Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

«$$e-seal»

«$$QrCode»

*Dieser Text ist ein Vorabdruck.
Verbindlich ist die Version, welche
im Bundesblatt veröffentlicht wird.*

24.xxx

Botschaft zu einem Verpflichtungskredit zum Aufbau einer Swiss Government Cloud

vom …

Sehr geehrter Herr Nationalratspräsident
Sehr geehrte Frau Ständeratspräsidentin
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf eines Bundesbeschlusses zu einem Verpflichtungskredit zum Aufbau einer Swiss Government Cloud.

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrte Frau Ständeratspräsidentin, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

…

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Viola Amherd
Der Bundeskanzler: Viktor Rossi

Übersicht

Mit der vorliegenden Botschaft beantragt der Bundesrat dem Parlament einen Verpflichtungskredit in der Höhe von 246,9 Millionen Franken für den Aufbau der Hybrid-Multi-Cloud-Infrastruktur Swiss Government Cloud. Diese Infrastruktur ist eine entscheidende Grundlage für die erfolgreiche Bewältigung der anstehenden grossen Digitalisierungsherausforderungen des Bundes.

Ausgangslage

Im Zuge ihrer Digitalisierungsbemühungen sieht sich die Bundesverwaltung mit einer wachsenden Nachfrage nach IT-Lösungen und gesteigerten Anforderungen an eine leistungsfähige, zuverlässige und sichere IT-Infrastruktur konfrontiert. Cloud-Dienste gewinnen in diesem Zusammenhang als Schlüsselelement der digitalen Transformation zunehmend an Bedeutung. Aus diesem Grund hat der Bundesrat am 11. Dezember 2020 die Cloud-Strategie der Bundesverwaltung verabschiedet, um die Grundlagen für deren Nutzung zu schaffen.

Diese Strategie gilt es auch im Bundesamt für Informatik und Telekommunikation, dem grössten IKT-Leistungserbringer der Bundesverwaltung, umzusetzen. Dessen aktuelle Cloud-Infrastruktur (Systemlandschaft Atlantica) ist jedoch zunehmend technologisch veraltet und kann den Anforderungen an eine leistungsfähige IKT-Infrastruktur immer weniger gerecht werden. Aufgrund des geringen Industrialisierungsgrads der heutigen Cloud-Lösung führen Kapazitätserhöhungen zur Deckung der Nachfrage zu einem massiven Anstieg der Betriebskosten. Es gilt daher, rechtzeitig eine geeignete Hybrid-Multi-Cloud-Infrastruktur bereitzustellen, mit der den anstehenden grossen Herausforderungen der Digitalisierung begegnet werden kann.

Inhalt der Vorlage

Mit der Swiss Government Cloud plant der Bundesrat den Aufbau einer neuen, auf die Anforderungen und Bedürfnisse des Bundes zugeschnittenen Hybrid-Multi-Cloud-Infrastruktur: «Hybrid» bedeutet, dass die Swiss Government Cloud sowohl Public-Cloud-Dienste von externen Cloud-Dienstleistern als auch bundesverwaltungseigene Private-Cloud-Dienste in sich vereint. «Multi» impliziert, dass die Angebote mehrerer externer Cloud-Anbieter zur Verfügung stehen, sodass Abhängigkeiten reduziert werden können. Damit soll es die Swiss Government Cloud der Bundesverwaltung künftig ermöglichen, das Massengeschäft im Cloud-Bereich über eine einheitliche Gesamtlösung abzuwickeln. Zu diesem Zweck wird ein ganzheitlicher Ansatz verfolgt: Nebst dem Aufbau der Hybrid-Multi-Cloud-Infrastruktur werden auch Investitionen in die Bereiche «Ausbildung, Beratung und Governance», «Betriebs- und kommerzielle Prozesse», «Cybersicherheit» und «Netzwerkinfrastruktur» getätigt. Damit wird sichergestellt, dass die Swiss Government Cloud zielgerichtet, effizient und sicher aufgebaut und genutzt werden kann. Kantone, Städte und Gemeinden sollen bei Interesse ebenfalls vom Angebot der SGC profitieren können.

Die Generalsekretärin des Eidgenössischen Finanzdepartements wird als Auftraggeberin des Programms Swiss Government Cloud amten. Weiter werden ein Programm-

und ein Fachausschuss mit Vertreterinnen und Vertretern der IKT-Leistungserbringer und -Leistungsbezüger sowie der Bundeskanzlei (Bereich Digitale Transformation und IKT-Lenkung) eingerichtet. Die Ausschüsse sollen sicherstellen, dass die IKT-Leistungserbringer angemessen beteiligt sind und die Bedürfnisse der Leistungsbezüger berücksichtigt werden. Aufgrund der Grösse und der Komplexität des Vorhabens wird zudem ein starkes, unabhängiges Qualitäts- und Risikomanagement aufgebaut, das über alle Verantwortungsstufen die Qualität der Arbeiten überprüft sowie die Risiken erfasst und bewertet.

Das Programm wird 2024 initialisiert. Die Realisierung erfolgt in den Jahren 2025–2032. Ab 2027 soll der Aufbau der Swiss Government Cloud soweit fortgeschritten sein, dass mit der Migration der Fachanwendungen aus der Systemlandschaft Atlantica und dem Cloud Service Broker des Bundesamtes für Informatik und Telekommunikation begonnen werden kann. Die Migrationsarbeiten sollen bis Ende 2030 abgeschlossen sein.

Verpflichtungskredit

Der beantragte Verpflichtungskredit beläuft sich auf 246,9 Millionen Franken.

Der Verpflichtungskredit wird in zwei Tranchen aufgeteilt: Die Freigabe der ersten Tranche von 103,2 Millionen Franken für die Jahre 2025–2027 erfolgt durch die Bundesversammlung mit dem Bundesbeschluss. Die zweite Tranche von 143,7 Millionen Franken für die Jahre 2028–2032 wird durch den Bundesrat freigegeben, sobald die entsprechenden Voraussetzungen erfüllt sind.

Inhaltsverzeichnis

Übersicht **2**

1 Ausgangslage **6**

1.1 Problemlage und Anlass des Finanzbegehrens, Bedeutung des zu finanzierenden Vorhabens 6

1.2 Zielbild und Vorgehen 7

1.3 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates 8

1.4 Verzicht auf Vernehmlassungsverfahren 9

2 Inhalt des Kreditbeschlusses **10**

2.1 Antrag des Bundesrates und Begründung 10

2.2 Inhalt der Vorlage im Einzelnen 10

2.2.1 Aufbau der Hybrid-Multi-Cloud-Infrastruktur 10

2.2.1.1 Public Cloud 11

2.2.1.2 Public Cloud On-Prem 12

2.2.1.3 Private Cloud On-Prem 12

2.2.2 Ausbau der Netzwerkinfrastruktur 13

2.2.3 Ausbau der Cybersicherheit 14

2.2.3.1 Datenschutz und Informationssicherheit 15

2.2.3.2 Herausforderungen der Cybersicherheit 16

2.2.3.3 Zielbild der Cybersicherheit 17

2.2.3.4 IT-Compliance 18

2.2.4 Betriebs- und kommerzielle Prozesse 19

2.2.4.1 Betriebsprozesse 19

2.2.4.2 Kommerzielle Prozesse 19

2.2.5 Ausbildung, Beratung und Governance 20

2.2.5.1 Ausbildungsangebot 20

2.2.5.2 SGC Competence Center 21

2.2.5.3 Innovation Center 21

2.2.5.4 SGC-weite Cloud-Governance 21

2.3 Geprüfte Varianten für Aufbau und Sequenz 22

2.4 Bedürfnisanalyse und Bedarfserhebung 23

2.5 Risiken 24

2.5.1 Kontext der Risikobetrachtung 24

2.5.2 Risiko, die Ziele nicht zu erreichen 25

2.5.3 Massnahmen für die Zielerreichung 26

2.5.4 Budgetrisiko 26

2.5.5 Massnahmen zur Einhaltung der Kosten und des Budgets 27

2.5.6 Zeitrisiko 27

2.5.7 Massnahmen zur Termineinhaltung 27

2.6 Programmstruktur 29

2.7 Systematische Prüfung 31

3 Auswirkungen **32**
3.1 Auswirkungen auf den Bund 32
3.1.1 Finanzielle Auswirkungen 32
3.1.1.1 Annahmen zur Ausgabenschätzung 32
3.1.1.2 Programmausgaben 2024–2032 33
3.1.1.3 Verpflichtungskredit 36
3.1.1.4 Betriebsausgaben nach dem Programm 37
3.1.1.5 Einsparungen während und nach dem Programm 37
3.1.1.6 Wirtschaftlichkeit 38
3.1.2 Konsequenzen bei Nichtrealisierung 40
3.1.3 Migrationskosten 40
3.1.4 Zweitmeinungen 41
3.2 Auswirkungen auf Kantone und Gemeinden 42
4 Rechtliche Aspekte **43**
4.1 Verfassungs- und Gesetzmässigkeit 43
4.2 Erlassform 43
4.3 Unterstellung unter die Ausgabenbremse 43
5 Abkürzungsverzeichnis **44**
6 Glossar **46**

Botschaft

1 Ausgangslage

1.1 Problemlage und Anlass des Finanzbegehrens, Bedeutung des zu finanzierenden Vorhabens

Als einer der IKT-Leistungserbringer der Bundesverwaltung ist das Bundesamt für Informatik und Telekommunikation (BIT) damit beauftragt, seinen Kunden in der Bundesverwaltung bedürfnisgerechte, sichere und effiziente Informatiksysteme zur Verfügung zu stellen und die Verwaltungseinheiten zuverlässig bei der Abwicklung ihrer digitalen Geschäftsprozesse zu unterstützen. Die Bedingungen zur Erfüllung dieses Auftrags haben sich in den letzten Jahren stark verändert: Im Zuge zunehmender Digitalisierungsbestrebungen steigen sowohl die Nachfrage nach innovativen IT-Leistungen (z. B. im Bereich der künstlichen Intelligenz) als auch die Anforderungen an eine leistungsfähige, zuverlässige und sichere IT-Infrastruktur. An Bedeutung gewinnt in diesem Zusammenhang insbesondere der Einsatz von Cloud-Diensten: So ist das Geschäftsumfeld der Bundesverwaltung von zunehmender Komplexität und Dynamik geprägt. Verwaltungseinheiten müssen – trotz steigendem Kostendruck und grassierendem Fachkräftemangel – auf sich schnell verändernde Geschäftsanforderungen reagieren können, um ihren Leistungsauftrag gegenüber der Öffentlichkeit auch weiterhin zu erfüllen. Die digitale Transformation ist notwendig, und Cloud-Dienste können diese aufgrund ihres hohen Standardisierungsgrads, ihrer Skalierbarkeit, ihrer hohen Zuverlässigkeit und ihrer Innovationskraft kosteneffizient unterstützen und beschleunigen.

Um die notwendigen Grundlagen für eine geordnete, sichere und effiziente Nutzung der Cloud-Technologie zu schaffen, hat der Bundesrat am 11. Dezember 2020[1] die Cloud-Strategie der Bundesverwaltung[2] verabschiedet. Darin vorgesehen ist ein Hybrid-Multi-Cloud-Ansatz; Verwaltungseinheiten des Bundes sollen künftig sowohl bundesinterne als auch von verschiedenen externen Dienstleistern bereitgestellte Cloud-Infrastrukturen und -Dienste nutzen und zur optimalen Erfüllung der jeweiligen Anforderungen miteinander kombinieren können.

Die erwähnte Cloud-Strategie gilt es auch im BIT umzusetzen. Dabei gibt es insbesondere Folgendes zu beachten:

- Systemlandschaft Atlantica: Die heutige Private-Cloud-Lösung des BIT, die Systemlandschaft Atlantica, muss aus technologischer Sicht ab 2027 abgelöst werden, da Teile davon am Ende ihres Lebenszyklus angelangt sind. Zudem stösst die derzeitige Infrastruktur durch die zunehmende Digitalisierung sowohl in Bezug auf vorhandene Kapazitäten als auch bezüglich der

1 www.admin.ch > Dokumentation > Medienmitteilungen > Medienmitteilungen des Bundesrats > 11.12.2020 (Stand 26.3.2024)

2 www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Vorgaben > Strategien und Teilstrategien > SB020 – Cloud-Strategie der Bundesverwaltung (Stand 26.3.2024)

geforderten Flexibilität an ihre Grenzen; sie ist den anstehenden Herausforderungen im Digitalisierungsbereich entsprechend nicht mehr gewachsen. Es muss daher ein neues Fundament für Digitalisierungsprojekte gelegt werden, um deren Umsetzung technisch überhaupt zu ermöglichen und dabei gleichzeitig einen massiven Anstieg der IT-Kosten zu verhindern.

- WTO-Ausschreibung 20007*:* Die mit der WTO-Ausschreibung 20007 geschaffene Beschaffungsgrundlage, über welche die Bundesverwaltung derzeit via den Cloud Service Broker des BIT (CSB-BIT) Public-Cloud-Lösungen beziehen kann, wird dereinst ausgeschöpft sein oder, voraussichtlich 2026, auslaufen. Will die Bundesverwaltung ihre Hybrid-Cloud-Strategie umsetzen, wird deshalb eine Nachfolgelösung benötigt.

Mit der Swiss Government Cloud (SGC) plant der Bundesrat daher den Aufbau einer neuen, auf die Anforderungen und Bedürfnisse des Bundes zugeschnittenen Hybrid-Multi-Cloud-Infrastruktur, die sowohl verschiedene Public-Cloud- als auch Private-Cloud-Angebote in sich vereint. Die SGC ist somit eine einheitliche Gesamtlösung für das Massengeschäft im Cloud-Bereich der Bundesverwaltung.

1.2 Zielbild und Vorgehen

Mit der SGC wird der in der Cloud-Strategie der Bundesverwaltung vorgesehene Hybrid-Multi-Cloud-Ansatz weiter umgesetzt. Das gesamte Spektrum an Cloud-Diensten – von der Public Cloud bis hin zur Private Cloud in den Rechenzentren des Bundes (On-Prem) – kann über dieselbe Gesamtlösung bezogen werden; die SGC-weite Governance stellt sicher, dass in der SGC betriebene Lösungen möglichst einfach in die Systemlandschaft des Bundes eingebunden werden können. Dadurch können Aufwände reduziert und wertvolle Ressourcen in die Digitalisierung von Geschäftsprozessen investiert werden.

Zudem ermöglicht die SGC dem Bund, die Chancen der Digitalisierung zu nutzen, indem sie einen kostengünstigen Zugang zu Innovation bietet. Auf neue Entwicklungen im Geschäftsumfeld können Leistungsbezüger dank geeigneter Cloud-basierter Lösungen schnell reagieren; die digitale Resilienz der Bundesverwaltung wird damit gestärkt. Durch kontinuierliche Investitionen wird sichergestellt, dass die SGC den Digitalisierungsbedürfnissen des Bundes auch langfristig gerecht wird. Kantone, Städte und Gemeinden sollen bei Interesse ebenfalls vom Angebot profitieren können. Für den privaten Sektor wird die SGC hingegen keine Dienstleistungen erbringen.

