

EIDGENÖSSISCHE FINANZKONTROLLE  
CONTRÔLE FÉDÉRAL DES FINANCES  
CONTROLLO FEDERALE DELLE FINANZE  
SWISS FEDERAL AUDIT OFFICE



# Prüfung des DTI-Schlüsselprojektes RZPlus – Ausfallsichere Rechenleistung

Bundesamt für Meteorologie und Klimatologie  
(MeteoSchweiz)

Bestelladresse	Eidgenössische Finanzkontrolle (EFK)
Adresse de commande	Monbijoustrasse 45
Indirizzo di ordinazione	3003 Bern
Ordering address	Schweiz
Bestellnummer	23623.002
Numéro de commande	
Numero di ordinazione	
Ordering number	
Zusätzliche Informationen	<a href="http://www.efk.admin.ch">www.efk.admin.ch</a>
Complément d'informations	<a href="mailto:info@efk.admin.ch">info@efk.admin.ch</a>
Additional information	+ 41 58 463 11 11
Abdruck	Gestattet (mit Quellenvermerk)
Reproduction	Autorisée (merci de mentionner la source)
Riproduzione	Autorizzata (indicare la fonte)
Reprint	Authorized (please mention source)

# Inhaltsverzeichnis

Das Wesentliche in Kürze.....	5
L'essentiel en bref .....	7
L'essenziale in breve .....	10
Key facts.....	13
<b>1 Auftrag und Vorgehen .....</b>	<b>16</b>
1.1 Ausgangslage .....	16
1.2 Prüfungsziel und -fragen.....	16
1.3 Prüfungsumfang und -grundsätze .....	16
1.4 Unterlagen und Auskunftserteilung .....	17
1.5 Schlussbesprechung .....	17
<b>2 Aufbau einer georedundanten, ausfallsicheren Rechenleistung .....</b>	<b>18</b>
2.1 RZPlus reduziert das Risiko signifikanter technischer Betriebsunterbrüche bei MeteoSchweiz .....	18
2.2 Ausfallsicherheit ist mehr als Georedundanz.....	19
2.3 Die Migration in die Cloud darf erst nach Abschluss der Risikoanalyse und der Umsetzung der Massnahmen erfolgen .....	21
<b>3 Verfügbarkeits-, Integritäts- und Vertraulichkeitsanforderungen an RZPlus .....</b>	<b>25</b>
3.1 Leistungsvereinbarungen mit Kunden werden systematisch vereinbart und überprüft .....	25
3.2 Die durchgängige Ableitung von Informationssicherheitskriterien ist erst im Aufbau	27
<b>4 Programm- und Projektsteuerung.....</b>	<b>30</b>
4.1 Das Programm wird gut gesteuert und ist auf Kurs, ungeachtet der verspäteten Projekte.....	30
4.2 RZPlus und der unternehmensweite Kulturwandel sind aufeinander angewiesen ....	32
4.3 Die Budgeteinhaltung ist unsicher.....	33
4.4 Der Risikomanagementprozess und das Qualitäts- und Risikomanager-Reporting werden noch verfeinert.....	34
<b>5 Statusübersicht des Bereichs Digitale Transformation und IKT-Lenkung.....</b>	<b>36</b>
<b>Anhang 1: Rechtsgrundlagen.....</b>	<b>38</b>
<b>Anhang 2: Abkürzungen.....</b>	<b>39</b>

**Anhang 3: Glossar.....40**

# Prüfung des DTI-Schlüsselprojektes RZPlus – Ausfallsichere Rechenleistung Bundesamt für Meteorologie und Klimatologie (MeteoSchweiz)

## Das Wesentliche in Kürze

---

MeteoSchweiz ist eine kritische Infrastruktur und erbringt für die Schweiz unverzichtbare Dienstleistungen wie etwa Unwetterwarnungen, Ausbreitungsanalysen von Schadstoffen usw. Wenn diese ausfallen oder nur reduziert erbracht werden, können Menschenleben gefährdet sein und grosse wirtschaftliche Schäden eintreten. Mit dem Programm RZPlus erhöht MeteoSchweiz die Ausfallsicherheit ihrer Dienstleistungen. Hierfür baut sie die geschäftskritischen Fachanwendungen und dazu benötigten IKT-Mittel neu georedundant<sup>1</sup> auf und passt die IKT-Betriebsprozesse an. Basierend auf Public Cloud Services und geeigneten Architekturen werden die Fachanwendungen nach Möglichkeit voneinander entkoppelt und die Ausfallsicherheit damit weiter erhöht. RZPlus hat ab dem Projektauftrag eine Laufzeit von 2022 bis 2028 und kostet rund 39 Millionen Franken. Die Eidgenössische Finanzkontrolle (EFK) prüfte das Programm zum ersten Mal und legt den Fokus auf die Programmsteuerung und das Risikomanagement.

Die Prüfung zeigte, dass das Programm von einem motivierten und professionellen Team zielgerichtet durchgeführt wird. Es kommt trotz erheblicher extern verursachter Verzögerungen gut voran. Mit dem Cloud-Einsatz verfolgt MeteoSchweiz einen zweckmässigen Ansatz zur Erreichung der Programmziele. Problematisch ist, dass die systematische und vollständige Erarbeitung von risikomindernden Massnahmen sowie die Akzeptanz der Risiken noch ausstehen.

### **RZPlus: ein zentrales Vorhaben gegen schwere Betriebsunterbrüche bei MeteoSchweiz**

Bisher ist die Informatik von MeteoSchweiz zentral in einem Rechenzentrum am Flughafen Zürich untergebracht. Mit RZPlus wird das Risiko signifikanter technischer Betriebsunterbrüche bei MeteoSchweiz reduziert und eine Empfehlung der EFK von 2014 umgesetzt.<sup>2</sup> Die Wahl einer Public Cloud zur Verbesserung der Ausfallsicherheit sowie der Skalierbarkeit basiert auf der Digitalen Strategie MeteoSchweiz von 2022. Die Datenkommunikation wird weiterhin vom Bundesamt für Informatik betrieben, aber neu georedundant in zwei Bundesrechenzentren.

Das Swiss National Supercomputing Centre (CSCS) wird von der Eidgenössischen Technischen Hochschule (ETH) betrieben und ist als Institution nicht Teil von RZPlus, die darauf installierten kritischen Anwendungen (Wettermodelle) sind es hingegen schon. Erfreulicherweise hat die ETH im Sommer 2023 entschieden, den CSCS-Hochleistungsrechner auch georedundant aufzubauen und zu betreiben.

---

<sup>1</sup> Als Georedundanz bezeichnet man den Einsatz von zwei Rechenzentren an voneinander ausreichend entfernten Standorten, die denselben Datenstand besitzen und jederzeit die Funktion des jeweils anderen übernehmen können.

<sup>2</sup> «Prüfung der IT-Governance MeteoSchweiz» vom 1. Dezember 2014 (PA 14419).

## **Gesamtrisiken Cloud müssen rasch konkretisiert und formell akzeptiert werden**

Mit dem ersten Abruf von Services aus der WTO-Beschaffung Public Cloud des Bereichs Digitale Transformation und Informatik (DTI) betritt MeteoSchweiz Neuland.<sup>3</sup> Die Herausforderung besteht darin, dass RZPlus hochspezialisiertes Wissen benötigt, um eine Cloud-Plattform sicher aufzubauen. Nicht hilfreich ist, dass die Bundesverwaltung damit wenig Erfahrung hat und Hilfsmittel, Informationen sowie Vorgaben erst im Entstehen sind. MeteoSchweiz muss entsprechende Lücken füllen und Personal mit Fachwissen beschaffen.

MeteoSchweiz hat bereits in den Vorarbeiten zu RZPlus sowie der Programminitialisierung Risiken identifiziert, die untrennbar mit der Nutzung von Cloud-Dienstleistungen verbunden sind: Einfluss von Drittstaaten, Digitale Souveränität, Verfügbarkeit, Unterlieferanten-Management etc. Was noch fehlt, ist die vollständige Definition risikomindernder Massnahmen und die Akzeptanz der verbleibenden Restrisiken durch die Geschäftsleitung. Dies ist dringend notwendig, um den gewählten Architekturansatz zu bestätigen und anschliessend Fachanwendungen produktiv in der Cloud zu betreiben. MeteoSchweiz sollte auch abklären, ob sie als zivile kritische Infrastruktur in die Public Cloud migrieren sollte.

## **Interne Herausforderungen hemmen das Programm**

Die Bestimmung der Informationssicherheitsanforderungen für die geschäftskritischen Fachanwendungen ist komplexer und aufwendiger als erwartet. Diese von RZPlus zwingend benötigten Informationen und Vorgaben für eine Migration in die Cloud fehlen mehrheitlich. Das Programm kann diese Lücke nicht selber schliessen. Dazu müssen die Kunden-, Dienstleistungs- oder Produktverantwortlichen sowie die Business-Continuity- und IT-Service-Management-Verantwortlichen ein gemeinsames Verständnis über die Ableitung der Anforderungen an die Fachanwendungen und IKT-Mittel erarbeiten. Der dazu nötige Prozess muss zentral bei MeteoSchweiz auf Ebene des Top-Management geführt werden.

RZPlus verändert die Organisation, Aufgabenteilung, Prozesse bis hin zu neuen Berufsbildern. Dies ist nicht nur auf die Informatik beschränkt, sondern betrifft das ganze Amt. Für den Programmerfolg ist ein zentral verantworteter Kulturwandel folglich entscheidend.

## **Programmziele trotz externer Verzögerungen bisher nicht gefährdet**

Die Projekte «Aufbau & Inbetriebnahme RZ Campus und Cloud» sowie «IT-Governance & Migration Fachanwendungen» sind gegenüber der Projektplanung von 2021 um zwölf Monate und mehr verzögert. Die Ursachen dafür lagen ausserhalb des Einflussbereiches von RZPlus bzw. von MeteoSchweiz. Durch Neuplanungen und verstärkten Ressourceneinsatz konnte das Programm die Verzögerungen kompensieren. Dennoch führt die immer kürzere Zeit für gleichbleibend viele und komplexe Aufgaben zu einem erhöhten Gesamtrisiko. Aufgrund der Verzögerungen reichen Zeit und Kapazitäten möglicherweise nicht für den Umbau und die Migration aller geschäftskritischen Fachanwendungen in die Cloud. Vorsorglich hat RZPlus deshalb einen «Plan B» entwickelt. Die aktuellen Aufwandschätzungen für die Migration der geschäftskritischen Fachanwendungen sind höher, als im Verpflichtungskredit angenommen. Das Programm RZPlus hat deshalb einen Erhebungs- und Verifikationsprozess etabliert, der noch nicht abgeschlossen ist. Falls nötig kann MeteoSchweiz für RZPlus finanzielle Reserven einsetzen. Zuverlässige Aussagen zu den Betriebskosten Cloud sind aktuell noch nicht möglich.

---

<sup>3</sup> Siehe auch Website Digitale Transformation und IKT-Lenkung (DTI) zu Public Clouds Bund.

# Audit du projet TNI clé RZPlus – Sécurisation de la puissance de calcul

## Office fédéral de météorologie et de climatologie (MétéoSuisse)

### L'essentiel en bref

---

MétéoSuisse est une infrastructure critique qui fournit des services indispensables à la Suisse, tels que des alertes lors d'intempéries, des analyses concernant la propagation de polluants etc. Si ces services sont interrompus ou s'ils sont fournis de manière limitée, des vies humaines peuvent être mises en danger et entraîner d'importants dommages économiques. Avec le programme RZPlus, MétéoSuisse augmente la sécurisation de ses prestations. Pour ce faire, elle met en place une nouvelle géoredondance<sup>1</sup> des applications spécialisées critiques et des moyens TIC nécessaires et adapte les processus d'exploitation TIC. Sur la base de services en nuage public (*public cloud services*) et d'architectures appropriées, les applications spécialisées sont découplées autant que possible les unes des autres, ce qui permet d'augmenter encore la sécurisation de ses services. RZPlus s'étend de 2022 à 2028 et coûte environ 39 millions de francs. Le Contrôle fédéral des finances (CDF) a audité le programme pour la première fois et met l'accent sur le pilotage du programme et la gestion des risques.

L'audit a montré que le programme est exécuté de façon ciblée par une équipe motivée et professionnelle. Sa mise en œuvre avance bien, malgré d'importants retards imputables à des causes externes. En optant pour l'utilisation de services en nuage, MétéoSuisse adopte une approche appropriée pour atteindre les objectifs du programme. Le fait que la mise en place de mesures systématiques et complètes de réduction des risques et que l'acceptation des risques résiduels font défaut restent un problème.

### **RZPlus : un projet central pour prévenir les interruptions importantes de l'exploitation de MétéoSuisse**

Jusqu'à présent, l'informatique de MétéoSuisse est centralisée dans un centre de calcul de l'aéroport de Zurich. RZPlus réduit le risque d'interruptions techniques significatives de MétéoSuisse et met en œuvre une recommandation émise par le CDF en 2014.<sup>2</sup> Le choix d'un nuage public pour améliorer la sécurisation et l'adaptabilité se fonde sur la stratégie numérique de MétéoSuisse de 2022. La transmission des données continuera d'être assurée par l'Office fédéral de l'informatique et de la télécommunication, mais elle sera désormais géoredondante dans deux centres de calcul de la Confédération.

Le Centre suisse de calcul scientifique (CSCS) est géré par l'École polytechnique fédérale (EPF) et ne fait pas partie du programme RZPlus en tant qu'institution, mais les applications critiques qu'il héberge (modèles météorologiques) le sont. L'EPF a heureusement décidé à l'été 2023 de mettre en place et d'exploiter l'ordinateur à hautes performances du CSCS de manière géoredondante.

