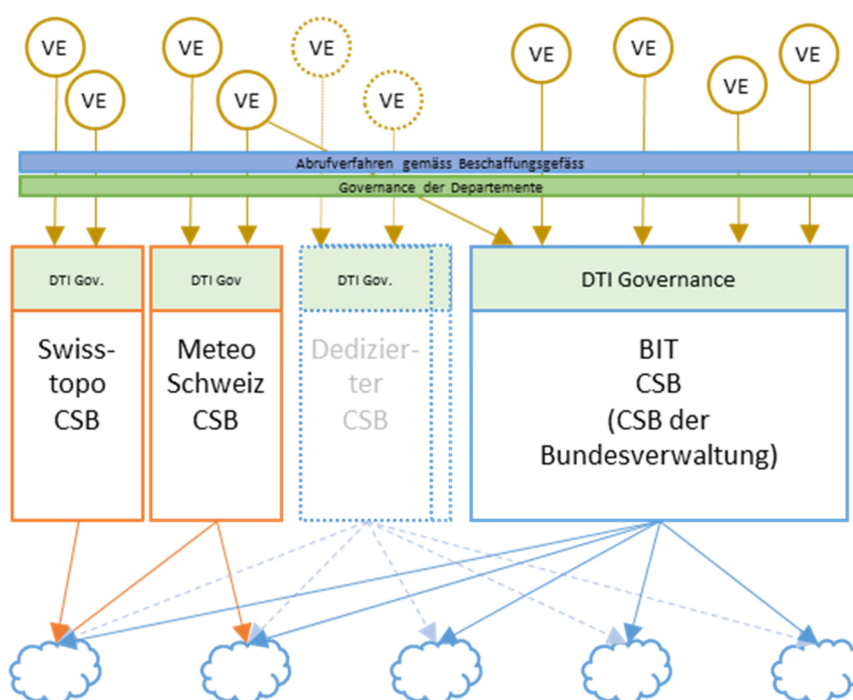


Abbildung 4: Zusammenspiel DTI – CSB – VE

Wie einleitend in Kapitel 3 beschrieben, stellt der CSB für seine Kunden, den effizienten und sicheren Zugang zu Public-Cloud-Diensten und die entsprechende Governance sicher. Der Bereich DTI der BK definiert zentral die Governance für alle CSBs und Verwaltungseinheiten (vgl. Cloud-Prinzipien der Bundesverwaltung [2]). Der Bezug von Public-Cloud-Diensten über ein spezifisches Beschaffungsgefäss (wie z.B. die WTO 20007) unterliegt dem jeweils definierten Abrufverfahren.

Für die CSBs gilt folgendes:

- Der **CSB der Bundesverwaltung** stellt Public-Cloud-Dienste aller zugelassenen Cloud-Anbieter gemäss den Governance-Vorgaben des Bereichs DTI der BK bereit.

Der Digitalisierungsrat Bund (DRB) hat am 28.6.2022 festgelegt, dass das BIT diese Rolle übernehmen soll (eine Ausdehnung auf weitere Leistungserbringer ist möglich, diese müssten aber dieselben Vorgaben erfüllen und die Wirtschaftlichkeit wäre vorgängig mit dem Bereich DTI der BK zu klären).

- Ein **dedizierter CSB** eines Fachamts wie MeteoSchweiz, Swisstopo (und ggf. weitere) stellt ein reduziertes Angebot von Public-Cloud-Diensten gemäss den Vorgaben des Bereichs DTI der BK bereit.

Der CSB der Bundesverwaltung und die dedizierten CSBs sind grundsätzlich unabhängig voneinander. Dennoch pflegen sie zusammen mit dem Bereich DTI der BK die Zusammenarbeit untereinander und nutzen Synergien.

Die Eskalationsstufe für Unstimmigkeiten zwischen den CSBs ist beim Bereich DTI der BK.