Die Realisierung des Vorhabens erfolgt in den Jahren 2025–2032. Bereits ab 2026 sollen erste Ergebnisse der einzelnen Massnahmen nutzbar sein. Ab diesem Zeitpunkt werden neu entwickelte oder zu erneuernde Fachanwendungen, wenn immer möglich, direkt auf der SGC realisiert. Ab 2027 soll ihr produktiv nutzbarer Funktionsumfang ausreichen, um mit der Migration der Fachanwendungen aus der Systemlandschaft Atlantica und dem CSB-BIT beginnen zu können. Ziel ist, die Migration bis Ende 2030 abgeschlossen zu haben und die Systemlandschaft Atlantica danach möglichst rasch abzubauen. Systeme und Anwendungen, die aktuell noch nicht in einer der Cloud-Plattformen des BIT betrieben werden (Legacy-Systeme), sind jedoch nicht

Teil dieser Migrationsarbeiten. Es liegt in der Verantwortung der Leistungsbezüger, die Modernisierung dieser Lösungen einzuplanen und zu beauftragen. Die Ablösung der Legacy-Systeme birgt weiteres Sparpotenzial. Das Thema wird daher im Digitalisierungsrat Bund parallel zur SGC prioritär angegangen.

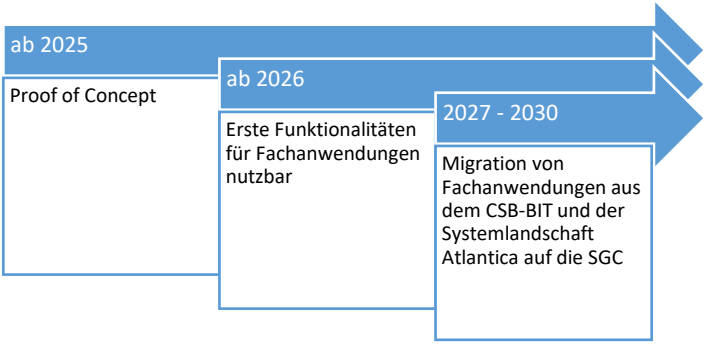

Abbildung 1: Zeitrahmen für den Aufbau der SGC und die Migration der Fachanwendungen

Bereits während der Migration und bis zum Ende des Vorhabens 2032 werden Optimierungs- und Weiterentwicklungsarbeiten an der SGC getätigt, um die Bedarfsgerechtigkeit und Innovativität der Lösung sicherzustellen.

1.3 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates

Die SGC fusst auf der am 11. Dezember 2020 vom Bundesrat verabschiedeten Cloud-Strategie der Bundesverwaltung. Die Umsetzung des Vorhabens verläuft zudem in Einklang mit den Konzepten zum Rechenzentren-Verbund (bei der Stufe III), der Netzwerkstrategie[3] sowie den Cloud-Prinzipien der Bundesverwaltung[4].

Mit der SGC wird das Fundament für eine erfolgreiche Bewältigung der anstehenden grossen Digitalisierungsherausforderungen in der Bundesverwaltung gelegt. Das Vorhaben unterstützt entsprechend die Umsetzung der Strategie Digitale Bundesverwaltung[5] und leistet damit auch einen Beitrag zur Strategie Digitale Verwaltung Schweiz 2024–2027[6].

3 www.bk.admin.ch > Dokumentation > Medienmitteilungen > Strategie „Netzwerke des Bundes“ (Stand 26.3.2024)
4 www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Vorgaben > Architekturen > AR010 – Cloud-Prinzipien der Bundesverwaltung (Stand 26.3.2024)
5 www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Digitale Bundesverwaltung (Stand 26.3.2024)
6 BBl **2024** 45

Das Vorhaben ist in der Botschaft vom 24. Januar 2024[7] zur Legislaturplanung 2023–2027 im Rahmen des Ziels 8 «Der Bund erbringt seine Leistungen effizient und fördert die Digitalisierung» als erforderliches Geschäft zur Zielerreichung berücksichtigt.

1.4 Verzicht auf Vernehmlassungsverfahren

Das Vorhaben erfüllt keine der Voraussetzungen nach Artikel 3 Absatz 1 des Vernehmlassungsgesetzes vom 18. März 2005[8]. Von der Durchführung eines Vernehmlassungsverfahrens wird daher abgesehen.

7 BBl **2024** 525
8 SR **172.061**

2 Inhalt des Kreditbeschlusses

2.1 Antrag des Bundesrates und Begründung

Das Vorhaben für den Aufbau einer Swiss Government Cloud umfasst Gesamtprogrammausgaben in der Höhe von 319,4 Millionen Franken (Schätzgenauigkeit ± 20 %) für die Jahre 2024–2032. Davon erbringt das BIT Eigenleistungen im Umfang von 70,9 Millionen Franken über dieselbe Zeitperiode. Im Jahr 2024 werden noch keine mehrjährigen Verpflichtungen eingegangen, es fallen jedoch bereits Kosten in der Höhe von 1,6 Millionen Franken für Vorarbeiten an, welche durch das BIT finanziert werden.

Mit der vorliegenden Botschaft beantragt der Bundesrat den eidgenössischen Räten die Bewilligung eines Verpflichtungskredits von 246,9 Millionen Franken. Zudem soll mit dem Bundesbeschluss eine erste Tranche freigegeben werden. Über die Freigabe der zweiten Tranche soll der Bundesrat entsprechend dem Realisierungsfortgang entscheiden (siehe Kapitel 3.1.1.3 «Verpflichtungskredit»). Zudem soll der Bundesrat Verschiebungen zwischen den Tranchen vornehmen können, sodass gegebenenfalls Verpflichtungen für erwartete Mehrausgaben in einer Tranche durch die andere aufgefangen werden können.

2.2 Inhalt der Vorlage im Einzelnen

Damit die SGC zielgerichtet, effizient und unter Nutzung von Synergien aufgebaut und verwendet werden kann, bedarf es Arbeiten in verschiedenen Bereichen. Bei diesen handelt es sich um den Aufbau der Hybrid-Multi-Cloud-Infrastruktur (Stufen I & IIa, IIb und III) sowie um Investitionen in «Ausbildung, Beratung und Governance», «Betriebs- und kommerzielle Prozesse», «Cybersicherheit» und «Netzwerkinfrastruktur»:

Abbildung 2: Darstellung der im Rahmen des Projekts SGC adressierten Handlungsfelder sowie des übergreifenden Programm-Managements

Diese Handlungsfelder seien nachfolgend kurz erläutert.

2.2.1 Aufbau der Hybrid-Multi-Cloud-Infrastruktur

Die SGC ist eine Gesamtlösung für das Massengeschäft der Bundesverwaltung im Cloud-Bereich und wird zukünftig die Stufen I–III des DTI-Cloud-Stufen-Modells (Cloud-Stufen-Modell der Abteilung Digitale Transformation und IKT-Lenkung [DTI] der Bundeskanzlei [BK]) in den Bereichen «Infrastructure as a Service» (IaaS) und «Plattform as a Service» (PaaS) abdecken (siehe Abbildung 3). Damit bildet sie auch die Grundlage für interne und externe Anbieter, innovative «Software as a Service»- (SaaS)-Lösungen in der Private Cloud der SGC (Stufe III) bereitzustellen respektive diese aus dem Leistungsportfolio der Public-Cloud-Anbieter (Stufe I und II) zu beziehen.

Zwischen 2027 und Ende 2030 werden die heutigen Cloud-Lösungen des BIT, die Systemlandschaft Atlantica und der CSB-BIT, durch die SGC abgelöst respektive in diese überführt.

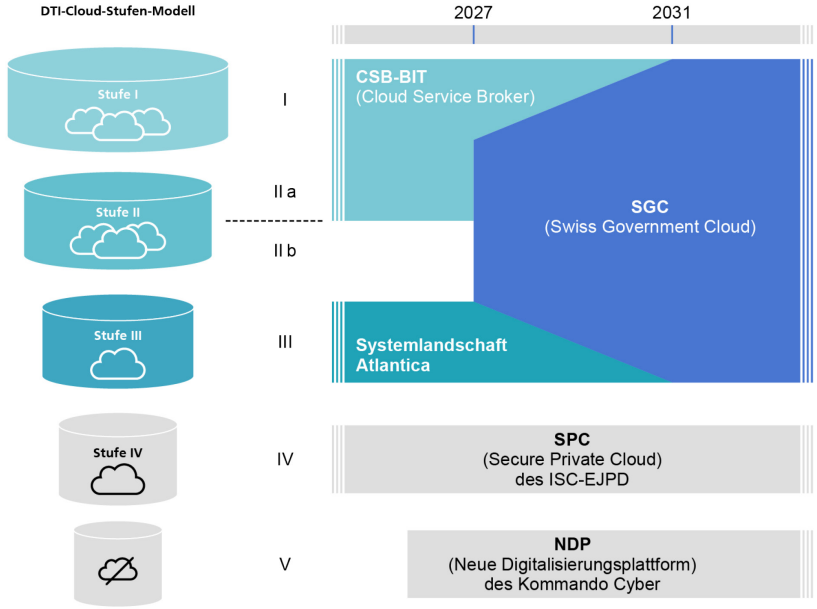

Abbildung 3: Die SGC im Kontext des DTI-Cloud-Stufen-Modells

Für die Stufe IV des Cloud-Stufen-Modells (Private Cloud für spezielle Vorgaben) können Verwaltungseinheiten auf das Angebot «Secure Private Cloud» (SPC) des Informatik Service Centers des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD) zurückgreifen. Für einsatzkritische Systeme der Armee und des Sicherheitsverbunds Schweiz wird das Kommando Cyber die Lösung «Neue Digitalisierungsplattform» (NDP) betreiben (Stufe V).

Beim Einsatz von Cloud-Diensten gilt es stets, verschiedene Anforderungen in den Bereichen des Datenschutzes, der Informationssicherheit, der digitalen Souveränität, der Funktionalität und der Kosteneffizienz gegeneinander abzuwägen. Mit ihrer aus drei Teilen bestehenden Lösung ist die SGC in der Lage, die verschiedenen Anforderungen und Bedürfnisse der Verwaltungseinheiten flexibel abzudecken:

2.2.1.1 Public Cloud

Der erste Teil der Lösung beinhaltet die Public-Cloud-Dienste, die das BIT den Leistungsbezügern über etablierte Public-Cloud-Anbieter zur Verfügung stellt, und deckt damit die Stufen I (Public Clouds Standard) und einen Teil der Stufe II (Stufe IIa –

Public-Cloud-Produkte mit zusätzlichen Vorgaben) des DTI-Cloud-Stufen-Modells ab. Die Public Cloud zeichnet sich insbesondere durch ihre hohe Skalierbarkeit und ihr grosses Portfolio an innovativen Leistungen aus.

Aus wirtschaftlicher und technologischer Sicht ist der Einsatz von Public-Cloud-Diensten interessant, da im Vergleich zur Private Cloud die Kosten der einzelnen Leistungen tiefer sind und das Leistungsportfolio viel umfangreicher ist. Aus diesem Grund soll die Public Cloud unter Einhaltung der rechtlichen Vorgaben bevorzugt eingesetzt werden. Die Public-Cloud-Anbieter müssen in der Lage sein, zusätzliche gesetzliche und technische Vorgaben erfüllen zu können, die im Rahmen des Pflichtenheftes definiert werden.

Beziehen die Verwaltungseinheiten Public-Cloud-Leistungen aus der SGC, sparen sie Zeit und Kosten, da sie von Vorleistungen profitieren; insbesondere von einer vom BIT bereits durchgeführten Beschaffung (d. h., es muss keine eigene WTO-Ausschreibung vorgenommen werden), von garantierter Grundschutzkonformität sowie von vorkonfigurierten und mit den Basisdiensten des Bundes kompatiblen Diensten.

2.2.1.2 Public Cloud On-Prem

Der zweite Teil, die Public Cloud On-Prem, deckt einen Teil der Stufe II (Stufe IIb) des DTI-Cloud-Stufen-Modells ab. Dabei werden Lösungen von etablierten Public-Cloud-Anbietern in den Rechenzentren des Bundes betrieben (sogenannter On-Premise- oder On-Prem-Betrieb). So können Leistungsbezüger Vorteile von Public-Cloud-Diensten auch On-Prem nutzen und die Daten möglichst direkt dort verarbeiten, wo sie anfallen (sogenanntes Edge-Computing). Insbesondere Letzteres ist für datenintensive Anwendungen – etwa in den zukunftsträchtigen Bereichen Internet of Things (IoT) oder Data Analytics – von grossem Vorteil: So können im Vergleich zu den Stufen I und IIa (Public Cloud) tiefere Latenzzeiten und damit eine bessere Leistung sowie eine geringere Netzwerkbelastung erreicht werden, was mit Kosteneinsparungen einhergeht. Aufgebaut wird die Stufe IIb jedoch nur, wenn eine entsprechende Nachfrage nachgewiesen werden kann, und Kapazitätserhöhungen erfolgen nur auf expliziten Kundenwunsch.

2.2.1.3 Private Cloud On-Prem

Der dritte Teil der SGC umfasst die Private Cloud On-Prem und deckt damit die Stufe III des DTI-Cloud-Stufen-Modells ab. Im Gegensatz zur Public Cloud wird hier die komplette Cloud-Infrastruktur im Rechenzentren-Verbund des Bundes betrieben. Die Datenhaltung und -verarbeitung erfolgen gemäss DTI-Cloud-Stufen-Modell auf Basis eines Standard-Produkts für Cloud-Infrastruktur- und Plattform-Leistungen ausschliesslich auf den eigenen Systemen in den Rechenzentren der Bundesverwaltung. Der Betrieb der Private Cloud On-Prem soll, wenn nötig, ausschliesslich durch die Bundesverwaltung sichergestellt werden können (betriebliche Autonomie bei Bedarf).

2.2.2 Ausbau der Netzwerkinfrastruktur

Die Netzwerkinfrastruktur ist ein zentraler Baustein für eine erfolgreiche digitale Transformation; sie ist die Grundlage für sämtliche Leistungen der derzeitigen und zukünftigen Hybrid-Multi-Cloud-Infrastruktur des BIT. Die Netzwerkinfrastruktur der Bundesverwaltung ist sowohl über direkte Leitungen zum Internet als auch über dedizierte Verbindungen mit den Anbietern von Public-Cloud-Leistungen verbunden.

Mit der vermehrten Nutzung von Public-Cloud-Diensten im Hybrid-Cloud-Modell verändern sich auch die Anforderungen an die Netzwerkinfrastruktur. Dies betrifft sowohl die bestehenden Netzwerke in und zwischen den Rechenzentren der Bundesverwaltung als auch die beiden Verbindungen zum Internet und den Anbietern von Public-Cloud-Leistungen. Für beide Verbindungstypen sind substanzielle Ausbauten notwendig, die sich folgendermassen zusammenfassen lassen:

Erhöhung der Netzwerkbandbreiten und Verbesserung der Verfügbarkeit der Netzwerkinfrastruktur

Bedingt durch die zunehmende Verwendung von Fachanwendungen der Bundesverwaltung über das Internet, die vermehrte Einbindung von Diensten von Public-Cloud-Anbietern, die höhere digitale Vernetzung mit anderen Verwaltungen im In- und Ausland sowie den allgemein steigenden Digitalisierungsgrad innerhalb der Bundesverwaltung nimmt der Bedarf an Netzwerkbandbreite zu. Der Netzwerkverkehr verschiebt sich vom On-Prem-Rechenzentrum hin zu externen Dienstleistern. Bereits heute stösst die bestehende Netzwerkinfrastruktur aufgrund dieser Entwicklungen teilweise an ihre Grenzen (z. B. für die Echtzeit-Verarbeitung von Video-Daten im Zollbereich, die Analyse von grossen Datenmengen in der Public Cloud, oder das Backup von Daten aus der Public Cloud zurück ins Bundesnetz). Treibt die Bundesverwaltung ihre Digitalisierung weiter voran, ist absehbar, dass sich dieses Problem verschärfen wird: Erfahrungswerte zeigen, dass sich aktuell rund alle drei Jahre eine Verdoppelung des Bandbreitenbedarfs ergibt. Aufgrund der oben beschriebenen Entwicklungen geht das BIT davon aus, dass zukünftig sogar alle zwei Jahre eine Verdoppelung zu erwarten ist.

