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

Prüfung des DTI-Schlüsselprojektes Cloud Enabling Büroautomation

Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei

EFK-23740 | inkl. Stellungnahmen | 29. Februar 2024

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	104.23740
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch + 41 58 463 11 11

Inhaltsverzeichnis

Prüfung des DTI-Schlüsselprojektes Cloud Enabling Büroautomation

Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei

Das Wesentliche in Kürze

Das Projekt Cloud Enabling Büroautomation (CEBA) wurde 2019 initialisiert und wird durch den Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei geführt. Ziel ist, die derzeit auf den Arbeitsplatzsystemen der Bundesverwaltung eingesetzte Office Produktsuite «Microsoft Office LTSC Professional Plus 2021» durch «Microsoft Office 365» (M365) zu ersetzen. Die neue Version ist an die öffentliche Microsoft Cloud angebunden.

Die technische Durchführung des Projektes findet in zwei Teilprojekten bei IKT-Leistungserbringern des Bundes, dem Bundesamt für Informatik und Telekommunikation (BIT) sowie der Informatik des Eidgenössischen Departementes für auswärtige Angelegenheiten, statt. Das Projekt wurde 2022 als IKT-Schlüsselprojekt des Bundes eingestuft. Die Einstufung erfolgte nicht aufgrund des Volumens von 26,5 Millionen Franken, sondern aufgrund der Auswirkungen auf die Arbeitsweise der nahezu gesamten Bundesverwaltung.

Die Prüfungsergebnisse zeigen ein gemischtes Bild: Die Realisierung des Projektes schreitet mit leichten Verzögerungen voran, die Einführung in den Departementen ist ab 2024 vorgesehen. Das Projekt basiert auf der Annahme, dass ein lokaler Betrieb der Microsoft Office Produktpalette ab 2026 nicht mehr möglich ist.[1] Inzwischen gibt es Anzeichen, dass ein solcher länger möglich ist.[2] Dies ist durch das Projekt zu validieren. Die mit der Cloud-Nutzung einhergehenden, aus Sicht der Eidgenössischen Finanzkontrolle (EFK) teilweise signifikanten (Rest-)Risiken sind zum Prüfungszeitpunkt noch nicht abschliessend erhoben und akzeptiert worden. Auch fehlt teilweise ein gemeinsames Verständnis mit den späteren Nutzerinnen und Nutzern. Die möglicherweise veränderte Ausgangslage könnte dem Projekt zusätzliche Zeit verschaffen, um u. a. diese Situation zu bereinigen.

Die Risiken und die Steuerung des Dienstleisters sind vor der Einführung zu klären

Gemäss Roadmap von Microsoft werden die Support-Leistungen für die bestehende Office-Version ab 2026 eingestellt. Das Projekt basiert auf der Grundannahme, dass M365 eingeführt werden muss, da danach nur noch mit der Cloud integrierte, abonnementbasierte Installationen unterstützt werden. Das Projekt eröffnet den Departementen die Möglichkeit, auf die Cloud-basierte Lösung M365 zu wechseln. Zum Prüfungszeitpunkt waren auf einer Website des Herstellers Informationen verfügbar, gemäss denen ein weiteres Release der Microsoft Office-Suite zum einmaligen Bezug erfolgen soll. Dies würde die Grundlage für das Projekt verändern. Die EFK empfiehlt dem Bereich DTI, mit Microsoft zu klären, inwieweit und für wie lange mit diesem Release eine Lösung ohne Anbindung an die Cloud möglich bleibt. Je nach Ergebnis könnten Lösungsansätze möglich

[1] Siehe Roadmap von Microsoft: https://learn.microsoft.com/en-us/lifecycle/products/?products=office.

[2] Siehe FAQ-Webseite von Microsoft: https://support.microsoft.com/en-us/office/office-2021-and-office-ltsc-for-windows-and-mac-faq-d574cf0b-3ebc-42cf-9035-a3b837e0463c.

werden, die der Bundes-verwaltung mehr Zeit einräumen, sich auf die mit dem Gang in die Cloud verbundene veränderte Risikosituation einzustellen.

Der Stellenwert des Partners Microsoft verändert sich für die Bundesverwaltung durch die Einführung von CEBA: Wo ein Bezüger-Verhältnis zu einem Software-Lieferanten bestand, intensiviert sich nun eine Dienstleisterbeziehung. Daten der Bundesverwaltung, die zuvor auf eigenen Systemen gespeichert wurden, werden zum Dienstleister und seinen Subakkordanten übertragen. Dies verlangt nach einer Weiterentwicklung der Steuerung und Kontrolle des Dienstleisters. Insbesondere müssen die vertraglichen Zusicherungen und Sicherheitsmassnahmen durch den Bund kontrolliert werden. Hierzu fehlt derzeit noch ein abgestimmtes Konzept. Die EFK empfiehlt dem Bereich DTI, dieses unter Berücksichtigung der Zuständigkeiten der beteiligten Ämter zu erarbeiten und umzusetzen.

Restrisiken einer Cloud Nutzung sind bewusst einzugehen, der Parallelbetrieb ist kurz zu halten

Die mit der Cloud-Nutzung verbundenen Restrisiken wurden vom Projekt erhoben und mit Stand Ende Konzeptphase gegenüber Generalsekretärenkonferenz (GSK) und Bundesrat offengelegt. Abnahme und Freigabe vor Einführung durch den Bundeskanzler und den Delegierten DTI stehen noch aus. Da der Projekterfolg davon abhängt, dass die zuständigen Stellen die Restrisiken tragen, ist die Analyse unter Einbezug aller Departemente rasch zu finalisieren und abzunehmen. Wichtig ist, dass die Vollständigkeit und die möglichen Massnahmen breit abgestützt sind und damit auch ein gleiches Verständnis für die Restrisiken erreicht wird. Im Falle signifikanter Veränderungen sollten mindestens die zuvor informierten Instanzen GSK und Bundesrat erneut informiert werden.

Mit der Einführung von Microsoft Teams entstehen neue Doppelspurigkeiten: Die Ablösung der heute eingesetzten Telefonielösung «Skype for Business» erfolgt in einem eigenen Projekt mit eigenem Zeitplan ausserhalb von CEBA. Nach Angaben des DTI erfolgt dies, um die Komplexität von CEBA durch die über 70 Telefonie-Sonderlösungen beim Bund nicht weiter zu erhöhen. Beide Lösungen sollen zunächst parallel eingesetzt werden. Die EFK empfiehlt dem Bereich DTI, den Zeitraum dieses Parallelbetriebs möglichst kurz zu halten.

Die Infrastruktur der Bundesverwaltung darf nur kontrolliert geöffnet werden

Der Bezug von M365-Dienstleistungen aus der öffentlichen Microsoft Cloud erfordert eine automatisierte Öffnung der Netzwerkinfrastruktur der Bundesverwaltung. Um hierfür keine generellen Ausnahmen in Kraft zu setzen, hat DTI bestehende Weisungen ergänzt. In der Ergänzung wird der Grundsatz einer Öffnung «so viel wie nötig, aber so wenig wie möglich» festgeschrieben.

Unklar bleibt jedoch, wie dieser Grundsatz auf Einhaltung überprüft werden kann. Die EFK empfiehlt DTI festzulegen, wie sichergestellt wird, dass automatisierte Öffnungen der Infrastruktur des Bundes nicht über das minimal notwendige Niveau hinausgehen.

Stakeholder müssen adäquat in das Projekt eingebunden bleiben

Das Augenmerk ist auf den Eidgenössischen Datenschutz- und Öffentlichkeits-Beauftragten (EDÖB) zu richten. Dieser wurde im Rahmen der Abklärungen zu Daten- und Informationsschutz-Themen vom Projekt CEBA konsultiert. Es ist wichtig, dass das Projekt die vom EDÖB erhaltenen Rückmeldungen ausreichend berücksichtigt und weiterhin kontinuierlich abstimmt.

Audit du projet TNI clé Cloud Enabling Bureautique
Secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale

L'essentiel en bref

Le projet Cloud Enabling Bureautique (CEBA) a été lancé en 2019 et est dirigé par le secteur Transformation numérique et gouvernance de l'informatique (TNI) de la Chancellerie fédérale. L'objectif est de remplacer la suite de produits Office « Microsoft Office LTSC Professional Plus 2021 » actuellement utilisée pour les postes de travail de l'administration fédérale par « Microsoft Office 365 » (M365). La nouvelle version est reliée au nuage public de Microsoft.

La réalisation technique du projet s'effectue dans le cadre de deux sous-projets menés par des fournisseurs de prestations TIC de la Confédération, l'Office fédéral de l'informatique et de la télécommunication (OFIT) ainsi que la Division informatique du Département fédéral des affaires étrangères. Le projet a été classé comme projet informatique clé de la Confédération en 2022. Cette décision n'est pas due au volume de 26,5 millions de francs, mais à son impact sur le fonctionnement de la quasi-totalité de l'administration fédérale.

Les résultats de l'audit présentent un tableau mitigé : la réalisation du projet progresse avec de légers retards, le déploiement dans les départements est prévu à partir de 2024. Le projet repose sur l'hypothèse qu'une exploitation locale de la gamme de produits Microsoft Office ne sera plus possible à partir de 2026.[1] Entre-temps, certaines informations suggèrent qu'une telle exploitation sera possible plus longtemps.[2] Cela doit être validé dans le cadre du projet. Au moment de l'audit, les risques (résiduels) liés à l'utilisation des services en nuage, en partie significatifs du point de vue du Contrôle fédéral des finances (CDF), n'ont pas encore été définitivement évalués et acceptés. Il manque aussi parfois une compréhension commune avec les futurs utilisatrices et utilisateurs. Le possible changement de situation de départ pourrait donner plus de temps au projet, notamment pour remédier à cette situation.

Les risques et la gestion du prestataire doivent être clarifiés avant le déploiement

Selon la feuille de route de Microsoft, les prestations d'assistance pour la version d'Office existante cesseront à partir de 2026. Le projet repose sur l'hypothèse selon laquelle M365 doit être déployé, car seules les installations intégrées au nuage et basées sur un abonnement seront prises en charge par la suite. Le projet permet aux départements de passer à la solution M365 basée sur le nuage. Au moment de l'audit, des informations étaient disponibles sur un site web du fabricant, selon lesquelles une nouvelle version de la suite Microsoft Office serait disponible sous la forme d'un achat unique. Cet élément modifierait le fondement sur lequel repose le projet. Le CDF recommande au secteur TNI de clarifier avec Microsoft dans quelle mesure et pour combien de temps une solution sans connexion au nuage reste possible avec cette version. Selon les résultats, des solutions pourraient être

[1] Voir la feuille de route de Microsoft : https://learn.microsoft.com/fr-ch/lifecycle/products/?products=office.
[2] Voir la FAQ de Microsoft : https://support.microsoft.com/fr-fr/office/faq-sur-office-2021-et-office-ltsc-pour-windows-et-mac-d574cf0b-3ebc-42cf-9035-a3b837e0463c.

envisagées permettant à l'administration fédérale de disposer de plus de temps pour s'adapter aux nouveaux risques liés au passage à des services en nuage.

Le projet CEBA signifie un changement dans la position de Microsoft en tant que partenaire pour l'administration fédérale : une relation d'achat avec un fournisseur de logiciels devient désormais une relation plus étroite de fourniture de prestations. Les données de l'administration fédérale, auparavant enregistrées dans ses propres systèmes, seront transmises au prestataire et à ses sous-traitants. Cela nécessite un développement de la gestion et du contrôle du prestataire. En particulier, les garanties contractuelles et les mesures de sécurité doivent être contrôlées par la Confédération. Or, il n'existe pas encore de concept coordonné en la matière. Le CDF recommande au secteur TNI d'élaborer et de mettre en œuvre un tel concept en tenant compte des compétences des offices concernés.