Beispiel Zusammenspiel der verschiedenen Public-Cloud-Akteure im Kontext WTO 20007:

Im Anhang 7 wird das Zusammenspiel der verschiedenen Public-Cloud-Akteure und deren Beziehungen im Kontext der Beschaffung WTO 20007 beschrieben.

3.2 Finanzierung Leistungen CSB

Die Leistungen, die der CSB der Bundesverwaltung für die Verwaltungseinheiten erbringt (siehe Kapitel 4), müssen finanziert werden. Hier werden verschiedene Arten von Leistungen unterschieden:

- **Initialer Aufbau Grundleistung** (z.B. Aufbau und Automatisierung Cloud Foundation bzw. Landing Zones, Automatisierung des Bestellprozesses):

Finanzierung hauptsächlich durch zentrale Mittel der Bundesverwaltung

- **Laufender Betrieb und Wartung** (z.B. Überprüfung und Aktualisierung von Policies auf Landing Zones, Sicherstellung und Anpassungen der Verrechnungsprozesse, Controlling und Reporting Aufgaben, Integration neuer gemeinsamer Services in Landing Zones, Life-Cycle, notwendige Anpassungen durch Angebotsänderungen der Hypercaler, Anpassung durch Änderung von Umsystemen, des Bedarfs & der Vorgaben):

Verrechnung der Cloud Consumption mit Marge an die Verwaltungseinheiten, u.U. abhängig von Volumen und Art der Consumption.

- **Dienstleistungen des CSB** für konkrete Projekte (z.B. Begleitung des Abrufverfahrens, Architektur-Beratung, Unterstützung bei Security Fragen):

Aufwand-basierte Verrechnung über das jeweilige Projekt der Verwaltungseinheit.

4 Aufgaben, Kompetenzen und Verantwortlichkeiten eines CSB

In der Cloud Strategie [1] nimmt der CSB eine wichtige Rolle ein. Er ermöglicht durch Beratung, Unterstützung und technische Massnahmen die geordnete, sichere und effiziente Nutzung von Public Clouds. Hierzu delegiert der Bereich DTI der BK gezielt Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) an den CSB der Bundesverwaltung und die dedizierten CSBs der Fachämter. Die nachfolgend beschriebenen AKV sind allgemeingültig und dienen als Grundlage für die Vereinbarung zwischen dem Bereich DTI der BK und den CSBs. Einzelne AKV betreffen nur den CSB der Bundesverwaltung resp. die dedizierten CSBs.

4.1 Aufgaben eines CSB

In diesem Kapitel werden mögliche Aufgaben aufgelistet, die je nach Bedarf vom CSB unterschiedlich ausgestaltet werden können.

ID	Kategorie	Beschreibung	Betrifft	
			CSB der BVerw.	Dedizierter CSB
A.1	Architektur	Provisionierung von operativen Landing Zones der Public-Cloud-Umgebungen. Hierfür können provider-spezifische bzw. proprietäre Public-Cloud-Dienste oder auch Cloud-Provider-agnostische Lösungen zum Einsatz kommen.	x	x
A.2	Architektur	Bereitstellen von Shared-Services je nach Bedarf einer Verwaltungseinheit, wie beispielsweise Anbindung der Cloud Foundation an ein zentrales IAM-System, Bereitstellung von Billing-Funktionalitäten, Basis-Konfiguration für Security (IT-Grundschutz), Logging- und Monitoring sowie Connectivity.	x	x
A.3	Finanzen	Anbieten von Finanz-Dashboards zur Kostenkontrolle für Verwaltungseinheiten / interne Kunden. Dadurch wird ein einfacher und schneller Überblick über alle kostenrelevanten Daten und Metriken ermöglicht. Z.B. Dashboard bei Cloud Providern mit Kosten-Infos plus CSB-Dashboard mit Infos zur internen Verrechnung (z.B. BIT MLR).	x	x
A.4	Organisation	Beratung und Unterstützung der Verwaltungseinheiten, um adäquat ihren Teil des Public-Cloud-Shared-Responsibility-Models wahrnehmen zu können.	x	x
A.5	Organisation	Förderung von Know-how-Sharing unter den Verwaltungseinheiten / internen Kunden und CSBs in	x	