Überlastungen der Netzwerkinfrastruktur von und zu den Internetdienstleistern beeinträchtigen die Stabilität und Zuverlässigkeit der Netzwerkleistungen; Verlangsamungen oder gar Ausfälle der Fachanwendungen des Bundes sind die Folge. Um dieses Risiko zu minimieren, ist es zentral, dass die Netzwerkinfrastruktur von und zu den Anbietern von Public-Cloud-Leistungen und die direkten Verbindungen zum Internet durch einen Ausbau rechtzeitig auf eine erhöhte Nutzung von Bandbreiten ausgelegt werden. Nebst diesem Ausbau der Bandbreiten muss auch die Ausfallsicherheit verbessert werden. Diese Verbesserung wird durch zusätzliche Hardware mit entsprechender Leistungsfähigkeit ermöglicht. Änderungen an der Netzwerkinfrastruktur, inklusive Bandbreitenerhöhungen, benötigen Zeit für die Umsetzung und müssen mit Voraussicht geplant werden.

Ausbau der Netzwerkinfrastrukturen in den Rechenzentren der Bundesverwaltung

Um den Zusatzbedarf, der durch die erhöhte Nutzung von digitalen Leistungen entsteht, abzudecken, müssen die Netzwerkinfrastrukturen in den Rechenzentren der Bundesverwaltung ausgebaut werden.

Erhöhung der Automatisierung im Netzwerk und Erleichterung einer verursachergerechten Verrechnung in den Rechenzentren der Bundesverwaltung

Damit Anwendungen schneller und kostengünstiger bereitgestellt werden können, muss auch die Automatisierung im darunterliegenden Netzwerk erhöht werden. Repetitive Aufgaben und Routineprozesse werden automatisiert. Dies führt zu einer erheblichen Erhöhung der Sicherheit und Effizienz, da Zeit und Ressourcen für manuelle Eingriffe reduziert werden. Die Automatisierung ermöglicht zudem eine schnellere Reaktion auf sich ändernde Anforderungen und minimiert potenzielle Ausfallzeiten. Dies ist entscheidend, um flexibel auf neue Projekte, Dienste oder Technologien reagieren zu können, ohne dabei die Netzwerkleistung zu beeinträchtigen. Mit der SGC soll IKT-Leistungserbringern und -Leistungsbezügern die flexible, auf ihre Bedürfnisse abgestimmte Nutzung von Cloud-Diensten ermöglicht werden. Die Bedürfnisse der einzelnen Verwaltungseinheiten sind unterschiedlich; entsprechend unterscheiden sich auch die genutzten Leistungen und die dafür benötigten Bandbreiten. Aus diesem Grund werden im Rahmen der Arbeiten an der Netzwerkinfrastruktur auch die notwendigen netzwerktechnischen Voraussetzungen für eine verursachergerechte und transparente Verrechnung der bezogenen Netzleistungen sowohl innerhalb des Bundesnetzwerkes als auch zum Internet geschaffen. Die Möglichkeit, die Nutzung von Netzwerkressourcen genau zu erfassen und zu verrechnen, erleichtert eine präzise Budgetierung und Kostenkontrolle. Die Bundesverwaltung kann somit ihre finanziellen Ressourcen effektiver verwalten.

Ausbau der sicherheitstechnischen Netzwerk-Komponenten

Angesichts des erhöhten Netzwerkverkehrs ist der Ausbau sicherheitstechnischer Netzwerkkomponenten unerlässlich. Dieser stellt sicher, dass die Sicherheitsvorkehrungen mit der gesteigerten Datenlast Schritt halten können. Die Erweiterung der Sicherheitsinfrastruktur gewährleistet eine robuste Abwehr potenzieller Bedrohungen und gewährleistet die Integrität des Netzwerksystems.

2.2.3 Ausbau der Cybersicherheit

Im Zuge der Umsetzung der Hybrid-Multi-Cloud-Strategie der Bundesverwaltung werden Daten vermehrt ausserhalb der bundeseigenen Rechenzentren bearbeitet. Als Folge muss der Schutz dieser Daten an die neuen Gegebenheiten angepasst werden. Mit den im Rahmen der SGC vorgesehenen Massnahmen werden potenziell vorhandene Lücken geschlossen sowie mögliche Synergien genutzt. Zudem werden damit die Voraussetzungen für die weitere Umsetzung der Nationalen Cyberstrategie[9] sowie der Informationssicherheitsvorgaben der Bundesverwaltung[10] geschaffen.

9 www.ncsc.admin.ch > NCS Strategie (Stand 26.3.2024)
10 www.ncsc.admin.ch > Dokumentation > Informatiksicherheitsvorgaben Bund (Stand 26.3.2024)

2.2.3.1 Datenschutz und Informationssicherheit

Das Datenschutzgesetz vom 25. September 2020[11] (DSG) verlangt eine dem Risiko angemessene Datensicherheit. Dazu müssen geeignete technische und organisatorische Massnahmen getroffen werden. Es wird sichergestellt, dass die SGC die notwendigen technischen und organisatorischen Voraussetzungen erfüllt, um dem Anspruch des DSG an die Datensicherheit zu genügen.

Um die Anforderungen des DSG an die Datensicherheit zu erfüllen, wird das Sicherheitsverfahren des Bundesamtes für Cybersicherheit angewendet.[12] Die Auslagerung der zu bearbeitenden Daten auf die einzelnen Stufen der SGC kann erst dann erfolgen, wenn nach durchgeführter Einzelfallprüfung durch das jeweils verantwortliche Bundesorgan erwiesen ist, dass das entsprechende Vorhaben und die mit dem Vorhaben verbundene Datenbearbeitung in einer der Stufen der SGC rechtlich zulässig sind. Massgebend dafür ist die konkrete Prüfung einer bestimmten Datenbearbeitung in Bezug auf das anwendbare Recht.

Gegebenenfalls kann die Einzelfallprüfung ergeben, dass die Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt. Ist dies der Fall, muss durch das verantwortliche Bundesorgan eine Datenschutz-Folgenabschätzung durchgeführt werden. Ergibt die Datenschutz-Folgenabschätzung trotz der vorgesehenen Massnahmen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so ist eine Stellungnahme des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten einzuholen.

Eine strikt schematische oder automatische Zuordnung von Personendaten und sensiblen Informationen zu einer der Cloud-Stufen ist daher nicht möglich. Insbesondere kann im Einzelfall die Bearbeitung von Personendaten in einer Public Cloud – wegen der besonderen Risiken eines allfälligen Zugriffs durch die Anbieter, ihre Herkunftsstaaten oder Dritte – unzulässig sein.

Gemäss DSG dürfen Personendaten grundsätzlich ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet oder die dafür im DSG statuierten Voraussetzungen erfüllt sind. Auch dies gilt es im Einzelfall zu prüfen.

Das Informationssicherheitsgesetz vom 18. Dezember 2020[13] (ISG), die Informationssicherheitsverordnung vom 8. November 2023[14], die Verordnung vom 8. November 2023[15] über Personensicherheitsprüfungen, die Verordnung vom 8. November 2023[16] über das Betriebssicherheitsverfahren (VBSV) und die Verordnung vom 19.

11 SR **235.1**
12 www.ncsc.admin.ch > Dokumentation > Informatiksicherheitsvorgaben Bund > Sicherheitsverfahren (Stand 26.3.2024)
13 SR **128**
14 SR **1285.1**
15 SR **128.31**
16 SR **128.41**

Oktober 2016[17] über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes bezwecken die Gewährleistung der sicheren Bearbeitung der Informationen, für die der Bund zuständig ist, und des sicheren Einsatzes der Informatikmittel des Bundes.

Das ISG legt die Klassifizierungsstufen «intern», «vertraulich» und «geheim» fest. Weiter sind die Sicherheitsstufen «Grundschutz», «hoher Schutz» und «sehr hoher Schutz» vorgegeben, wobei die Sicherheitsstufe «Grundschutz» für alle Informatikmittel, sofern sie nicht höher eingestuft werden müssen, gilt.

Die SGC wird so konzipiert, dass Informationen bis und mit Klassifizierung «hoher Schutz» sicher bearbeitet werden können. Auf die Bearbeitung von Informationen der Sicherheitsstufe «sehr hoher Schutz» wird hingegen verzichtet. Die SGC wird demnach keine Lösung für Daten der Klassifizierungsstufe «geheim» gemäss ISG bieten. In Bezug auf das Cloud-Stufen-Modell der DTI deckt die SGC die Stufen I–III ab.

Die technischen Voraussetzungen für eine sichere Bearbeitung der Informationen bis und mit Klassifizierung «hoher Schutz» werden sowohl von der bundeseigenen On-Prem-Cloud-Infrastruktur als auch potenziell von etablierten Public-Cloud-Anbietern erfüllt.

Die Verantwortung für die Informationssicherheit liegt bei den verpflichteten Behörden und Organisationen. Die Verwaltungseinheiten beurteilen laufend die Risiken für die Schutzobjekte, setzen die notwendigen Massnahmen um und kontrollieren deren Wirkung. Die ausgewiesenen Restrisiken müssen von der jeweils verantwortlichen Stelle explizit akzeptiert werden.

Die im ISG und in den zugehörigen Verordnungen definierte Governance ist föderalistisch ausgelegt und liegt bei den verpflichteten Behörden und Organisationen. Für die SGC ist es dennoch wichtig, möglichst standardisierte Dienstleistungen anzubieten, um die notwendige Automatisierung umzusetzen und gleichzeitig Synergien zu nutzen. Es ist daher geplant, ein SGC-Kompetenzzentrum (SGC Competence Center) einzurichten, das die Leistungsbezüger entsprechend berät. Damit soll auch ein Beitrag zur wirtschaftlichen Nutzung der Cloud-Infrastrukturen geleistet werden.

2.2.3.2 Herausforderungen der Cybersicherheit

Die Cybersicherheit hat die Aufgabe, dafür zu sorgen, dass die Informatikmittel, die zur Erfüllung der gesetzlichen Aufgaben eingesetzt werden, vor Missbrauch und Störung geschützt werden. Die Herausforderungen, mit denen sie sich in diesem Zusammenhang konfrontiert sieht, haben sich jedoch grundlegend verändert. Während IT-Systeme früher zentral in Rechenzentren betrieben und Arbeitsplätze in Bundesgebäuden angesiedelt waren, ermöglicht die heutige Technologie ortsunabhängiges Arbeiten und den Zugriff auf das Bundesnetz mit verschiedenen Geräten, wobei auch die Nutzung der Public Cloud eine immer grössere Rolle spielt.

17 SR **172.010.59**

Diese Entwicklung hat den traditionellen Sicherheitsperimeter aufgeweicht und erfordert eine Anpassung der Cybersicherheitsstrategien. Angesichts immer professionellerer Angreifer, die ihre Methoden stetig verfeinern, zum Beispiel durch künstliche Intelligenz, ist es notwendig, neue Verteidigungsstrategien zu entwickeln. Public-Cloud-Anbieter haben mit ihren umfassenden Sicherheitsmassnahmen und globalen Sicherheitsteams grosses Potenzial, die Sicherheitsinfrastruktur der Bundesverwaltung zu stärken.

Es ist wichtig, zwischen der «Sicherheit der Cloud» (Betriebsverantwortung des Public-Cloud-Anbieters) und der «Sicherheit in der Cloud» (Betriebsverantwortung des Kunden) zu unterscheiden. Um die Zuständigkeiten zwischen den beiden Verantwortungsbereichen zu regeln, wurde das Modell der «geteilten Verantwortung» entwickelt. Dieses definiert, wer welchen Teil der Infrastruktur verantwortet und bildet damit das zentrale Element der Governance für den Betrieb der Fachanwendungen. Damit wird die Bundesverwaltung entlastet und kann sich auf ihre Kernkompetenzen konzentrieren.

2.2.3.3 Zielbild der Cybersicherheit

Die Ziele der Cybersicherheit sind der Schutz der Informationen und Daten sowie die Einhaltung der Vorgaben der Bundesverwaltung. Um diese zu erreichen, werden in Anlehnung an das etablierte Cyber Security Framework des US-amerikanischen National Institute of Standards and Technology (NIST Cyber Security Framework)[18] Massnahmen in fünf Teilbereichen getroffen. Diese werden nachfolgend mit Fokus auf die SGC erläutert.

Identifizieren

Um die Cybersicherheit professionell gestalten zu können, braucht es ein zuverlässiges Inventar. In der schnelllebigen IT-Welt muss dieses Inventar automatisch aktualisiert werden können. Durch die Einführung der SGC weitet sich das Inventar erheblich aus. Deshalb beinhaltet das Handlungsfeld Cybersicherheit die Einführung eines Werkzeugs zur automatischen Erfassung von eingesetzter Software und allenfalls zur Detektion vorhandener Sicherheitslücken.

Schützen

Ist das Inventar bekannt und aktuell, gilt es, einen risikobasierten adäquaten Schutz aufzubauen. Für die SGC bedeutet das eine Ausweitung des Lizenzbedarfs für die Schutzwerkzeuge, damit der vorgeschriebene Grundschutz überall sichergestellt werden kann. Darüber hinaus muss ein neues Schutzkonzept entwickelt und umgesetzt werden.

Darüber hinaus ist es wichtig, neben den in der VBSV vorgesehenen Massnahmen vertraglich auch die Möglichkeit unabhängiger Audits bei den Lieferanten vorzusehen.

[18] csrc.nist.gov > Glossary > Search > NIST Framework for Improving Critical Infrastructure Cybersecurity (Stand 26.3.2024)

Detektieren

Die generellen Bedrohungen und spezifischen Angriffsmethoden im Cybersicherheitsbereich entwickeln sich stetig weiter. Es ist daher unmöglich, einen 100-prozentigen Schutz aufzubauen. Aus diesem Grund ist es zentral, eine leistungsfähige Detektion aufzubauen. Sollte ein Angreifer erfolgreich sein und in die Infrastruktur der Bundesverwaltung eindringen, gilt es, den Angriff so rasch als möglich zu bemerken, um den Schaden so klein wie möglich zu halten. Dazu müssen bestehende Massnahmen ausgebaut und einige neue hinzugefügt werden. Die wichtigste neue Massnahme ist ein Werkzeug zur Detektion von verdächtigem Verhalten im Netzwerk. Im Rahmen der SGC werden die notwenigen Ausrüstungen und Lizenzen beschafft sowie die Mitarbeitenden befähigt, Anomalien im Netzverkehr zu entdecken und Gegenmassnahmen zu ergreifen.

Reagieren

Wurde ein Angreifer oder eine Schadsoftware detektiert, geht es darum, Gegenmassnahmen zu ergreifen. Möglichst rasch handeln zu können, ist hier essenziell. Deshalb soll mit der SGC eine Teilautomatisierung für die Reaktion auf Angriffe und Schadsoftware eingeführt werden.

Wiederherstellen

Nachdem ein Angriff oder eine Schadsoftware abgewehrt sind, gilt es, aus dem Vorfall zu lernen und die Detektionswerkzeuge zu aktualisieren, damit dieselben Angriffsmethoden oder Schadsoftwares nicht mehr erfolgreich sein können. Hier sind in der SGC keine weiteren technischen Massnahmen, sondern es ist eine personelle Aufstockung vorgesehen.