Les risques résiduels liés à l'utilisation de services en nuage doivent être pris en compte en connaissance de cause et l'exploitation parallèle doit être limitée dans le temps

Les risques résiduels liés à l'utilisation des services en nuage ont été relevés dans le cadre du projet et présentés à la Conférence des secrétaires généraux (CSG) et au Conseil fédéral à la fin de la phase de conception. Le chancelier de la Confédération et le délégué TNI doivent encore en prendre connaissance et les valider avant le déploiement. Comme le succès du projet dépend de la prise en charge des risques résiduels par les services compétents, l'analyse doit être finalisée et validée rapidement, avec la participation de tous les départements. Il est important que l'ensemble des risques et des mesures possibles bénéficient d'un large soutien, ce qui permettra aussi d'aboutir à une définition commune des risques résiduels. En cas de modifications significatives, il conviendra à nouveau d'informer au moins les instances préalablement informées, soit la CSG et le Conseil fédéral.

L'introduction de Microsoft Teams crée de nouvelles redondances : le remplacement de la solution de téléphonie « Skype for Business » fait l'objet d'un projet distinct avec un calendrier propre, en dehors du projet CEBA. Selon le secteur TNI, il s'agit d'éviter de complexifier davantage le projet CEBA. En effet, la Confédération dispose de plus de 70 solutions de téléphonie spéciales. Dans un premier temps, les deux solutions seront donc exploitées en parallèle. Le CDF recommande au secteur TNI de limiter autant que possible la durée de cette exploitation parallèle.

L'infrastructure de l'administration fédérale ne doit être ouverte que de manière contrôlée

L'acquisition de prestations M365 basées sur le nuage public de Microsoft nécessite une ouverture automatisée de l'infrastructure réseau de l'administration fédérale. Afin de ne pas instituer d'exceptions générales en la matière, le secteur TNI a complété les directives existantes. Le complément établit le principe selon lequel l'infrastructure est ouverte autant que nécessaire, mais aussi peu que possible.

Les directives ne précisent toutefois pas comment le respect de ce principe sera vérifié. Le CDF recommande au secteur TNI de préciser comment il entend s'assurer que les ouvertures automatisées de l'infrastructure de la Confédération ne vont pas au-delà du minimum nécessaire.

Les parties prenantes doivent rester impliquées de manière adéquate dans le projet

Une attention particulière doit être portée au Préposé fédéral à la protection des données et à la transparence (PFPDT). Ce dernier a été consulté dans le cadre des clarifications relatives à la protection des données et à la sécurité des informations pour le projet CEBA. Il est important que le projet tienne suffisamment compte des retours d'information reçus du PFPDT et continue à se coordonner en permanence.

Texte original en allemand

Verifica del progetto chiave TDT «Cloud Enabling Büroautomation»

Settore Trasformazione digitale e governance delle TIC della Cancelleria federale

L'essenziale in breve

Il progetto «Cloud Enabling Büroautomation» (CEBA) è stato avviato nel 2019 ed è diretto dal settore Trasformazione digitale e governance delle TIC (settore TDT) della Cancelleria federale. Il suo obiettivo è sostituire il pacchetto Office «Microsoft Office LTSC Professional Plus 2021», in uso presso le postazioni di lavoro dell'Amministrazione federale, con il pacchetto «Microsoft Office 365» (M365). La nuova versione è collegata al cloud pubblico di Microsoft.

L'esecuzione tecnica del progetto si articola in due progetti parziali, affidati a due fornitori di prestazioni TIC della Confederazione, ossia l'Ufficio federale dell'informatica e della telecomunicazione (UFIT) e la divisione Informatica del Dipartimento federale degli affari esteri. Nel 2022 il progetto è stato classificato come progetto chiave TIC della Confederazione. Tale classificazione non è dovuta alla portata finanziaria, quantificata a 26,5 milioni di franchi, bensì alle ripercussioni che il progetto ha sul modo di lavorare di quasi tutti gli impiegati dell'Amministrazione federale.

I risultati della verifica mostrano un quadro eterogeneo: la realizzazione procede con lievi ritardi e l'introduzione nei dipartimenti è prevista a partire dal 2024. Il progetto parte dal presupposto che, dopo il 2026, l'esercizio a livello locale del pacchetto Microsoft Office non sarà più possibile.[1] Da alcune informazioni è emerso invece il contrario.[2] Ciò deve essere tuttavia appurato nel quadro del progetto. Al momento della verifica, alcuni rischi (residui) correlati all'utilizzo del cloud, in parte significativi secondo il Controllo federale delle finanze (CDF), non sono stati rilevati e accettati in maniera definitiva. Talvolta manca anche una definizione dei rischi comune ai futuri utenti. L'eventuale cambiamento della situazione iniziale consentirebbe di guadagnare tempo per risolvere anche questo problema.

Chiarire i rischi e la gestione del fornitore di servizi prima dell'introduzione

Secondo la roadmap di Microsoft, le prestazioni di supporto per l'attuale versione di Office cesseranno a partire dal 2026. Il progetto, che si fonda sull'ipotesi secondo cui è necessario introdurre M365 perché in seguito saranno supportate soltanto le installazioni abbonate e integrate nel cloud, offre ai dipartimenti la possibilità di passare alla soluzione M365 basata su cloud. Al momento della verifica, le informazioni disponibili sul sito Internet del fabbricante precisavano che una versione aggiornata del pacchetto Microsoft Office sarebbe disponibile come acquisto unico. Tale condizione modificherebbe le basi del progetto. Il CDF raccomanda al settore TDT di chiarire con Microsoft in che misura e per quanto tempo questa versione consenta ancora di utilizzare una soluzione senza

[1] Cfr. la roadmap di Microsoft: https://learn.microsoft.com/en-us/lifecycle/products/?products=office.

[2] Cfr. la pagina delle FAQ di Microsoft: https://support.microsoft.com/en-us/office/office-2021-and-office-ltsc-for-windows-and-mac-faq-d574cf0b-3ebc-42cf-9035-a3b837e0463c.

collegamento al cloud. A seconda della risposta potrebbero essere ipotizzabili soluzioni che concedono più tempo alla Confederazione per adattarsi alla mutata situazione di rischio derivante dal passaggio al cloud.

Il progetto CEBA cambia la posizione di Microsoft quale partner dell'Amministrazione federale: il rapporto di acquirente di software si trasforma in un rapporto di fornitore di servizi. I dati dell'Amministrazione federale, che prima erano salvati su sistemi propri, saranno trasmessi al fornitore di servizi e ai rispettivi subappaltatori. Ciò esige un perfezionamento della gestione e del controllo del fornitore di servizi. In particolare, la Confederazione deve controllare le garanzie contrattuali e le misure di sicurezza. Al momento manca un piano armonizzato in merito. Il CDF raccomanda al settore TDT di elaborarne uno e di attuarlo, tenendo conto delle competenze degli uffici coinvolti.

Assumere consapevolmente i rischi residui legati all'utilizzo del cloud e limitare la durata dell'esercizio parallelo

I rischi residui legati all'utilizzo del cloud sono stati rilevati nell'ambito del progetto e presentati alla Conferenza dei segretari generali (CSG) e al Consiglio federale alla fine della fase concettuale. Il cancelliere della Confederazione e il delegato TDT devono ancora effettuare il collaudo e l'approvazione prima dell'introduzione. Poiché la riuscita del progetto dipende dall'assunzione dei rischi residui da parte dei servizi competenti, l'analisi deve essere portata a termine rapidamente e approvata coinvolgendo tutti i dipartimenti. È importante che la totalità dei rischi e le possibili misure siano ampiamente accettate e che si giunga a una visione d'intenti comune riguardo ai rischi residui. In caso di cambiamenti importanti dovrebbero essere informate di nuovo almeno le istanze già informate in precedenza, vale a dire la CSG e il Consiglio federale.

L'introduzione di Microsoft Teams crea nuovi doppioni: la sostituzione della soluzione di telefonia «Skype for Business» ora in uso sarà realizzata mediante un progetto e delle scadenze propri, al di fuori del progetto CEBA. Secondo il settore TDT, questo modo di procedere evita di aumentare ulteriormente la complessità di CEBA, considerando il fatto che la Confederazione dispone di oltre 70 diverse soluzioni di telefonia. Inizialmente le due soluzioni dovranno essere utilizzate in contemporanea. Il CDF raccomanda al settore TDT di limitare, per quanto possibile, la durata dell'esercizio parallelo.

Consentire un'apertura soltanto controllata dell'infrastruttura dell'Amministrazione federale

L'acquisto delle prestazioni di servizi di M365 basate sul cloud pubblico di Microsoft Cloud richiede un'apertura automatizzata dell'infrastruttura di rete dell'Amministrazione federale. Per non dover introdurre eccezioni di carattere generale, il settore TDT ha integrato le istruzioni vigenti mediante un'aggiunta, secondo cui l'apertura deve avvenire secondo il principio «tanto quanto è necessario, ma il meno possibile».

Tuttavia, le istruzioni non specificano come verificare il rispetto di questo principio. Il CDF raccomanda al settore TDT di stabilire in che modo garantirà che l'apertura automatizzata dell'infrastruttura della Confederazione non superi il livello minimo necessario.

Continuare a coinvolgere adeguatamente gli interlocutori nel progetto

L'attenzione deve essere rivolta all'incaricato federale della protezione dei dati e della trasparenza (IFPDT), che è stato consultato nel quadro degli accertamenti sugli aspetti inerenti

alla protezione dei dati e delle informazioni per il progetto CEBA. È importante prendere sufficientemente in considerazione, nell'ambito del progetto, i riscontri ricevuti dall'IFPDT e continuare a consultare quest'ultimo.

Testo originale in tedesco

Audit of the DTI key project Cloud Enabling Office Automation

Digital Transformation and ICT Steering Sector of the Federal Chancellery

Key facts

The Cloud Enabling Office Automation (CEBA) project was launched in 2019 and is managed by the Digital Transformation and ICT Steering (DTI) Sector of the Federal Chancellery. The aim is to replace the Microsoft Office LTSC Professional Plus 2021 product suite currently in use on the Federal Administration's workstation systems with Microsoft Office 365 (M365). The new version is connected to the public Microsoft Cloud.

The technical implementation of the project is taking place in two subprojects with ICT service providers for the Confederation, the Federal Office of Information Technology, Systems and Telecommunication (FOITT) and the IT section of the Federal Department of Foreign Affairs. The project was classed as an ICT key project in 2022. This was not due to the volume of CHF 26.5 million, but because of its effects on the way in which practically the entire Federal Administration works.

The audit results reveal a mixed picture: The implementation of the project is progressing with minor delays, with the roll-out in the departments scheduled from 2024 onwards. The project is based on the assumption that it will no longer be possible to operate the Microsoft Office product range locally as of 2026.[1] There are now indications that this may be possible for longer.[2] This will be validated by the project. The (residual) risks involved in using the cloud, some of which are considered significant by the Swiss Federal Audit Office (SFAO), had not been fully ascertained and accepted at the time of the audit. In some areas, there is no common understanding with the future users. As the original conditions may have changed, the project could gain more time to resolve this situation and others.

Risks and supervision of the service providers must be clarified before roll-out

According to Microsoft's roadmap, support for the existing versions of Office will be discontinued from 2026. The project is based on the assumption that it is necessary to introduce M365, as support will subsequently only be available for cloud-integrated, subscription-based installations. The project gives the departments the opportunity to change over to the cloud-based solution M365. At the time of the audit, one of the manufacturer's websites stated that there would be a further release of the Microsoft Office suite available for one-time purchase. This would change the basis for the project. The SFAO recommends that the DTI Sector clarify with Microsoft how long and to what extent this release will continue to provide a solution without having to connect to the cloud. Depending on the outcome, approaches may become possible that would give the Federal Administration more time to prepare for the changed risk situation associated with moving to the cloud.