---

<sup>1</sup> La géoredondance désigne l'emploi de deux centres de calcul situés sur des sites suffisamment éloignés, dont l'état des données est identique et qui peuvent à tout moment reprendre les fonctions l'un de l'autre.

<sup>2</sup> « Audit de la gouvernance dans le domaine informatique – MétéoSuisse » du 1<sup>er</sup> décembre 2014 (n° d'audit 14419).

## **Les risques globaux liés au nuage doivent rapidement être identifiés et formellement acceptés**

En commandant pour la première fois des services issus de l'appel d'offres OMC pour l'achat de services en nuage public du secteur Transformation numérique et informatique (TNI), MétéoSuisse s'aventure en terrain inconnu.<sup>3</sup> L'enjeu est le suivant : RZPlus a besoin de connaissances hautement spécialisées pour mettre en place une plateforme en nuage en toute sécurité. Le fait que l'administration fédérale n'ait que peu d'expérience en la matière et que les outils d'aide, les informations et les directives soient encore en cours d'élaboration n'est pas non plus d'un grand soutien. MétéoSuisse doit combler les lacunes existantes et recruter du personnel spécialisé.

Dans le cadre des travaux préparatoires de RZPlus et de l'initialisation du programme, MétéoSuisse a déjà identifié des risques indissociablement liés à l'utilisation de services en nuage : influence d'États tiers, souveraineté numérique, disponibilité, gestion des sous-traitants etc. Il reste à définir exhaustivement les mesures de réduction des risques et l'acceptation des risques résiduels par la direction. Il est urgent de confirmer l'approche architecturale choisie et d'exploiter ensuite les applications spécialisées de manière productive dans le nuage. MétéoSuisse doit aussi déterminer, en sa qualité d'infrastructure civile critique, de l'opportunité de migrer vers un nuage public.

## **Des difficultés internes entravent l'avancement du programme**

La définition des exigences auxquelles doivent satisfaire les applications spécialisées critiques en matière de sécurité de l'information est plus complexe et coûteuse que prévu. Les informations et directives indispensables à la migration vers des services en nuage dans le cadre du projet RZPlus manquent pour la plupart. Le programme ne peut pas combler seul ces lacunes. Les responsables de la clientèle, des services et des produits ainsi que les responsables de la continuité des affaires et de la gestion des services informatiques doivent s'accorder sur la fixation des exigences pour les applications spécialisées et les outils TIC. Le processus nécessaire doit être géré de manière centralisée au niveau de la direction de MétéoSuisse.

RZPlus fait évoluer l'organisation, la répartition des tâches, les processus et fait émerger de nouveaux profils professionnels. Ces changements ne concernent pas uniquement l'informatique, mais tout l'office. Un changement de culture de manière centralisée est donc essentiel à la réussite du projet.

## **Les objectifs du programme ne sont actuellement pas menacés malgré des retards externes**

Les projets « Mise en place et mise en service du centre de calcul Campus et du service en nuage » et « Gouvernance informatique et migration des applications spécialisées » sont reportés de douze mois voire plus par rapport à la planification de 2021. Ces retards ne sont imputables ni au programme RZPlus, ni à MétéoSuisse. Il a été possible de les compenser par de nouvelles planifications et par le recours à des ressources supplémentaires. Cependant, la réduction du temps accordé à la réalisation de tâches restées nombreuses et complexes génère une augmentation du risque global. En raison des retards, il se peut que le temps et les capacités ne suffisent pas pour la transformation et la migration de toutes les applications spécialisées critiques vers le nuage. Par précaution, RZPlus a donc développé un « plan B ». Les estimations actuelles des dépenses pour la migration des applications

---

<sup>3</sup> Voir aussi la page Internet « Public Clouds Confédération » du secteur TNI.

spécialisées critiques excèdent celles fixées dans le cadre du crédit d'engagement. En conséquence, le programme RZPlus a mis en place un processus de collecte de données et de vérification qui n'est pas encore achevé. Si nécessaire, MétéoSuisse peut engager des réserves financières en faveur du programme. Il n'est pas encore possible d'estimer de manière fiable les coûts d'exploitation des services en nuage.

**Texte original en allemand**

# Verifica del progetto chiave TDT RZPlus – infrastruttura di calcolo a prova di guasto

Ufficio federale di meteorologia e climatologia (MeteoSvizzera)

## L'essenziale in breve

---

MeteoSvizzera è un'infrastruttura critica e fornisce alla Svizzera prestazioni di servizio indispensabili come ad esempio le allerte in caso di maltempo, le analisi sulla diffusione di sostanze nocive eccetera. Se tali prestazioni non sono fornite o lo sono solo in parte, possono essere messe in pericolo vite umane e si possono verificare gravi danni economici. Grazie al programma RZPlus, MeteoSvizzera aumenta l'affidabilità delle sue prestazioni di servizi. A tal fine, concepisce nuovamente le applicazioni specializzate critiche e i mezzi TIC necessari in modo georidondante<sup>1</sup> e adegua i processi operativi TIC. Basandosi su servizi di cloud pubblici e architetture adeguate, MeteoSvizzera scinde, nella misura del possibile, le applicazioni specializzate le une dalle altre, aumentando così ulteriormente l'affidabilità dei propri servizi. Il progetto RZPlus è stato lanciato nel 2022 a seguito del mandato corrispondente e si concluderà nel 2028. I costi si aggirano sui 39 milioni di franchi. Il Controllo federale delle finanze (CDF) ha svolto una prima verifica del programma, concentrandosi sulla direzione dello stesso e sulla gestione dei rischi.

Dalla verifica è emerso che il programma viene svolto in modo mirato da un team motivato e professionale. Nonostante i notevoli ritardi imputabili a cause esterne, il progetto procede bene. Utilizzando i servizi cloud, MeteoSvizzera mette in atto un approccio appropriato per raggiungere gli obiettivi del programma. Si constatano tuttavia lacune nella messa a punto di misure sistematiche e complete di riduzione dei rischi nonché nell'accettazione dei rischi residui.

### **RZPlus: un progetto chiave per prevenire importanti interruzioni delle attività di MeteoSvizzera**

Attualmente l'informatica di MeteoSvizzera è centralizzata in un centro di calcolo dell'aeroporto di Zurigo. RZPlus riduce il rischio di interruzioni tecniche importanti delle attività di MeteoSvizzera e attua una raccomandazione del CDF del 2014.<sup>2</sup> La scelta di un cloud pubblico per migliorare l'affidabilità e la scalabilità dei servizi forniti si basa sulla strategia digitale di MeteoSvizzera del 2022. La comunicazione dei dati continuerà a essere gestita dall'Ufficio federale dell'informatica e della telecomunicazione, ma in modo georidondante, in due centri di calcolo.

Il Centro nazionale di supercomputing (Swiss National Supercomputing Centre, CSCS) è gestito dal Politecnico federale (PF) e, in qualità di istituzione, non è interessato da RZPlus. Lo sono invece le applicazioni critiche (modelli meteorologici) installate su di esso. Fortunatamente, il PF nell'estate 2023 ha deciso di concepire e gestire in maniera georidondante anche il supercalcolatore CSCS.

---

<sup>1</sup> Per georidondanza si intende l'impiego di due centri di calcolo in siti sufficientemente distanti tra loro, che dispongono dello stesso livello dei dati di sistema e che possono assumere l'uno la funzione dell'altro in qualsiasi momento.

<sup>2</sup> «Verifica della Governance informatica MeteoSvizzera» del 1° dicembre 2014 (PA 14419).

## **I rischi complessivi del cloud devono essere rapidamente concretizzati e formalmente accettati**

Ricorrendo per la prima volta alla possibilità di ordinare servizi cloud pubblici aggiudicati mediante bando di concorso OMC del settore Trasformazione digitale e governance delle TIC (TDT), MeteoSvizzera si avventura su un terreno nuovo.<sup>3</sup> Il progetto RZPlus richiede infatti conoscenze altamente specializzate al fine di costruire una piattaforma di cloud sicura. L'Amministrazione federale ha poca esperienza in materia e gli strumenti di aiuto, le informazioni e le direttive sono ancora in fase di sviluppo. MeteoSvizzera deve quindi colmare le relative lacune e reclutare personale con conoscenze specialistiche.

Già durante i lavori preliminari per il progetto RZPlus e la fase di avvio del programma, MeteoSvizzera ha identificato dei rischi indissolubilmente legati all'utilizzo dei servizi cloud: influenza da parte di Stati terzi, sovranità digitale, disponibilità, gestione dei subappaltatori eccetera. Manca ancora la definizione completa delle misure di riduzione del rischio e l'accettazione dei rischi residui da parte della direzione. Ciò è urgentemente necessario per confermare l'approccio architettonico scelto e, in seguito, per gestire in modo produttivo le applicazioni specializzate nel cloud. MeteoSvizzera dovrebbe inoltre chiarire se, in qualità di infrastruttura civile critica, debba migrare al cloud pubblico.

## **Le difficoltà interne ostacolano il programma**

La determinazione dei requisiti che devono soddisfare le applicazioni specializzate considerate critiche in materia di sicurezza delle informazioni è più complessa e dispendiosa del previsto. Manca la maggior parte delle informazioni e dei requisiti indispensabili per la migrazione al cloud nel quadro del progetto RZPlus. Il programma non può colmare da solo tali lacune. A tal fine i responsabili della clientela, dei servizi o dei prodotti nonché i responsabili della gestione della continuità operativa e della gestione dei servizi informatici devono accordarsi sulla definizione dei requisiti cui sottoporre le applicazioni specializzate e gli strumenti TIC. Compete all'alta dirigenza di MeteoSvizzera dirigere in maniera centralizzata il processo necessario a tale scopo.

Il programma RZPlus fa evolvere l'organizzazione, la ripartizione dei compiti e i processi in seno a MeteoSvizzera e crea nuovi profili professionali. Questi cambiamenti non riguardano solo l'informatica, ma tutto l'Ufficio. Apportare un cambiamento culturale a livello centrale è quindi fondamentale per condurre a buon fine il programma.

## **Nonostante i ritardi esterni gli obiettivi del programma non sono ancora compromessi**

I progetti relativi all'approntamento e alla messa in esercizio nel centro di calcolo Campus e nel cloud nonché il progetto di governance informatica e di migrazione delle applicazioni specializzate hanno subito un ritardo di dodici mesi o più rispetto alla pianificazione del 2021. I motivi esulano dalla sfera di influenza del programma RZPlus e di MeteoSvizzera. È stato possibile compensare tali ritardi grazie a una nuova pianificazione e al ricorso a risorse supplementari. Tuttavia, la riduzione dei tempi per la realizzazione di compiti tuttora numerosi e complessi comporta un aumento del rischio complessivo. A causa dei ritardi, potrebbero mancare il tempo e le capacità necessarie per la ristrutturazione e la migrazione al cloud di tutte le applicazioni specializzate critiche per l'operatività. A titolo precauzionale, i responsabili del progetto RZPlus hanno quindi elaborato un «piano B». Le attuali stime dei

---

<sup>3</sup> Si consulti anche la pagina «Cloud pubblico della Confederazione» alla rubrica Trasformazione digitale e governance delle TIC.

costi per la migrazione delle applicazioni specializzate critiche per l'operatività sono superiori a quelle fissate nel quadro del credito d'impegno. Per questo motivo il programma RZPlus ha avviato un processo di rilevamento e di verifica che è ancora in corso. Se necessario, MeteoSvizzera potrà utilizzare riserve finanziarie per il progetto. Attualmente non è ancora possibile pronunciarsi in maniera affidabile sui costi d'esercizio dei servizi cloud.

**Testo originale in tedesco**

# Audit of the DTI key project RZPlus – fail-safe computing power

## Federal Office of Meteorology and Climatology (MeteoSwiss)

### Key facts

---

MeteoSwiss is a critical infrastructure and provides essential services for Switzerland, such as severe weather warnings, analyses of the spread of pollutants and so on. If these services fail or are only provided to a limited extent, human lives can be put at risk and major economic damage may result. With the RZPlus programme, MeteoSwiss is increasing the reliability of its services. To this end, it is reorganising the business-critical specialist applications and the ICT resources required for them in a geo-redundant manner<sup>1</sup> and adapting the ICT operating processes. Based on public cloud services and suitable architectures, the specialist applications will be decoupled from each other wherever possible, thereby further increasing fail-safe performance. RZPlus started in 2022 and will run until 2028, costing around CHF 39 million. The Swiss Federal Audit Office (SFAO) audited the programme for the first time and focused on programme and risk management.

The audit showed that the programme is being implemented in a targeted manner by a motivated and professional team. It is progressing well despite considerable external delays. MeteoSwiss's use of the cloud is an appropriate approach to achieving the programme's objectives. One problem is that the systematic and complete development of risk-mitigating measures and the acceptance of residual risks are still pending.

#### **RZPlus: a central project to prevent serious interruptions to operations at MeteoSwiss**

Until now, MeteoSwiss IT has been housed centrally in a data centre at Zurich Airport. RZPlus reduces the risk of significant technical service interruptions at MeteoSwiss and implements a recommendation made by the SFAO in 2014.<sup>2</sup> The choice of a public cloud to improve reliability and scalability is based on the 2022 MeteoSwiss digital strategy. Data communication will continue to be operated by the Federal Office of Information Technology, Systems and Telecommunication, but will now be geo-redundant in two federal data centres.