ID	Kategorie	Beschreibung	Betrifft	
			CSB der BVew.	Dedizierter CSB
		der gesamten Bundesverwaltung durch Dokumentation.		
A.6	Organisation	Einbindung in die bestehenden Incident-Management-Prozesse der betroffenen Verwaltungseinheit.	x	x
A.7	Organisation	Beratung und Unterstützung der Verwaltungseinheiten / internen Kunden beim Public-Cloud-Onboarding und bei der Public-Cloud-Nutzung (z.B. durch Lösungsarchitekten, die mit dem CSB im Austausch sind).	x	x
A.8	Organisation	Beratung und Unterstützung der Verwaltungseinheiten / internen Kunden beim Design von Applikationsarchitekturen nach Cloud-native Best Practices (z.B. durch Lösungsarchitekten, die mit dem CSB im Austausch sind).	x	x
A.9	Organisation	Beratung und Unterstützung der Verwaltungseinheiten / internen Kunden bei der Planung und Durchführung von Cloud-Migrationen (z.B. durch Lösungsarchitekten, die mit dem CSB im Austausch sind).	x	x
A.10	Organisation	Beratung und Unterstützung der Verwaltungseinheiten / internen Kunden bei der Public-Cloud-Nutzung und Kostenoptimierungen ihrer Workloads (z.B. durch Lösungsarchitekten, die mit dem CSB im Austausch sind).	x	x
A.11	Organisation	Unterstützung von weitergehendem Know-how-Sharing zwischen CSBs und Verwaltungseinheiten/ internen Kunden, z.B. Zugang zu Code Repository (Infrastructure-as-Code (IaC)), Teilen von Scripts und Configs, Roundtables, Roadshows, Brown-Bag Lunches.	x	x
A.12	Organisation	Organisation eines regelmässigen Treffens (nach Bedarf) mit den CSB-Leistungsbezügern (Kunden) und dem Bereich DTI der BK zur Förderung der Zusammenarbeit und des Erfahrungsaustauschs.	x	
A.13	Security, Risk & Compliance	Unterstützung der Verwaltungseinheiten / internen Kunden bei der Sicherstellung eines adäquaten DDOS-Schutzes für ihre Workloads auf den Public-Cloud-Plattformen.	x	x
A.14	Security, Risk & Compliance	Unterstützung der Verwaltungseinheiten / internen Kunden bei der Überwachung von Workloads auf den Public-Cloud-Plattformen hinsichtlich der für die Anwendung relevanter SLAs.	x	x