[1] See Microsoft roadmap: https://learn.microsoft.com/en-us/lifecycle/products/?products=office.

[2] See Microsoft FAQ website: https://support.microsoft.com/en-us/office/office-2021-and-office-ltsc-for-windows-and-mac-faq-d574cf0b-3ebc-42cf-9035-a3b837e0463c.

The roll-out of CEBA will mean a change in Microsoft's position as a partner for the Federal Administration. While this was previously a relationship between a purchaser and a software provider, this will now become a closer relationship with a service provider. Federal Administration data that was previously stored on its own systems will be transferred to the service provider and its sub-contractors. This will require enhanced supervision and monitoring of the service provider. The contractual assurances and security measures in particular will need to be monitored by the Confederation. There is currently no coordinated concept for this. The SFAO recommends that the DTI Sector should draw this up and implement it, taking into account the responsibilities of the two offices.

Residual risks of cloud use must be entered into consciously, and parallel operations should be minimised

The residual risks involved in using the cloud were ascertained by the project, and their status at the end of the concept phase disclosed to the Conference of Secretaries General (CSG) and the Federal Council. They still need to be accepted and approved by the Federal Chancellor and the DTI delegates before the roll-out. As the success of the project depends on the offices responsible bearing the residual risks, the analysis involving all the departments needs to be finalised and accepted quickly. It is important that the completeness and possible measures receive broad support, and that a consistent understanding of the residual risks is achieved. In the event of significant changes, at least the CSG and the Federal Council, which were previously informed, should be notified again.

The introduction of Microsoft Teams will create new duplications: The replacement of the current Skype for Business telephony solution will take place in a separate project with its own timetable outside of CEBA. According to the DTI this is to avoid increasing the complexity of CEBA even further with the 70-plus individual telephony solutions at the Confederation. Both solutions will be used in parallel at first. The SFAO recommends that the DTI Sector keep the period of parallel operation as short as possible.

Federal Administration infrastructure may only be opened up in a controlled manner

The use of M365 services from the public Microsoft Cloud requires the automated opening up of the Federal Administration's network infrastructure. To avoid having to create any general exceptions for this, DTI has expanded the existing directives. The addition states that the infrastructure should be opened "as much as necessary, but as little as possible".

However, it is still unclear how compliance with this principle can be monitored. The SFAO recommends that DTI specifies how it intends to ensure that the automated opening of the federal infrastructure does not go beyond the minimum level required.

Stakeholders should remain adequately involved in the project

Attention should be focused on the Federal Data Protection and Information Commissioner (FDPIC), who was consulted as part of the clarifications on the data and information protection issues in the CEBA project. It is important that the project takes sufficient account of the feedback received from the FDPIC and continues with the ongoing coordination.

Original text in German

Generelle Stellungnahme des Bereiches Digitale Transformation und IKT-Lenkung der Bundeskanzlei

Die BK bedankt sich bei den Vertretern der EFK, mit welchen im Rahmen dieser Prüfung ein intensiver, offener und konstruktiver Meinungsaustausch stattgefunden hat.

Das Projekt CEBA hat primär einen Lifecycle des Arbeitsplatzes zum Inhalt. Das Ziel von CEBA ist der Erhalt der BA-Funktionalität über die nächsten Jahre (nicht ein Change der IKT-Bundesarchitektur im Sinne eines Green-Field Ansatzes). Das Projekt wurde 2019 gestartet und steht kurz vor der Einführung der neuen Lösung.

Die Feststellungen und Empfehlungen der EFK gehen aus Sicht DTI teilweise über das eigentliche Prüfungsziel hinaus und haben neben dem Projekt auch allgemeine Cloudrisiken zum Gegenstand. Das Projekt orientiert sich an den strategischen Grundsätzen, welche in der IKT-Strategie Bund, IKT-Teilstrategie BA und der Cloudstrategie des Bundes festgelegt wurden und den bereits getroffenen Beschlüssen (z.B. Einführung von M365 vom 15. Februar 2023).

Im Prüfzeitpunkt stand die Realisierung von M365 unmittelbar bevor (technischer «point of no return») und das Bewusstsein für die Restrisiken hatte sich gegenüber dem Zeitpunkt des Entscheids zur Einführung (Januar 2023) erhöht. Aus diesen Gründen hat der Digitalisierungsrat Bund (DRB) im Januar 2024 erneut eine ausführliche Diskussion geführt, was sich u.E. mit dem Anliegen der EFK deckt.

Die Konsultation des Digitalisierungsrates Bund hat ergeben, dass das langjährige Projekt planmässig umgesetzt werden soll. Zur Risikominimierung wurden ergänzende Massnahmen definiert.

Auf Basis der Konsultation des Digitalisierungsrates Bund haben der Bundeskanzler und der Leiter DTI die Restrisiken übernommen sowie die minimierenden Massnahmen in Auftrag gegeben. Zudem haben sie das ISDS Konzept finalisiert und unterzeichnet. Das Projekt hat auf dieser Basis entschieden, M365 nach Plan auszurollen. Die BK hat den Bundesrat über ihren Entscheid Mitte Februar 2024 informiert.

Generelle Stellungnahme des Bundesamtes für Informatik und Telekommunikation

Das BIT dankt der EFK für die Möglichkeit der Stellungnahme zum Bericht. Beim Projekt CEBA handelt es sich um ein komplexes Vorhaben mit diversen Stakeholdern. Das Ziel ist eine Büroautomation abzulösen, welche auf einer mehr als 20-jährigen Plattform basiert und eng mit verschiedenen Services und Lieferanten verzahnt ist. Mit CEBA sollen nicht nur neue Technologien eingeführt werden, welche gänzlich neue Arten der Zusammenarbeit in der Bundesverwaltung ermöglichen und dadurch die Produktivität steigern werden, sondern auch die Aufrechterhaltung der notwendigen Funktionalitäten, des Cyberschutz und der Schnittstellen (z.B. Callcenterlösung) sicherstellt.

Generelle Stellungnahme der Informatik Direktion für Ressourcen

IT EDA dankt der EFK für den Bericht zur Prüfung des DTI-Schlüsselprojekts CEBA. Wir haben keine Anmerkungen zu den Prüfergebnissen und zu den Empfehlungen.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Der Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei entwickelt und führt IKT-Standarddienste zugunsten der zentralen und dezentralen Bundesverwaltung. Die konkrete technische Bereitstellung dieser Standarddienste und die Abwicklung des täglichen Betriebs wird von einem oder mehreren IKT-Leistungserbringern (LE) des Bundes übernommen.

DTI wurde per Bundesratsentscheid vom 3. April 2020 aus seiner Vorläuferorganisation, dem Informatiksteuerungsorgan des Bundes (ISB), geschaffen und organisatorisch in die Bundeskanzlei eingegliedert. Die heutige Rolle des DTI in Bezug auf Standarddienste des Bundes bestand bereits zu Zeiten des ISB. Sie wurde im Wesentlichen fortgeführt.

DTI führt seit dem 20. August 2020 das Projekt Cloud Enabling Büroautomation (CEBA) durch. Das Projekt hat zum Ziel, die Büro-Anwendungssoftware im Standarddienst Büroautomation (SD-BA) zu aktualisieren und zukünftig das Produkt Microsoft 365 (M365) einzusetzen. Die Büroautomatisierung des Standarddienstes ist aktuell auf den meisten Arbeitsplatz-Systemen des Bundes im Einsatz. Über das Produkt M365 soll eine Anbindung an die Cloud-Dienstleistungen des Herstellers Microsoft realisiert werden. Das Projekt rechnet derzeit mit Kosten von 26,5 Millionen Franken. Es befindet sich zum Prüfungszeitpunkt in der Realisierungsphase. Der Rollout in den Departementen ist ab Anfang 2024 geplant.

Das Projekt wurde 2022 aufgrund seiner Tragweite für die Arbeitsweise der nahezu gesamten Bundesverwaltung als Schlüsselprojekt des Bundes eingestuft. Die EFK prüft das Projekt zum ersten Mal.

1.2 Prüfungsziel und -fragen

Ziel der Prüfung war zu beurteilen, ob die Projektorganisation zielführend aufgestellt ist und die erforderlichen Führungs- und Steuerungsinstrumente implementiert sind und funktionieren. Die folgenden Fragen werden beantwortet:

1. Läuft das Projekt inhaltlich, zeitlich und kostenmässig nach Plan?
2. Sind Instrumente zur Führung und Steuerung des Projektes implementiert und werden diese eingesetzt?
3. Besteht ein angemessenes Risiko- und Qualitätsmanagement?
4. Sind die Angaben im letzten halbjährlichen Reporting über die IKT-Schlüsselprojekte des Bundes zuhanden der Finanzdelegation verlässlich bzw. plausibel?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Martin Scheid (Revisionsleiter), Christian Brunner und Hans-Ulrich Wiedmer vom 7. August bis 8. September 2023 durchgeführt. Sie erfolgte unter der Federführung von Oliver Sifrig. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach Abschluss der Prüfungsdurchführung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von den Geprüften umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechungen fanden am 12. und 20. Dezember 2023 statt. Teilgenommen haben am 12. Dezember seitens Bundeskanzlei (BK) der Delegierte des Bundesrates für die Digitale Transformation und IKT-Lenkung, der Leiter Digitaler Arbeitsplatz und die Projektleiterin. Seitens des Bundesamtes für Informatik und Telekommunikation (BIT) der Direktor, der Leiter Domestic Services und der Teilprojektleiter. Seitens der Informatik des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) der Vizedirektor und der Teilprojektleiter. Seitens des Eidgenössischen Datenschutz- und Öffentlichkeits-Beauftragten (EDÖB) der Leiter Datenschutz und die Leiterin Team 3. Von der EFK haben der Vizedirektor, der Mandatsleiter, der Fachbereichsleiter, der Revisionsleiter und ein Teammitglied teilgenommen. Am 20. Dezember haben seitens Bundeskanzlei der Delegierte des Bundesrates für die Digitale Transformation und IKT-Lenkung, der Leiter Digitaler Arbeitsplatz und die Projektleiterin teilgenommen. Von der EFK haben der Mandatsleiter, der Fachbereichsleiter, der Revisionsleiter und ein Teammitglied teilgenommen.

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

EIDGENÖSSISCHE FINANZKONTROLLE

2 Das Projekt Cloud Enabling Büroautomation

2.1 Vorarbeiten und Entstehung des Projektes

Im Rahmen der Abklärungen zur möglichen Weiterentwicklung des Standarddienstes BURAUT/UCC (heute SD-BA) hat das ISB 2017 eine Studie «Evolution BA-Technologie» (EBT) durchgeführt. In dieser Studie wurde, infolge der damaligen Einschätzung der Entwicklung der Office-Produktsuite durch Microsoft, die Erweiterung der bereits genutzten Microsoft Technologien in die (gemäss damaliger Produktbezeichnung) Office 365 Cloud als Zielbild festgelegt. Ausgehend von den Ergebnissen der Studie hat der damalige Leiter des Standard-dienstes BURAUT/UCC am 16. April 2019 den Auftrag zur Initialisierung des Projektes Cloud Enabling erteilt.

Während der Initialisierungsarbeiten wurde eine weitere Studie durchgeführt. Diese hatte das Ziel, mögliche Alternativen zur Microsoft Cloud zu untersuchen und zu bewerten. Zwei Produktsuiten, Office 365 von Microsoft sowie die G-Suite von Google, wurden von zwei spezialisierten Systemhäusern untersucht und durch das Projektteam bewertet. Als Ergebnis der Studie hat die Projektleitung die Variante «Microsoft Hybrid Cloud» zur Umsetzung empfohlen.