2.2.3.4 IT-Compliance

Bei der Einführung der drei Stufen der SGC muss darauf geachtet werden, die Sicherheits- und Compliance-Vorgaben einzuhalten. Aus diesem Grund werden international anerkannte Sicherheitsregeln implementiert, und ein stringentes IT-Compliance-Testing wird eingeführt. Um diesem Anspruch gerecht zu werden, muss neues Personal mit entsprechenden Fähigkeiten rekrutiert werden.

Das BIT ist nach der ISO-Norm 27001 zertifiziert und betreibt seit Jahren ein entsprechendes Informationssicherheits-Managementsystem (ISMS). Darüber hinaus werden die im BIT betriebenen staatsrechnungsrelevanten Applikationen im Auftrag der Eidgenössischen Finanzkontrolle (EFK) jährlich durch eine externe Firma nach dem Prüfstandard ISAE 3402 geprüft. Das DSG sieht ebenfalls eine Zertifizierung vor. Mit dem zertifizierten ISMS erfüllt das BIT die Voraussetzungen, um darauf basierend auch den Datenschutz zertifizieren zu lassen. Für die Ausdehnung der Zertifizierung gemäss ISO 27001 auf die Public Cloud wird ein höherer Personalaufwand eingeplant. Mehraufwände, die durch das neue DSG entstehen, sind in der SGC nicht berücksichtigt, weil diese von der jeweiligen Applikation und somit vom jeweiligen Leistungsbezüger zu tragen sind.

2.2.4 Betriebs- und kommerzielle Prozesse

Die steigende Dynamik im Digitalisierungsumfeld, insbesondere im Bereich Public Cloud, verlangt nach industrialisierten und hochautomatisierten Lösungen zum Betrieb der Hybrid-Multi-Cloud-Umgebung (Betriebsprozesse) und zur Auftragsabwicklung – von der Bestellung der Cloud-Dienste durch die Kunden im Self-Service-Portal bis hin zur vollständigen und verursachergerechten Verrechnung der genutzten Leistungen (kommerzielle Prozesse). Im Rahmen des Handlungsfelds «Betriebs- und kommerzielle Prozesse» wird deshalb die gesamte Prozesskette automatisiert.

2.2.4.1 Betriebsprozesse

Hochautomatisierte Betriebsprozesse gewährleisten eine schnelle und konsistente Bereitstellung und technische Aktualisierung von Infrastrukturen und Leistungen, minimieren Inkonsistenzen und Fehler, ermöglichen eine effiziente Nutzung bestehender sowie die automatische Deaktivierung ungenutzter Ressourcen und entlasten das IT-Fachpersonal von manuellen, wiederkehrenden Tätigkeiten.

Mit der SGC soll daher ein neues industrialisiertes Betriebsmodell eingeführt werden. Dieses ermöglicht zum einen, personelle Ressourcen im Bereich des Infrastruktur- und Plattform-Betriebs signifikant zu reduzieren. Mit den freiwerdenden Ressourcen könnten stattdessen kundennahe Bereiche, wie zum Beispiel die Entwicklung von Fachanwendungen oder die Beratung, gestärkt werden, die für die Leistungsbezüger den grössten Mehrwert generieren. Zum anderen können durch die konsequente Automatisierung von Prozessen und die Standardisierung des Leistungskatalogs langfristig Betriebskosten eingespart werden.

Um diese Veränderung sozialverträglich zu gestalten, wird die anstehende Pensionierungswelle der geburtenstarken Jahrgänge genutzt (in den nächsten 10 Jahren wird fast ein Drittel der BIT-Mitarbeitenden pensioniert); Personen, die in Pension gehen, werden durch Personen mit Profilen ersetzt, die den Anforderungen des neuen Betriebsmodells entsprechen.

«IT Service Provider for IT Service Provider»-Modell

Des Weiteren soll es auch anderen IKT-Leistungserbringern möglich sein, ihren Kunden aus dem Bund sowie anderen Stellen der öffentlichen Verwaltung Leistungen aus der SGC anzubieten. Durch technische Funktionalitäten und organisatorische Massnahmen stellt die SGC ein «IT Service Provider for IT Service Provider»-Modell zur Verfügung. Damit sollen Leistungen aus der SGC nicht zwingend direkt über das BIT, sondern prinzipiell über alle IKT-Leistungserbringer des Bundes bezogen werden können. So sollen bundesinterne Synergien genutzt werden.

2.2.4.2 Kommerzielle Prozesse

Um die gesamte Prozesskette automatisieren zu können, werden im Rahmen der SGC auch die kommerziellen Prozesse in den Fokus gerückt. Ziel ist es, den administrativen Aufwand sowohl für Leistungsbezüger als auch für die Mitarbeitenden des BIT deutlich zu reduzieren. Darüber hinaus profitieren Leistungsbezüger von einer gesteigerten Transparenz.

Self-Service-Portal

Mit der SGC sollen IKT-Leistungserbringer und -Leistungsbezüger die Vorteile von Cloud-Diensten möglichst einfach nutzen können. Dazu wird die SGC an ein neues Self-Service-Portal des BIT angebunden, über das die Leistungsbezüger ihre Leistungen zentral über verschiedene Cloud-Plattformen hinweg unkompliziert beziehen und verwalten können. Damit sollen die Sicherheit, die Effizienz, die Agilität und die Benutzerfreundlichkeit der Cloud-Nutzung weiter gefördert werden.

Reporting und Abrechnung der Cloud-Dienste (360-Grad-Cockpit)

Die Verwaltung der Ressourcennutzung in einer Hybrid-Multi-Cloud-Umgebung erfordert eine effektive Überwachung, Abrechnung und Fakturierung der genutzten Leistungen. Aus diesem Grund wird das Self-Service-Portal ein 360-Grad-Cockpit bereitstellen, das Verwaltungseinheiten jederzeit die volle Übersicht und Kontrolle über die Nutzung und Kosten ihrer Cloud-Ressourcen bietet.

Über das Cockpit können Verwaltungseinheiten an einem zentralen Ort den Ressourcenverbrauch über verschiedene Cloud-Anbieter hinweg verfolgen und auswerten. Transparente Berichte über den Ressourcenverbrauch und die damit verbundenen Kosten sowie integrierte Kostenkontrollmechanismen ermöglichen den Verwaltungseinheiten eine detaillierte Analyse von Nutzungstrends, damit sie ihre Ausgaben im Blick behalten und die Nutzung ihrer Cloud-Ressourcen planen und optimieren können.

Integration von spezifischen kommerziellen Prozessen für das «IT Service Provider for IT Service Provider»-Modell

Damit IKT-Leistungserbringer, die ihren Leistungsbezügern in Einklang mit dem «IT Service Provider for IT Service Provider»-Modell Leistungen aus der SGC anbieten, die SGC nahtlos in ihre kommerziellen Prozesse integrieren können, wird die SGC entsprechende Schnittstellen und Funktionalitäten zur Verfügung stellen. So werden die erwähnten IKT-Leistungserbringer ebenfalls in der Lage sein, ihren Leistungsbezügern automatisiert transparente Verbrauchsberichte und verursachergerechte Rechnungen zur Verfügung zu stellen.

2.2.5 Ausbildung, Beratung und Governance

Verwaltungseinheiten sollen die SGC sicher, effizient und zielgerichtet nutzen können. Mit dem Handlungsfeld «Ausbildung, Beratung und Governance» sollen sie bei Bedarf bei der Nutzung der Hybrid-Multi-Cloud-Umgebung umfassend begleitet werden. Damit soll sichergestellt werden, dass die Verwaltungseinheiten die Vorteile der Umgebung und der damit verbundenen Technologien voll ausschöpfen und gleichzeitig allfällige Risiken minimieren können.

2.2.5.1 Ausbildungsangebot

Mit der SGC halten neue Cloud-Technologien, -Plattformen und -Dienste sowie neue Prozesse in die Bundesverwaltung Einzug. Damit Mitarbeitende die erforderlichen Kenntnisse und Fähigkeiten entwickeln, um den grösstmöglichen Nutzen aus diesen

neuen Möglichkeiten zu ziehen, wird unter dem Namen «SGC Academy» ein qualitativ hochwertiges Ausbildungsangebot für den Aufbau und die Sicherung von SGC-spezifischem Fachwissen bereitgestellt. Ziel ist, Kurse für ein möglichst breites Rollenspektrum anzubieten, um die Verwaltungseinheiten beim Wissensaufbau in den jeweils erforderlichen Bereichen optimal zu unterstützen, wobei der Hauptfokus auf Weiterbildungen für IT-Fachkräfte liegen wird.

2.2.5.2 SGC Competence Center

Das SGC Competence Center soll interessierte Verwaltungseinheiten in der Erarbeitung und Umsetzung ihrer Cloud-Strategie sowie dazugehöriger Vorhaben beraten, unterstützen und begleiten (z. B. hinsichtlich der Wahl der passenden Cloud-Dienste oder Aufzeigen von Best Practices). Im Zentrum stehen dabei Themen wie Cloud-Funktionalität und -Architektur, Kosteneffizienz und -kontrolle, Cloud-Governance sowie digitale Souveränität. Das SGC Competence Center berät die interessierten Verwaltungseinheiten bei der Wahl der richtigen Cloud-Stufe respektive hilft, deren Bezug zu koordinieren, und leistet so einen wichtigen Beitrag zur wirtschaftlichen Nutzung der drei Stufen der SGC.

2.2.5.3 Innovation Center

Die Leistungen und Konzepte der SGC sollen greifbar gemacht werden. Indem es ihnen Möglichkeiten aufzeigt, wie sie ihre Digitalisierung mit Hilfe der SGC vorantreiben können, soll das Innovation Center als Inspiration für die Leistungsbezüger dienen. Damit kann dem strategischen Ziel der SGC, die Digitalisierung zu beschleunigen, Rechnung getragen werden. Das Innovation Center ermöglicht einen offenen Austausch über erfolgreich durchgeführte Cloud-Vorhaben und neu verfügbare, innovative Leistungen (zum Beispiel im Bereich KI) sowie die damit verbundenen Best Practices zwischen Verwaltungseinheiten und anderen interessierten Stellen.

2.2.5.4 SGC-weite Cloud-Governance

In Einklang mit der Hybrid-Multi-Cloud-Strategie der Bundesverwaltung sollen Verwaltungseinheiten künftig unterschiedliche Cloud-Leistungen nutzen und miteinander kombinieren können – sowohl eingekaufte als auch durch die Bundesverwaltung aufgebaute. Um dabei eine geordnete, sichere und effiziente Nutzung von Cloud-Diensten sicherzustellen, sind personelle, vertragliche, organisatorische und technische Massnahmen notwendig. Diese werden im Rahmen der Cloud-Governance festgelegt.

Der Bereich DTI der BK hat mit den Cloud-Prinzipien der Bundesverwaltung die Grundregeln definiert, die bei der Nutzung von Public- und Private-Cloud-Diensten zu berücksichtigen sind. Darauf basierend stellt die SGC-weite Cloud-Governance sicher, dass alle Cloud-Ressourcen und -Dienste einheitlichen Richtlinien und Standards folgen, damit die verschiedenen Cloud-Umgebungen konsistent verwaltet werden und keine Inkompatibilitäten auftreten. Des Weiteren ermöglicht die Governance, Sicherheitsrichtlinien und -massnahmen über alle Stufen der SGC hinweg zu implementieren und durchzusetzen. Dies gewährleistet einen einheitlichen Schutz vor Bedrohungen und hilft bei der Einhaltung der Compliance-Anforderungen und Datenschutzbestimmungen. Dazu werden im Rahmen der SGC vorkonfektionierte,

vorkonfigurierte und bereits mit den Standard-Diensten des Bundes kompatible Dienste bereitgestellt, auf die IKT-Leistungserbringer für die Entwicklung und Umsetzung ihrer Lösungen zurückgreifen können.

In einem hybriden Cloud-Modell müssen verschiedene Cloud-Umgebungen einfach miteinander kombiniert werden können. Eine übergreifende Cloud-Governance beinhaltet die Implementierung von Mechanismen zur Interoperabilität der verschiedenen Cloud-Angebote der SGC. Dadurch soll ein möglichst einfacher Wechsel von einem Cloud-Anbieter zu einem anderen und von einer Cloud-Stufe in eine andere ermöglicht werden (sogenannte «Exit-Strategie»). Indem es die SGC-weite Cloud-Governance dem Bund erlaubt, zum Beispiel auf ungünstige Veränderungen der Konditionen bei Bedarf mit einem Wechsel zu reagieren, leistet sie einen wichtigen Beitrag, um die Wirtschaftlichkeit der SGC langfristig sicherzustellen

2.3 Geprüfte Varianten für Aufbau und Sequenz

Im Rahmen der Konzeption der SGC wurden mehrere Varianten für den sequenziellen Aufbau der Hybrid-Multi-Cloud-Infrastruktur geprüft und gemäss den nachfolgenden Kriterien bewertet:

- Kosteneinsparung IKT-Leistungserbringer (LE) BIT
- Kosteneinsparung Leistungsbezüger (LB)
- Migrationsaufwand
- Planungssicherheit
- Erhöhung der Betriebsstabilität
- Pensionierungswelle nutzen
- Kosten für Aufbau und Parallelbetrieb

Die beste Bewertung erhielt die Variante, die von Anfang an die Beschaffungsgrundlagen für alle drei Stufen der SGC schafft. Die Stufen I & IIa sowie III werden anschliessend parallel aufgebaut. Die Stufen IIb und III werden zunächst mit den für die Migration erforderlichen Infrastruktur-Ressourcen ausgestattet und anschliessend bedarfsgerecht skaliert. Die Stufe IIb soll dabei erst aufgebaut werden, wenn ein konkreter Kundenbedarf besteht. Basierend auf der Bedürfnisanalyse geht das BIT davon aus, dass erste Leistungsbezüger das Angebot IIb ab 2029 nutzen wollen.

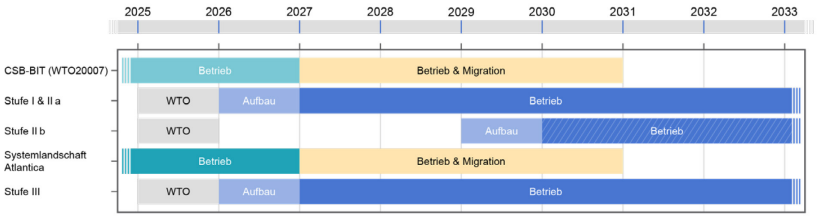

Abbildung 4: Zeitrahmen für die Variante Parallelaufbau der Stufen I, IIa und III

Dank diesem Vorgehen können umfangreiche Kosteneinsparungen erzielt (siehe Kapitel 3.1.1.5 «Einsparungen während und nach dem Programm») und es kann die Betriebsstabilität dank konsequenter Automatisierung und Standardisierung stark erhöht werden (siehe auch Kapitel 2.2.4 «Betriebs- und kommerzielle Prozesse»). Darüber hinaus wird die Planungssicherheit der Leistungsbezüger und der anderen IKT-Leistungserbringer des Bundes sichergestellt, da die technologische Ausstattung der Stufen der SGC frühzeitig feststeht. Dies vereinfacht insbesondere die Migrationsplanung in die Stufen sowie die Planung von Lifecycle-Vorhaben für in die Jahre gekommene Fachanwendungen, die dringend erneuert werden müssen, erheblich.