ID	Kategorie	Beschreibung	Betrifft	
			CSB der BV/ew.	Dedizierter CSB
A.15	Security, Risk & Compliance	Unterstützung der Verwaltungseinheiten / internen Kunden bei der Umsetzung adäquater Schutz- und Sicherheitsmassnahmen zur Absicherung von Workloads und der unterliegenden Infrastruktur, z.B. Verschlüsselung beim Datenaustausch (Data-in-Transit) oder bei der Datenspeicherung (Data-at-Rest).	x	x
A.16	Security, Risk & Compliance	Unterstützung der Verwaltungseinheiten / internen Kunden bei der Sicherstellung der Vergabe und Überprüfung von Zugriffsberechtigungen von persönlichen wie technischen Benutzern, so dass diese möglichst restriktiv vergeben werden (Least Privilege und Need to Know Prinzipien). Die Berechtigungen sollen den benötigten Arbeitsablauf ermöglichen, aber nicht mehr.	x	x
A.17	Security, Risk & Compliance	Unterstützung der Verwaltungseinheiten / internen Kunden, sich einen einfachen und schnellen Überblick über den Betriebszustand von Services mit Service-Level-relevanten Daten und Metriken zu verschaffen.	x	x
A.18	Security, Risk & Compliance	Unterstützung der Verwaltungseinheiten / internen Kunden, sich einen einfachen und schnellen Überblick über alle Governance-, Compliance- und Security-relevanten Daten und Metriken zu verschaffen.	x	x
A.19	Security, Risk & Compliance	Regelmässiges Auffordern der CSB-Leistungsbezügern, ihre Zugriffsberechtigungen von persönlichen wie technischen Benutzern auf die minimal benötigten Rechte zu überprüfen und nicht mehr benötigte Zugriffrechte zu entziehen.	x	x
A.20	Security, Risk & Compliance	Unterstützung des Security Operation Center (SOC) bei der zentralen Überwachung von Workloads auf den Public-Cloud-Plattformen hinsichtlich Security: Single Pane of Glass für Security. Die Verantwortung für die Sicherheit von ausgelagerten Applikation bzw. Workloads und Daten liegt grundsätzlich beim jeweiligen Departement und dessen Verwaltungseinheit.	x	x
A.21	Security, Risk & Compliance	Sicherstellung der Kommunikation zwischen dem Public-Cloud-Anbieter und der betroffenen Verwaltungseinheit / interne Kunden im Falle eines Sicherheitsvorfalls (z.B. Data Breach). Der CSB sorgt unter anderem dafür, dass die Verwaltungseinheit umgehend über einen Data Breach oder weitere	x	x

ID	Kategorie	Beschreibung	Betrifft	
			CSB der BV/erw.	Dedizierter CSB
		Ereignisse, welche die Daten der Verwaltungseinheit gefährden könnten, informiert werden.		
A.22	Security, Risk & Compliance	Bei Bedarf Durchführung von Audits bei den Cloud-Anbietern im Namen der Bundesverwaltung durch. z.B. im Auftrag einer Verwaltungseinheit. Der CSB kann für diese Aufgabe Dritte beiziehen.	x	x
A.23	Service-Angebot	Unterstützung der Verwaltungseinheiten / internen Kunden bei der kontinuierlichen Überwachung und Optimierung (Shared Services, Volumen-Discounts u.a.) der Cloud-Nutzung hinsichtlich der Kosten.	x	x
A.24	Service-Angebot	Ermöglichung des Zugangs zu Public-Cloud-Diensten für Tests, PoCs oder Spikes von potentiellen Lösungsmustern, z.B. mittels Playgrounds.	x	
A.25	Sourcing & Beschaffung	Unterstützung und Beratung der IT-Projekte der Verwaltungseinheiten / internen Kunden bei Sourcing-Entscheiden.	x	x
A.26	Sourcing & Beschaffung	Unterstützung und Beratung der IT-Projekte der Verwaltungseinheiten / internen Kunden beim Cloud Abrufverfahren [5] (z.B. bei Bewertung der Kriterien)	x	x

Tabelle 1: Aufgaben eines CSB

4.2 Kompetenzen eines CSB

In diesem Kapitel sind Kompetenzen aufgelistet, die ein CSB hat. Im Rahmen dieser Kompetenzen trifft der CSB Entscheidungen.