Die Studie hat die Möglichkeit eines klassischen Sourcing-Modells, für einzelne Bestandteile der Büroautomations-Produktpalette oder der Office-Suite als Ganzes, in Verbindung mit einer Fortführung des bereits bestehenden «on-premises» (engl. sinngemäss «vor Ort», siehe Glossar) Betriebsmodells und der dazugehörigen, bereits beschafften Infrastruktur, nicht betrachtet. Dies aufgrund der Annahme, dass die gemäss Roadmap auf Oktober 2026 abgekündigte «on-premises» betriebene Software von Microsoft in Zukunft nur noch als an die Cloud angebundene Variante unterstützt werde.

Am 20. August 2020 wurden der Projektauftrag freigegeben und die Arbeiten zur Konzeption des Bezuges von M365 für die Bundesverwaltung aus der Public Cloud aufgenommen. Seit dem 27. Oktober 2022 befindet sich das Projekt CEBA in der Realisierungsphase.

Seit den Grundsatzentscheiden zugunsten einer Cloud-Lösung hat Microsoft sein Leistungsangebot verändert. So ist zum Prüfungszeitpunkt von Seiten Microsoft ein «weiteres Release» von Office zum einmaligen Bezug, analog zum heute eingesetzten Produkt «Office 2021 LTSC», angekündigt. DTI hat die Grundausrichtung von CEBA aufgrund der notwendigen Vorlaufzeit von zwei bis drei Jahren für neue Major-Releases wegen Abhängigkeiten zu Fachanwendungen nicht hinterfragt. Auch lag DTI zum Prüfungszeitpunkt keine offizielle Abkündigung des «on-premises»-Angebots von Microsoft vor.

Die Lösungskonzeption zum Bezug der Microsoft 365 Dienste wurde sowohl der Generalsekretärenkonferenz als auch dem Bundesratsausschuss Digitalisierung vorgelegt. Der Bundesrat beschloss am 15. Februar 2023, den Antrag des Projektes auf einen Verpflichtungskredit (VK) in Höhe von 14,6 Millionen Franken gut zu heissen. Anschliessend stimmten die eidg. Räte diesem zu.

Im Rahmen der Arbeiten zur Exit-Strategie von CEBA hat DTI eine Studie zu Open Source Software (OSS) Alternativen für die Büroautomation (BOSS-Studie) durchgeführt. Diese wurde bei der Berner Fachhochschule in Auftrag gegeben und bis Mai 2023 abgeschlossen. Basierend auf den Studienergebnissen beabsichtigt DTI, ab 2024 eine OSS Labor- und Testumgebung mit 30 Arbeitsplätzen aufbauen zu lassen. Auf diese Weise sollen im Bund

Erfahrungen mit OSS gesammelt und konkrete Bedürfnisse im Kontext des BCM erfüllt werden.

DTI hat die Restrisiken des Vorhabens sowohl der Generalsekretärenkonferenz als auch dem Bundesrat summarisch zur Kenntnis gebracht. Eine Zustimmung zu den Risiken wurde nicht verlangt, da die Entscheidungsbefugnis dazu in der Zuständigkeit des Delegierten DTI liegt. Die Departemente hätten jedoch die Möglichkeit, einen Entscheid auf die nächsthöhere Stufe weiterzutragen. DTI erachtet den politischen Prozess als abgeschlossen und das Vorhaben mit seinen Restrisiken als ausreichend legitimiert. Die erfolgreiche Einführung der Lösung wird letztendlich davon abhängen, ob die zuständigen Stellen bereit sind, die Restrisiken zu tragen (siehe Kapitel 5.2, Empfehlung 8).

Beurteilung

Die EFK erachtet die im Vorfeld und bei der Initialisierung des Projektes durchgeführten Studien als zu wenig breit angelegt. Konkret befasst sich die EBT-Studie lediglich mit der Machbarkeit einer MS (Office) 365 Cloud Integration. Die CEBA-Studie untersucht neben M365 nur die Google G-Suite als weiteren Kandidaten. Nicht betrachtet wurden Aspekte eines klassischen Sourcing-Modells. Dies folgt der Grundannahme aus dem Jahr 2017, dass ab 2026 keine Unterstützung mehr für Microsoft-Produkte ohne Anbindung an die Cloud bestehen werde. Dies ist grundsätzlich nachvollziehbar.

Zu bemängeln ist hingegen, dass DTI an dieser Grundannahme festhält, trotz möglicherweise in Aussicht gestellter Verlängerung einer «on premises»-Lösung. Sollte sich der Bezug und Einsatz eines weiteren Releases von Office ohne Cloud als möglich herausstellen, kann dies für die Bundesverwaltung bedeuten, dass die spezifischen Risiken einer Cloud-Nutzung länger als erwartet vermieden werden können.

Dies kann dem Projekt Zeit verschaffen, um prioritär die zum Prüfungszeitpunkt offenen Fragen rund um die mit dem Gang in die Cloud verbundenen Risiken und den für die Infrastruktur der Bundesverwaltung angemessenen risikomindernden Massnahmen zu lösen. Ebenso müssen die Themen zur Kontrolle des Dienstleisters, der Verantwortung in Sicherheitsfragen und der Kostenverteilung beim Aufbau individueller Lösungen in Bezug auf M365 vorgängig vertieft bearbeitet werden.

Das Projekt selbst hält fest, dass sich die Abhängigkeit von Microsoft durch die Anbindung an die Cloud weiter verstärkt. Dass DTI Massnahmen wie zum Beispiel die BOSS-Studie vorsieht, ist daher als positiv zu bewerten.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt dem Bereich DTI, mit dem Anbieter Microsoft belastbar zu validieren, bis wann ein Einsatz der Microsoft Office Suite ohne Cloud-Anbindung unterstützt wird. Kann dies über das bisher angenommene Enddatum hinaus gewährleistet werden, ist zu klären ob Anpassungen im Projekt möglich sind, die zu einer Reduktion der Gesamtrisikosituation führen.

Die Empfehlung ist akzeptiert.

Stellungnahme des Bereiches DTI der Bundeskanzlei

DTI und BIT sind laufend im Austausch mit Microsoft. Auf der Roadmap von Microsoft [1] ist die Verfügbarkeit der MS-Produkte ersichtlich. Eine zusätzliche Validierung bei Microsoft hat bereits stattgefunden. Microsoft konnte nicht garantieren, dass die Funktionalitäten

und Schnittstellen der heutigen OnPrem-Version für die breite Anwendung über 2026 sichergestellt werden.

Aufgrund der hohen Verzahnung der Büroautomation mit geschäftskritischen Fachanwendungen (wie z.B. SAP und GEVER) wäre Zuwarten auf eine alternative Lösung oder Beibehaltung des Status-Quo fahrlässig, weil solche Projekte einen grossen zeitlichen Vorlauf benötigen. Zudem würde eine Projektsistierung oder -verzögerung erhebliche Kosten verursachen und die betrieblichen Aspekte (Support der Schnittstellen, Patching, etc.) ungenügend garantieren.

Aufgrund der Empfehlungen des Digitalisierungsrates Bund ist die BK zum Schluss gelangt, dass das langjährige Projekt nicht sistiert werden soll – zumal die Departemente in den Diskussionen immer darauf hingewiesen haben, wie wichtig ihnen die Funktionen von M365 sind.

[1] https://learn.microsoft.com/en-us/lifecycle/products/?products=office

2.2 Projektorganisation und Stand der Arbeiten zum Prüfungszeitpunkt

Das Projekt CEBA gliedert sich in vier Teilprojekte (TP):

- TP «CEBA agil»: Betrieb einer Testumgebung für die Bundesverwaltung in der Testumgebung der M365-Cloud. Dieser Testaufbau diente technischen Validierungen während der Konzeptphase und der Erprobung erster Betriebsprozesse. Die Testumgebung wird noch bis zum Projektende weiter betrieben und steht interessierten Mitarbeitenden der Bundesverwaltung zur Ansicht der M365 Produkte und Dienstleistungen offen. Eine Integration mit der heutigen Office-Produktpalette auf den Arbeitsplatzsystemen der Bundesverwaltung besteht nicht.
- TP «CEBA Ziellösung»: Konzeption, Realisierung und Pilot-Rollout der M365-Dienste in der Microsoft-Cloud sowie Konfiguration und Paketierung der für die Cloud-Integration notwendigen Software-Komponenten auf den Arbeitsplatzsystemen der Bundesverwaltung. «CEBA Ziellösung» wird beim IKT-Leistungserbringer Bundesamt für Informatik und Telekommunikation (LE BIT) durchgeführt. Bis Ende 2023 soll die Realisierungsphase abgeschlossen und die Einführung freigegeben werden.
  Zum Zeitpunkt der Prüfung wurde im TP «CEBA Ziellösung» durch den LE BIT auf die Auslieferung des ersten Release der lokal installierten Office-Software-Komponenten hingearbeitet. Für die Auslieferung dieses Release bestand jedoch ein Verzug von sechs Wochen. Gemäss Ausführungen der Teilprojektleitung sind die Gründe hierfür im Wesentlichen bei der Netzwerk-Konnektivität zu Microsoft und somit im Bereich der Firewalls zu verorten. Sofern keine weiteren unerwarteten Verzögerungen auftreten, sei der Zeitplan einzuhalten.
- TP «Cloud@Ausland»: Konzeption und Realisierung der M365-Dienste zum Bezug durch das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) und Betrieb durch den IKT-Leistungserbringer Informatik EDA (IT-EDA), insbesondere an den über 160 internationalen Standorten des Departements.
  Im Vorfeld der Projektausschuss-Sitzung vom 15. Mai 2023 hat die Geschäftsleitung der Direktion für Ressourcen EDA entschieden, dass ein eigener Cloud-Tenant

(ein eigener logischer Bereich für den Kunden in der Microsoft Cloud, in welchem Dienste individuell freigeschaltet und konfiguriert oder verborgen werden können, vgl. Kapitel 3.2) für die Bereitstellung der M365-Dienstleistungen angestrebt wird. Am Projektausschuss vom 15. Mai 2023 wurde das EDA beauftragt, bis Ende September eine Information zur «Aufarbeitung Entscheid EDA betreffend eigenem Tenant» zu erarbeiten. Die entsprechende IKT-Anforderung gemäss Weisung P035 sei dem Bereich DTI zur Genehmigung einzureichen. Anschliessend werden die Zeit- und Budget-Auswirkungen auf das Projekt CEBA als Projekt-Change erfasst und entschieden.

IT-EDA ist der Ansicht, dass sich das Projekt durch diesen Entscheid nicht verzögern wird und auch keine Mehraufwände entstehen. Dies aufgrund der Einschätzung, dass bei einem Entscheid für einen gemeinsamen Tenant die spezifischen Anforderungen des EDA im Gesamtsystem ebenso hätten berücksichtigt werden müssen, was zusätzliche Kosten für die gesamte Bundesverwaltung ergeben hätte.

Der Terminplan für das Gesamtprojekt CEBA sieht zum Prüfungszeitpunkt vor, dass «Cloud@Ausland» im 3. Quartal 2023 die Konzeptphase abschliessen wird, und im 2. Quartal 2024 der Übergang von der Realisierung zur Einführung im Departement EDA stattfindet. «Cloud@Ausland» wird damit gegenüber der ursprünglichen Planung um voraussichtlich sechs Monate verspätet mit der Realisierung beginnen.