2.4 Bedürfnisanalyse und Bedarfserhebung

Mit der SGC soll im Einklang mit der Cloud-Strategie der Bundesverwaltung eine auf die Anforderungen und Bedürfnisse des Bundes zugeschnittene Hybrid-Multi-Cloud-Infrastruktur aufgebaut werden. Um dieses Ziel zu erreichen, wurden im Rahmen der Vorarbeiten zur SGC zwei Befragungen durchgeführt:

Mit der Bedürfnisanalyse wurden die Bedürfnisse und Anforderungen der Verwaltungseinheiten der Bundesverwaltung sowie der Parlamentsdienste ermittelt, um die SGC konsequent daran ausrichten zu können. Die Ergebnisse dienen dazu, die spezifischen Anforderungen der Leistungsbezüger hinsichtlich Skalierbarkeit, Funktionsumfang sowie Sicherheit und Compliance der Infrastruktur zu verstehen. Die weitere Planung des Vorhabens sowie die öffentliche Ausschreibung für den Aufbau der SGC basieren auf den erwähnten Ergebnissen. Die Analyse zeigt, dass die Verwaltungseinheiten den Aufbau einer Hybrid-Multi-Cloud-Infrastruktur begrüssen, welche die vielfältigen geschäftlichen, sicherheitsbezogenen und technischen Anforderungen des Bundes erfüllt.

Im Rahmen der Bedarfserhebung wurden die Departemente und IKT-Leistungserbringer der Bundesverwaltung sowie die Parlamentsdienste dazu befragt, ob für die geplante Einführung des «IT Service Provider for IT Service Provider»-Modells ein Bedarf besteht und welche Anforderungen das Modell aus ihrer Sicht erfüllen muss. Die Befragung ergab, dass die Einführung dieses Modells von allen begrüsst wird.

Des Weiteren wurde nach einer Schätzung des zukünftigen Bedarfs, also der voraussichtlichen Bezugsvolumen und nach deren prozentualer Verteilung auf die Cloud-Stufen der SGC, gefragt, um darauf basierend die Beschaffungsvolumen der öffentlichen Ausschreibungen für den Aufbau der SGC festzulegen und die Kostenschätzung zu validieren.

Zusammenfassend wurde von allen IKT-Leistungserbringern des Bundes gemeldet, dass, Stand heute, voraussichtlich folgende Volumen aus den drei Stufen der SGC bezogen würden:

- Fachanwendungen: 1027
- Virtuelle Maschinen: 9413
- Container: 8200
- Speicher: 108,9 Petabyte
- Prozessorkerne: 19 868

Die durchschnittliche Verteilung der Cloud-Nutzung des Bundes gestaltet sich gemäss heutiger Einschätzung des zukünftigen Bedarfs wie folgt:

	Zum Zeitpunkt der Migration im Jahr 2027	**Zum Abschluss des Programms im Jahr 2032**
Stufe I und IIa – Public Cloud	8 %	68 %
Stufe IIb – Public Cloud On-Prem	0 %	10 %
Stufe III – Private Cloud On-Prem	92 %	22 %

Tabelle 1: Prozentuale Verteilung der voraussichtlichen Nutzung der Cloud-Stufen

Der Tabelle ist zu entnehmen, dass die IKT-Leistungserbringer eine relative Verlagerung ihrer Datenmengen von der Private in die Public Cloud prognostizieren. Diese Prognose deckt sich mit den Einschätzungen der ausländischen Regierungen und des Marktanalysten Gartner, die im Rahmen der Vorarbeiten zur SGC befragt wurden. Angesichts der erwähnten Verlagerung werden alle Stufen der SGC skalierbar konzipiert. Die benötigte Hardware zum Aufbau der On-Prem-Lösungen soll daher über ein «Pay as You Use»-Modell bezogen und nicht gekauft werden. Bei der Interpretation der Tabelle gilt es zu beachten, dass basierend auf Erfahrungswerten über alle Stufen hinweg insgesamt ein starker Zuwachs der Datenvolumen zu erwarten ist.

Aufgrund der sich stetig ändernden Anwendungs- und Technologielandschaft sowie weiterer Entwicklungen ist zu erwarten, dass sich die genannten Zahlen bis zum Beginn der Migration im Jahr 2027 noch verändern werden. Das BIT wird die Bedarfserhebung daher jährlich aktualisieren, damit die skalierbare Infrastruktur der SGC im effektiv benötigten Umfang aufgebaut werden kann.

2.5 Risiken

2.5.1 Kontext der Risikobetrachtung

Für die Risikobeurteilung wird von der Bewilligung des Verpflichtungskredits SGC durch das Parlament und der späteren Finanzierung des Vorhabens ausgegangen.

Der Fokus der Betrachtung liegt auf den Risiken, die im Rahmen des Programms direkt adressiert werden. Es handelt sich dabei um nicht erfüllte Aufgaben und Zielvorgaben gemäss Kapitel 2.1.

2.5.2 Risiko, die Ziele nicht zu erreichen

Generell: Das Risiko, die geplanten Ergebnisse nicht zu erreichen, kann entstehen, wenn die anfänglich definierten Programmziele im Verlaufe der Umsetzung des Vorhabens geändert werden müssen; etwa aufgrund der sich rasch verändernden Technik, wie zum Beispiel der künstlichen Intelligenz oder der zunehmenden Digitalisierung des täglichen Lebens. Werden die Programmziele angepasst, um auf solche Entwicklungen reagieren zu können, hat das einen direkten Einfluss auf die Kosten und die Umsetzungstermine.

Konkret: Der angestrebte einheitliche Zugang zum gesamten Spektrum der Cloud-Dienste der Stufen I–III kann nicht realisiert werden, weil die IT-Governance der Bundesverwaltung eine andere Lösung beschliesst.

Sicherheit und Compliance: Hier ist das Ziel, dass notwendige Informationen zur richtigen Zeit unverändert den richtigen Personen zur Verfügung stehen, damit möglichst gut abgestützte Entscheide gefällt werden können. Die grösste Gefahr geht aktuell von sogenannten Ransomware-Angriffen aus, bei denen Informationen verschlüsselt werden und gedroht wird, gestohlene Daten zu veröffentlichen. Ein weiteres Ziel ist die Einhaltung von Gesetzen, Vorgaben und vertraglichen Vereinbarungen.

Technische Risiken: Es ist das Ziel, eine technisch moderne und zukunftsorientierte Infrastruktur bereitzustellen. Es besteht die Gefahr, von disruptiven Innovationen überrascht zu werden und während der Projektdauer neue Technologien einzuführen, die zu Kompatibilitätsproblemen führen können. Es geht darum, möglichst keine technischen Schulden aufzubauen.

Marktrisiken: Der Cloud-Markt ist volatil und derzeit von der Konsolidierung verschiedener technischer Lösungen geprägt. Das birgt das Risiko, in Lösungen zu investieren, die sich am Markt nicht durchsetzen und damit zu technischen Schulden führen. Ein weiterer Aspekt ist der Trend zu vertikalen Angeboten der Cloud-Anbieter, das heisst, es werden immer mehr Leistungen angeboten, die auf bestimmte Branchen (z. B. Gesundheits- oder Industriebranche) zugeschnitten sind. Diese Tendenz ist auch für das Marksegment der öffentlichen Verwaltungen zu beobachten. Setzt die öffentliche Verwaltung dennoch auf individuelle oder stark angepasste Lösungen statt Standardangebote der Cloud-Anbieter, besteht die Gefahr, hohe Kosten zu generieren.

Akzeptanzrisiken: Die SGC soll so konzipiert werden, dass sie den Anforderungen und Bedürfnissen der öffentlichen Verwaltung gerecht wird. Sonst besteht die Gefahr, dass die im Rahmen des Vorhabens aufgebaute Lösung bei den zukünftigen Nutzerinnen und Nutzern nicht auf die nötige Akzeptanz stösst. Es gilt, mögliche Fehlinvestitionen zu vermeiden.

2.5.3 Massnahmen für die Zielerreichung

Generell: Das Programm SGC begegnet diesem Risiko auf vier Ebenen: Zusammenarbeit mit Hochschulen und einem renommierten Marktanalyse-Unternehmen, sorgfältige Beobachtung des Marktes im Bereich neu aufkommender Technologien und stringentes Änderungsmanagement.

Sicherheit und Compliance: Das BIT ist schon heute nach ISO-Norm 27001 zertifiziert und betreibt ein umfassendes Kontrollsystem. Darüber hinaus werden staatsrechnungsrelevante Applikationen einer jährlichen Prüfung durch eine von der EFK beauftragte Firma unterzogen. Damit reduziert das BIT die Informationssicherheitsrisiken. Weiter stellen über 50 Cyber Champions (interne Mitarbeitende beim BIT mit Zusatzausbildungen im Bereich Cybersicherheit) die Einhaltung der Vorgaben sicher.

Technische Risiken: Mit der neuen Stelle des Chief Technology Officers (CTO), der einen Technologie-Radar führt, hat das BIT die Voraussetzungen geschaffen, die technischen Risiken zu minimieren.

Marktrisiken: Die Marktrisiken werden durch eine gründliche Evaluation möglicher Lösungen und eine darauf aufbauende Beschaffung minimiert. Dazu wurden verschiedene Cloud-Anbieter zu ihren aktuellen und zukünftigen Leistungsportfolios befragt. Zur Minimierung von Beschaffungsrisiken wird seit Beginn der entsprechenden Vorarbeiten ein enger Kontakt mit den Beschaffungsstellen der Bundesverwaltung gepflegt, der im Rahmen des Vorhabens fortgeführt werden soll.

Akzeptanzrisiken: Die wichtigste Massnahme, um Akzeptanzrisiken zu begegnen, ist das Stakeholdermanagement. Das Programm SGC stellt die nötigen Ressourcen bereit, um auch nach den durchgeführten Bedarfserhebungen und Bedürfnisanalysen einen kontinuierlichen Dialog mit seinen zukünftigen Nutzern sicherstellen zu können. Zudem soll ein Fachausschuss eingerichtet werden (siehe Kapitel 2.6 «Programmstruktur»), in dem die Nutzerinnen und Nutzer der SGC die Projektergebnisse beurteilen und entsprechende Rückmeldungen direkt in das Programm einfliessen lassen können.

2.5.4 Budgetrisiko

Ein Budgetrisiko entsteht, wenn das Programm das ursprünglich festgelegte Budget überschreitet. Grund dafür kann eine unrealistische oder zu wenig detaillierte Budgetierung in der Projektplanungsphase sein.

Trotz einer sorgfältigen und detaillierten Planung der SGC besteht die Möglichkeit, dass das Budget überschritten wird oder Kosten zu spät eingespart werden können. Ersteres kann zum Beispiel der Fall sein, wenn die Hardwarekosten aufgrund der Teuerung oder des technologischen Wandels höher als geplant ausfallen. Das Risiko, Sparpotentiale nicht termingerecht ausschöpfen zu können, entsteht beispielsweise durch einen längeren Betrieb der bestehenden Plattform.

Da die Beschaffung zum aktuellen Zeitpunkt noch ausstehend ist, sind weder das exakte Service-Portfolio noch die dazugehörigen Preismodelle bekannt. Daher gibt es derzeit nur einen Kostenrahmen, nicht jedoch eine Kosten-Nutzen-Analyse.

2.5.5 Massnahmen zur Einhaltung der Kosten und des Budgets

Das Programm SGC begegnet diesen Risiken einerseits mit der Einberechnung eines Risikozuschlags von 15 bis 20 Prozent, um Mehraufwände infolge von technologischem Wandel oder von Beschaffungsrisiken abdecken zu können. Die Kostenschätzung wurde im Rahmen der Vorarbeiten zur SGC durch unabhängige Dritte geprüft (siehe Kapitel 3.1.4 «Zweitmeinungen») und wird spätestens für die nächste Bedarfsmeldung im Jahr 2025 erneut geprüft und aktualisiert, um die Planungsgenauigkeit sicherzustellen. Andererseits werden IKT-Leistungserbringer und -Leistungsbezüger frühzeitig eingebunden, um die Migrationen im geplanten Zeitraum durchzuführen und diese möglichst gleichmässig über die für die Migration zur Verfügung stehende Zeitspanne hinweg zu verteilen.

Darüber hinaus werden für jedes Projekt klare Ziele definiert, Risiken und Herausforderungen identifiziert, effiziente und effektive Vorgehensweisen gewährleistet, Machbarkeitsstudien erstellt und, wo sinnvoll, Proofs of Concept durchgeführt, welche die Lösung in der Praxis testen und die Kosten des Projekts voraussehbarer machen.

2.5.6 Zeitrisiko

Das Zeitrisiko besteht darin, dass Aufgaben des Programms länger dauern als ursprünglich erwartet. Verzögerungen im Zeitplan können sich auf andere Aspekte wie die Kosten, den Termin der Realisierung oder die Gesamtleistung auswirken.

Konkret: Sollten die ersten Leistungen nicht wie geplant ab 2026 zur Verfügung stehen, zum Beispiel, weil die Beschaffung mehr Zeit in Anspruch nimmt als geplant, würde sich die Migration verschieben. Dadurch würden nebst Sicherheitsrisiken auch Mehrkosten entstehen, da die Systemlandschaft Atlantica länger betrieben werden müsste.

Entscheidend ist die Einhaltung des geplanten Zeitfensters für die Migrationen der Fachanwendungen auf die SGC. Gründe wie die Unterschätzung des Arbeitsaufwandes, fehlende Ressourcen, mangelnde Expertise, ausstehende Entscheide oder der Abgang von Schlüsselpersonen können zu einer Verzögerung führen. Das Resultat wäre ein signifikanter Anstieg der Kosten, weil der Parallelbetrieb der alten und neuen Cloud-Infrastruktur länger als geplant notwendig wäre.

2.5.7 Massnahmen zur Termineinhaltung

Als prioritäre Massnahme wird ein besonderes Augenmerk auf die Beschaffungen und die Migrationen der Applikationen gelegt, um frühzeitig auf Abweichungen von der Terminplanung reagieren zu können. Mit einer detaillierten und regelmässig aktualisierten Planung wird das Risiko solcher Abweichungen minimiert. Mit der Planung der Migrationen wird frühzeitig unter Einsatz klar zugeteilter Ressourcen begonnen. Das Ziel ist, den Leistungsbezügern rechtzeitig alle für ihre Planung relevanten Informationen zur Verfügung zu stellen.

Weiter werden die einzelnen Projekte für eine möglichst konsequente Termineinhaltung mithilfe klarer Zielsetzungen, regelmässiger Anpassungen an die Projekt- und Ressourcenplanung, strikter Überwachung der Erreichung der Meilensteine und sorgfältiger Steuerung der Abhängigkeiten realisiert.

Zudem ist es wichtig, klare und kurze Entscheidungswege zu definieren sowie ein sorgfältiges Stakeholdermanagement und eine adäquate Kommunikation sicherzustellen. Sowohl die Kommunikation als auch das Stakeholdermanagement werden daher direkt bei der Programmleitung angesiedelt, und es werden die dafür notwendigen Ressourcen bereitgestellt.

Letztlich besteht die Gefahr, dass das Vorhaben bei den zukünftigen Nutzern nicht auf die nötige Akzeptanz stösst. Um diesem Risiko zu begegnen, ist auch hier das Stakeholdermanagement die wichtigste Massnahme. Das Programm SGC stellt die nötigen Ressourcen bereit, um auch nach den durchgeführten Bedarfserhebungen und Bedürfnisanalysen einen kontinuierlichen Dialog mit seinen zukünftigen Nutzern sicherstellen zu können. Zudem soll ein Fachausschuss eingerichtet werden (siehe Kapitel 2.6 «Programmstruktur»), in dem die Nutzer der SGC die Projektergebnisse beurteilen und entsprechende Rückmeldungen direkt in das Programm einfliessen lassen können.