The Swiss National Supercomputing Centre (CSCS) is operated by the Swiss Federal Institute of Technology (ETH) and is not part of RZPlus as an institution, whereas the critical applications (weather models) installed on it are. Fortunately, ETH decided in summer 2023 to set up and operate the CSCS high-performance computer with geo-redundancy.

#### **Overall cloud risks must be swiftly defined and formally accepted**

MeteoSwiss is entering uncharted territory with the first call-off of services from the Digital Transformation and ICT Steering (DTI) Sector's WTO public cloud procurement.<sup>3</sup> The challenge is that RZPlus requires highly specialist knowledge in order to securely set up a cloud

---

<sup>1</sup> Geo-redundancy refers to the use of two data centres at sufficiently distant locations that have the same data status and can assume the other's role at any time.

<sup>2</sup> "MeteoSwiss, Audit of IT governance" of 1 December 2014 (audit mandate 14419).

<sup>3</sup> See also the Digital Transformation and ICT Steering (DTI) website on "Public Clouds Bund".

platform. The fact that the Federal Administration has little experience with this and that tools, information and guidelines are still being developed does not help. MeteoSwiss must fill the relevant gaps and recruit employees with specialist knowledge.

MeteoSwiss already identified risks that are inextricably linked to the use of cloud services during the preparatory work for RZPlus and the programme launch: influence from third countries, digital sovereignty, availability, subcontractor management, etc. However, a comprehensive definition of risk-mitigating measures and acceptance of the remaining residual risks by the Management Board are still lacking. These are urgently needed in order to confirm the chosen architectural approach and subsequently operate specialist applications in a productive setting in the cloud. MeteoSwiss should also clarify whether it should migrate to the public cloud as a civilian critical infrastructure.

### **Internal challenges are hampering the programme**

Determining the information security requirements for the business-critical specialist applications is more complex and time-consuming than expected. Most of the information and specifications required by RZPlus for migration to the cloud are missing. The programme cannot bridge this gap itself. To do this, the client, service or product managers and the business continuity and IT service management managers must develop a common understanding of how to identify the requirements for the specialist applications and ICT resources. The necessary process must be managed centrally at MeteoSwiss, at top management level.

RZPlus changes the organisation, division of tasks and processes, and even creates new job profiles. This is not just limited to IT, but affects the entire federal office. A centrally managed cultural change is therefore crucial in order for the programme to succeed.

### **Programme objectives not yet at risk despite external delays**

The projects "Construction & commissioning of the CAMPUS data centre and cloud" and "IT governance & migration of specialist applications" have been delayed by twelve months or more compared to the project schedule for 2021. The reasons for this were beyond the control of RZPlus and MeteoSwiss. The programme was able to compensate for the delays by rescheduling and deploying more resources. Nevertheless, the ever-shorter time for the same number of complex tasks means an increased overall risk. Due to the delays, there may not be enough time and capacity for all business-critical specialist applications to be converted and migrated to the cloud. As a precaution, RZPlus has therefore developed a "plan B". The current cost estimates for migrating the business-critical specialist applications are higher than assumed in the guarantee credit. The RZPlus programme has therefore established a survey and verification process that has not yet been completed. If necessary, MeteoSwiss can draw on financial reserves for RZPlus. No reliable conclusions can yet be made regarding the cloud operating costs.

**Original text in German**

## Generelle Stellungnahme MeteoSchweiz

Das Bundesamt für Meteorologie und Klimatologie MeteoSchweiz bedankt sich für die angenehme Zusammenarbeit und die gründliche Analyse, welche MeteoSchweiz über den vorliegenden Bericht hinaus als wertvoll und unterstützend ansieht. MeteoSchweiz ist mit dem vorliegenden Bericht und den darin enthaltenen Aussagen einverstanden.

# 1 Auftrag und Vorgehen

## 1.1 Ausgangslage

Mit dem vom Parlament am 2. März 2022<sup>4</sup> freigegebenen Programm RZPlus wird MeteoSchweiz eine georedundante, ausfallsichere Rechenleistung und Datenkommunikation erstellen. Damit soll das Risiko von Betriebsunterbrüchen reduziert und eine Empfehlung der EFK<sup>5</sup> von 2014 zur Georedundanz umgesetzt werden.

Das Programm hat am 1. Januar 2022 begonnen und soll bis 31. Dezember 2028 dauern. Die einmaligen Programmaufwände betragen 31,34 Millionen Franken. Ausserdem erbringt MeteoSchweiz Eigenleistungen von 7,52 Millionen Franken. Für wiederkehrenden Aufwände wurde das jährliche Globalbudget für Personal ab 2023 und für Sach-/Betriebsaufwände ab 2024 dauerhaft erhöht.

Die Eidgenössische Finanzkontrolle (EFK) prüft das DTI-Schlüsselprojekt RZPlus zum ersten Mal.

## 1.2 Prüfungsziel und -fragen

Ziel der Prüfung ist die Beurteilung des Programms und der Programmrisiken hinsichtlich der Zielerreichung.

Prüffragen:

- Läuft das Programm RZPlus zeitlich, inhaltlich und kostenmässig nach Plan?
- Sind die Angaben im letzten halbjährlichen DTI-Schlüsselprojekt-Reporting verlässlich bzw. plausibel?
- Werden die Anforderungen der geschäftskritischen Dienstleistungen an RZPlus sichergestellt?
- Wurde die Empfehlung 14419.008 umgesetzt: «Die EFK empfiehlt MeteoSchweiz, dass im Rahmen des laufenden Business-Continuity-Management-Projekts (BCM) die Notwendigkeit eines Mehrstandortkonzepts untersucht und beurteilt wird. Bevor der Bau oder die Miete eines weiteren RZ in Erwägung gezogen wird, ist unbedingt zu prüfen, ob bzw. wie die bestehenden bzw. die geplanten Rechenzentren des Bundes mitgenutzt werden können.»

## 1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Luc Pelfini (Revisionsleiter), Petra Kuhn, Martin Scheid und Dieter Lüthi vom 10. Juli bis 11. August 2023 durchgeführt. Sie erfolgte unter der Federführung von Oliver Sifrig. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Prüfungsdurchführung.

---

<sup>4</sup> 21.062 – Bundesbeschluss über einen Verpflichtungskredit zum Aufbau einer ausfallsicheren Rechenleistung und der dazu nötigen Transformation der IKT von MeteoSchweiz, Beschluss vom 2. März 2022, BBl 2022 77.

<sup>5</sup> «Prüfung der IT-Governance MeteoSchweiz» vom 1. Dezember 2014 (PA 14419).

## 1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von MeteoSchweiz umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen (sowie die benötigte Infrastruktur) standen dem Prüftteam vollumfänglich zur Verfügung.

## 1.5 Schlussbesprechung

Die Schlussbesprechung fand am 27. Oktober 2023 statt. Teilgenommen haben von MeteoSchweiz: Der Amtsdirektor MeteoSchweiz, der Programmleiter RZPlus, der Bereichsleiter Informations- und Kommunikationstechnologie, der Bereichsleiter Planung und Kundenbeziehungen, der Abteilungsleiter Sicherheit und Qualität, der Enterprise-Architekt RZPlus und die Programm Management Officer RZPlus. Das Generalsekretariat des Eidgenössischen Departements des Innern (GS-EDI) wurde vertreten durch den Leiter Informatik EDI, der Bereich Digitale Transformation und IKT-Lenkung durch die Leiterin Transformation und Interoperabilität. Seitens EFK waren dabei: die Mandatsleiterin, der Fachbereichsleiter und der Revisionsleiter.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

## 2 Aufbau einer georedundanten, ausfallsicheren Rechenleistung

### 2.1 RZPlus reduziert das Risiko signifikanter technischer Betriebsunterbrüche bei MeteoSchweiz

MeteoSchweiz ist eine kritische Infrastruktur und erbringt für die Schweiz unverzichtbare Dienstleistungen (Unwetterwarnungen, Flugwetter, Ausbreitungsanalysen von Schadstoffen, ...). Wenn diese ausfallen oder nur reduziert erbracht werden, können Menschenleben gefährdet sein und grosse wirtschaftliche Schäden eintreten.

Für ihre Leistungserbringung ist MeteoSchweiz auf die weitgehend selber entwickelten rund 300 Fachanwendungen, verschiedenste Messstationen sowie nationale und internationale Partner angewiesen. Beispiele sind das Swiss National Supercomputing Centre (CSCS) der Eidgenössischen Technischen Hochschule (ETH) oder das Europäische Zentrum für Mittelfristige Wettervorhersagen (EZMW). Die Fachanwendungen betreibt MeteoSchweiz selber im eigenen Rechenzentrum am Flughafen Kloten. Die Berechnung des COSMO-Wettermodells<sup>6</sup> ist an das CSCS ausgelagert. Sowohl die Fachanwendungen als auch das COSMO-Wettermodell werden jeweils nur in einem Rechenzentrum betrieben. Sollte eines davon ausfallen, kann MeteoSchweiz seine Dienstleistungen und Produkte nicht oder nur unzureichend erstellen.

Wegen der fehlenden Verteilung der Rechenleistung auf zwei Standorte (Georedundanz) hat MeteoSchweiz im Risikomanagement Bund seit 2014 das Top-Risiko «signifikante technische Betriebsunterbrüche bei MeteoSchweiz» rapportiert. Aufgrund der hohen Kosten und fehlender finanzieller Mittel hat MeteoSchweiz die Georedundanz bisher nicht umgesetzt. Mit den seit 2022 bewilligten Mitteln kann MeteoSchweiz mit dem Programm RZPlus eine georedundante, ausfallsichere Rechenleistung und Datenkommunikation für sich selbst erstellen.

#### Beurteilung

MeteoSchweiz ist nicht nur selber eine kritische Infrastruktur, sondern erbringt auch für andere kritische Infrastrukturen (bspw. Bundesamt für Bevölkerungsschutz, Bundesamt für Zivilluftfahrt, Armee, Skyguide) Dienstleistungen, auf welche diese angewiesen sind. Da bei einem längeren Ausfall von geschäftskritischen Dienstleistungen Menschenleben gefährdet sein und grosse wirtschaftliche Schäden entstehen können, ist RZPlus dringend notwendig zur Verbesserung der Ausfallsicherheit und Resilienz. Mit dem Programm RZPlus wird nicht nur für MeteoSchweiz das Ausfallrisiko von geschäftskritischen Prozessen wesentlich reduziert, sondern auch für andere Verwaltungseinheiten.

<sup>6</sup> COSMO (steht für Consortium for Small-scale Modeling) ist das numerische Wettervorhersagemodell von MeteoSchweiz für die Produktion von regionalen und lokalen Vorhersageprodukten im Alpenraum.

## 2.2 Ausfallsicherheit ist mehr als Georedundanz

Nach Abschluss von RZPlus laufen die heute im eigenen Rechenzentrum betriebenen geschäftskritischen Fachanwendungen neu georedundant in der Cloud in mindestens zwei Verfügbarkeitszonen. Zudem werden sie bevorzugt als Cloud-native-Anwendung (siehe Glossar) in die Cloud migriert, wodurch technische Abhängigkeiten zwischen den Fachanwendungen nach Möglichkeit entkoppelt werden. Parallel dazu werden die Betriebsprozesse an die neue IKT-Landschaft angepasst. So wird die Ausfallsicherheit über eine reine Georedundanz hinaus verbessert.

Ausserdem soll der Cloud-Einsatz die von MeteoSchweiz benötigte Skalierbarkeit von Rechen- und Speicherleistung sowie die Fähigkeit zur Zusammenarbeit mit europäischen und internationalen Partnern verbessern. Die Verwendung einer Cloud-Architektur entspricht der Digitalen Strategie MeteoSchweiz von 2022 (cloud first).

MeteoSchweiz kann die für RZPlus benötigten Cloud-Services aus der von der Bundeskanzlei – Bereich Digitale Transformation und IKT-Lenkung (DTI) durchgeführten WTO-Ausschreibung Public Cloud abrufen. Damit ist MeteoSchweiz eine der ersten Verwaltungseinheiten, die Leistungen aus der Public-Cloud-Beschaffung des DTI bezieht.

Die Datenkommunikation ist das Rückgrat von MeteoSchweiz und verbindet die verschiedenen Sensoren, Datenquellen und Standorte untereinander. Aufgrund der besonderen fachlichen Anforderungen kann sie nicht in die Cloud verschoben werden. Daher wird diese Leistung weiter vom Bundesamt für Informatik und Telekommunikation (BIT) bezogen und neu georedundant und on-premise in zwei Bundesrechenzentren betrieben.