ID	Kategorie	Beschreibung	Betrifft	
			CSB der BVerw.	Dedizierter CSB
K.1	Architektur	Ausgestaltung der Public-Cloud-Foundation mit CSB Shared Services über die Grundkonfiguration hinaus oder weitergehender nützlicher Services für die Verwaltungseinheiten.	x	x
K.2	Architektur	Die Einbindung in die IT-Infrastruktur der Bundesverwaltung kann die zentrale Connectivity mit dem Standarddienst DAKO oder durch eine spezifische dedizierte Lösung bewerkstelligt werden. Die Leistungsbezüger und CSB entscheiden gemeinsam, wie die Connectivity im jeweiligen Kontext am besten bewerkstelligt wird.	x	x
K.3	Finanzen	Gestaltung der verursacher- und sachgerechten Verrechnung seiner Beratungs-, Beschaffungs- und Unterstützungsleistungen.	x	
K.4	Organisation	Konkretisierung und Erweiterung der bestehenden allgemeingültigen Public-Cloud-Prinzipien. Diese Anpassungen gelten dann nur für die Verwaltungseinheiten des jeweiligen CSB.	x	x
K.5	Organisation	Definition technischer Leitplanken mittels zentralen Policies (z.B. basierend auf den Cloud-Prinzipien der Bundesverwaltung oder Departementsvorgaben).	x	x
K.6	Organisation	Gestaltung der Form und des Umfangs der Beratungs-, Beschaffungs- und Unterstützungsleistungen.	x	x
K.7	Organisation	Durch das Bestellen oder die Eröffnung einer Landing Zone (kundenspezifische Public-Cloud-Umgebung, z.B. als AWS Account oder Azure Subscription) entsteht eine Abhängigkeit zwischen CSB und Verwaltungseinheit. Ob und wie dies vereinbart oder vertraglich geregelt ist, ist dem jeweiligen CSB überlassen.	x	x
K.8	Security, Risk & Compliance	Definition weitergehenden Policies über zentrale Policies der Bundesverwaltung hinaus, z.B. verschärfte Security-Vorgaben oder auch Blacklisting von Public-Cloud-Diensten.	x	x

ID	Kategorie	Beschreibung	Betrifft	
K.9	Service-Angebot	Aufbau des Angebots der Dienste auf Basis der Angebote von Public-Cloud-Diensten der Hyperscaler, d.h. es gibt kein eingeschränktes bundesspezifisches Public-Cloud-Dienste-Angebot. Dem CSB steht es frei, ein eingeschränktes Public-Cloud-Dienste-Angebot zu unterstützen oder gewisse Dienste explizit auszuschliessen.	x	x

Tabelle 2: Kompetenzen eines CSB

4.3 Verantwortlichkeiten eines CSB

In diesem Kapitel sind Verantwortlichkeiten aufgelistet, die ein CSB zwingend tragen muss.

ID	Kategorie	Beschreibung	Betrifft	
			CSB der BVerw.	Dedizierter CSB
V.1	Architektur	Nutzung von Security-Services, Break-Glass-Accounts, Policy Management, Logging und Monitoring, etc. für Grundkonfiguration der Public-Cloud-Foundation und CSB Shared Services.	x	x
V.2	Finanzen	Sicherstellung der verursacher- und sachgerechten Verrechnung seiner Beratungs- und Unterstützungsleistungen.	x	
V.3	Finanzen	Sicherstellung der zentralen Abrechnung für die Verwaltungseinheiten über den SAP Debitoren Workflow.	x	
V.4	Finanzen	Korrekte und verbrauchsorientierte Abrechnung an die Verwaltungseinheiten / internen Kunden für Nutzung von Public-Cloud-Diensten mit Kostenzuschlägen aus Umverteilung der CSB Shared Services Kosten. Transparente Darstellung der Kostenzuschläge bei Abrechnung an die Verwaltungseinheiten (Einhaltung des Finanzhaushaltsgesetzes, FHG; SR 611.0).	x	x
V.5	Organisation	Hat die Rolle und Funktion des Cloud Competence Centers (bzw. Cloud Center of Excellence) und stellt Beratung und Unterstützung der Leistungserbringer bei ihren Public Cloud Vorhaben sicher.	x	
V.6	Organisation	Stellt Zusammenarbeit mit dem Bereich DTI der BK und Einbringung seiner Kompetenzen sicher.	x	
V.7	Organisation	Hinweisen der zugehörigen Verwaltungseinheiten auf die allgemeingültigen Public-Cloud-Prinzipien [2], damit diese zur Anwendung kommen.	x	x