- TP «Transition»: Konzeption, Umsetzung und Durchführung von Schulungen für die Mitarbeitenden der Bundesverwaltung in Bezug auf die Neuerungen und Änderungen im Bereich Büroautomation. Das Teilprojekt ist initialisiert, die Arbeiten an konkretem Schulungsmaterial sollen in enger Zusammenarbeit zwischen dem Bereich DTI der Bundeskanzlei und dem Eidgenössischen Personalamt (EPA) ab dem Zeitpunkt des Pilot-Rollouts im TP «CEBA Ziellösung» beginnen.

Ab Anfang 2024 ist geplant, das im TP «CEBA Ziellösung» entstandene, an die M365-Cloud-Dienste von Microsoft angebundene Release der Office-Softwarekomponenten mittels departementaler Rollout-Projekte über eineinhalb Jahre hinweg in der Bundesverwaltung einzuführen. Das Projekt CEBA führt für diese departementalen Projekte eine zentrale Terminplanung des Rollouts und unterstützt die Departemente durch die im TP «Transition» entstandenen Schulungen. Die Rollout-Projekte werden eigenständig durch die Departemente und Verwaltungseinheiten in Zusammenarbeit mit ihrem Leistungserbringer (BIT bzw. IT-EDA für das EDA) erbracht, und sollen grundsätzlich dem bereits definierten Vorgehen zum Rollout eines SD-BA Standard-Release für neue Office-Produktversionen folgen. Der Abschluss der departementalen Rollout-Projekte ist auf Ende Juni 2025 geplant.

Beurteilung

Es besteht ein Risiko, dass Konzepte die durch «Cloud@Ausland» erarbeitet wurden, hinfällig werden, wenn die erwähnte IKT-Anforderung oder der Projekt-Change nicht genehmigt werden. Auch ist nicht auszuschliessen, dass konzeptionelle Mehraufwände entstehen und Doppelspurigkeiten verfestigt werden.

Aus Sicht der EFK ist es daher wesentlich, dass der geplante Change durch «Cloud@Ausland» nur auf Basis von klar ausgewiesenen Kosten sowie erkennbarem Mehrwert für das EDA und die Bundesverwaltung genehmigt wird.

3 Lösungskonzeption und Einordnung im Bundesumfeld

3.1 Paradigmenwechsel bei der Netzwerk-Sicherheit – wie muss der Bund reagieren?

Die grundlegende Sicherheitsdokumentation bestehend aus Schutzbedarfsanalyse (Schuban) und dem Konzept Informationsschutz wurde erstellt. Das Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept), dessen genauer Zuschnitt hinsichtlich der enthaltenen Dienstleistungen und die Datenschutz-Folgenabschätzung (DSFA) befinden sich zum Prüfungszeitpunkt noch in Erarbeitung.

Der IKT-Grundschutz Bund kann nach aktuellem Stand der Arbeiten im Teilprojekt «CEBA Ziellösung» eingehalten werden. Die Webproxy-Richtlinie Si004 wurde um die neue Beilage «M365 Netzwerkanbindungen» erweitert, gemäss welcher bis anhin geltende Sicherheitsmassnahmen für bestimmte Netzwerk-Verkehrskategorien anders implementiert werden müssen. Damit wird gestattet, dass die Arbeitsplatzsysteme der Bundesverwaltung direkt mit Microsoft-Cloud Services kommunizieren und hierfür auf dem Webproxy des Bundes automatisiert freigeschaltet werden. Für welche Zielsysteme und Dienste dies gilt, wird hierbei von Microsoft mittels einer Konfigurationsdatei festgelegt, welche von den Systemen der Bundesverwaltung importiert wird.

Von der Projektleitung wurde ursprünglich vorgesehen, diese Änderung im Bereich der Sicherheit über das Ausnahme-Management des Bundes (P035-Prozess) zu behandeln. Dies wurde vonseiten der Sicherheitsorganisationen von DTI und BIT jedoch verworfen und stattdessen eine Lösung über eine neue Beilage der Webproxy-Richtlinie Si004 umgesetzt. Diese lag zum Prüfungszeitpunkt im Entwurf vor. Ein Grundsatz, demzufolge Einschränkungen der Sicherheit im kleinstmöglichen Rahmen zu halten sind, wurde im Entwurf der Beilage festgeschrieben. In der Richtlinie ist jedoch nicht ausgeführt, wie dieser Grundsatz in Zukunft insbesondere bei den automatisch eingespielten Konfigurationsdateien von Microsoft auf Einhaltung überprüft werden kann.

Gemäss Absprachen zwischen der Sicherheitsorganisation des LE BIT und dem Projekt müssen daher erweiterte Sicherheitsmassnahmen auf den Arbeitsplatzsystemen vorgesehen werden. Diese sind derzeit im TP «CEBA Ziellösung» in Erarbeitung.

Beurteilung

Die EFK erachtet die Veränderung von über Jahre hinweg gewachsenen und bewährten Sicherheitsvorkehrungen durch das Projekt als problematisch. Positiv bewertet die EFK, dass das Projekt dafür gesorgt hat, dass die entsprechenden Sicherheitsvorgaben des DTI abgeändert bzw. ergänzt werden, um eine Ausnahmeregelung zu vermeiden.

Es muss dennoch sichergestellt werden, dass die betreffenden Öffnungen der Firewall im kleinstmöglichen Rahmen gehalten werden.

Es besteht das Risiko, dass künftig mehr als nur die minimal notwendigen Freigaben im Webproxy automatisch konfiguriert werden. Dies vergrössert die potenziellen Angriffsflächen auf die IKT-Infrastruktur der Bundesverwaltung und ist folglich zu unterlassen.

In diesem Zusammenhang bewertet die EFK die geplante Einführung erweiterter Sicherheitsmassnahmen auf den Arbeitsplatzsystemen als positiv, auf eine entsprechende Empfehlung wird daher verzichtet.

Empfehlung 2 (Priorität 2)

Die EFK empfiehlt dem Bereich DTI festzulegen, wie und von wem sichergestellt werden soll, dass Sicherheitseinschränkungen der IKT-Infrastruktur des Bundes nicht über das minimal notwendige Niveau hinausgehen. DTI soll damit sicherstellen, dass den geänderten Rahmenbedingungen und insbesondere der Menge an Anpassungen angemessen Rechnung getragen wird.

Die Empfehlung ist akzeptiert.

Stellungnahme des Bereiches DTI der Bundeskanzlei

Der Prozess zu Netzwerkanbindungen wurde dokumentiert und Ende 2023 als Anhang zur Si004 publiziert.

DTI beauftragt den LE zu prüfen, wie oft und in welchem Umfang Überprüfungen von Konfigurationsänderungen während dem Betrieb durchgeführt werden und dies zu dokumentieren.

3.2 Der Cloud-Betrieb hängt von ausstehenden Grundsatzentscheiden ab

Das Projekt CEBA wird die Dienstleistungen in einem eigenen sog. Cloud-Tenant der Microsoft Cloud bereitstellen. Ein Tenant (engl. Mieter) ist hierbei vergleichbar mit dem System der Mandantentrennung bei ERP-Systemen: Ein eigener logischer Bereich wird in der Microsoft Cloud für den Kunden generiert, in welchem Dienste nach individuellen Bedürfnissen freigeschaltet und konfiguriert oder verborgen werden können.

Das Projekt CEBA ist nicht das erste Projekt, bei dem Einheiten der Bundesverwaltung in Kontakt mit der Microsoft Cloud treten. Zum Prüfungszeitpunkt bestehen über 30 Tenants des Bundes in der Microsoft Cloud, welche mehr oder weniger aktiv genutzt und betrieben werden.

Exkurs: Betriebstätigkeiten für einen M365 Cloud-Tenant

Für einen auf Dauer sicheren Betrieb eines Cloud-Tenants sind spezifische Betriebsrollen notwendig. Microsoft stellt den Kunden eine Tabelle zur Verfügung, mittels welcher die für den Betrieb eines Cloud-Tenants notwendigen Betriebsaufwände pro bezogenem Service und auftretender Regelmässigkeit (z. B. ad hoc, wöchentlich, monatlich, …) geschätzt werden können. Beispielsweise generiert Microsoft Mitteilungen zuhanden des Tenant Messaging Centers mit Informationen zu Sicherheitsvorfällen beim eigenen Tenant (konkrete Warnmeldungen, aktuelle Verwundbarkeiten wie auch allgemeine Informationen). Diese müssen von einem Betriebsmitarbeiter aktiv entgegengenommen, quittiert und verarbeitet werden.

Der LE BIT ist derzeit dabei, in den Betriebsprozessen für die CEBA Tenants die Entgegennahme und Verarbeitung derartiger Meldungen zu konzipieren.

Die Ämter und Verwaltungseinheiten, die einen eigenen Microsoft Cloud Tenant betreiben, müssen von dieser und den weiteren sicherheitsrelevanten Notwendigkeiten ebenfalls Kenntnis nehmen und ihrerseits entsprechende Prozesse etablieren, sowie die für einen für den Bund sicheren Betrieb notwendigen Betriebsressourcen bereitstellen. Es wäre zu klären, ob dies bei allen Betreibern eigener Cloud-Tenants entsprechend umgesetzt ist.

Seit 2018 besteht für die dem Geltungsbereich der Verordnung über die digitale Transformation und die Informatik (VDTI) unterstehenden Ämter und Verwaltungseinheiten eine Vorgabe, dass neue Tenants in der Microsoft Cloud durch DTI als IKT-Anforderung gem. P035 bewilligt werden müssen. Im Rahmen der Prüfung konnte für mehrere der bereits bestehenden Tenants der Bundesverwaltung nicht nachvollzogen werden, dass eine solche Genehmigung ersucht respektive erteilt wurde. Darüber hinaus bestehen zum Prüfungszeitpunkt keine Vorgaben, wie ein Cloud Tenant betrieben werden muss, um für den Bund kein Sicherheitsrisiko darzustellen. In Ermangelung derartiger Vorgaben wird heute der Entscheid, ob und wie ein eigener Tenant in der Microsoft Cloud zu betreiben ist, von den Departementen bzw. Amtsdirektoren getroffen.

Das Projekt CEBA beabsichtigt, die SD-BA Dienste der Teilprojekte «CEBA Ziellösung» sowie «Cloud@Ausland» in je einem eigenen Tenant einzurichten. Derjenige des TP «CEBA Ziellösung» soll hierbei vom LE BIT betrieben werden, «Cloud@Ausland» vom LE IT-EDA. Ob und welche Dienste der Microsoft Cloud (genannt «Microsoft Azure») ausserhalb des Standarddienstes Büroautomation zukünftig ebenfalls in diesen Tenants bereitgestellt werden sollen, war zum Prüfungszeitpunkt noch nicht abschliessend geklärt.

Der Grundlagenentscheid, welche Dienstleistungen zukünftig gemäss welchem Zuschnitt im gleichen oder separierten Tenants der Microsoft Cloud angeboten werden sollen, zahlt direkt auf die notwendigen Sicherheitskonzepte und -massnahmen ein. Diese befinden sich im Projekt CEBA derzeit in der Finalisierung. Sie müssen die Best Practices des Herstellers zur Härtung von Cloud-Tenants erfüllen, auf die departementalen Rollout-Projekte im 2024 hin fertiggestellt werden und für die LE nutzbar umgesetzt sein.

Beurteilung

Es ist zu erwarten, dass die Anzahl der architektonisch voneinander abweichenden Lösungen, die Leistungserbringer (LE) des Bundes bei einem Cloud-Anbieter bereitstellen, in Zukunft wachsen wird. Die Standardisierung der Governance mit klar definierten Rechten und Pflichten eines LE im Cloud-Umfeld ist für einen sicheren Betrieb somit unerlässlich.