2.6 Programmstruktur

Die Organisation des Programms SGC entspricht den Vorgaben des Bundesrates zur Umsetzung von Schlüsselprojekten.

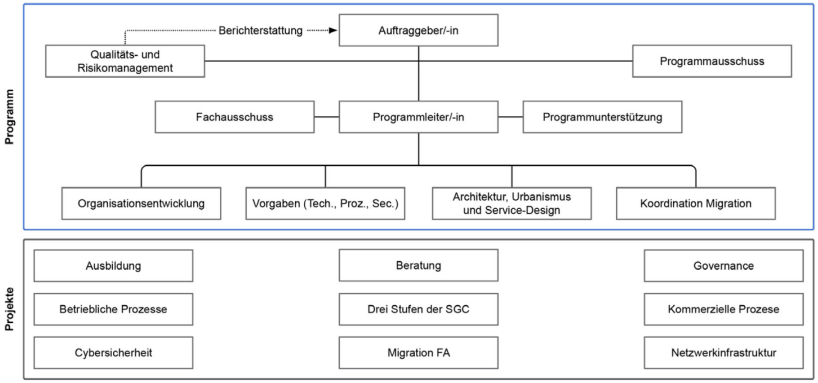

Abbildung 5: Darstellung der Struktur des Programms SGC

Auftraggeberin

Die Generalsekretärin EFD wird als Auftraggeberin des Programms SGC amten.

Programmausschuss

Um sicherzustellen, dass die Leistungsbezüger und die BK-DTI angemessen beteiligt sind und deren Bedürfnisse berücksichtigt werden, soll ein Programausschuss eingerichtet werden.

Qualitäts- und Risikomanagement

Aufgrund der Grösse und der fachlichen Komplexität des Vorhabens verlangt der Bundesrat ein starkes, unabhängiges Qualitäts- und Risikomanagement (QRM), das über alle Verantwortungsstufen hinweg die Qualität der Arbeiten überprüft und die Risiken verwaltet. Seine Empfehlungen richtet das QRM direkt an die Auftraggeberin.

Programmleiter/-in

Die Programmleiterin oder der Programmleiter unterstützt die Auftraggeberin bei der Umsetzung der SGC; sie oder er führt und kontrolliert die Arbeiten auf Stufe Programm, koordiniert die Abhängigkeiten und konsolidiert die Berichterstattung sowie

die Kommunikation. Die Programmleiterin oder der Programmleiter soll bereits Programme von ähnlicher Grösse und Komplexität im Umfeld der Bundesverwaltung erfolgreich umgesetzt haben.

Programmunterstützung

Die Programmunterstützung hilft der Programmleitung in organisatorischen, administrativen und weiteren Belangen des Programmmanagements. Dazu gehören:

- Kommunikation
- Controlling
- Finanzen
- Rechtliches
- Beschaffung
- Project Management Office (PMO)
- Personalmanagement

Je nach Situation unterstützt die Programmunterstützung auch die Projektleitungen.

Fachausschuss

Um sicherzustellen, dass die IKT-Leistungserbringer und die BK-DTI angemessen beteiligt sind und deren Bedürfnisse berücksichtigt werden, soll ein Fachausschuss eingerichtet werden. Die Mitglieder des Fachausschusses sollen die Programmleitung bei der Beurteilung der Ergebnisse unterstützen.

Programmsteuerung

Die Programmsteuerung beinhaltet programmspezifische Fachführungs- und Koordinationsaufgaben, um Governance und Steuerung projektübergreifend sicherzustellen:

- Organisationsentwicklung: Organisatorisches Change Management, d. h. Transformation innerhalb des BIT
- Vorgaben*:* Projektübergreifende Vorgaben zu Technologie, Prozessen, Sicherheit usw.
- Urbanismus, Architektur und Service-Design: Fachverantwortung für das Gesamtprodukt SGC mit seinen (Markt-)Leistungen
- Koordination Migration: Koordination der Migrationsaufgaben mit den betroffenen Kunden und innerhalb des BIT

Projekte

Basierend auf den fünf Handlungsfeldern der SGC werden mehrere Projekte aufgesetzt.

2.7 Systematische Prüfung

Das Programm SGC wurde aufgrund seines Ressourcenbedarfs, seiner strategischen Bedeutung, seiner Komplexität und der mit ihm verbundenen Risiken gemäss Artikel 20 der Verordnung vom 25. November 2020[19] über die digitale Transformation und die Informatik als Schlüsselprojekt der Bundesverwaltung definiert. Es gilt somit ein umfangreicherer Prüfprozess. Die EFK führt im Rahmen des Finanzkontrollgesetzes vom 28. Juni 1967[20] bei den Schlüsselprojekten periodisch systematische Prüfungen durch.

19 SR **172.010.58**
20 SR **614.0**

3 Auswirkungen

3.1 Auswirkungen auf den Bund

Die Umsetzung der SGC ist für den Bund sowohl mit finanziellen als auch mit personellen Auswirkungen verbunden. Im nachfolgenden Kapitel werden diese im Detail ausgeführt.

3.1.1 Finanzielle Auswirkungen

3.1.1.1 Annahmen zur Ausgabenschätzung

Die Ausgabenschätzung erfolgte unter Berücksichtigung der folgenden Annahmen:

- Die Leistungen betreffen im Wesentlichen nur den Bund. Eine Skalierung auf die Kantone ist nicht in der Kostenschätzung enthalten.
- Dauer des SGC-Programms: 9 Jahre
- Die Aufbauarbeiten werden bis 2027 soweit fortgeschritten sein, dass die SGC für die Ablösung der Systemlandschaft Atlantica bereitsteht.
- Für die Cloud-Stufen IIb und III wird von einem «Pay as You Use»-Modell der Hardware ausgegangen.
- Dauer der Migration von bestehenden Systemen in die SGC: max. 4 Jahre
- Es werden keine neuen wesentlichen Vorgaben oder Regulierungen erlassen.
- Die benötigten finanziellen und personellen Ressourcen stehen für die Realisierung des Vorhabens zur Verfügung.
- Keine grundsätzlichen Veränderungen im Marktumfeld.
- Der Aufbau der Stufe IIb ist ab 2029 eingeplant, erfolgt jedoch nur, wenn ein konkreter Bedarf durch einen Kunden besteht.

Der Teuerungsannahme liegen daher die Prognosen zum Landesindex der Konsumentenpreise (LIK) nach den volkswirtschaftlichen Eckwerten für die Finanzplanung und die Mittelfristperspektiven vom Dezember 2023 zugrunde:

in %	2024	2025	2026	2027	2028	2029	2030	2031	2032	**Ø Δ 2024-2028**	**Ø Δ 2029-2032**
Teuerung Konsumentenpreise (LIK)	1.9	1.1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	**1.2**	**1.0**

Tabelle 2: Prognose zum LIK

3.1.1.2 Programmausgaben

In den Jahren 2022 und 2023 fielen Vorarbeiten im Umfang von rund 2,3 Millionen Franken an, wovon 2,2 Millionen Franken Eigenleistungen in Form von personellen Ressourcen darstellten. Die Vorarbeiten beinhalteten die Sicherstellung der Finanzierung, die Vorbereitung der WTO-Beschaffungen, den Aufbau der Fachorganisation sowie Konzeptarbeiten. Diese Ausgaben sind nicht in den Programmausgaben enthalten.

Durch die notwendige Ablösung der Systemlandschaft Atlantica müssen die betroffenen Fachanwendungen von Leistungsbezügern im Rahmen eigener Projekte migriert werden – unabhängig davon, ob die SGC realisiert wird oder nicht. Die Aufwände für diese Migration werden von den Leistungsbezügern getragen und sind somit auch nicht in den Programmausgaben enthalten.

Im 2024 fallen Ausgaben für die Initialisierung des Programmes an. Zwischen 2025 und 2032 fallen Programmausgaben an, die sich aus dem Programm-Management, den Aufbauarbeiten und dem Parallelbetrieb ergeben. Gesamthaft belaufen sich die Ausgaben zwischen 2024 und 2032 auf 319,4 Millionen Franken. Details zu Annahmen, die den Ausgabenschätzungen zugrunde liegen, finden sich im Kapitel 3.1.1.1 «Annahmen zur Ausgabenschätzung».

Von den einmaligen Programmausgaben erbringt das BIT 70,9 Millionen Franken an Eigenleistungen in Form von personellen Ressourcen. Zusätzlich werden Eigenmittel im Umfang von 20,6 Millionen Franken eingesetzt.

Tabelle zeigt, wie sich die Ausgaben auf die zuvor beschriebenen Handlungsfelder verteilen (± 20 % Ungenauigkeit):

in Mio. CHF	**2024**	**2025**	**2026**	**2027**	**2028**	**2029**	**2030**	**2031**	**2032**	**Total**
Aufbau der Hybrid-Multi-Cloud-Infrastruktur	0.5	2.3	15.4	27.1	24.0	20.9	15.1	9.7	5.1	120.1
└*Public Cloud*	*0.1*	*0.2*	*1.1*	*2.0*	*1.7*	*1.0*	*0.6*	*0.3*	*0.1*	*7.1*
└*Public Cloud On-Prem*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*2.4*	*0.9*	*0.7*	*0.5*	*4.5*
└*Private Cloud On-Prem*	*0.4*	*2.1*	*14.3*	*25.1*	*22.3*	*17.5*	*13.6*	*8.7*	*4.5*	*108.5*
Netzwerkinfrastruktur	0.0	4.2	2.9	4.3	3.2	2.7	2.1	1.3	1.5	22.2
└*Bandbreitenerhöhung*	*0.0*	*0.0*	*0.0*	*2.0*	*2.2*	*1.9*	*1.5*	*0.9*	*0.4*	*8.9*
└*Ausbau und Erneuerung*	*0.0*	*4.2*	*2.9*	*2.3*	*1.0*	*0.8*	*0.6*	*0.4*	*1.1*	*13.3*
Cybersicherheit	0.8	3.5	6.4	10.2	9.4	6.9	3.8	1.5	0.0	42.5
└*Identifizieren*	*0.0*	*0.5*	*0.4*	*0.7*	*0.5*	*0.4*	*0.2*	*0.1*	*0.0*	*2.8*
└*Schützen*	*0.5*	*0.4*	*2.7*	*5.6*	*5.9*	*4.4*	*2.6*	*1.4*	*0.0*	*23.5*
└*Detektieren*	*0.3*	*2.0*	*2.4*	*3.6*	*2.8*	*2.0*	*1.0*	*0.0*	*0.0*	*14.1*
└*Reagieren*	*0.0*	*0.6*	*0.8*	*0.2*	*0.1*	*0.1*	*0.0*	*0.0*	*0.0*	*1.8*
└*Erholen*	*0.0*	*0.0*	*0.1*	*0.1*	*0.1*	*0.0*	*0.0*	*0.0*	*0.0*	*0.3*
Betriebs- und kommerzielle Prozesse	0.2	1.3	3.0	6.6	4.8	2.9	1.4	0.9	0.5	21.6
Ausbildung, Beratung und Governance	0.9	2.8	5.5	4.8	4.0	2.5	1.2	0.4	0.1	22.2
Programm-Management	2.9	3.7	7.3	7.6	8.1	6.9	4.0	2.7	2.3	45.5
Programmausgaben (exkl. Reserven)	**5.3**	**17.8**	**40.5**	**60.6**	**53.5**	**42.8**	**27.6**	**16.5**	**9.5**	**274.1**
Reserven	0.0	0.0	6.1	9.1	10.7	8.6	5.6	3.3	1.9	45.3

Programmausgaben (inkl. Reserven)	**5.3**	**17.8**	**46.6**	**69.7**	**64.2**	**51.4**	**33.2**	**19.8**	**11.4**	**319.4**
Davon Eigenleistung in Form von pers. Ressourcen	3.7	7.4	12.0	11.5	10.4	8.3	8.6	5.9	3.1	70.9
Davon Ausgaben im 2024	1.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.6
Verpflichtungskredit	**0.0**	**10.4**	**34.6**	**58.2**	**53.8**	**43.1**	**24.6**	**13.9**	**8.3**	**246.9**

Tabelle 3: Programmausgaben pro Handlungsfeld

Der Mittelbedarf steigt während dem Aufbau der SGC bis 2027 kontinuierlich an und bleibt während der ersten drei Jahre der Migrationsphase auf einem konstanten Niveau, bevor er gegen Ende des Programms deutlich reduziert werden kann. Die Begründung dafür ist, dass sich die Aufwände mit Fortschreiten des Vorhabens zunehmend von Programmausgaben zu Betriebsausgaben verlagern, die keine zusätzliche Finanzierung erfordern und nicht unter den Verpflichtungskredit fallen. Auch nach Abschluss des Vorhabens wird in die Weiterentwicklung der SGC investiert. Die dafür erforderlichen Mittel werden über den Betrieb finanziert.

Nachfolgend werden die Programmausgaben pro Handlungsfeld weiter ausgeführt.

- Aufbau der Hybrid-Multi-Cloud: In diesem Punkt enthalten sind Ausgaben für den Aufbau der Public Cloud (7,1 Mio. CHF), der Public Cloud On-Prem (4,5 Mio. CHF) und der Private Cloud On-Prem (108,5 Mio. CHF). Beim Aufbau der Private Cloud on-Prem stellt der Posten Beschaffung, Installation und Bewirtschaftung mit rund 50 Millionen Franken den grössten Ausgabenblock dar. Weitere grössere Ausgabenblöcke sind die Aufwände für die Erarbeitung eines Service-Portfolios (19,5 Mio. CHF), das Testing der einzelnen Komponenten und Prozesse (11 Mio. CHF) sowie die Migrationsunterstützung (12,9 Mio. CHF).

- Netzwerkinfrastruktur: In diesem Posten enthalten sind der Ausbau der Bandbreiten zum Internet und zu den Anbietern von Cloud-Leistungen (8,9 Mio. CHF) sowie der Ausbau und die Modernisierung der Netzwerke (13,3 Mio. CHF). Zu diesem Posten gehören unter anderem die Verbesserung der Netzwerk- und Ausfallsicherheit.

- Cybersicherheit: Die Ausgaben verteilen sich auf die Bereiche Identifizieren, Schützen, Detektieren, Reagieren und Erholen, die in Kapitel 2.2.3.3 «Zielbild der Cybersicherheit» beschrieben sind. Die grössten Ausgabenblöcke sind die Umsetzung des Zero-Trust-Konzepts (18,4 Mio. CHF), die Sicherstellung der Detektionsfähigkeit (10,4 Mio. CHF) und das Vulnerability-Management (2,4 Mio. CHF).
- Ausbildung, Beratung und Governance: Unter diesen Ausgabenpunkt fallen die Konzipierung und Durchführung von Ausbildungen, der Aufbau des Innovation Centers, der Aufbau des SGC Competence Centers und die Erstellung der SGC-weiten Cloud-Governance.
- Betriebs- und kommerzielle Prozesse: Hier enthalten sind die Aufwände für die Digitalisierung der Prozessketten, die Umsetzung einer zentralen Kundenplattform, die Implementierung eines Cockpits und von Schnittstellen.

- Programm-Management: Unter diesen Punkt fallen personelle Aufwände für die fachliche und technische Gesamtplanung und Gesamtkoordination, die Programmunterstützungen, die Umsetzung von Change-Massnahmen, die Personalführung und das Stakeholder-Management.

Personelle Auswirkungen 2024–2032

Das Vorhaben kann mit den bestehenden Personalressourcen des BIT umgesetzt werden.