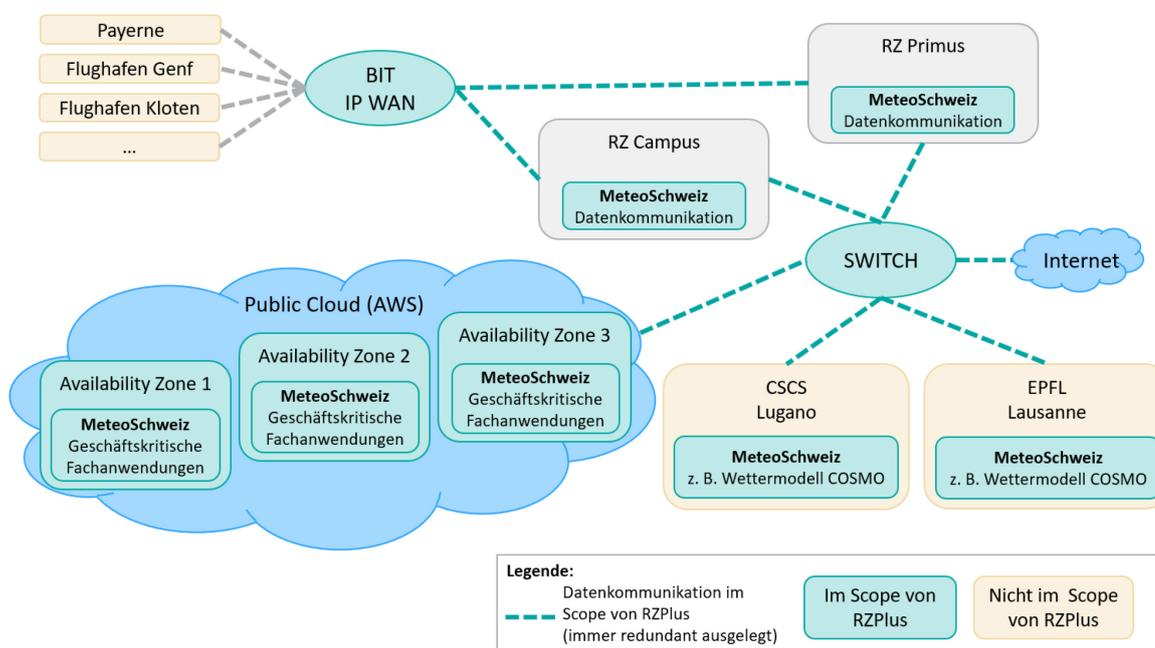


Abbildung 1 : Zielvorstellung RZPlus, Darstellung EFK

Nicht im Umfang von RZPlus enthalten ist insbesondere die Resilienz gegenüber kriegerischen Handlungen. Dies ist gemäss Bundesratsbeschluss<sup>7</sup> und Programmauftrag explizit ausgeschlossen.

Die mehrfach tägliche Berechnung des Wettervorhersagemodells COSMO am CSCS der ETH in Lugano ist für die Leistungserbringung von MeteoSchweiz unentbehrlich. Das CSCS wird von der ETH betrieben und ist als Institution nicht Teil des Programms RZPlus, wohl aber die dort installierten kritischen Geschäftsanwendungen. Die Schulleitung der ETH hat Mitte 2023 entschieden, den für die Berechnung der Wettermodelle benötigten Rechner neu georedundant zu betreiben. Damit wird ein bisheriger single-point-of-failure ausserhalb des direkten Einflusses von MeteoSchweiz behoben.

### Beurteilung

Das Programm hat eine zweckmässige und strategiekonforme Architektur gewählt. Sie ermöglicht die Erhöhung der Ausfallsicherheit und reduziert das Risiko für signifikante technische Betriebsunterbrüche aufgrund von lokalen Ereignissen. Die Empfehlung der EFK von 2014, die Notwendigkeit für georedundante Rechenleistung abzuklären, ist damit auch erfüllt.

Positiv ist, dass mit RZPlus die Ausfallsicherheit umfassender verbessert und nicht nur die bestehende Informatik an zwei Standorten georedundant betrieben wird. Erfreulich ist auch, dass der Hochleistungsrechner im CSCS von der ETH georedundant aufgebaut wird und damit ein single-point-of-failure eliminiert wird.

Es ist nachvollziehbar, dass die Massnahmen von RZPlus primär zur Aufrechterhaltung der Verfügbarkeit auf die «normale Lage<sup>8</sup>» ausgerichtet sind. Damit verbleibt aber insbesondere das Restrisiko «Ausfall von MeteoSchweiz-Dienstleistungen» bei ausserordentlichen Lagen wie Katastrophen und kriegerischen Ereignissen, was unter Umständen nicht allen Stakeholdern bewusst ist.

### Empfehlung 1 (Priorität 1)

Die EFK empfiehlt MeteoSchweiz, für ihre relevanten Dienstleistungen die notwendigen End-to-End-Informationsflüsse, Verarbeitungsprozesse und Abhängigkeiten von Dritten zu analysieren. Ausfallrisiken, die ausserhalb des Programm-Scope von RZPlus liegen, müssen identifiziert und bewertet werden. Daraus muss MeteoSchweiz allfälligen weiteren Handlungsbedarf ableiten und die von Ausfallrisiken betroffenen Kunden informieren.

*Die Empfehlung ist akzeptiert.*

### Stellungnahme MeteoSchweiz

Die Analyse der End-to-End Prozesse (Dienstleistungen, Informationsflüsse, Verarbeitungsprozesse und Abhängigkeiten) ist im Oktober 2023 von der Geschäftsleitung MeteoSchweiz als Basis für das Projekt RGF (IT-Governance und Fachanwendungen) festgelegt worden. Im 2024 werden in Arbeitsgruppen bestehend aus MeteoSchweiz Fachpersonal/Stakeholdern und RZPlus Projektmitarbeitern themengerecht die bestehenden Informationsflüsse, Verarbeitungsprozesse und Abhängigkeiten analysiert und erfasst. Daraus wird der Handlungsbedarf (inkl. Priorisierung) abgeleitet und der Informationsfluss sowie die Kommunikationsmassnahmen für die von Ausfallrisiken betroffenen Kunden/Stakeholdern definiert.

<sup>7</sup> 21.062 – Botschaft zu einem Verpflichtungskredit zum Aufbau einer ausfallsicheren Rechenleistung und der dazu nötigen Transformation der IKT von MeteoSchweiz vom 8. September 2021, BBl 2021 2161.

<sup>8</sup> Siehe Glossar.

## 2.3 Die Migration in die Cloud darf erst nach Abschluss der Risikoanalyse und der Umsetzung der Massnahmen erfolgen

### **Der Einsatz von Public Cloud ist Neuland und bringt neue Risiken mit sich**

MeteoSchweiz hat erkannt, dass mit der Wahl einer Cloud-Lösung teilweise völlig neue Risiken verbunden sind. Diese wurden beim Variantenentscheid für die Cloud berücksichtigt, bisher aber nicht systematisch erhoben und bewertet. Somit fehlt die Grundlage um die notwendigen, risikomindernde Massnahmen festzulegen und die Restrisiken auszuweisen. Auch wenn die Cloud-Nutzung auf Departementsebene freigegeben wurde, verbleibt die Verantwortung für den Gang in die Cloud beim Amtsdirektor von MeteoSchweiz.

Auch die Bundeskanzlei (DTI) hält auf ihrer Website zur Bundesarchitektur Cloud fest: «Bei Public-Cloud-Diensten muss die Verwaltung Informationssicherheit und Datenschutz mit zusätzlicher Sorgfalt prüfen, da diese ausserhalb der eigenen Rechenzentren laufen. Dazu gehört unter anderem eine Prüfung der rechtlichen Vorgaben, des Schutzbedarfs und der Risiken. Basierend darauf entscheidet die zuständige Verwaltungseinheit, in welches Cloud-Angebot und mit welchen vorkehrenden Massnahmen sie eine Anwendung einführt.»<sup>9</sup>

DTI stellt den Verwaltungseinheiten unter anderem einen Risiko-/Massnahmenkatalog<sup>10</sup> mit spezifischen Risiken und Massnahmen bei der Nutzung von Public-Cloud-Diensten zur Verfügung. Dieser umfasst politische, Business Continuity, Compliance sowie technische Risiken und Massnahmen. Beispielsweise muss sich eine Verwaltungseinheit damit auseinandersetzen, dass ein Cloud Service Provider (CSP) aufgrund ausländischer Gesetze oder politischem Druck möglicherweise ohne Vorankündigung Daten herausgibt (Datensouveränität) oder Dienstleistungen einstellt (digitale Souveränität). Rechtliche Zusicherungen und Vereinbarungen sind grundsätzlich nur schwer durchsetzbar. Bei grossen, internationalen Anbietern müssen diese Aspekte in die Risikobeurteilung einbezogen werden. Hinzu kommt, dass neben neuen Risiken auch bekannte Risiken bei einer Cloud-Nutzung höher sind als bei einem on-premise-Betrieb oder Outsourcing (z. B. Ausübung der Kontrollrechte beim Cloud Service Provider oder laufende Veränderungen an den Cloud-Services und Unteraffordanten).

### **Die Dokumentation der Restrisiken und Massnahmen fehlt als Grundlage für einen informierten Entscheid zur Cloud-Nutzung**

MeteoSchweiz hat sich dazu entschlossen, für ihre Cloud-Plattform bei Amazon Web Services (AWS) als Ganzes eine Risikoanalyse durchzuführen, notwendige Massnahmen zu definieren und die Restrisiken auszuweisen. In der Schutzbedarfsanalyse (Schuban) für die neue Cloud-Plattform hat MeteoSchweiz für die Verfügbarkeit einen erhöhten Schutzbedarf festgestellt. Dementsprechend wird ein Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept) notwendig. In diesem werden die Anforderungen an die Informationssicherheit<sup>11</sup> und den Datenschutz vervollständigt, eine detaillierte Risikoanalyse erstellt und Schutzmassnahmen definiert. Die Risiken müssen sowohl für AWS und deren

---

<sup>9</sup> Website der Abteilung Digitale Transformation und IKT-Lenkung > Bundesarchitektur > Cloud, abgerufen am 27.7.2023.

<sup>10</sup> Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung, Anhang C: Risiken und Massnahmen zum Bericht Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung.

<sup>11</sup> Ausführlichere Informationen finden sich im Glossar unter «Informationssicherheit».

Unterlieferanten, die gewählte Architektur und die einzelnen eingesetzten Cloud-Produkte respektive Services beurteilt werden. Diese Arbeiten sind noch nicht abgeschlossen.

Der Kanton Bern hat ebenfalls für eine Cloud-Plattform ähnliche Überlegungen angestellt. Das Informatikamt ist einen interessanten Weg gegangen. Als Basis für den Grundsatzentscheid des Regierungsrates über den Einsatz der cloudbasierten Microsoft-365-Lösung erstellte es eine umfassende Analyse.<sup>12</sup> Diese enthält auch für nicht IT-affine Leser verständlich formulierte Risiken, Sicherheitsmassnahmen und Restrisiken und unterstützt das Verständnis von Entscheidungsträgern und Bürgern.

### **Beurteilung**

Verwaltungseinheiten, die eine Public Cloud nutzen wollen, haben einen aufwendigen, komplexen und risikobehafteten Weg vor sich, um einen informierten Entscheid dafür oder dagegen zu fällen. Neue und erhöhte Risiken müssen beurteilt und daraus die notwendigen Massnahmen ergriffen werden (vergleiche DTI Risiko-/Massnahmenkatalog). Schlussendlich müssen die Verantwortlichen einer Verwaltungseinheit so transparent und verständlich informiert werden, dass sie die Aufwände zur Umsetzung der Massnahmen und die Restrisiken dem erhofften Nutzen gegenüberstellen können. Diese Arbeiten sind die Voraussetzung für eine differenzierte Beurteilung, welche Anwendungen und Daten angesichts der Restrisiken in die Cloud verschoben werden dürfen. Die Erstellung eines Management Summaries analog zum Kanton Bern ist empfehlenswert.

Erst nach der formellen Dokumentation und Freigabe der Cloud-Risiken und Massnahmen durch die Geschäftsleitung sollte mit der produktiven Nutzung der AWS Public Cloud für MeteoSchweiz begonnen werden. Es wäre fatal, wenn die Restrisiken nicht übernommen werden können. Deshalb ist vordringlich diese Beurteilung rasch zu fällen, um den strategischen Entscheid Cloud-first auch aus dieser Optik zu untermauern.

### **Empfehlung 2 (Priorität 1)**

Die EFK empfiehlt MeteoSchweiz, die systematische Erhebung der mit einer Cloud-Nutzung verbundenen Risiken, die Umsetzung von notwendigen Massnahmen und die formelle Akzeptanz von Restrisiken rasch abzuschliessen. Dies muss geschehen, bevor Fachanwendungen für den produktiven Betrieb in die Cloud migriert werden.

*Die Empfehlung ist akzeptiert.*

### **Stellungnahme MeteoSchweiz**

MeteoSchweiz, als Teil der zentralen Bundesverwaltung, führt das Risikomanagement gemäss dem durch die EFV zentral gesteuerten Risikomanagement-Prozess. Die Erhebung und Überprüfung der mit der Cloud-Nutzung verbundenen Risiken werden im Rahmen des ordentlichen (bundesweiten) Review-Prozesses 2024 zum Risikomanagement analysiert. Basierend auf der Analyse werden die Risiken identifiziert und eingeordnet, Mitigationsmassnahmen festgelegt und der Umgang mit Restrisiken beschlossen.

<sup>12</sup> Bericht des kantonalen Informatikamtes über die Einführung von Microsoft 365 vom 28. Juni 2023 zuhanden des Regierungsrates Kanton Bern.

## **MeteoSchweiz beurteilt technisches Sicherheitsniveau in der Cloud als ausreichend**

Aufgrund von Vorabklärungen und mehrerer Proof of Concept Projekten sind die Verantwortlichen von RZPlus zum Schluss gekommen, dass die verfügbaren Architekturen, Sicherheitsfunktionen und Schlüsselkontrollen der Cloud Service Provider ein hohes Sicherheitsniveau ermöglichen (Verfügbarkeit, Integrität und Vertraulichkeit). Anforderungen zur Erreichung des Sicherheitsniveaus hat MeteoSchweiz im anbieterneutralen Pflichtenheft zum Abruf aus der WTO Public Cloud gestellt: Georedundanz, Standort Schweiz, VPN-Verbindung, Load Balancer, starke Verschlüsselung etc. Ein Abgleich mit den konkreten Sicherheitsanforderungen der einzelnen Fachanwendungen hat noch nicht stattgefunden (vgl. dazu Kapitel 3).