ID	Kategorie	Beschreibung	Betrifft	
V.8	Sourcing & Beschaffung	Bedarfsorientierte Bereitstellung von Public-Cloud-Diensten, die gemäss den Vorgaben des Bereichs DTI der BK (z.B. Cloud Prinzipien) erfolgt.	x	x
V.9	Sourcing & Beschaffung	Prüfung des anbieterneutralen Pflichtenhefts und des Kriterienkatalogs der Bedarfsstelle (Verwaltungseinheiten / internen Kunden) im Rahmen des Cloud Abrufverfahrens [5].	x	
V.10	Sourcing & Beschaffung	Stellt die Kommunikation mit den Cloud-Anbietern im Rahmen des Cloud Abrufverfahrens [5] sicher, sowohl im Falle von Fragen während der Bewertung eines Kriterienkatalogs wie auch bei der Information über den Bezugsentscheid.	x	x
V.11	Sourcing & Beschaffung	Ein dedizierter CSB eines Fachamts, wie Meteo-Schweiz, Swisstopo (ggf. weitere), stellen ein spezifisches Angebot von Public-Cloud-Diensten für die eigene Verwaltungseinheit und gemäss den Vorgaben des Bereichs DTI der BK (z.B. Cloud Prinzipien) bereit. Falls die Anforderungen einer Verwaltungseinheit vom eigenen CSB nicht abgedeckt werden, erfolgt der Bezug von Public-Cloud Dienste beim CSB der Bundesverwaltung.		x
V.12	Sourcing & Beschaffung	Stellt die Unterstützung der Verwaltungseinheiten / internen Kunden und Bereich DTI der BK bei der Überwachung und Einhaltung des Beschaffungsbudgets beim Bezug von Public-Cloud-Leistungen sicher. Stellt die Meldung bisheriger Bezüge periodisch an den Vertragsverantwortlichen sicher. Der CSB berichtet dem Bereich DTI der BK mindestens monatlich Informationen zu Abrufen der Verwaltungseinheit und bisherigem Verbrauch («Consumption») pro Abruf und Cloud Provider. Dabei sind folgende Informationen bereitzustellen: <ul style="list-style-type: none"> - Jahressumme pro Cloud Provider, aufgeschlüsselt nach einzelnen Abrufen der Verwaltungseinheiten - Pro Abruf die Zuschlagssumme - Pro Abruf die verbrauchte Summe - Pro Abruf VE, Titel und Nummer (z.B. BAG Covid Tool 2024, 0005) 	x	x
V.13	Service Angebot	Austausch mit den Public-Cloud-Anbietern. Der CSB ist z.B. verantwortlich, eingehende Informationen vom Public-Cloud-Anbieter bezüglich sich ändernden Services oder über die Dekommissionierung von Services, zeitnah an die Verwaltungseinheit weiterzuleiten.	x	x

ID	Kategorie	Beschreibung	Betrifft	
V.14	Security, Risk & Compliance	<p>Die Verantwortlichkeiten hinsichtlich Security wird in den Public-Clouds im Sinne des Shared Responsibility Models zwischen Kunde, CSB und Public-Cloud-Anbieter geteilt (mehr dazu in Kapitel 3.).</p> <p>Die Verantwortung des Workload inkl. dessen Daten, Security, Governance und Compliance liegt beim Kunden.</p> <p>Die Verantwortung für die Cloud Fondation in Bezug auf Security, Risk & Compliance (inkl. IT-Grundschutz) liegt beim CSB.</p>	x	x

Tabelle 3: Verantwortlichkeiten eines CSB

5 Glossar

Begriff / Abkürzung	Definition
API	Application Programming Interface
BA	Bundesamt
BK	Bundeskanzlei
BVerw	Bundesverwaltung
CSB	Cloud Service Broker
SD DAKO	Standarddienst Datenkommunikation
DDOS	Distributed Denial of Service Attack
DRB	Digitalisierungsrat Bund
eIAM	Standarddienst IAM / Identity and Access Management
Fach CSB	CSB in seinem fachlichen Kontext für nur zugehöriges Fachamt, z.B. Swisstopo oder MeteoSchweiz
IaC	Infrastructure-as-Code
IAM	Identity and Access Management
ISBO	Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten
ISDS	Informationssicherheits- und Datenschutzkonzept (ISDS)
PCSP	Public Cloud Service Provider
SCHUBAN	Schutzbedarfsanalyse
SLA	Service-Level-Agreement
VE	Verwaltungseinheit
Workload	Als Workload wird eine in der Public-Cloud betriebene Applikation oder die Verarbeitung von Daten mit Hilfe eines Public-Cloud-Dienstes bezeichnet.