Ziel ist, möglichst rasch viele Aufgaben der SGC mit internen BIT-Mitarbeitenden erledigen zu können. Aus diesem Grund sollen bereits in den Jahren 2024–2029 schrittweise bis zu 50 Vollzeitstellen, sogenannte Full Time Equivalences (FTE) von BIT-internen Mitarbeitenden in die SGC-Organisation verschoben werden. Parallel zum Aufbau der SGC müssen die bestehenden Systeme der Systemlandschaft Atlantica weiterbetrieben werden (siehe Tabelle 5 unter «Unterstützung im Betrieb»). Um diese Mehrfachbelastung bewältigen und die durch die Verschiebung der internen Mitarbeitenden entstandenen Lücken schliessen zu können, sind in diesen Jahren zusätzliche externe Mitarbeitende erforderlich.

Die Planung sieht vor, dass nach der Migration der Fachanwendungen und Leistungen in die SGC immer mehr Systeme der Systemlandschaft Atlantica abgeschaltet werden können. Die dabei freiwerdenden internen Personalressourcen sollen Schritt für Schritt in die SGC-Organisation verschoben respektive die freiwerdenden externen FTE abgebaut werden.

in Vollzeitstellen (FTE)	**2024**	**2025**	**2026**	**2027**	**2028**	**2029**	**2030**	**2031**	**2032**
Bedarf intern	17.8	35.0	50.0	50.0	50.0	50.0	70.0	75.0	80.0
Bedarf extern	2.1	10.2	42.6	77.7	77.6	67.4	33.9	23.0	15.2
Unterstützung im Programm	*1.3*	*9.4*	*23.9*	*45.6*	*45.9*	*36.9*	*27.7*	*23.0*	*15.2*
Unterstützung im Betrieb	*0.8*	*0.8*	*18.7*	*32.1*	*31.7*	*30.5*	*6.2*	*0.0*	*0.0*
Gesamtbedarf (exkl. Reserve)	**19.9**	**45.2**	**92.6**	**127.7**	**127.6**	**117.4**	**103.9**	**98.0**	**95.2**
Reserve	0.0	0.0	13.9	19.2	25.5	23.5	20.8	19.6	19.0
Gesamtbedarf (inkl. Reserve)	**19.9**	**45.2**	**106.5**	**146.9**	**153.2**	**140.9**	**124.7**	**117.6**	**114.2**

Tabelle 4: Personalbedarf

Mit der SGC soll ein neues Betriebsmodell etabliert werden, das es dem BIT erlaubt, personelle Ressourcen im Bereich des Infrastruktur- und Plattformbetriebs zu reduzieren. Die dadurch freiwerdenden internen Mitarbeitenden (aktuell geht das BIT von bis zu 100 FTE aus) können dann zum Beispiel genutzt werden, um Bereiche, die kundennahe Leistungen anbieten, zu stärken oder um externe Mitarbeitende durch interne zu ersetzen. So können Kosten gespart und die Abhängigkeit von externen Lieferanten kann reduziert werden.

Reserven

Die ausgewiesenen Reserven sind durch mögliche Mehraufwände begründet, die sich infolge von Anpassungen an den technologischen Fortschritt, aus Beschaffungsrisiken und Verzögerungen im Zeitplan ergeben können.

Die Reserven wurden für den Zeitraum 2026–2027 auf 15 Prozent und, aufgrund der späteren Umsetzung und der damit verbundenen höheren Unsicherheit, für den Zeitraum von 2028–2032 auf 20 Prozent festgelegt.

Die Reserven sollen nicht im Voraus ausfinanziert werden. Sollten gewisse Risiken eintreten, dann werden allfällig zusätzlich benötigte Mittel dem Parlament über den jährlichen Voranschlag beziehungsweise dessen Nachträge beantragt.

in Mio. CHF	2024	2025	2026	2027	2028	2029	2030	2031	2032	Total
Reserven im Programm	0.0	0.0	6.1	9.1	10.7	8.6	5.6	3.3	1.9	45.3

Tabelle 5: Reserven

3.1.1.3 Verpflichtungskredit

Der Verpflichtungskredit für finanzielle Verpflichtungen gegenüber Dritten beläuft sich auf 246,9 Millionen Franken. Er wird in zwei Tranchen freigegeben: Die Freigabe der ersten Tranche von 103,2 Millionen Franken erfolgt durch die Bundesversammlung mit dem Bundesbeschluss. Die zweite Tranche von 143,7 Millionen Franken wird durch den Bundesrat freigegeben, sobald die folgenden Voraussetzungen erfüllt sind:

- Die SGC steht per 2027 zur Ablösung der Systemlandschaft Atlantica bereit.
- Bestätigung der erfüllten Sicherheits- und Compliance-Anforderungen durch das unabhängige Qualitäts- und Risikomanagement und Freigabe für den Produktivbetrieb durch den/die Programmauftraggeber/-in.

Der Bundesrat kann unter den freigegebenen Tranchen des Verpflichtungskredits Verschiebungen vornehmen, sodass gegebenenfalls Verpflichtungen für erwartete Mehrausgaben in einer Tranche durch die andere aufgefangen werden können.

Die Mittelverwendung steht unter dem Vorbehalt der jährlichen Kreditanträge und -beschlüsse der zuständigen Organe des Bundes zu Voranschlag und Finanzplan.

in Mio. CHF	2025	2026	2027	2028	2029	2030	2031	2032	Total
Verpflichtungskredit Tranche 1	10.4	34.6	58.2	0.0	0.0	0.0	0.0	0.0	103.2
Verpflichtungskredit Tranche 2	0.0	0.0	0.0	53.8	43.1	24.6	13.9	8.3	143.7
Total Verpflichtungskredit	**10.4**	**34.6**	**58.2**	**53.8**	**43.1**	**24.6**	**13.9**	**8.3**	**246.9**

Tabelle 6: Verpflichtungskredit

3.1.1.4 Betriebsausgaben nach dem Programm

Die jährlichen Betriebsausgaben des BIT nach Abschluss des Programms (ab 2033) belaufen sich gemäss aktueller Schätzung auf 64,1 Millionen Franken. Durch die Einsparungen können die Betriebsausgaben des BIT reduziert werden (siehe hierzu Kapitel 3.1.1.5 «Einsparungen während und nach dem Programm»).

3.1.1.5 Einsparungen während und nach dem Programm

Insgesamt können während der Programmdauer etwa 241,2 Millionen Franken an internen Kosten reduziert und teils für die SGC eingesetzt werden. Abzüglich der geschätzten Betriebsausgaben von 179,5 Millionen Franken ergibt sich somit eine erwartete Einsparung von 61,7 Millionen Franken während der Programmdauer.

Die jährlichen Betriebsausgaben des BIT nach Abschluss des Programms (ab 2033) belaufen sich gemäss aktueller Schätzung auf 64,1 Millionen Franken. Da die interne Kostenreduktion zu diesem Zeitpunkt jährlich 88 Millionen Franken betragen wird, können voraussichtlich 23,9 Millionen Franken pro Jahr im Betrieb beim BIT eingespart werden.

Die Ausbauten in den Bereichen Cybersicherheit, Netzwerkinfrastruktur sowie im Bereich Betriebs- und kommerzielle Prozesse führen zu zusätzlichen wiederkehrenden Betriebskosten. Da diese Arbeiten auch ohne die SGC durchgeführt werden müssen, würden die Betriebskosten in jedem Fall steigen. Mit der SGC können im Betrieb dank der Ablösung der Systemlandschaft Atlantica und durch die Internalisierung von Ressourcen jedoch trotzdem Einsparungen erzielt werden. Dadurch können zusätzliche Betriebskosten vermieden beziehungsweise die zukünftigen Betriebskosten reduziert werden.

Während und nach dem Programm ergeben sich so voraussichtlich die folgenden Einsparungen:

in Mio. CHF	**Gesamttotal während Programm 2024–2032**	**Jährlich nach Programmabschluss (ab 2033)**
geschätzte Betriebsausgaben	179.5	64.1
interne Kostenreduktion BIT	-241.2	-88.0
Erwartete Einsparungen	**-61.7**	**-23.9**

Tabelle 7: Einsparungen

Die Umsetzung des Vorhabens führt zu folgenden internen Kostenreduktionen im BIT:

- Ablösung Systemlandschaft Atlantica: Per Ende 2027 soll die SGC zur Ablösung der Systemlandschaft Atlantica bereitstehen. Mit der Migration auf die SGC fallen die Kosten der Systemlandschaft Atlantica weg. Es wird angenommen, dass 2028–2030 jeweils ein Viertel der Fachanwendungen in die SGC migriert werden können. 2031 wird das letzte Viertel migriert. Im Anschluss kann die Systemlandschaft Atlantica zurückgebaut werden.

- Interne Personalressourcen: Das interne Personal für die SGC soll von anderen Bereichen im BIT ersatzlos in die SGC verschoben werden, das heisst, es werden keine zusätzlichen internen Personalressourcen für die SGC benötigt.

- Internalisierung Ressourcen: Durch die Prozessautomatisierung und Standardisierung des Leistungskataloges im Betrieb «Plattformen und Infrastruktur» können hier bis zu 100 interne Stellen reduziert und stattdessen für die interne Entwicklung eingesetzt werden. Durch diese Verschiebung können nach Programmabschluss im Bereich Entwicklung 100 externe Stellen abgebaut werden (siehe Kapitel 3.1.1.2 «Programmausgaben 2024 bis 2032»).

Die Kostenreduktionen von 241,2 beziehungsweise 88 Millionen Franken sind folgendermassen verteilt:

in %	**Gesamttotal während Programm 2024-2032**	**Jährlich nach Programmabschluss (ab 2033)**
Ablösung Systemlandschaft Atlantica	55	46
Interne Personalressourcen	16	16
Internalisierung Ressourcen	29	38

Tabelle 8: Interne Kostenreduktion BIT

3.1.1.6 Wirtschaftlichkeit

Die Wirtschaftlichkeit der SGC wird folgendermassen sichergestellt:

- *Ausrichtung auf die Geschäftsanforderungen des Bundes:* Im Rahmen der Vorarbeiten wurde mit der Bedarfserhebung bei den IKT-Leistungserbringern der Bundesverwaltung sowie den Parlamentsdiensten und der Bedürfnisanalyse bei den Leistungsbezügern der Grundstein gelegt, um die SGC konsequent auf die Geschäftsanforderungen auszurichten und die benötigten Leistungen zur Bewältigung der anstehenden Digitalisierungsherausforderungen zur Verfügung zu stellen.

- *Umsichtige Konzeption und Kostenschätzung:* Zur seriösen Einschätzung der Wirtschaftlichkeit wurde einerseits eine umfangreiche Analyse der Kostenstruktur der Systemlandschaft Atlantica durchgeführt, andererseits verifizierte das BIT seine Strategie im Rahmen von Erfahrungsaustauschen mit Regierungen anderer Länder. Zudem wurde durch Gespräche mit Public-Cloud-Anbietern sichergestellt, dass die Pläne der SGC zukunftsträchtig sind. Die Stringenz der Kostenschätzung wurde durch einen unabhängigen Experten geprüft.
- *Kostenvorteile im Vergleich zur Ist-Situation:* Die Berechnungen zeigen, dass die Kosten der Weiterführung der Ist-Situation die kalkulierten Gesamtausgaben der SGC um über 150 Millionen Franken übersteigen würden (vgl. Kapitel 3.1.2 «Konsequenzen bei Nichtrealisierung»).

- *Übergreifende Governance:* Durch eine übergreifende Cloud-Governance wird sichergestellt, möglichst einfach von einem Cloudanbieter zum anderen und von einer Cloudstufe in eine andere wechseln zu können.
- *Koordination des Bezugs von Cloud-Leistungen:* Das Competence Center berät die interessierten Verwaltungseinheiten bei der Wahl der richtigen Cloud-Stufe und hilft, deren Bezug zu koordinieren. Es leistet so einen wichtigen Beitrag zur wirtschaftlichen Nutzung der drei Stufen der SGC.
- *Nutzung von Synergien dank dem Modell «IT Service Provider for IT Service Provider»:* Die SGC wird so konzipiert, dass sie von allen IKT-Leistungserbringern des Bundes genutzt werden kann und so Synergien für das Massengeschäft der Bundesverwaltung im Cloud-Bereich genutzt werden können.
- *Bereitstellung von vorgefertigten Leistungen:* Im Rahmen der SGC werden Leistungsbezügern vorgefertigte und bereits mit den Standard-Diensten des Bundes kompatible Dienste bereitgestellt, auf die sie bei der Konzeption und Umsetzung ihrer Lösungen zurückgreifen können.
- *Hohe Skalierbarkeit:* Die SGC selber wie auch die zur Verfügung gestellten Leistungen sind hoch skalierbar. Auf veränderte Kapazitätsanforderungen kann damit rasch und flexibel – zu grossen Teilen automatisiert – reagiert werden. Dank des vorgesehenen «Pay as You Use»-Modells fallen nur Kosten für die effektiv bezogenen Leistungen an. Schwankende Einnahmen aufgrund von variierenden Bezugsvolumen können dadurch grösstenteils kompensiert werden.
- *Industrialisiertes Betriebsmodell:* Mit der SGC soll ein neues industrialisiertes Betriebsmodell eingeführt werden. Durch die konsequente Automatisierung von Prozessen und die Standardisierung des Leistungskatalogs können langfristig Betriebskosten eingespart werden.
- *Kostenkontrolle und -transparenz:* Durch den Einsatz von Tools und Dashboards, zum Beispiel in Form eines 360-Grad-Cockpits, können Cloud-Kosten wirkungsvoll überwacht werden. Darüber hinaus können unnötige Kosten einfach identifiziert und eliminiert werden.
- *Beratung und Ausbildung:* Beratung und Ausbildung befähigt die Leistungsbezüger und IKT-Leistungserbringer, Cloud-Infrastrukturen der SGC wirtschaftlich zu nutzen.
- *Schaffung der Voraussetzung zur Ablösung von Legacy-Anwendungen:* Mit der SGC wird die Grundlage für die Modernisierung oder Ablösung veralteter Anwendungen gelegt, deren Betrieb meist mit erheblichen Aufwänden verbunden ist. Entsprechende Vorhaben müssen von den Leistungsbezügern initialisiert werden.
- *Jährliche Mittelfreigabe*: Es ist vorgesehen, dass die Mittelfreigabe zugunsten der SGC auf der Grundlage einer Planung des BIT und einer jährlich aktualisierten Bedarfserhebung durch die Auftraggeberin jedes Jahr geneh-

migt wird. So werden skalierbare Teile der SGC-Infrastruktur nur bei nachgewiesenem Bedarf gebaut und eine im Hinblick auf die Kosten, den Nutzen und die Risiken optimierte Verwendung der Mittel wird sichergestellt.

3.1.2 Konsequenzen bei Nichtrealisierung

Um die Kosten einer Weiterführung der Ist-Situation aufzuzeigen, wurden die Kosten der aktuellen Systemlandschaft Atlantica und des CSB-BIT auf die Jahre 2024–2032 hochgerechnet, um diese den Kosten der Realisierung der SGC gegenüberstellen zu können. In der Hochrechnung wurde ein eher konservativ geschätztes jährliches Wachstum von fünf Prozent eingerechnet. Zudem wurde eine Teuerung gemäss dem LIK (siehe Kapitel 3.1.1.1 «Annahmen zur Ausgabenschätzung») einkalkuliert. Um ein ganzheitliches Bild der Kosten darzustellen, wurden auch die notwendigen Investitionen der übrigen Handlungsfelder der SGC (wie z. B. Cybersicherheit oder Ausbau der Netzwerkinfrastruktur) berücksichtigt, die bei einer Nicht-Realisierung des Vorhabens SGC trotzdem anfallen würden. Analog zur SGC Kostenschätzung in Kapitel 3.1.1.2 «Programmausgaben 2024–2032» wurde auch hier ein Risikozuschlag von 15 Prozent für den Zeitraum 2026–2027 und von 20 Prozent für den Zeitraum 2028–2032 eingerechnet. Der Risikozuschlag auf die Systemlandschaft Atlantica und den CSB-BIT dient primär dazu, allfällige zusätzliche Investitionskosten decken zu können, die bei einer Weiterführung der Lösung anfallen würden. Bei den restlichen Positionen dient der Risikozuschlag dazu, mögliche Mehraufwände infolge technologischen Fortschritts und der Beschaffungsrisiken abfangen zu können.