Bezüglich Vertraulichkeit kommt MeteoSchweiz zum Schluss, dass mit dem Abruf von AWS Anwendungen und Daten bis und mit Schutzstufe 2 (Vertraulich) in die Cloud migriert werden könnten. Bis auf Weiteres erlaubt MeteoSchweiz aber erst die Schutzstufen 0 (Public) und 1 (Intern). Hinsichtlich Verfügbarkeit erfüllt AWS mit mehreren Verfügbarkeitszonen in der Schweiz und den notwendigen Services die Anforderungen von RZPlus.

## **Unsicherheiten bei Cloud-spezifischen Sicherheitsmassnahmen**

Aus Geheimhaltungsgründen ist der Zugang zum Rahmenvertrag WTO Public Cloud äusserst restriktiv. Die Sicherheitsspezialisten und Architekten von MeteoSchweiz haben bisher keinen Zugang dazu und können sich selber kein Bild über vereinbarte Sicherheitsmassnahmen verschaffen. Somit können sie die Restrisiken und den Bedarf für ergänzende Massnahmen nicht beurteilen. Beispiele sind die Einhaltung des IKT-Grundschatz, die Definition und Überprüfbarkeit eines Internen Kontrollsystems beim Cloud-Anbieter, die Übertragung des Amtsgeheimnisses, die weisungsgemässe Bearbeitung von Daten, den Umgang mit Unterlieferanten etc. Gemäss MeteoSchweiz hat DTI mündlich zugesichert, dass mit dem Rahmenvertrag der WTO Public Cloud der IKT-Grundschatz eingehalten werde.

Da sich Sicherheitsmassnahmen in einer Cloud teilweise erheblich von denjenigen für einen standortgebundenen Betrieb (on-premise) oder ein Outsourcing unterscheiden, reicht der IKT-Grundschatz der Bundesverwaltung<sup>13</sup> für RZPlus nicht aus. Aus diesem Grund erarbeitet der Informatiksicherheitsbeauftragte (ISBO) von MeteoSchweiz gemeinsam mit den Architekten und Cloudspezialisten von RZPlus ergänzende Sicherheitsmassnahmen.

Die Grundsatzfrage, ob eine kritische Infrastruktur in eine Public Cloud migrieren darf bzw. soll, ist auf Bundesebene nicht geregelt. Deshalb trägt MeteoSchweiz alle mit diesem Entscheid verbundenen Risiken.

### **Exkurs: Lücken bei Cloud-Regelungen und -Prozessen in der Bundesverwaltung**

MeteoSchweiz ruft als eine der ersten Verwaltungseinheiten Leistungen aus der WTO-Beschaffung von Public Cloud Services für die Bundesverwaltung ab.<sup>14</sup> Zur Unterstützung von Verwaltungseinheiten hat DTI zur Cloud-Nutzung verschiedene Vorgaben und Hilfsmittel erstellt. Wie der erste Abruf durch MeteoSchweiz zeigt, fehlen noch einige Vorgaben und Hilfsmittel, was Aufwände, Unsicherheit und Risiken für abrufende Verwaltungseinheiten bedeutet. Das Thema ist nicht ganz neu. Bereits 2021 hat die Bundeskanzlei eine Empfehlung der EFK akzeptiert, die einen Handlungsbedarf in diese Richtung aufgenommen hat:

<sup>13</sup> Si001 – IT-Grundschatz in der Bundesverwaltung.

<sup>14</sup> Siehe auch Medienmitteilung des Bundesrates vom 27. September 2022 zum Abschluss der Verträge zum Bezug von Public-Cloud-Leistungen für die Bundesverwaltung (WTO Public Cloud), Ausschreibung auf simap.ch (Meldungsnummer 1136825), Zuschlag auf simap.ch (Meldungsnummer 1202937).

«Die EFK empfiehlt, dass die Bundeskanzlei (DTI) unter Einbezug des Nationalen Zentrums für Cybersicherheit und des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten allgemein verbindliche Vorgaben sowie Hilfsmittel für den Einsatz von Cloud-Technologien ausarbeiten und in Kraft setzen sollte.»<sup>15</sup>

Da eine Empfehlung zur Bereitstellung von Hilfsmitteln und Vorgaben bereits ausgesprochen wurde und die vorliegende Prüfung deren Umsetzung nicht untersucht hat, verzichtet die EFK auf eine Beurteilung.

### Beurteilung

Es erschwert die Aufgabe von MeteoSchweiz erheblich, dass die Informationssicherheits-spezialisten keinen Zugang zum Rahmenvertrag der WTO Public Cloud haben und Bundesvorgaben zur Nutzung von Public Cloud für kritische Infrastrukturen fehlen. Eine mündliche Bestätigung von DTI zum Grundschutz reicht nicht aus und überlässt das Risiko MeteoSchweiz.

Dass MeteoSchweiz den Bedarf für eine Cloud-spezifische Erweiterung des IKT-Grundschutzes erkannt hat und diese erarbeitet, ist positiv.

### Empfehlung 3 (Priorität 2)

Die EFK empfiehlt MeteoSchweiz, sich bei Bedarf betreffend Vorgaben, Hilfsmitteln, Massnahmen und (Rest-)Risiken im Zusammenhang mit einer Nutzung der Public Cloud formell mit den verantwortlichen Stellen (BK, DTI, BIT, NCSC sowie GS EDI ...) abzustimmen. Damit sollen Lösungen gefunden werden, um Lücken zu schliessen.

*Die Empfehlung ist akzeptiert.*

### Stellungnahme MeteoSchweiz

Da MeteoSchweiz ein eigenständiger Leistungserbringer für meteorologische Fachapplikationen und neu eigenständiger Fach-CSB (Cloud Service Broker) ist, wird die Teilnahme in der Informatikbetreiberkonferenz Bund (IBK) angestrebt. Dadurch wird die MeteoSchweiz formal in einem wichtigen Gremium direkt eingebunden, um sich mit den anderen Stellen abzustimmen. Zusätzlich ist gemäss CSB Pflichtenheft eine Zusammenarbeit zwischen den verschiedenen CSBs im Bund unter der Leitung von DTI vorgesehen. Gemäss CSB Pflichtenheft ist ebenfalls vorgesehen, dass die CSBs Zugriff auf die WTO20007 Rahmenverträge erhalten. Das CSB-Pflichtenheft ist zum Zeitpunkt der Stellungnahme auf Stufe IBK in Review.

<sup>15</sup> «Prüfung des IKT-Schlüsselprojektes SUPERB» (PA 21451), 19. April 2022, verfügbar auf der Website der EFK.

## 3 Verfügbarkeits-, Integritäts- und Vertraulichkeitsanforderungen an RZPlus

### 3.1 Leistungsvereinbarungen mit Kunden werden systematisch vereinbart und überprüft

Die EFK hat die Leistungsvereinbarungen von MeteoSchweiz mit Kunden für kritische Dienstleistungen/Produkte anhand von drei Stichproben geprüft: Flugwetter zivil, Flugwetter Luftwaffe und Publikation Naturgefahren. Vereinbarungen werden in jedem Bereich formell abgeschlossen und periodisch gemeinsam mit den Kunden auf Aktualität und Einhaltung überprüft. In den Stichproben waren die Rückmeldungen der Kunden durchwegs positiv, auch was die konkrete Leistungserbringung betrifft. Die periodischen Review-Prozesse unterscheiden sich voneinander, unter anderem wegen abweichender regulatorischer Vorgaben.

In den Leistungsvereinbarungen zum Flugwetter zivil sind verschiedenste Anforderungen mit messbaren Kriterien (Key Performance Indicators, KPI) definiert: späteste Lieferzeit, Verfügbarkeit, Integritätsanforderungen, räumliche Auflösung etc.

In den Leistungsvereinbarungen zu Flugwetter Luftwaffe und Publikation Naturgefahren sind praktisch keine KPI definiert.

## Verfügbarkeit

Im Normalbetrieb sollte mittels «IT-Service Continuity Management» auch bei Störungen die unterbruchfreie Verfügbarkeit im Rahmen der im Service Level Agreement vereinbarten Verfügbarkeit gewährleistet werden. Bei Notfällen auftretende Unterbrüche muss der Betrieb mit dem «IT-Desaster Recovery» und Notfallplänen innerhalb der definierten Frist (maximale Ausfallzeit) wiederhergestellt werden. Bis zu Wiederherstellung stellt das Business Continuity Management eine Überbrückung mit allenfalls reduzierter Leistung für eine beschränkte Zeit sicher. Im Krisenfall ermöglichen alle zur Sicherstellung der Verfügbarkeit ergriffenen Massnahmen eine rasche Wiederherstellung eines Notfall- oder Normalbetriebs nach best effort.

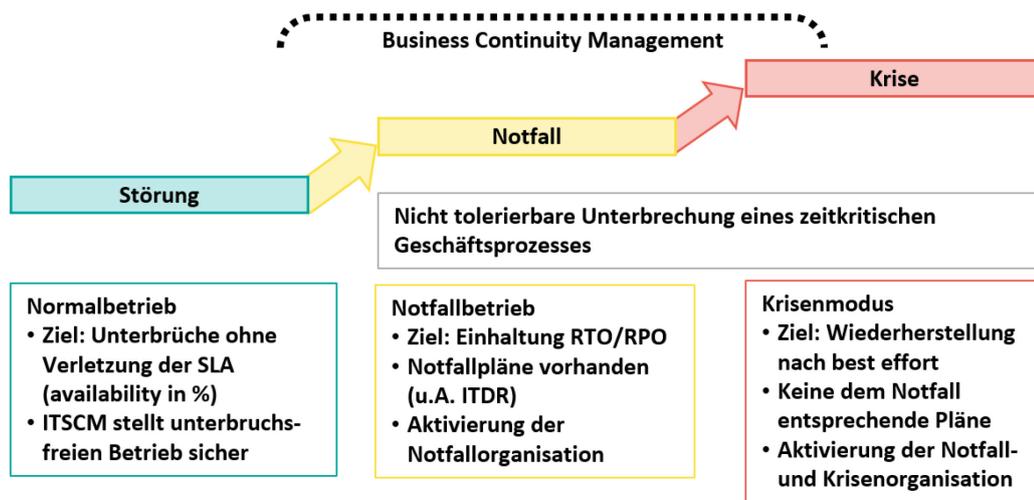


Abbildung 2 : Eskalationsstufen von Störung bis zur Krise, Abbildung der EFK basierend auf BSI-Standard 200-4 CD 2.0

## Beurteilung

Positiv ist, dass MeteoSchweiz mit allen Kunden Vereinbarungen abschliesst, periodisch formelle Gespräche und Umfragen zur Kundenzufriedenheit durchführt und diese gemäss den Stichproben durchwegs gut ausgefallen sind.

Kritisch hingegen ist, dass dort, wo keine messbaren Anforderungen mit Kunden vereinbart sind, die Anforderungen an die Geschäftsprozesse, Fachanwendungen und IKT-Mittel nicht konsequent abgeleitet werden können. Wenn Kunden zwingend auf Verfügbarkeits-, Integritäts- oder Vertraulichkeitsanforderungen angewiesen sind, müssten sie mit MeteoSchweiz konkrete Leistungsvereinbarungen abschliessen. Bei Untererfüllung der Anforderungen entstehen Risiken für die Kunden, bei Übererfüllung möglicherweise unnötige Mehraufwände für MeteoSchweiz.

### Empfehlung 4 (Priorität 2)

Die EFK empfiehlt MeteoSchweiz, messbare Anforderungen (Key Performance Indicators) zu Verfügbarkeit, Integrität und Vertraulichkeit aus dem gesetzlichen Auftrag abzuleiten und festzulegen, resp. diese mit Schlüsselkunden zu vereinbaren. Diese Anforderungen müssen als Zielwerte für RZPlus verwendet werden.

*Die Empfehlung ist akzeptiert.*

### **Stellungnahme MeteoSchweiz**

MeteoSchweiz hat für die Flugwetter-Dienstleistungen bereits Schlüsselindikatoren (KPI) erarbeitet. Auf dieser Basis werden die KPI für die weiteren Dienstleistungen der MeteoSchweiz festgelegt und wo sinnvoll mit den Schlüsselkunden abgestimmt.

## **3.2 Die durchgängige Ableitung von Informationssicherheitskriterien ist erst im Aufbau**

Damit RZPlus eine «angemessene Informationssicherheit»<sup>16</sup> konzipieren und umsetzen kann, sind konkrete Anforderungen an die geschäftskritischen Fachanwendungen und IKT-Systeme notwendig. Diese umfassen mindestens die Verfügbarkeit (siehe Glossar), die Datenintegrität und die Vertraulichkeit. MeteoSchweiz ist eine kritische Infrastruktur und daher sind insbesondere die Verfügbarkeitsanforderungen hoch. Anforderungen an die Integrität kommen gemäss erster Übersicht von RZPlus weniger häufig vor und solche an die Vertraulichkeit nur selten.

MeteoSchweiz hat die Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit bereits vor RZPlus aus unterschiedlichen Blickwinkeln analysiert und dokumentiert. Konkrete Vereinbarungen mit Kunden (vgl. Kap. 3.1) sind dazu nur eine Quelle. Eine weitere ist die sogenannte Liste Rot, in der rund zwanzig geschäftskritische und Safety-relevante Dienstleistungen aufgeführt sind. Die einzelnen Quellen bieten Hinweise für RZPlus, sind aber nicht miteinander verknüpft und nicht immer konsistent. Eine durchgängige Ableitung der Sicherheitsanforderungen aus Compliance-Anforderungen (Verträge, regulatorische Anforderungen etc.) über Geschäftsprozesse bis zu einzelnen Fachanwendungen und IKT-Systemen ist erst im Aufbau.