Der Bereich DTI und die LE müssen Kenntnis darüber haben, welche Daten mit weiteren Tenants ausgetauscht werden sollen. Ferner muss definiert sein, welche zusätzlichen Microsoft Azure-Dienste im selben Tenant betrieben werden sollen. Das Risiko besteht, dass ohne eine ausreichende Klärung dieser architektonischen Fragen – idealerweise basierend auf allgemeingültigen Grundsätzen für die gesamte Bundesverwaltung – es für den SD-BA nicht möglich ist, Fragestellungen der benötigten Sicherheitsmassnahmen abschliessend zu klären.

Die EFK nimmt zur Kenntnis, dass der Digitalisierungsrat Bund (DRB) sich der Problematik bewusst ist. In seiner Sitzung vom September 2023 wurde zu den vorgenannten Themen der Auftrag formuliert, bis Ende des 1. Quartals 2024 eine einheitliche Governance zu erarbeiten. Aus diesem Grund verzichtet die EFK an dieser Stelle auf eine Empfehlung.

3.3 Fehlendes Konzept zur Überwachung und Kontrolle des Dienstleisters

Das Projekt CEBA beabsichtigt, Dienste die heute rein aus lokaler, bei Leistungserbringern des Bundes selbst betriebener Infrastruktur bezogen werden, teilweise und mit Aussicht auf wachsenden Umfang vom Dienstleister Microsoft zu beziehen.

In der Vergangenheit war Microsoft für die Bundesverwaltung ein Software-Lieferant, welcher zu Zwecken von Schulung oder Training wie auch Beratung hinsichtlich seiner Produktpalette konsultiert wurde. Für die eingesetzten Produkte, sowie Schulung und Beratung wurde eine Lizenz erworben, die Software sodann lokal von einem IKT-LE des Bundes installiert und konfiguriert. Für sicherheitsrelevante Aspekte oder Fehler in der Software werden von Microsoft regelmässig Updates bereitgestellt und lokal vom Betreiber eingespielt.

Mit dem Bezug von Cloud-Dienstleistungen von Microsoft ändert diese Rolle. Der Software-Hersteller wird neu auch zum Betreiber der bezogenen serverseitigen Dienste. Die Dienste werden in den Rechenzentren von Microsoft betrieben. Microsoft oder deren Subakkordanten halten die Dienste operativ aufrecht und aktualisieren sowohl die Software der Services, als auch die darunter liegenden Betriebssystem- und Hardware-Plattformen. Sie stellen die Netzwerk-Konnektivität zu den Diensten aus dem öffentlichen Internet sicher.

Dies erfordert, dass dieser externe Partner der Bundesverwaltung nicht mehr ausschliesslich wie ein Lieferant geführt und gesteuert wird, sondern wie ein Dienstleister. Mit einem Dienstleister werden üblicherweise Leistungskennzahlen vereinbart. Diese führen aus, welche Verfügbarkeit dem Abnehmer garantiert werden kann, zu welchem Preis wann Service- und Support-Dienstleistungen in Anspruch genommen werden dürfen, und ab wann eine allfällige Konventionalstrafe bei Nichteinhaltung von vereinbarten Leistungsgrössen greift – die sogenannten Service Level Agreements (SLA).

Es liegt in der Verantwortung eines Service-Bezügers, die operative Einhaltung der vereinbarten SLAs zu messen, um allfällige Nichteinhaltung oder Diskrepanzen in der Leistungserbringung mit dem Dienstleister zu klären und abzustellen. Im Projekt CEBA sind die Service-Bezüger die IKT-LE BIT und IT-EDA. Ein entsprechendes operatives Monitoring-Konzept für den Dienstleister Microsoft und die bezogenen Dienste ist im Teilprojekt «CEBA Ziellösung» derzeit in Erstellung. Dieses muss auf den Beginn des produktiven Betriebs zum Zeitpunkt des Pilot-Rollouts fertiggestellt und umgesetzt sein.

Es sind jedoch auch weitergehende Aspekte der Kontrolle des Dienstleisters zu berücksichtigen. In einem System mit geteilter Verantwortung zwischen Dienstleister und Dienstleistungs-Empfänger gibt der Empfänger einen Teil seiner Möglichkeiten zur Kontrolle über z. B. Infrastruktur und Zugriffsmanagement an den Dienstleister ab. Im Austausch hierfür sollte er sich zusichern lassen, dass der Dienstleister seinerseits interne Kontrollen vorsieht, die diese Risiken angemessen abdecken. Ebenso sollte er grundsätzlich bereit sein ein Grundvertrauen aufzubringen, dass der Dienstleister die internen Kontrollen wie beschrieben und vorgesehen ausführt und vertragliche Zusicherungen, z. B. hinsichtlich dem Datenspeicherort, eingehalten werden.

Ob die überprüfbaren Zusagen des Dienstleisters retrospektiv tatsächlich eingehalten wurden, kann mit Hilfe von Prüfungen beim Dienstleister kontrolliert werden. Weiterhin gibt es hierfür das Konzept der sogenannten Kontrollberichte, in denen der Dienstleister über die Effektivität seines internen Kontrollsystems in regelmässigen Abständen von einem anerkannten Wirtschaftsprüfer Bericht erstatten lässt.

Microsoft stellt seinen Kunden Informationen über derartige Prüfungen des Kontrollsystems auf einer Kundenwebseite zum Abruf zur Verfügung. Ebenso ist der Bund gemäss Vertrag dazu berechtigt, eigene Prüfungen bei Microsoft zu veranlassen. Eine Strategie, wie der Bund von diesen ihm zur Verfügung stehenden Kontrollmitteln Gebrauch machen kann und soll, besteht jedoch noch nicht.

Darüber hinaus ist im Projekt CEBA nicht allen Beteiligten gleichermassen bekannt, welche Massnahmen der Bundesverwaltung zur Überprüfung der Leistungserbringer zur Verfügung stehen. Es fehlt ein Überblick über die Kontrollmöglichkeiten und deren zugrunde liegender Konzepte von interner Kontrolle über Systeme mit verteilter Verantwortung.

Exkurs: Aktuelle Vorfälle mahnen zur aktiven Wahrnehmung der Verantwortung

Insbesondere im Sommer 2023 wurden in den Medien Berichte über Vorfälle veröffentlicht, die sowohl den Bund und gewisse Dienstleister als auch Microsoft als Anbieter von Cloud-Lösungen kritisieren. Durch die Vorfälle um «STORM-0558» und «Xplain» wurde beispielhaft verdeutlicht, dass die Verantwortung für Daten bis hin zur korrekten Löschung beim Eigner verbleibt, auch wenn er diese einem Dienstleister übergibt.

Diese Vorfälle betreffen das Projekt CEBA nicht direkt bzw. wurden in dieser Hinsicht vom Projekt abgeklärt. Dennoch zeigen diese Vorfälle exemplarisch auf, dass der Bund für seine Daten bis hin zu den Subakkordanten eines Dienstleisters verantwortlich ist und bleibt. Diese Verantwortung muss von den zuständigen Stellen nicht zuletzt im eigenen Interesse effektiv wahrgenommen werden.

Ferner haben die aktuellen Vorfälle gezeigt, dass auch ein Dienstleister wie Microsoft nicht in allen Situationen Angriffe auf die Daten seiner Kunden verhindern kann. Die EFK stellt fest, dass das Risiko eines unautorisierten Zugriffs in die Infrastruktur der Bundesverwaltung durch kompromittierte Cloud-Tenants nicht ausgeschlossen werden kann. Die Bundesverwaltung muss dies in ihren Risikoüberlegungen berücksichtigen, damit sie im Falle von weiteren Vorfällen geplant agieren kann.

Beurteilung

Das Projekt CEBA beabsichtigt im Teilprojekt «CEBA Ziellösung», die in der Bundesverwaltung heute vorhandenen Ansätze zum Monitoring von Diensten und zur Messung von Betriebskennzahlen für die im Aufbau befindliche Cloud-Lösung zu übernehmen. Wo möglich sollen diese durch neue in der Cloud zur Verfügung stehende Mittel zur operativen Überwachung weiter ergänzt werden. Die EFK begrüsst diese Bestrebungen.

Zu einer umfassenden Kontrolle eines Dienstleisters gehört jedoch auch eine regelmässige retrospektive Überprüfung, ob Zusagen bei der Ausführung von internen Kontrollen, z. B. Bewirtschaftung der Sicherheit oder Kontrolle der logischen und physischen Zugänge des Dienstleisters und seiner Subakkordanten, eingehalten wurden.

Dazu sind Aktivitäten zu einer effektiven Kontrolle des Dienstleisters zu definieren.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt dem Bereich DTI sicherzustellen, dass die zur Verfügung stehenden Kontrollmöglichkeiten über den Dienstleister Microsoft bei den betroffenen IKT-Leistungserbringern der Bundesverwaltung bekannt sind. Darüber hinaus sollte festgelegt werden, durch wen und wie diese Kontrollmöglichkeiten genutzt werden sollen, sowie auf welche Weise die Massnahmen des Dienstleisters durch den Bund komplementär zu ergänzen sind. Dies gilt konkret für CEBA, ist aber im Grundsatz auch für weitere Cloud-Lösungen notwendig.

Die Empfehlung ist akzeptiert.

Stellungnahme des Bereiches DTI der Bundeskanzlei

Die Konzepte für den Betrieb, das Erstellen der Betriebshandbücher sowie das Implementieren der erforderlichen Kontrollmechanismen auf den Systemen und die operative Erprobung der Betriebsorganisation läuft aktuell im Rahmen der Phase Realisierung. Das Projekt fokussiert auf eine hohe Betriebsstabilität. Die Artefakte zum Sicherstellen der Kontrollmechanismen werden gemäss Planung fertiggestellt, abgenommen und implementiert. Als zusätzliche risikominimierende Massnahme wird DTI ein Audit der Microsoft Clouddienste durchführen. Mittels Audit wird geprüft, ob die technischen und vertraglichen Vereinbarungen von Microsoft eingehalten werden.

3.4 Die Funktionalitäten Kollaboration und Telefonie müssen eng abgestimmt werden

Per Oktober 2025 wird von Seiten Microsoft der Support für die derzeit in der Bundesverwaltung eingesetzte Sprach- und Videotelefonie-Lösung «Skype for Business» eingestellt. Es muss daher zeitgerecht für Ersatz dieser Lösung gesorgt werden. Ein Teil der ausgelieferten Office-Softwarelösung der CEBA Ziellösung wird die Chat- und Kollaborations-Software «Microsoft Teams» sein. Diese wird zwar durch CEBA ausgerollt, sie ersetzt aber nicht die Telefonie-Funktionalitäten von «Skype for Business», sondern stellt parallel eine weitere Möglichkeit für Chat und Videotelefonie dar.

Die Ablösung der heutigen «Skype for Business» Suite, insbesondere die Anbindung der Festnetz-Telefonie der Bundesverwaltung mit mehr als 70 Spezial-Lösungen, ist nicht Teil des Projektes CEBA. Diese Ablösung wird in einem parallelen Projekt beim Leistungserbringer BIT geführt.

Auch IT-EDA betreibt heute an den weltweit ca. 165 EDA-Standorten eine «Skype for Business»-Infrastruktur mit direkter Anbindung an die lokale Telefonie. Um die Komplexität im Projekt «Cloud@Ausland» nicht zusätzlich zu erhöhen, beabsichtigt IT-EDA ebenfalls, ein eigenes Projekt zur Ablösung der Skype-Telefonie zu lancieren.

Im Falle der Kollaborations-Programme Microsoft Teams und «Skype for Business» verdoppelt sich somit zunächst die Anzahl der verwendeten Tools für ein fast deckungsgleiches Leistungsspektrum.