Die Berechnungen zeigen, dass die Ausgaben für die Weiterführung der Ist-Situation von 688,1 Millionen Franken die kalkulierten Gesamtausgaben (Programm- und Betriebsausgaben) der SGC um über 150 Millionen Franken bis Ende 2032 übersteigen würden. Darüber hinaus würden auch die im Kapitel 3.1.1.5 «Einsparungen während und nach dem Programm» ausgewiesenen Sparpotenziale bei einer Nichtrealisierung der SGC nicht oder nur teilweise ausgeschöpft.

3.1.3 Migrationskosten

Im Rahmen des Vorhabens werden alle bisher in der Systemlandschaft Atlantica betriebenen Fachanwendungen auf die passende Stufe der SGC migriert. Es ist in den meisten Fällen grundsätzlich möglich, diese Migration durch eine Verschiebung von bestehenden Fachanwendungen aus der heutigen Cloud-Infrastruktur auf die neue abzuwickeln. In diesem Fall würden somit keine architektonischen Anpassungen an den Anwendungen vorgenommen und alle notwendigen Dienste würden nach Abschluss der Migration unverändert zur Verfügung stehen. Die vorliegende Migrationskostenschätzung wurde auf der Grundlage dieses Szenarios vorgenommen. Den Leistungsbezügern wird jedoch nahegelegt, die anstehende Migration mit den im Migrationszeitraum anstehenden Lifecycle-Anpassungen an ihren Fachanwendungen zu verbinden, das heisst, sie gleichzeitig auf den neusten technischen Stand zu bringen. Damit können die Aufwände für die technische Migration reduziert werden.

Die Migrationskosten einer Fachanwendung hängen von deren Komplexität, der Anzahl Betriebsumgebungen und weiteren Faktoren ab, die sich in den jährlichen Betriebskosten widerspiegeln, die das BIT den entsprechenden Leistungsbezügern berechnet.

Auf der Grundlage der Gesamtbetriebskostenrechnung des BIT vom September 2023 und Erfahrungen aus schon durchgeführten Lifecycle-Vorhaben, die ebenfalls eine Plattformmigration beinhalteten, hat das BIT einen Migrationskostenfaktor kalkuliert. Dieser beläuft sich auf 35 Prozent der jährlichen Betriebskosten. Systeme und Anwendungen, die aktuell noch nicht in einer der Cloud-Plattformen des BIT betrieben werden (sogenannte Legacy-Systeme), sind in der Schätzung der Migrationskosten nicht enthalten. Es liegt in der Verantwortung der Leistungsbezüger, die Modernisierung dieser Lösungen einzuplanen und zu beauftragen. Die Ablösung der Legacy-Systeme birgt weiteres Sparpotenzial. Das Thema wird daher im Digitalisierungsrat Bund parallel zur SGC prioritär angegangen.

Gesamthaft entstehen demnach Migrationskosten in der Höhe von 74 Millionen Franken. Es wird von einer Schätzgenauigkeit von ±20 Prozent ausgegangen. Diese schwankende Kostenschätzung ist auf den langen Planungshorizont zurückzuführen: Zwischen dem Zeitpunkt der Schätzung (Ende 2023) und dem Zeitpunkt der Migration (ab 2027) werden sich sowohl die Technologielandschaft auf dem Markt als auch die Anwendungslandschaft der Leistungsbezüger weiterentwickeln. Aufgrund der ausstehenden Beschaffung ist zudem auch die Zielplattform der Migration unbekannt. Eine genaue Schätzung der Migrationskosten ist daher zum jetzigen Zeitpunkt nicht möglich. Es besteht daher das Risiko, dass die effektiven Aufwände für die Migration höher ausfallen als geschätzt.

Im Rahmen der Umsetzung des Vorhabens ist vorgesehen, die Migrationskosten pro Fachanwendung im Detail zu analysieren und die jeweiligen Leistungsbezüger rechtzeitig darüber zu informieren.

3.1.4 Zweitmeinungen

Die Konzeption der SGC basiert auf umfangreichen Abklärungen: Nebst ausführlichen Gesprächen mit nationalen und internationalen Cloud-Anbietern zur Sondierung ihres Angebots fanden auch Erfahrungsaustausche mit anderen Ländern (Deutschland, Italien, Singapur, Österreich, Kroatien, Dänemark, Niederlande, Grossbritannien) statt, um in Bezug auf mögliche Chancen, Probleme und Risiken von deren Erkenntnissen profitieren zu können.

Das BIT hat zudem mehrere Zweitmeinungen eingeholt:

- Bezüglich der strategischen Ziele und des Umsetzungsplans der SGC wurde bestätigt, dass die Strategie den Bestrebungen vieler anderer Regierungsorganisationen entspricht und dass eine gute Balance zwischen Aufwand und Ertrag gefunden und die Lösung skalierbar sowie wirtschaftlich sinnvoll konzipiert wurde.
- Bezüglich der geschätzten Programmausgaben und Migrationskosten wurde bestätigt, dass die Schätzung der Programmausgaben schlüssig und

nachvollziehbar und die Schätzung der Migrationsaufwände im Rahmen der verfügbaren Daten fundiert und adäquat ist.

3.2 Auswirkungen auf Kantone und Gemeinden

Auch Kantone, Städte und Gemeinden möchten für die Umsetzung ihrer Digitalisierungsprojekte verstärkt auf Cloud-Dienste setzen. Viele haben jedoch nicht die Mittel, um eigene Cloud-Infrastrukturen aufbauen und rentabel betreiben zu können. Aus diesem Grund haben die sieben Mitgliedskantone der Conférence latine des directrices et directeurs de numérique sowohl gegenüber dem BIT als auch in ihrem Brief vom 2. Mai 2023 an die EFD-Vorsteherin ihr grosses Interesse an der Mitnutzung der SGC bekundet.

Eine erfolgreiche Digitalisierung der öffentlichen Verwaltung erfordert eine verstärkte Vernetzung der verschiedenen Verwaltungseinheiten – über alle föderalen Ebenen hinweg. Der Bundesrat begrüsst daher das Interesse der Kantone und möchte entsprechend auch ihnen die Möglichkeit geben, die SGC zu nutzen. Zwar wird die SGC in erster Linie für die Bedürfnisse des Bundes konzipiert. Technisch wird sie jedoch so aufgebaut, dass sie in Zukunft bei Interesse auch von Kantonen, Städten und Gemeinden genutzt werden könnte.

Mit Blick auf die Skalierbarkeit der SGC wird aktuell geklärt, gestützt auf welchen rechtlichen Vorgaben die SGC auch für Kantone, Städte und Gemeinden Leistungen erbringen könnte und ob hierfür Rechtsetzungsbedarf besteht. Zu diesen Arbeiten liegen noch keine Ergebnisse vor.

Für eine allfällige Mitnutzung der SGC werden Kantone, Städte und Gemeinden bezahlen müssen. Aufgebaut wird die SGC jedoch in der Bundesverwaltung und primär für den Bund. Daher ist nicht vorgesehen, dass sich Kantone, Städte und Gemeinden an den Aufbaukosten beteiligen. Sie waren darum auch nicht Teil der im Dokument erwähnten Bedarfserhebung und Bedürfnisanalyse. Dennoch wird im Umgang mit den Kantonen weiterhin auf eine offene Kommunikation gesetzt werden. Bereits heute wird im Rahmen des strategischen Schwerpunkts «Cloud-enabled-Government ermöglichen» der Strategie Digitale Verwaltung Schweiz 2024–2027 eng mit der DVS zusammengearbeitet.

4 Rechtliche Aspekte

4.1 Verfassungs- und Gesetzmässigkeit

Die Vorlage stützt sich auf die allgemeine Befugnis des Bundes, die notwendigen Massnahmen zur Erfüllung seiner Aufgaben zu treffen. Die Zuständigkeit der Bundesversammlung für den vorliegenden Kreditbeschluss ergibt sich aus Artikel 167 der Bundesverfassung (BV)[21].

4.2 Erlassform

Nach den Artikeln 163 Absatz 2 BV und 25 Absatz 2 des Parlamentsgesetzes vom 13. Dezember 2002[22] ist für den vorliegenden Fall ein Erlass in der Form des einfachen, also nicht dem Referendum unterstellten Bundesbeschlusses vorgesehen.

4.3 Unterstellung unter die Ausgabenbremse

Artikel 1 des Bundesbeschlusses untersteht der Ausgabenbremse nach Artikel 159 Absatz 3 Buchstabe b BV, da dieser eine einmalige Ausgabe von mehr als 20 Millionen Franken nach sich zieht. Der Verpflichtungskredit von insgesamt 246,9 Millionen ist demnach von den eidgenössischen Räten mit der Zustimmung der Mehrheit der Mitglieder beider Kammern zu verabschieden.

21 SR **101**
22 SR **172.10**

5 Abkürzungsverzeichnis

Abkürzung	Bedeutung
BACS	Bundesamt für Cybersicherheit
BIT	Bundesamt für Informatik und Telekommunikation
BK	Bundeskanzlei
BV	Bundesverfassung
CC SGC	Competence Center SGC
CoP	Community of Practice
CSB	Cloud Service Broker
DSG	Datenschutzgesetz
DTI	Digitale Transformation und IKT-Lenkung
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EJPD	Eidgenössisches Justiz- und Polizeidepartement
IaaS	Infrastructure as a Service
IKT	Informations- und Kommunikationstechnik
ISAE	International Standard on Assurance Engagements
ISG	Informationssicherheitsgesetz
ISMS	Information Security Management System
IT	Informationstechnologie
LB	Leistungsbezüger
LE	Leistungserbringer
NIST	National Institute of Standards and Technology
PaaS	Plattform as a Service
ParlG	Parlamentsgesetz
SaaS	Software as a Service

SAP	Systemanalyse Programmentwicklung (Softwareunternehmen)
SGC	Swiss Government Cloud
SR	Systematische Sammlung des Bundesrechts

6 Glossar

Begriff	Bedeutung
Cloud Service Broker	Ein Cloud Service Broker (CSB) schafft alle erforderlichen Voraussetzungen, damit die Public-Cloud-Dienste verwaltungsintern abgerufen und gemäss den definierten Vorgaben in der IKT-Landschaft der Bundesverwaltung integriert und betrieben werden können. Hierfür stellt der CSB Hilfsmittel (Werkzeuge, Dienstleistungen, Expertise, Kontroll-Mechanismen) für die Nutzung von (Public-) Cloud-Diensten gemäss definierten Prinzipen bereit.
Digitale Souveränität	Unter digitaler Souveränität sind unter anderem folgende Aspekte zu verstehen: • Daten- und Informationssouveränität: Kontrolle der Dateninhaber über ihre Daten (sowohl personenbezogene wie auch nicht-personenbezogene Daten) sowie deren Erhebung, Speicherung, Verarbeitung und Weitergabe. • Operative bzw. betriebliche Autonomie: Darunter ist die Dauer, während derer das BIT mit eigenem Personal den Betrieb von bereits laufenden Systemen und Anwendungen aufrechterhalten kann, zu verstehen, ohne dass auf die Dienste von bundesexternen Partnern zurückgegriffen werden muss.
Fully Managed Service	Fully Managed Services beinhalten die Bereitstellung, Aktualisierung, initiale Konfiguration, den Support- und die Überwachung der entsprechenden Leistung.
Hybrid-Multi-Cloud-Ansatz	Bei einem Hybrid-Cloud-Ansatz werden sowohl Public- als auch Private-Cloud-Dienste genutzt und miteinander kombiniert. «Multi» bedeutet, dass Cloud-Dienste von mehreren Public-Cloud-Anbietern zur Verfügung stehen.
Infrastructure as a Service	Infrastructure as a Service (IaaS) ist ein Modell des Cloud Computing, bei dem Unternehmen IT-Infrastrukturressourcen wie Rechenleistung, Speicherplatz und Netzwerkressourcen von einem Cloud-Anbieter mieten, anstatt physische Hardware und Infrastruktur vor Ort zu betreiben.
On-Prem	On-Prem bedeutet, dass die Lösung in den Rechenzentren der Bundesverwaltung betrieben wird.

Pay as You Use	Kunden bezahlen nur für die Leistungen oder Ressourcen, die sie effektiv bezogen resp. genutzt haben. Im Gegensatz zu einem Kauf fallen bei diesem Modell keine separaten Lifecycle-Kosten an, da der Anbieter der Leistungen oder Ressourcen für den Unterhalt und die Erneuerung des Angebots verantwortlich ist und diese Aufwände in den Preisen enthalten sind.
Platform as a Service	Platform as a Service (PaaS) ist ein Modell des Cloud Computing, bei dem Unternehmen eine Plattform von einem Cloud-Anbieter mieten, um Anwendungen zu entwickeln, zu testen und bereitzustellen. Im Gegensatz zu Infrastructure as a Service (IaaS), wo nur die Infrastruktur bereitgestellt wird, stellt PaaS auch Services bereit, die für die Entwicklung und den Betrieb von Anwendungen benötigt werden. Dazu gehören zum Beispiel Datenbanken oder Container-Plattformen.
Private Cloud	Die Private Cloud ist eine eigene Cloud-Umgebung, die in einem abgeschlossenen, internen Netzwerk aufgebaut und betrieben wird – im Falle der SGC in den Rechenzentren der Bundesverwaltung. Die Daten werden damit in den eigenen Rechenzentren gehalten.
Public Cloud	Der Begriff «Public Cloud» bezeichnet eine Cloud-Umgebung, die von einem externen Cloud-Anbieter bereitgestellt wird. Das bedeutet nicht, dass die Daten öffentlich sind, sondern, dass sie auf der Infrastruktur eines externen Cloud-Anbieters gehalten werden.
Software as a Service	Software as a Service (SaaS) ist ein Modell des Cloud Computing, bei dem Software-Anwendungen in der Cloud bereitgestellt und von einem Cloud-Anbieter betrieben werden. Anstatt die Software auf lokalen Computern oder Servern zu installieren und zu warten, können Benutzerinnen und Benutzer über das Internet auf die Anwendung zugreifen und diese verwenden.
Swiss Government Cloud	Die SGC ist eine auf die Anforderungen und Bedürfnisse des Bundes ausgerichtete Cloud-Infrastruktur, über welche künftig sowohl Public- als auch Private-Cloud-Leistungen bezogen werden können.
Systemlandschaft Atlantica	Unter der Systemlandschaft Atlantica versteht das BIT alle von ihm betriebenen On-Prem-Cloud-Plattformen im Bereich IaaS und PaaS. Diese sind Stand 2023 die VM-basierte IaaS-Plattform, die durch die WTO 1434 (Cumulus) beschafft wurde, die durch das BIT selbst entwickelte VM-basierte IaaS-Plattform Serverbazar und die durch

	das AMBOSS-Programm aufgebaute Container-basierte PaaS-Plattform Red Hat OpenShift. Des Weiteren beinhaltet der Begriff alle zu den genannten Plattformen durch das BIT angebotenen (Markt-)Leistungen.