Im Rahmen eines Business-Continuity-Management-Projektes hat MeteoSchweiz ihre relevanten Dienstleistungen festgelegt und Massnahmen umgesetzt. Mit diesen können Unterbrüche wegen Notfällen<sup>17</sup> für begrenzte Zeit entweder überbrückt, oder zumindest eine reduzierte Leistungserbringung sichergestellt werden. Entgegen den Erwartungen von RZPlus stehen aus dem BCM-Projekt nur für wenige Fachanwendungen die konkreten Informationssicherheitsanforderungen zur Verfügung. Das Programm ist aber auf diese Vorgaben angewiesen, um angemessene Verfügbarkeit, Integrität und Vertraulichkeit der Cloud-Plattform zu konzipieren, umzusetzen und zu betreiben.

Am Programmausschuss vom 18. April 2023 hat RZPlus als eines von drei Top-Risiken gemeldet, dass die Geschäftsvorgaben an Ausfallsicherheit nicht final sind. Um den Programmfortschritt nicht zu gefährden, geht das Programm pragmatisch zweispurig vor und hat zusätzlich einen Klärungsprozess angestossen.

- Einerseits ermittelt RZPlus anhand der vielen Einzelinformationen, welchen Anforderungen die Cloud-Plattform mindestens genügen muss. Dementsprechend wird die Cloud-Plattform konzipiert, aufgebaut und betrieben.
- Andererseits erarbeitet RZPlus Architekturmuster für Fachanwendungen, die unterschiedliche Informationssicherheitsniveaus sicherstellen. Sobald die konkreten

<sup>16</sup> Siehe Glossar unter «Informationssicherheit».

<sup>17</sup> Notfälle können durch Ausfall von Gebäuden, Fachanwendungen, IKT-Systemen oder Personal verursacht werden. Siehe auch Exkurs zu «Verfügbarkeit» in Kap. 3.1.

Sicherheitsanforderungen durchgängig bzw. ganzheitlich ermittelt wurden, beraten Cloud-Spezialisten die Fachanwendungsverantwortlichen bei der Auswahl des geeigneten Architekturmusters für die Migration in die Cloud.

- Ergänzend zu den beiden genannten Massnahmen hat RZPlus einen Klärungsprozess angestoßen, welche Anforderungen an das IT-Service Continuity Management, das IT-Disaster Recovery und das Business Continuity Management gestellt werden. Das betrifft nicht nur die reine Verfügbarkeit in % pro Jahr oder die maximale Ausfallzeit in Stunden, sondern auch qualitative Mindestanforderungen, beispielsweise die minimale Häufigkeit von Messwerten oder die maximale räumliche Auflösung bei der Berechnung von Wettermodellen.

Bis zum Abschluss der Prüfung blieb offen, wie die durchgängige Ableitung der Anforderungen aus Verträgen, Business-Impact-Analysen, der Liste Rot und weiteren Quellen auf konkrete Informationssicherheitskriterien für die einzelnen Fachanwendungen erfolgen soll.

### **Beurteilung**

Es besteht ein erhebliches Risiko, dass von RZPlus geplante Informationssicherheitsmassnahmen schlussendlich nicht den tatsächlichen Bedürfnissen der Kunden entsprechen. Betreffend Verfügbarkeit gilt dasselbe für IT-Service Continuity, IT-Disaster Recovery und Business Continuity Management, die während der gesamten Programmlaufzeit parallel zu den Fachanwendungsmigrationen angepasst werden müssen.

Der von RZPlus eingeschlagene Lösungsansatz ermöglicht vorerst die Weiterarbeit in den Projekten. Bevor aber Fachanwendungen den Migrationsprozess in die Cloud beginnen können, müssen die konkreten Informationssicherheitsanforderungen definiert und das entsprechende Architekturmuster abgeleitet sein. Dabei sind Abhängigkeiten zwischen Fachanwendungen zu berücksichtigen, damit in einer Prozesskette nicht ein schwaches Glied mit zu tiefen Anforderungen den Gesamtprozess gefährdet.

Zu bemängeln ist, dass kein durchgängiger Prozess zur Ermittlung der Sicherheitsanforderungen etabliert ist. Dieser ist notwendig und kann nicht alleine vom Programm RZPlus sichergestellt werden. Die Anforderungsermittlung müsste unternehmensweit erfolgen und in der Verantwortung der Dienstleistungs-, Produkte- oder Geschäftsprozess-Verantwortlichen liegen. Als Grundlage dafür ist ein einheitliches Verständnis von Business Continuity, IT-Service Continuity Management und verwandten Themen notwendig. Erfahrungsgemäss ist dabei die konsequente Ausrichtung an einem etablierten Standard hilfreich, wie beispielsweise dem BSI 200-4 «Business Continuity Management» des deutschen Bundesamtes für Sicherheit in der Informationstechnik.<sup>18</sup>

### **Empfehlung 5 (Priorität 2)**

Die EFK empfiehlt MeteoSchweiz, rasch einen durchgängigen Prozess zu etablieren, mit dem Anforderungen aus Vereinbarungen, Business-Impact-Analysen und der Liste Rot systematisch auf Informationssicherheitskriterien für Fachanwendungen und IKT-Systeme abgeleitet werden. Dieser Prozess muss sicherstellen, dass die Anforderungen in der Verantwortung von Kunden-, Dienstleistungs- oder Produkte-Verantwortlichen liegen.

<sup>18</sup> Website des Bundesamtes für Sicherheit in der Informationstechnik, Business Continuity Management Standard BSI 200-4 vom Mai 2023, abgerufen am 27. Juli 2023.

*Die Empfehlung ist akzeptiert.*

#### **Stellungnahme MeteoSchweiz**

MeteoSchweiz hat im 2023 zwei neue Prozesse zum Business Continuity Management entworfen ('Business-Impact-Analyse durchführen' sowie 'Business Continuity planen und BCM-Massnahmen umsetzen'). Zusammen mit dem bereits existierenden Prozess 'Kundenproduktportfolio steuern' besteht eine gute Grundlage für die Umsetzung der EFK Empfehlung im 2024.

#### **Empfehlung 6 (Priorität 1)**

Die EFK empfiehlt MeteoSchweiz, ihr Business Continuity Management zu aktualisieren und das IT-Service Continuity Management sicherzustellen. Dies insbesondere, um das RZPlus Top-Risiko von Betriebsausfällen rasch zu reduzieren bzw. die Resilienz der Leistungserbringung bei einem Ausfall zu gewährleisten.

*Die Empfehlung ist akzeptiert.*

#### **Stellungnahme MeteoSchweiz**

MeteoSchweiz hat die Notwendigkeit einer Aktualisierung ihres Business Continuity Managements und der Sicherstellung des IT Service Continuity Managements ebenfalls erkannt und im Rahmen des Entwicklungsrahmens für 2025/26 entsprechende personelle Ressourcen beantragt. Aus bestehenden Mitteln sollen in den Jahren 2024/25 die existierenden Grundlagen aktualisiert und erweitert werden. Dazu wird eine externe Unterstützung für mind. 24 Monaten ab Januar 2024 beigezogen. Das zugehörige Beschaffungsverfahren steht zum Zeitpunkt der Stellungnahme kurz vor Abschluss.

## 4 Programm- und Projektsteuerung

### 4.1 Das Programm wird gut gesteuert und ist auf Kurs, ungeachtet der verspäteten Projekte

Für RZPlus wurde vom Parlament ein Verpflichtungskredit von 34,3 Millionen Franken gesprochen, der in zwei Tranchen zugänglich gemacht wird. Die erste Tranche hat das Parlament bereits freigegeben. Die zweite Tranche wird nur dann vom Bundesrat freigegeben, wenn RZ Campus und die Cloud bei AWS erfolgreich in Betrieb genommen sowie erste Fachanwendungen in die Cloud migriert wurden. Ausserdem muss die übergeordnete Zielerreichung aufgrund des Arbeitsfortschrittes und der Entwicklungen im Umfeld nach wie vor realistisch sein.

Neben den einmaligen Aufwänden für das Programm hat das Parlament auch eine gestaffelte Erhöhung des jährlichen Globalbudgets für Personal- und Sachleistungen genehmigt.

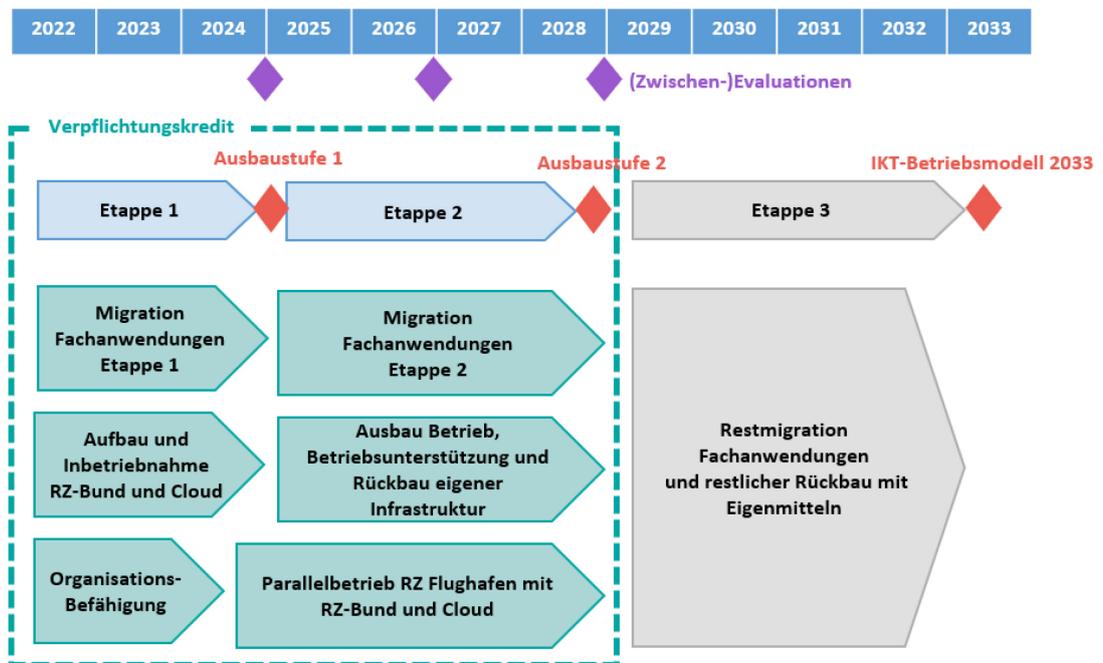


Abbildung 3: Etappierung von RZPlus gem. Bundesratsbeschluss vom 8. September 2021 (Darstellung der EFK basierend auf der Botschaft zum Verpflichtungskredit)

#### Programmsteuerung und -fortschritt

Das Programm RZPlus besteht aus drei Projekten: Inbetriebnahme RZ Campus, Inbetriebnahme Cloud, sowie IT-Governance & Migration Fachanwendungen. Alle drei sind gegenüber der Planung von 2021 um rund ein Jahr in Verzug. Die Ursachen liegen primär ausserhalb des Einflussbereiches von RZPlus bzw. MeteoSchweiz:

- Die Inbetriebnahme Cloud ist verspätet, weil es Einsprachen zum Vergabeentscheid des DTI bei der WTO Public Cloud gegeben hat.

- Es fehlen Cloud-Spezialisten zur Unterstützung der Cloud-Einführung. Da deren Beschaffung auf Bundesebene abgebrochen wurde, muss MeteoSchweiz dies selber in die Hand nehmen.
- Längere Verhandlungen und Abklärungen haben die Unterzeichnung des Dienstleistungsvertrages für RZ Campus mit dem BIT erheblich verzögert.
- Die Verzögerungen der beiden Plattformprojekte und der Beschaffung von Cloud-Spezialisten haben zu einer Verschiebung des Projektes IT-Governance & Migration Fachanwendungen geführt.

Aufgrund der Programm-Roadmap und des kritischen Pfades sieht der Programmleiter trotzdem keine Gefährdung des Endtermins. Auch der Rückbau des Rechenzentrums am Flughafen Zürich sollte termingerecht auf Ende des Mietvertrages möglich sein.

Für den Fall, dass nicht alle geschäftskritischen Fachanwendungen bis zum Programmende Cloud-fähig migriert werden können, hat MeteoSchweiz einen «Plan B» entwickelt. Die betroffenen Fachanwendungen würden weitgehend unverändert in einen gesonderten Teil der Cloud verschoben. Dadurch könnte die Georedundanz bis Programmende sichergestellt werden. Für diese Anwendungen würden die Optimierung der Ausfallsicherheit und der Betriebsprozesse sowie die Reduktion der Betriebskosten nicht erreicht werden.

### **Projektübergreifende Programm- und Ressourcensteuerung etabliert**

MeteoSchweiz führt ein Projektportfolio, um die personellen und finanziellen Ressourcen der verschiedenen Projekte bzw. Programme zu steuern. Der entsprechende Steuerungsprozess des Projektportfolios ist dokumentiert und wird halbjährlich durchlaufen.

Entsprechend dem Projektportfolio und der sogenannten Heatmap Ressourcenbedarf verfügt das Programm RZPlus 2023 über die erforderlichen internen Personalressourcen. Das heisst, die Zuteilung interner Projektmitarbeitenden ist zwischen den Abteilungsleitenden und dem Programmleiter verbindlich vereinbart. Die Planung für 2024 findet im zweiten Halbjahr 2023 statt.