Mit der Möglichkeit zur Datenablage in der M365-Cloud erhalten die Mitarbeitenden der Bundesverwaltung ebenfalls eine weitere Speichermöglichkeit. Es ist die Aufgabe jedes einzelnen Benutzers zu entscheiden, wo erfasste Daten gespeichert werden dürfen. Das Projekt CEBA unterstützt den Benutzer hierbei durch Bereitstellung einer Labelling-Lösung zur Klassifizierung von Office-Dokumenten. Eine Speicherung von Inhalten in der Cloud mit Einstufung «vertraulich» und höher soll vom System unterbunden werden. Die Klassifizierung der Dokumente ist jedoch von den Benutzern von Hand vorzunehmen, die Komplexität nimmt für diese daher eher zu.

Beurteilung

Die Lösung schafft durch die Möglichkeit, Daten in der Cloud zu speichern, neue Doppelspurigkeiten die die Standardisierung von Datenablagen in der Bundesverwaltung unterminieren, z. B. die Nutzung von GEVER für alle geschäftsrelevanten Daten. Zudem ist der Benutzer bei jeder Speicherung gefordert, denn diesem obliegt die Entscheidung, wo

das Dokument abgelegt werden darf bzw. soll. Der von CEBA verfolgte Labelling-Ansatz baut eine technische Sicherheit ein, erhöht aber auch den Aufwand beim Nutzer.

Darüber hinaus sorgt der geplante Parallelbetrieb der beiden Lösungen «Skype for Business» und «Microsoft Teams» dafür, dass dem Benutzer zwei Werkzeuge für den gleichen Zweck zur Verfügung stehen. Es erscheint daher aus Anwendersicht sinnvoll, den Rollout von Microsoft Teams zeitlich möglichst eng an das Lifecycle-Projekt zur Ablösung von «Skype for Business» zu binden.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt dem Bereich DTI, eine enge Abstimmung der Funktionalitäten «Kollaboration» und «Telefonie» sicherzustellen und neue Doppelspurigkeiten zu vermeiden. Darüber hinaus ist sicherzustellen, dass die Dauer eines Parallelbetriebes von MS Teams und «Skype for Business» auf das mögliche Minimum beschränkt bleibt.

Die Empfehlung ist akzeptiert.

Stellungnahme des Bereiches DTI der Bundeskanzlei

Die Umsetzung der Telefonie Anbindung erfolgt im Projekt «Hybrid Telefonie» seitens Leistungserbringer BIT. Eine enge Abstimmung ist sowohl organisatorisch in der Projektorganisation (z.B. mit identischer Projektleitung wie beim Teilprojekt CEBA-Ziellösung) wie auch technisch durch die hohen Abhängigkeiten mit M365, gegeben. Es ist im Interesse aller Beteiligten, den Parallelbetrieb auf das mögliche Minimum zu beschränken. Die konkrete Planung erfolgt im Rahmen des Projektes «Hybrid Telefonie».

4 Projektführung und -steuerung

4.1 Entscheide des Auftraggebers müssen dokumentiert werden

Die Sitzungen des Projektausschuss (PA) finden grundsätzlich auf monatlicher Basis statt. Der PA ist mit Vertretern aus allen Departementen sowie mit den Sicherheitsorganisationen und zukünftigen Leistungserbringern besetzt. Der Auftraggeber nutzt die Sitzungen zur Vorqualifikation von Themen, die richtungsweisende Entscheide im Projekt CEBA darstellen.

Gemäss den Vorgaben zum Projektmanagement im Bund organisiert sich das Projekt CEBA nach HERMES. HERMES gesteht der Rolle des Projektauftraggebers die Richtlinienkompetenz für Projektsteuerungsentscheide in alleiniger Verantwortung zu. Dies geschieht, damit klar und unmissverständlich geregelt ist, bei wem die Verantwortung für Projektentscheide liegt. Es ist jedoch möglich und vom Rahmenwerk her gestattet, im Vorfeld eines Entscheids den Projektausschuss anzuhören und dessen Ausführungen in der Entscheidungsfindung zu berücksichtigen.

Das im Projekt CEBA gewählte Vorgehen mit Abstimmungen zu Vorlagen im PA ist dann gemäss der HERMES-Methodik möglich, wenn im Nachgang zur Abstimmung ein Entscheid durch den Projektauftraggeber erfolgt. In keinem von der EFK geprüften Protokoll ist ersichtlich, dass der Projektauftraggeber einen solchen Entscheid im Sinne der Methodik getroffen hätte. In den Protokollen ist das Abstimmungsverhalten der einzelnen Mitglieder sowie eine Zusammenfassung der Abstimmungsergebnisse enthalten.

Daraus ist jedoch konkret nicht ersichtlich, dass der Projektauftraggeber an einer Abstimmung teilgenommen hätte oder im Nachgang einen souveränen Steuerungsentscheid getroffen hat. In den von der EFK geprüften Protokollen gab es keine Situation, in welcher der Auftraggeber einen Entscheid revidieren musste.

Beurteilung

Wenn der Projektausschuss Entscheide zur Projektsteuerung fällt, steht dies nicht im Einklang mit den Vorgaben der HERMES-Projektmanagement-Methodik des Bundes.

Da nicht ausdrücklich protokolliert ist, ob und welche Entscheide der Auftraggeber trifft, besteht das Risiko, dass die Verantwortung für Projektsteuerungsentscheide dem PA als Gremium zugeordnet werden könnte. Um nachzuweisen, dass diese Verantwortung beim Auftraggeber liegt sollte dies künftig nachvollziehbar dokumentiert werden.

Empfehlung 5 (Priorität 3)

Die EFK empfiehlt dem Bereich DTI, die Entscheidungen des Auftraggebers in den Protokollen der Projektausschusssitzungen nachvollziehbar zu dokumentieren.

Die Empfehlung ist akzeptiert.

Stellungnahme des Bereiches DTI der Bundeskanzlei

Beschlussdispositive zu Handen Projektausschuss werden durch die Projektleitung vorbereitet und mit dem Auftraggeber vor Einreichen abgestimmt. Es gab im bisherigen Projekt keine Anträge an den Projektausschuss, mit denen der Auftraggeber nicht einverstanden ist. Im Protokoll des Projektausschusses wird in Zukunft pro Beschluss formell festgehalten, dass der Projektausschuss konsultiert wurde und der Auftraggeber den Beschluss gefällt hat.

4.2 Kernprozesse auf Stufe Gesamtprojekt sind etabliert

Die Projekt-Rollen mit Aufgaben, Kompetenzen und Verantwortlichkeiten sind definiert. Die Gremien des Projektes arbeiten in den vorgesehenen Strukturen zusammen. Es finden regelmässige Abstimmungen der Projektleitung mit den Teilprojektleitenden auf Stufe Gesamtprojekt statt.

Operatives Risikomanagement

Die Risikomanagement-Prozesse sowie die Risikomanagement-Governance sind definiert und umgesetzt. Die entsprechenden Rollen sind definiert und werden gelebt. Die Rolle des internen Risikomanagers ist besetzt, es gibt mehrere Stellen im Projekt welche sich mit den Risiken befassen; diese Stellen sind nebst dem internen Risikomanager die Teilprojektleiter und die Gesamtprojektleitung. Die Risiken werden im Projekt systematisch identifiziert, dokumentiert, bewertet und überwacht. Die Risiken auf Stufe Gesamtprojekt CEBA werden in einer Risikoliste geführt. Auf dieser sind auch die zugordneten Risikoeigner ersichtlich. Die Risikoliste wird anlässlich der regelmässigen PA-Sitzungen vorgestellt und diskutiert.

Operatives Qualitätsmanagement

Der für die Qualitätssicherung Verantwortliche in der Projektorganisation erstellt regelmässige Testberichte und Berichte über die Qualitätssicherung. Allfällige Empfehlungen werden in den PA eingebracht und dort behandelt. Erkannte Risiken aus den internen und externen QRM-Berichten werden anlässlich der PA-Sitzungen besprochen. Bei wesentlichen Risiken sind adäquate Risikominderungsmassnahmen definiert und wirksam. Risikominderungsmassnahmen werden nachweisbar durchgeführt. Diese sind in den Risikoinventaren der Projektleitung erfasst und werden dort aktuell gehalten. Die Projektleitung hat die Gesamtverantwortung über das Massnahmen-Controlling. Ein Eskalationsverfahren ist im Projektmanagementplan beschrieben.

Änderungs-Management

Änderungen am Projektvorgehen auf Stufe Gesamtprojekt werden in einem Projektstab oder Teilprojekt ausgearbeitet und mittels Entscheidvorlagen in den PA eingebracht.

Im Teilprojekt «CEBA Ziellösung» in der Zuständigkeit des LE BIT besteht ein dokumentiertes Vorgehen zur Erfassung und Verarbeitung von Änderungen. Auch hier ist der PA des Teilprojektes «CEBA Ziellösung» die genehmigende Instanz. Bei Notwendigkeit resp. bei Auswirkungen auf das Gesamtprojekt werden Änderungen durch die Teilprojektleitung darauffolgend in den PA auf Stufe Gesamtprojekt eingebracht.

Beurteilung

Die wesentlichen Instrumente für die Projektsteuerung sind etabliert und werden zielführend eingesetzt.

4.3 Alle Stakeholder müssen ausreichend einbezogen werden

Das Projekt erfährt intensive Unterstützung durch den Rechtsdienst der Bundeskanzlei, und es besteht eine aktive Mitarbeit der departementalen Mitglieder im PA. In Folge dessen wurden Themen zur Konzeptüberarbeitung oder Einbringen einer Änderung in das Projekt bis anhin erkannt und abgearbeitet. Die notwendigen Fachstellen in- und ausserhalb der Bundeskanzlei werden hierbei beigezogen, z. B. wurden Kommentare des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) punktuell bei der Erarbeitung der

Datenschutz-Folgenabschätzung (DSFA) berücksichtigt; beim notwendig gewordenen Wechsel des M365-Lizenzmodells hat das Bundesamt für Bauten und Logistik (BBL) unterstützt.

Im Rahmen der Prüfung sind die folgenden Sachverhalte zur Sprache gekommen, bei denen nach Einschätzung der EFK ein Potenzial besteht, den Projektverlauf negativ zu beeinflussen:

- Der EDÖB wurde zur Abgabe einer Einschätzung zu verschiedenen Grundlagendokumenten des Projektes mit Bezug zum Daten- und Informationsschutz konsultiert. Hierbei wurde umfangreiches und detailliertes Feedback an das Projekt zugestellt. Weitere Austausche mit der Organisation des Projektes CEBA waren zum Zeitpunkt der Prüfung nicht geplant. Die Erfüllung der Vorgaben des Datenschutzes wird daher voraussichtlich im Rahmen der normalen Aufsichtstätigkeit des EDÖB überprüft.
  Mit Inkrafttreten des neuen Datenschutzgesetzes (nDSG) per 1. September 2023 erhält der EDÖB im Bereich der Aufsicht neu die Kompetenz, mittels Verfügung Datenbearbeitungen anzupassen und zu unter- oder abzubrechen, bei denen ein Verstoss gegen Datenschutzvorschriften festgestellt wird.
  Es ist für den Projekterfolg notwendig, dass die erhaltenen Eingaben des EDÖB durch das Projekt adäquat adressiert werden und dass der EDÖB als externer Stakeholder über die Lösungskonzepte des Projektes mit Bezug zur Daten- und Informationsschutz-Gesetzgebung informiert ist.