6 Referenzen

- [1] Bundeskanzlei, Digitale Transformation und IKT Steuerung (DTI), [Cloud-Strategie der Bundesverwaltung](#), 2020.
- [2] Bundeskanzlei, Digitale Transformation und IKT Steuerung (DTI), [Cloud-Prinzipien der Bundesverwaltung](#), 2023.
- [3] IT-Business, [Was ist eine Landing Zone?](#), 2022 (letzter Zugriff am 08.03.2024).
- [4] Bundeskanzlei, Digitale Transformation und IKT-Steuerung (DTI), [Public Cloud Abrufverfahren über WTO 20007](#), 2023.
- [5] Bundesamt für Cybersicherheit (BACS), [Sicherheitsverfahren](#), 2022.

Anhang 1: Zusammenspiel Public-Cloud-Akteure im Kontext WTO 20007

Im Kapitel 3.1 wurden der CSB sowie das Zusammenspiel der verschiedenen Public-Cloud-Akteure allgemein kurz beschrieben. Abbildung 4 zeigt die Public-Cloud-Akteure und deren Beziehungen im Kontext der Beschaffung WTO 20007 in vereinfachter Form. Die folgende Abbildung 8 beschreibt nicht alle möglichen Situationen durch individuelle Public-Cloud-Rahmenverträge ausserhalb des Beschaffungsgefäss WTO 20007.

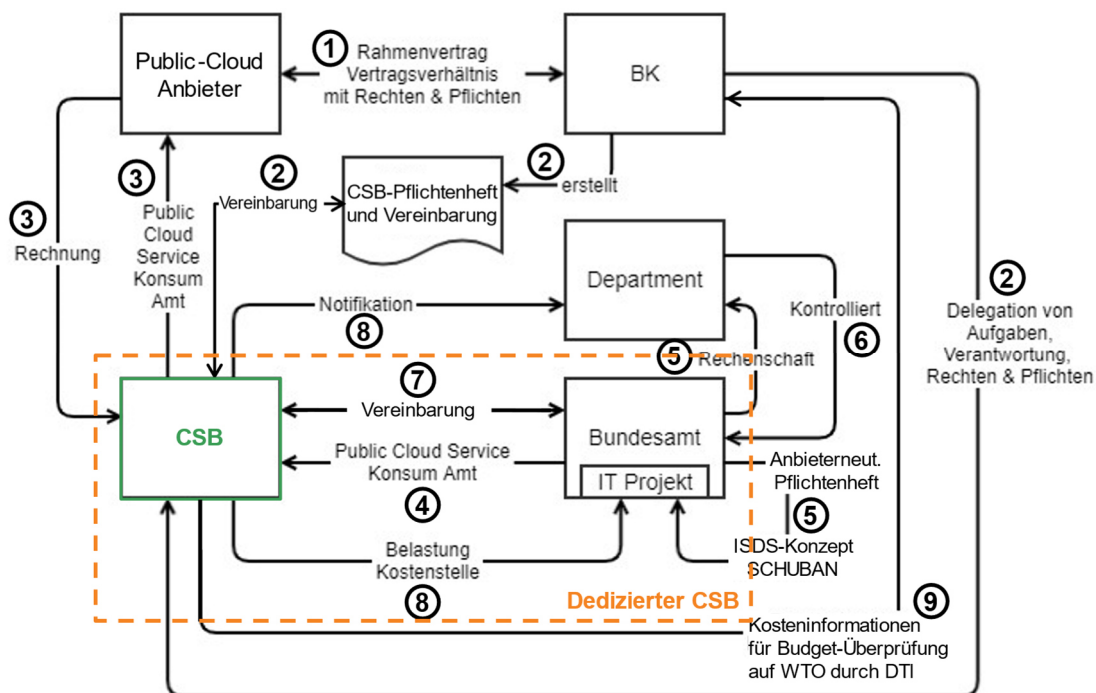


Abbildung 5: Beziehungen der Public-Cloud-Akteure

Nachfolgend sind die Beziehungen zwischen den Public-Cloud-Akteuren beschrieben:

1. Die vertragliche Vereinbarung zwischen den **Public-Cloud-Anbietern** und **BK** wird in Form von **Rahmenverträgen mit Rechten & Pflichten** abgeschlossen. Das Vertragsverhältnis besteht zwischen den **Public-Cloud-Anbietern** und der **BK**.
2. Die **BK delegiert gezielt Aufgaben und Verantwortlichkeiten** an den **CSB / dedizierte CSBs**, welche im vorliegenden **CSB-Pflichtenheft als Aufgaben, Kompetenzen und Verantwortlichkeiten** definiert werden. Zwischen der **BK-DTI** und dem **CSB** wird auf Basis dem **CSB-Pflichtenheft** eine **Vereinbarung** abgeschlossen
3. Der **Bezug und die Verrechnung von Public-Cloud-Diensten** erfolgt zwischen dem **CSB / dedizierten CSB** und **Public-Cloud-Anbietern** direkt.
4. Der **CSB der Bundesverwaltung** (grün in Abbildung) stellt Public-Cloud-Leistungen für IT-Projekte in beliebigen **Bundesämtern** resp. ein **dedizierter CSB** (orange gestrichelt in Abbildung) direkt für seine **Fachämter oder Fachbereiche** bereit.
5. Beim **Bezug von Public-Cloud-Leistungen** in einem **IT-Projekt** über den CSB gilt das entsprechend festgelegte Abrufverfahren gemäss WTO 20007 [5]. Der Abruf erfolgt immer über eine Evaluation mit Hilfe eines **anbieterneutralen Pflichtenhefts**. Zudem muss für jedes IT-Projekt eine **SCHUBAN** und bei Bedarf ein **ISDS-Konzept** erstellt werden; weitere Informationen sind den BACS (vormals NCSC) Vorgaben [5] zu entnehmen.

6. Die **IT-Projekte** werden durch die **Bundesämter** geführt und folgen den in der Bundesverwaltung etablierten Regeln und Vorgaben. Die **Governance-Verantwortung** liegt jeweils bei dem übergeordneten **Departement**; unter anderem für die in Ziff. 5 beschriebenen Aspekte.
7. Durch das Bestellen / Eröffnen einer Landing Zone (kundenspezifische Cloud Umgebung, z.B. als AWS Account oder Azure Subscription) entsteht eine Abhängigkeit zwischen **CSB und Verwaltungseinheit**. Ob und wie dies **vereinbart oder vertraglich geregelt** ist, ist dem jeweiligen CSB überlassen.
8. Die **monatliche Weiterverrechnung** der bezogenen Public-Cloud-Diensten erfolgt zwischen CSB und IT-Projekt resp. Bundesamt. Der Bedarfsträger (also die Verwaltungseinheit resp. der Leistungsbezüger) ist verantwortlich, alle etablierten Regeln und Vorgaben zu erfüllen, hierzu gehört auch die in Kenntnissetzung seines Departements bei Vorhaben und Abrufverfahren, die Führung der Vorhaben im IKT-Cockpit, usw. gemäss den spezifischen Vorgaben und Prozessen.
9. Der CSB liefert dem Bereich DTI der BK periodisch **Kosteninformationen** über den Bezug der Public-Cloud-Leistungen für die **Budget-Kontrolle** auf der WTO 20007. **Die Budget-Verantwortung liegt beim Bereich DTI der BK.**