### **Programm-Governance**

Die Programm-Governance ist etabliert. Die Steuerungs- und Koordinationsmeetings finden regelmässig statt und wesentliche Informationen werden in geeigneten Werkzeugen festgehalten (Confluence, Jira, Protokolle).

Bereits zu Beginn des Programms hat MeteoSchweiz festgestellt, dass es viele Abhängigkeiten innerhalb des Programms und zu anderen MeteoSchweiz-Projekten gibt und diese in einem Projektabhängigkeitsdiagramm ansatzweise dargestellt. Im März 2023 hat MeteoSchweiz einen Workshop mit über 20 Mitarbeitenden durchgeführt, um die Abhängigkeiten mit anderen strategischen oder dringlichen Projekten von MeteoSchweiz zu erheben und auf der Zeitachse darzustellen.

Um die Migration der rund 300 geschäftskritischen Fachanwendungen zu steuern und zu koordinieren hat MeteoSchweiz ein Domänenmodell entwickelt. In diesem sind die Fachanwendungen zu Anwendungsgruppen zusammengefasst und diese wiederum zu Geschäftsprozessen. Das Domänenmodell will MeteoSchweiz zudem als Steuerungsinstrument für die Fortschrittmessung der Planungen und der Modernisierungsfortschritte nutzen.

### Beurteilung

Die Programmsteuerung von RZPlus ist gut und die Programmleitung reagiert auf interne und externe Risiken und Probleme. Die Programm-Governance, das Projektportfoliomanagement und das Ressourcenmanagement sind geeignet zur Unterstützung der Programmsteuerung. Entscheidungsgrundlagen, Anträge und Entscheide werden angemessen dokumentiert und kommuniziert.

Externe Einflüsse haben zu Verzögerungen und Mehraufwänden in allen drei Projekten des Programms geführt, ohne dass die Programmziele (Umfang, Termine, Kosten) konkret gefährdet wären. Positiv ist zu werten, dass die Verantwortlichen von RZPlus und MeteoSchweiz jeweils rasch die möglichen Schritte eingeleitet haben. Dies waren beispielsweise Neuplanungen oder die Anstellung eines Experten für die Beschaffung der benötigten Cloud-Spezialisten in Eigenregie.

MeteoSchweiz hat erkannt, wie wichtig das Management der Abhängigkeiten zwischen allen Programmen und Projekten ist. Einerseits bestehen gegenseitige inhaltliche Abhängigkeiten mit RZPlus, andererseits müssen Ressourcen und Prioritäten bei konkurrenzierenden Bedürfnissen zugewiesen werden. Das von MeteoSchweiz erarbeitete «Domänenmodell» ist zweckmässig. Es ist ziel- und entscheidungsgerecht aufgebaut und sollte bald die Steuerung und Überwachung der Fachanwendungsmigrationen unterstützen.

Das Projekt IKT-Governance & Migration Fachanwendungen ist am stärksten von den Verzögerungen betroffen. Vorausschauend hat die Programm- und Projektleitung einen «Plan B» entwickelt, falls wider Erwarten nicht alle geschäftskritischen Fachanwendungen bis zum Programmende in die Cloud migriert werden können. Sollte dieser Ausweichplan notwendig werden, müssen allerdings Mehrkosten bzw. fehlende Einsparungen in Kauf genommen werden.

## 4.2 RZPlus und der unternehmensweite Kulturwandel sind aufeinander angewiesen

RZPlus hat Auswirkungen auf das ganze Amt MeteoSchweiz. Die erfolgreiche Transformation zu einer agilen, primär Cloud-basierten Informatik hängt davon ab, ob die gesamte Organisation diese Transformation mitvollzieht. Betroffen sind auch Rollen ausserhalb der Informatik, insbesondere die Produkt-, Fach- und Anwendungsverantwortlichen sowie die BCM-Verantwortlichen. RZPlus erarbeitet im Projekt IT-Governance und Migration Fachanwendungen die neue IT-Governance mit Aufgaben, Kompetenzen und Verantwortlichkeiten für die betroffenen Rollen. Bereits im Programmauftrag RZPlus ist definiert, dass ausserhalb der Programmorganisation ein eigenständiges Projekt die unternehmensweite Transformation steuern und verantworten muss.

Auch die Notwendigkeit eines durchgängigen Prozesses zur Ermittlung von Informationssicherheitsanforderungen an Fachanwendungen (siehe Kapitel 3.2) und die von den Fachverantwortlichen gesteuerte Migration der Fachanwendungen erfordert eine Anpassung der Governance und der internen Prozesse.

### Beurteilung

MeteoSchweiz durchläuft de facto einen tiefgreifenden Veränderungsprozess und Kulturwandel, der die ganze Organisation umfasst. Der Erfolg von RZPlus hängt massgeblich davon ab, dass sich die unternehmensweiten Prozesse und die Governance sowie der

Kulturwandel im Gleichtakt entwickeln. Damit der Kulturwandel Erfolg hat, muss er wie vorgesehen von einer eigenständigen Projektorganisation vorangetrieben und durch Geschäftsleitung und Management unterstützt werden.

Es besteht die Gefahr, dass RZPlus Entwicklungen anstösst und deshalb auch gleich die Verantwortung dafür übernehmen soll. Der Vorteil ist ein geringer Koordinationsaufwand, weil alles aus einer Hand kommt. Der Nachteil ist eine drohende Überlastung des Programms und im schlimmsten Fall eine «Entkoppelung» von Programm und Stammorganisation.

Letztlich muss die Geschäftsleitung das Zusammenspiel von RZPlus und dem Projekt Kulturwandel steuern. Positiv ist, dass zwei Geschäftsleitungsmitglieder im Programmausschuss RZPlus vertreten sind. Sie können Handlungsbedarf in die Geschäftsleitung tragen. Der Erfolg von RZPlus und dem von MeteoSchweiz beabsichtigten Kulturwandel hängt von einer ganzheitlichen Verantwortung und Steuerung des unternehmensweiten Veränderungsprozesses ab.

#### **Empfehlung 7 (Priorität 2)**

Die EFK empfiehlt der Geschäftsleitung von MeteoSchweiz sicherzustellen, dass die Koordination von RZPlus und dem Projekt zur Steuerung des Kulturwandels durch eine übergeordnete Instanz gesteuert wird. Die Aufgaben und Verantwortlichkeiten sind eindeutig zuzuordnen.

*Die Empfehlung ist akzeptiert.*

#### **Stellungnahme MeteoSchweiz**

MeteoSchweiz versteht die Notwendigkeit einer übergeordneten Steuerung des Kulturwandels. Entsprechende Aktivitäten wurden bereits eingeleitet. Aufgaben und Verantwortlichkeiten werden jedoch (auch aufgrund des bevorstehenden Wechsels in der HR-Leitung) erst im Verlauf des 2024 definitiv festgelegt.

### **4.3 Die Budgeteinhaltung ist unsicher**

Derzeit kann MeteoSchweiz nicht abschätzen, ob der Verpflichtungskredit von 34,3 Millionen Franken und die Erhöhung der jährlichen Globalbudgets ausreichen werden, um die Programmziele zu erreichen. Folgende Unsicherheitsfaktoren erschweren die Beurteilung:

- Bis Ende August 2023 müssen die Applikationsportfolio-Manager die Kosten der Modernisierung der Fachanwendungen schätzen. Die bisherigen Ergebnisse zeigen einen Mehrbedarf von rund 5 Millionen Franken, was noch verifiziert werden muss. Vor allem muss geklärt werden, welche Aufwände auf Versäumnisse im Lifecycle-Management zurückzuführen sind, die nicht von RZPlus getragen werden dürfen.
- Weil Cloud-Spezialisten zur Unterstützung der Anwendungsverantwortlichen fehlen (siehe Kap. 4.1), sind die Aufwandschätzungen für die Cloud-Migrationen noch nicht bestätigt.
- Mehraufwände für die Beschaffung von Cloud-Spezialisten durch MeteoSchweiz und möglicherweise höhere Tagessätze als bei der abgebrochenen Beschaffung auf Bundesebene.
- Ankündigung des BIT für höhere Preise für RZ Campus und die Datenkommunikation nach Ablauf des Dienstleistungsvertrags 2023 bis 2025.

- Folgekosten, falls nach Ablauf des Abrufs aus der WTO Public Cloud per Ende 2025 oder des WTO-Rahmenvertrages per Ende 2028 neue Preise gelten.

Ebenso kann MeteoSchweiz noch nicht abschätzen, ob die Erhöhung des Globalbudgets tatsächlich ausreichen wird, um den ausfallsicheren Betrieb zu garantieren. Das Projekt zum Aufbau der notwendigen Betriebsprozesse befindet sich noch in der Initialisierungsphase und die Aufwandschätzungen werden sobald möglich mit den Cloud-Spezialisten verifiziert.

Das Generalsekretariat des Eidgenössischen Departements des Innern ist über die verschiedenen laufenden Abklärungen zur Verifikation des Budgetbedarfs informiert.

#### **Beurteilung**

Aufgrund der frühen Projektphasen und noch in Arbeit befindlichen Aufwandschätzungen konnte MeteoSchweiz keine definitive Finanzplanung erstellen. Bis die Aufwandschätzungen abgeschlossen sind, besteht das Risiko, dass das Programmbudget und der Globalkredit für Personal- und Sachaufwände nicht ausreichen wird. Da RZPlus an den nötigen Abklärungen und Verifikationen arbeitet, verzichtet die EFK auf eine Empfehlung.

## 4.4 Der Risikomanagementprozess und das Qualitäts- und Risikomanager-Reporting werden noch verfeinert

Während der Prüfung hat der Programmleiter den Risikomanagementprozess weiterentwickelt. Die Projektleiter führen ihre Risiken in einer Exceltabelle. Diese Daten werden in eine Applikation zur Erstellung einer Risikoübersicht importiert. Damit erstellt der Programmleiter eine Riskmap, welche die Risiken übersichtlich gruppiert, sowie die Abhängigkeiten und Risikostufen (Ampelfarben) aufzeigt.

Zusätzlich hat der Programmleiter die Risiken und Massnahmen im Planungs- und Managementwerkzeug Jira für agil geführte Projekte erfasst. Dieses ist der operative Dreh- und Angelpunkt für die Steuerung und Führung der Projekte. Bei den Massnahmen hat der Programmleiter die Verantwortlichen zwischenzeitlich fast vollständig zugeteilt, bei den Risiken fehlen sie noch.

Alle zwei Wochen bespricht der Programmleiter die Risiken und Massnahmen anlässlich des sogenannten Action Meetings mit den Projektleitern und Schlüsselpersonen; alle ein bis zwei Wochen mit dem Delegierten des Programmauftraggebers.

Der Programmleiter aktualisiert die Programmriskiken monatlich im IKT-Cockpit. Sie sind referenziert und abstimmbare mit der Riskmap, Jira und den Exceltabellen.

#### **Beurteilung**

Die Dokumentation zum Risikomanagement hat der Programmleiter während der Prüfungsdurchführung aufgrund von Hinweisen der EFK rasch verbessert. Es gibt noch Optimierungspotenzial bei der formellen Zuteilung der Risikoeigner und der Ergebnisprotokollierung des Traktandums «Risiken und Massnahmen» anlässlich der Action Meetings. Angesichts der bereits getroffenen Verbesserungen verzichtet die EFK auf eine Empfehlung. Sie erwartet aber die konsequente Erfassung der Verantwortlichen für Risiken und Massnahmen.

MeteoSchweiz hat einen externen Spezialisten mit der Rolle «Programm Qualitäts- und Risikomanager» (QRM) beauftragt. Er erfüllt diese gemäss Beschreibung HERMES und leistet seine Arbeiten gemäss dem QRM-Konzept von MeteoSchweiz. Darin sind die Prozesse und Lieferobjekte aus seiner Arbeit festgehalten.

Laut HERMES ist der externe QRM befugt, die für die Beurteilung des Programms benötigten Informationen einzuholen. Er hat direkten Zugang zu allen Programm- und Projektbeteiligten. Gemäss dem QRM-Konzept steht der QRM an den Programmausschusssitzungen für Auskünfte und Risikodiskussionen zur Verfügung. In der Praxis wurde der QRM bisher nie an eine Ausschusssitzung eingeladen und erhielt auch die Traktandenliste und die dazugehörige Präsentation nicht. Nach einem Hinweis der EFK hat der Programmausschuss an der Sitzung vom 6. Juli 2023 entschieden, dass der QRM künftig online dem Traktandum «QRM-Bericht» beiwohnen wird.

Die QRM-Berichte werden erstellt und decken die Anforderungen von HERMES mit einer Ausnahme ab. Über die «Umfassende Beurteilung der Prozesse der Projektsteuerung, Projektführung und Projektabwicklung bei allen Projektpartnern» berichtet der QRM nicht in der erforderlichen Tiefe.

### **Beurteilung**

Die QRM-Berichte geben eine gute unabhängige Aussensicht über das Programm RZPlus. Informationen über die wesentlichen Prozesse im Programm wie Risiko- und Qualitätsmanagement erachtet die EFK als wichtig. Diesen Teilaspekten wird noch zu wenig Gewicht beigemessen. Sie erwartet, dass MeteoSchweiz diese vereinbarte Leistung konsequent einfordert und der QRM darüber berichtet.

MeteoSchweiz hat dem QRM mittlerweile die Kompetenz «Teilnahme am Traktandum QRM-Bericht» zugestanden, was weiterhin nicht den vollen Kompetenzen seiner Rolle nach HERMES entspricht. Da MeteoSchweiz bereits gehandelt hat, verzichtet die EFK auf eine Empfehlung. Sie weist jedoch darauf hin, dass der QRM künftig die Möglichkeit haben muss, selber anhand der vorgängigen verschickten Traktanden und Präsentation über seine Teilnahme an den Programmausschusssitzungen zu entscheiden.

## 5 Statusübersicht des Bereichs Digitale Transformation und IKT-Lenkung

Die letzte während der Prüfung verfügbare DTI-Statusübersicht stammt vom 31.12.2022. RZPlus hat darin berichtet, dass die Initialisierungsphasen für alle drei Projekte gestartet wurden.

	Status 30.6.2022	Status 31.12.2022	Tendenz
Gesamt	▲	▲	→
Ergebnisse	●	▲	↗
Kosten	▲	▲	↘
Termine	▲	▲	↗
Personal	■	▲	→
Risikowert	<b>79</b> (gross bis sehr gross)	<b>64</b> (bedeutend)	n. a.

Darstellung der EFK basierend auf dem DTI-Schlüsselprojekt Statusübersicht RZPlus vom 31. Dezember 2022

Die folgenden drei Top-Risiken wurden genannt:

- Verschiebung des Umzugs in ein Bundesrechenzentrum um zwei Jahre: Dieses Risiko ist eingetroffen wegen Verzögerungen bei der Ausarbeitung der Dienstleistungsvereinbarung für das Rechenzentrum Campus.
- Mehr Betriebsunterbrüche: Als Massnahme wurde die konsequent sequentielle Inbetriebnahme der einzelnen Plattformen vorgesehen. Im ersten Halbjahr 2023 wurden weitere risikomindernde Massnahmen zur Umsetzung vorgesehen (Aufbau Betriebscockpit und IT-Service Continuity Management).
- Hohe oder nicht kalkulierbare Betriebskosten für die Cloud-Nutzung: Als Massnahme wurde eine Kostentransparenz bei den Betriebskosten vorgesehen. Die dazu notwendigen Prozesse werden im Rahmen der Inbetriebnahme Cloud aufgebaut.

### Die Statusübersicht per 31. Dezember 2022 ist teils noch fehlerhaft

Das Berichtswesen von MeteoSchweiz ist dreistufig aufgebaut:

- Interne Programmstatusberichte (monatlich)
- Aus dem IKT-Cockpit erstellter Statusbericht (quartalsweise)
- Teilbericht für die Statusübersicht DTI (halbjährlich).

Die EFK hat die verschiedenen Berichte abgestimmt, um festzustellen, ob die Zahlen und Inhalte der Statusübersicht DTI per 31. Dezember 2022 richtig sind. Dies war der Fall. Einzige Ausnahme war der Status «Kosten», der in der DTI-Übersicht zu schlecht rapportiert wurde (gelb statt grün).

Bei den Terminen hat die EFK drei Fehler identifiziert. Der Termin der Projektinitialisierung wurde in allen drei Berichten jeweils falsch angegeben. Die Meilensteintermine fehlten im IKT-Cockpit. In der Statusübersicht DTI wurden sie falsch dargestellt. Dadurch war die Verspätung der Meilensteine nicht ersichtlich. Auch in den Kommentaren und Trendanalysen wurde nicht auf die Verspätung hingewiesen.

#### **Die Risikobewertung muss künftig weisungsgemäss erfolgen**

Das Risiko 1 «Umzug in ein Bundesrechenzentrum verzögert sich um 2 Jahre» ist eingetreten. Entsprechend der Weisung P038 dürfen eingetretene Risiken nicht mehr auf der Statusübersicht DTI aufgeführt werden. Sie wirken sich als Probleme auf die Statusampeln aus. Im IKT-Cockpit per 31. Dezember 2022 hingegen hat MeteoSchweiz das Risiko 1 korrekterweise nicht aufgeführt.

In der Statusübersicht DTI ist, verglichen mit dem IKT-Cockpit, bei den Risiken 2 «mehr Betriebsunterbrüche» und 3 «hohe nicht kalkulierbare Betriebskosten bei Cloud-Nutzung» der Risikowert insgesamt stimmig. Die einzelnen Werte für Eintretenswahrscheinlichkeit und Auswirkungsgrad hingegen wurden vertauscht aufgezeigt.

Per 31. Dezember 2022 hat bei den Risiken der rote Faden im Berichtswesen von MeteoSchweiz gefehlt. Zwischenzeitlich hat der Programmleiter diese Diskrepanz weitgehend behoben (siehe Kapitel 4.4).

#### **Beurteilung**

In der Berichterstattung per Dezember 2022 haben sich verschiedene Fehler und Ungeheimheiten eingeschlichen. Die EFK hat das Verbesserungspotenzial mit dem Programmleiter besprochen und dieser hat noch während der Prüfung Massnahmen und Korrekturen umgesetzt. Deshalb verzichtet die EFK auf eine Empfehlung.

# Anhang 1: Rechtsgrundlagen

## **Bundesbeschlüsse**

---

21.062 – Bundesbeschluss über einen Verpflichtungskredit zum Aufbau einer ausfallsicheren Rechenleistung und der dazu nötigen Transformation der IKT von MeteoSchweiz, Beschluss vom 2. März 2022, BBl 2022 777

---

21.062 – Bundesbeschluss über einen Verpflichtungskredit zum Aufbau einer ausfallsicheren Rechenleistung und der dazu nötigen Transformation der IKT von MeteoSchweiz (Entwurf) vom 8. September 2021, BBl 2021 2162

---

## **Botschaften**

---

21.062 – Botschaft zu einem Verpflichtungskredit zum Aufbau einer ausfallsicheren Rechenleistung und der dazu nötigen Transformation der IKT von MeteoSchweiz vom 8. September 2021, BBl 2021 2161

---

## **Weisungen**

---

P038 – Berichterstattung über die DTI-Schlüsselprojekte des Bundes

---

## Anhang 2: Abkürzungen

AWS	Amazon Web Services
BCM	Business Continuity Management
BIT	Bundesamt für Informatik und Telekommunikation
BK	Bundeskanzlei
CSCS	Swiss National Supercomputing Centre
DTI	Bereich Digitale Transformation und IKT-Lenkung
EFK	Eidgenössische Finanzkontrolle
ETH	Eidgenössische Technische Hochschule
IKT	Informations- und Kommunikationstechnologie
MeteoSchweiz	Bundesamt für Meteorologie und Klimatologie
QRM	Qualitäts- und Risikomanagement

## Anhang 3: Glossar

---

Bereich Digitale Transformation und IKT-Lenkung (DTI)	Der Bereich DTI sorgt für eine departementsübergreifende Sicht auf die Vorhaben, Mittel und Verwaltungsleistungen der digitalen Transformation und der IKT in der Bundesverwaltung. Es handelt sich um eine neue Zuständigkeit der Bundeskanzlei seit dem 1. Januar 2021.
Cloud Service Broker (CSB)	<p>Der CSB unterstützt Verwaltungseinheiten bei der Nutzung von Private- und Public-Cloud-Diensten. Er berät bei der Wahl der richtigen Cloud-Stufe für Anwendungen.</p> <p>Der zentrale CSB der Bundesverwaltung ist das Bundesamt für Informatik (BIT). Zusätzlich kann es weitere CSB geben, die die spezifischen Bedürfnisse einzelner Bundesämter abdecken.</p>
Cloud Service Provider (CSP)	Leistungserbringer für Cloud Services. Beispielsweise Microsoft, Amazon oder IBM.
Cloud-native	Cloud-native-Anwendungen sind darauf ausgelegt, die Vorteile einer Cloud-Architekturen voll zu nutzen. Sie zeichnen sich durch eine hohe Unabhängigkeit voneinander aus und profitieren von Cloud-Services (z. B. Services für georedundante Ausfallsicherheit). Cloud-native-Technologien unterstützen schnelle und häufige Änderungen, ohne die Servicebereitstellung zu beeinträchtigen. Sie ermöglichen skalierbare, flexible und belastbare Anwendungen. Bei Bedarf können Cloud-native-Anwendungen auch in einem Rechenzentrum (on-premise) betrieben werden.
Georedundanz	<p>Eine Anwendung oder ein IKT-System ist gleichzeitig an zwei Standorten vorhanden.</p> <p>Wie hoch die Ausfallsicherheit der beiden Systeme zusammen ist, hängt von der Betriebsart ab und nicht alleine von der Georedundanz (active/active, active/passiv, ...).</p>
HERMES	<p>eCH-0054: HERMES Projektmanagement-Methode</p> <p>HERMES ist die Projektmanagement-Methode für Informatik, Dienstleistung, Service und Geschäftsorganisationen und wurde von der schweizerischen Bundesverwaltung entwickelt. Die Methode steht als offener Standard vom Verein eCH allen zur Verfügung.</p>
IKT	Informations- und Kommunikationstechnik

---

Informationssicherheit	<p>Informationssicherheitskriterien sind Vertraulichkeit, Integrität und Verfügbarkeit. Je nach Definition sind Effektivität, Effizienz, Compliance und Zuverlässigkeit weitere Kriterien.</p> <p>Die «Angemessenheit» von Informationssicherheit ergibt sich aus der Gegenüberstellung von Auswirkungen bei Nicht-Erfüllung und den zur Sicherstellung notwendigen Aufwänden. Sobald es um die Einhaltung von Gesetzen, Verordnungen oder Verträgen geht, müssen die Anforderungen in der Regel ohne Kosten-/Nutzen-Abwägungen zwingend umgesetzt werden.</p>
Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)	<p>Wenn die Schutzbedarfsanalyse einen erhöhten Schutzbedarf ergibt, muss die Verwaltungseinheit basierend auf einer Risikoanalyse und ergänzend zum IKT-Grundschutz weitere Sicherheitsmassnahmen definieren und umsetzen. Das ISDS-Konzept<sup>19</sup> beinhaltet die Risikoanalyse, die Beschreibung der Sicherheitsmassnahmen sowie die verbleibenden Restrisiken.</p>
IT-Grundschutz der Bundesverwaltung	<p>Der IT-Grundschutz<sup>20</sup> legt die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich Informationssicherheit verbindlich fest.</p> <p>Die Umsetzung der Sicherheitsvorgaben und -massnahmen sind durch die verantwortlichen Verwaltungseinheiten zu dokumentieren und zu überprüfen. Neben der Verwaltungseinheit müssen auch alle beteiligten Leistungserbringer die sie betreffenden Anforderungen erfüllen.</p>
Jira	<p>Jira ist eine umfangreiche Anwendung für Projektmanagement, Aufgabenverwaltung, agiles Arbeiten und Service Management. Es fördert die Flexibilität und Transparenz innerhalb von Unternehmen, Teams und Projekten.</p>

<sup>19</sup> P042 – Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept).

<sup>20</sup> Si001 – IT-Grundschutz in der Bundesverwaltung.

Lage	<p>Differenziertere Unterscheidung von Lagen:</p> <p>Normale Lage: Situation, in der die ordentlichen Abläufe zur Bewältigung der anstehenden Aufgaben ausreichen.</p> <p>Besondere Lage: Situation, in der gewisse Aufgaben mit den ordentlichen Abläufen nicht mehr bewältigt werden können. Im Unterschied zur ausserordentlichen Lage ist die Tätigkeit der Behörden nur sektoriell betroffen. Typisch ist der Bedarf nach rascher Konzentration der Mittel und Straffung der Verfahren.</p> <p>Ausserordentliche Lage: Situation, in der in zahlreichen Bereichen und Sektoren die ordentlichen Abläufe nicht genügen, um die anstehenden Aufgaben zu bewältigen, beispielsweise bei Katastrophen und in Notlagen, die das ganze Land schwer in Mitleidenschaft ziehen, oder im Fall eines bewaffneten Konflikts.</p> <p>(Quelle: Bundesamt für Bevölkerungsschutz, Glossar der Risikobegriffe, Stand 29.04.2013)</p>
Maximale Ausfallzeit (RTO)	Die maximal zulässige Ausfallzeit eines Prozesses oder der benötigten Ressourcen.
Maximaler Datenverlust (RPO)	Maximales Alter, das verfügbare Daten haben dürfen, um zeitkritische Geschäftsprozesse nach einer Unterbrechung sinnvoll betreiben zu können.
normale Lage	Siehe «Lage»
on-premise	Rechen- und/oder Speicherleistung in einem standortgebundenen, physischen Rechenzentrum.
P038	Diese IKT-Vorgabe regelt sowohl den Prozess und die Termine für die Berichterstattung über den Stand der DTI-Schlüsselprojekte des Bundes zuhanden der parlamentarischen Oberaufsicht als auch den Umfang und den Detaillierungsgrad der für diese Berichterstattung zu liefernden Informationen.
Schutzbedarfsanalyse (Schuban)	Für jedes IKT-Projekt muss in der Initialisierungsphase eine Schuban <sup>21</sup> erstellt werden. Damit wird ermittelt, ob der IKT-Grundschutz ausreicht oder ob erhöhter Schutzbedarf besteht und ein ISDS-Konzept erarbeitet werden muss.

<sup>21</sup> P041 – Schutzbedarfsanalyse.

---

Verpflichtungskredit (VK)	VK im Sinne von Art. 10 Abs. 1 Finanzhaushaltverordnung (FHV) geben die Ermächtigung, für ein bestimmtes Vorhaben oder eine Gruppe gleichartiger Vorhaben bis zum bewilligten Höchstbetrag finanzielle Verpflichtungen einzugehen.
---------------------------	--

---

### **Priorisierung der Empfehlungen**

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).