- Wie in Kapitel 3.3 ausgeführt, ist in einer geschäftlichen Beziehung mit geteilter betrieblicher Verantwortung für die Sicherheit von Daten ein Vertrauen in den gewählten Dienstleister notwendig. Dies gilt umso mehr, wenn es sich bei dem Dienstleister um ein global agierendes Unternehmen handelt, welches den Anforderungen einer Vielzahl von Kunden und Jurisdiktionen gerecht werden muss, und wenn die Daten des Auslagernden in einer aus dem öffentlichen Internet zugänglichen Cloud-Lösung gespeichert werden.
  Die über den Sommer 2023 von Microsoft bekannt gemachten Zugriffe auf Datenspeicher von M365-Kunden durch nicht autorisierte Dritte wurden zur Kenntnis genommen und entsprechende Abklärungen getroffen. Das Thema wurde zwischenzeitlich auch durch departementale Vertreter im PA in einer kritischen Tonalität zur Diskussion traktandiert und an der Projektausschuss-Sitzung vom August 2023 besprochen.

Beurteilung

Für den Projekterfolg (möglichst viele Departemente sollen die Ziellösung mit Cloud-Anbindung beziehen) ist es notwendig auch kritische Stimmen zu überzeugen, dass der Dienstleister mit einem angemessenen Mass an Kontrolle durch den Auslagernden überwacht werden kann, siehe Empfehlung 3 in Kapitel 3.3.

Der Austausch mit dem EDÖB war zum Prüfungszeitpunkt nach Einschätzung der EFK aus materieller Sicht unzureichend und birgt das Risiko, dass dieser mittels Verfügung interveniert, was Verzögerungen nach sich ziehen oder im schlimmsten Fall zum Abbruch führen kann.

Empfehlung 6 (Priorität 2)

Die EFK empfiehlt dem Bereich DTI, das im Projekt gewählte Vorgehen bezüglich Daten- und Informationsschutz erneut mit dem EDÖB abzustimmen. Der Stand der Entwicklungen sollte regelmässig besprochen werden, nicht zuletzt um einschätzen zu können, ob eine allfällige Verfügung des EDÖB der Erreichung des Projektziels entgegensteht.

Die Empfehlung ist akzeptiert.

Stellungnahme des Bereiches DTI der Bundeskanzlei

Das Projekt CEBA hat sich bezüglich Rechtsgrundlagenanalyse und Sicherheitsdokumente mit dem EDÖB ausgetauscht; erste Gespräche haben bereits vor über einem Jahr stattgefunden. Weiter wurde er formal in der Ämterkonsultation zu den Unterlagen für den Antrag des VK und für den Review der E031 mit einbezogen.

Das Projekt wird weiterhin den EDÖB regelmässig informieren und dessen Feedback zur datenschutzrelevanten Dokumentation abholen. Ebenso wird die Datenschutzfolgeabschätzung dem EDÖB vorgelegt.

4.4 Ein externer QRM ist beauftragt

Die Aufgaben, Kompetenzen und Verantwortung für das externe Qualitäts- und Risikomanagement sind definiert. Zwei Mitarbeiter einer Wirtschaftsberatungs-Gesellschaft sind als externes QRM bestellt. Sie sind ausreichend unabhängig vom Projekt CEBA. Die Rolle ist gemäss den Vorgaben von HERMES auszuführen. Dem externen QRM wird Zugriff zu allen benötigten Dokumenten gewährt.

Zum Zeitpunkt der Prüfung ist der fünfte QRM-Bericht in Arbeit. Die Arbeiten und deren Ergebnisse werden direkt mit dem Auftraggeber und der Projektleitung abgestimmt. Der Projektauftraggeber ist hierbei für das externe QRM der primäre Ansprechpartner. Feststellungen und Empfehlungen des externen QRM werden in den PA Sitzungen präsentiert und diskutiert.

Die EFK hat festgestellt, dass die Vorlage QS und Risikobericht aus HERMES nicht verwendet wird, um über die Qualität und die Risikosituation des Projekts zu informieren. Das externe QRM lehnt sich aber bei der Berichterstattung an die Themen von HERMES an.

Beurteilung

Das externe QRM ist eingerichtet und wird gelebt.

Die EFK weist darauf hin, dass bei vereinbarten Abweichungen zu HERMES in Projekten eine schriftliche Dokumentation der mündlichen Verabredung zu bevorzugen ist. Aufgrund des von der Auftraggeberschaft gegenüber der EFK bestätigten Umfangs der Berichterstattung des externen QRM verzichtet die EFK auf eine Empfehlung.

5 Berichterstattung an den Bundesrat und an das Parlament

Die aktuellste halbjährliche Berichterstattung des Projektes CEBA zum Zeitpunkt der EFK-Prüfung war diejenige zum Stichtag 31. Dezember 2022. Die Berichterstattung per 30. Juni 2023 lag im Entwurf vor, war jedoch noch nicht finalisiert und durch den Bereich DTI freigegeben. Diese wurde folglich von der EFK nicht geprüft.

5.1 Mängel beim Volumen, den Meilensteinen und den ausgewiesenen Kosten

Im Volumen fehlen die Eigenleistungen der Departemente

In der Berichterstattung per 31. Dezember 2022 setzt sich das Volumen des Projektes von 26,5 Mio. Franken zusammen aus 25,6 Mio. Franken für übriger Aufwand und Investitionen plus den internen Personalaufwand (Eigenleistungen) des EPA und der BK von 0,9 Mio. Franken. Es fehlt jedoch der Aufwand der Departemente von insgesamt 3 Mio. Franken.

Die 3 Mio. Franken für die Leitung der Projekte in den Departementen bezahlen diese selber. Gemäss Ausführungen der Projektleitung wäre der Aufwand für die Erhebung der Ist-Kosten zu aufwendig. Diese würden deshalb nicht in der Berichterstattung aufgeführt. Aus Gründen der Transparenz will die BK im nächsten Bericht darauf hinweisen.

Die Kosten sind nicht vollständig nachvollziehbar

Die Ausgaben des Projektes CEBA werden auf Stufe Gesamtprojekt von der Projektleitung in einem Finanzplan geführt und kontrolliert. Gemäss der Ausgabenplanung für 2023 und der Vorschau auf die Jahre bis 2025 sind die Ausgaben im Plan. Das verbleibende Volumen des Verpflichtungskredites ist ausreichend. Der Finanzplan dient auch zur Information des PA. Der Stand der Kosten wurde anhand eines Auszuges aus dem Finanzplan im Halbjahresbericht CEBA mit Stand Dezember 2022 dem Projektausschuss am 26. Januar 2023 präsentiert. Der im Halbjahresbericht enthaltene Auszug wurde jedoch nach Freigabe nochmals verändert und stimmt nicht mehr mit der an der PA-Sitzung vorgelegten Version überein.

Die EFK hat bei einer Stichprobe im SAP Rechnungen aufgefunden, die mit dem Vermerk CEBA gekennzeichnet, aber nicht auf das Projekt verbucht waren. Diese fehlen in Konsequenz in der Aufstellung des Finanzplanes. Für das Jahr 2022 belaufen sich diese Rechnungen, die im Rahmen der Prüfung der EFK identifiziert wurden, auf eine Summe von gerundet 230 000 Franken. Die Projektleitung hat diesen Sachverhalt abgeklärt, als Fehler erkannt und im System behoben.

Es war der EFK nicht möglich, einen Abgleich zwischen den in der Berichterstattung per 31. Dezember 2022 rapportierten Kosten, dem Abschnitt Kosten (aus SAP) im Cockpit IKT mit Stichtag 31. Dezember 2022 sowie dem Finanzplan der Projektleitung für den Monat Dezember 2022 vorzunehmen.

Die Meilensteintrendanalyse ist fehlerhaft

In der Berichterstattung per 31. Dezember 2022 sind in der Meilensteintrendanalyse die Meilensteine «Abschluss Phase Konzept Cloud@Ausland» und «Abschluss Phase Realisierung Cloud@Ausland» vertauscht wiedergegeben bzw. die beiden Meilensteine sind in der Legende vertauscht.

Beurteilung

Auf Nachfrage der EFK zu den Differenzen im Finanzplan hat die Projektleitung die Sachverhalte abgeklärt und konnte die Abweichungen zwischen Finanzplan und SAP erklären. Die Basis für die in der Berichterstattung per 31. Dezember 2022 genannten Zahlen bleibt jedoch unzuverlässig, da sich nicht alle Zahlen direkt aus SAP abgleichen lassen. Eine Korrektur der zum Prüfungszeitpunkt bereits veröffentlichten Berichterstattung per 31. Dezember 2022 ist nicht erfolgt.

Die EFK weist darauf hin, dass die Qualitätskontrollen des Bereiches DTI ausreichen müssen um sicherzustellen, dass Fehler in der Berichterstattung zukünftig frühzeitig erkannt werden können.

Die EFK hat dem Bereich DTI in ihrem Bericht «Prüfung des DTI-Schlüsselprojektes SUPERB – Teilprojekt PPM»[3] die Empfehlung Nr. 4 abgegeben. In dieser wird dem Bereich DTI empfohlen, «die Verankerung der PPM-Lösung als Bestandteil eines integrierten Führungsinstrumentariums mit der Weiterentwicklung des PFCT Bund ab 2025 zu prüfen. Das PFCT Bund ist in der Initialversion so auszuprägen, dass künftige Ausbauschritte um strategische Elemente unterstützt, resp. nicht verunmöglicht werden.»

Ein integriertes Führungsinstrumentarium im Sinne der Empfehlung ist zweckmässig, um Differenzen zwischen Informationsregistern zu vermeiden. Deren Umsetzung ist noch offen, die EFK verzichtet daher an dieser Stelle auf eine erneute Empfehlung.

5.2 Risiken und Beurteilungen müssen durchgängig wiedergegeben werden

Projektrisiken

Die Projektleitung führt die drei Top-Risiken des Projektes auf monatlicher Basis im Cockpit IKT nach. Operativ werden die Projektrisiken in der Risikoliste auf Stufe Gesamtprojekt geführt, wie in Kapitel 4.2 beschrieben.

In der Berichterstattung per 31. Dezember 2022 sind nur zwei Risiken gemäss dem Cockpit IKT aufgeführt. Das am höchsten bewerteten Risiko fehlt. Anstelle dessen ist in der Berichterstattung ein weiteres, nicht im Cockpit IKT geführtes Risiko aufgeführt. Bei beiden in der Berichterstattung aufgeführten Risiken unterscheidet sich der Risikowert jedoch von den im Cockpit IKT geführten Bewertungen.

[3] Der Prüfbericht (PA 22741) ist auf der Website der EFK verfügbar.

Risiken zum produktiven Einsatz der Lösung

Das vom Projekt in der Entwurfsversion V0.7 vorgelegte CEBA ISDS-Konzept enthält eine Analyse und Aufstellung von 38 aus Sicht des Projektes «kritisch verbleibenden Restrisiken», die vor Einführung des Projekts formell zu akzeptieren sind.

In der Berichterstattung ist eine Projektbeschreibung enthalten. Diese führt im Abschnitt «Restrisiken und Massnahmen» aus, dass wesentliche Restrisiken bei der Verwendung von M365 Cloud-Diensten anfallen werden, und diese von den Verwaltungseinheiten getragen werden müssen. Diese Einschätzung der Restrisiken ist deckungsgleich auch im Informationspapier zuhanden der GSK vom 25. November 2022 enthalten. In dieser Projektbeschreibung wird eines der genannten Restrisiken als «moderat» eingeschätzt.

Der Beschreibung ist zu entnehmen, dass das erwähnte moderate Restrisiko die beiden Restrisiken R17 und R18 aus dem ISDS-Konzept zusammenfasst. Diese beiden Restrisiken sind im Entwurf des ISDS-Konzepts jedoch mit Auswirkungsgrad «wesentlich» und Eintretenswahrscheinlichkeit «möglich» eingeschätzt, siehe nachstehende Abbildung.

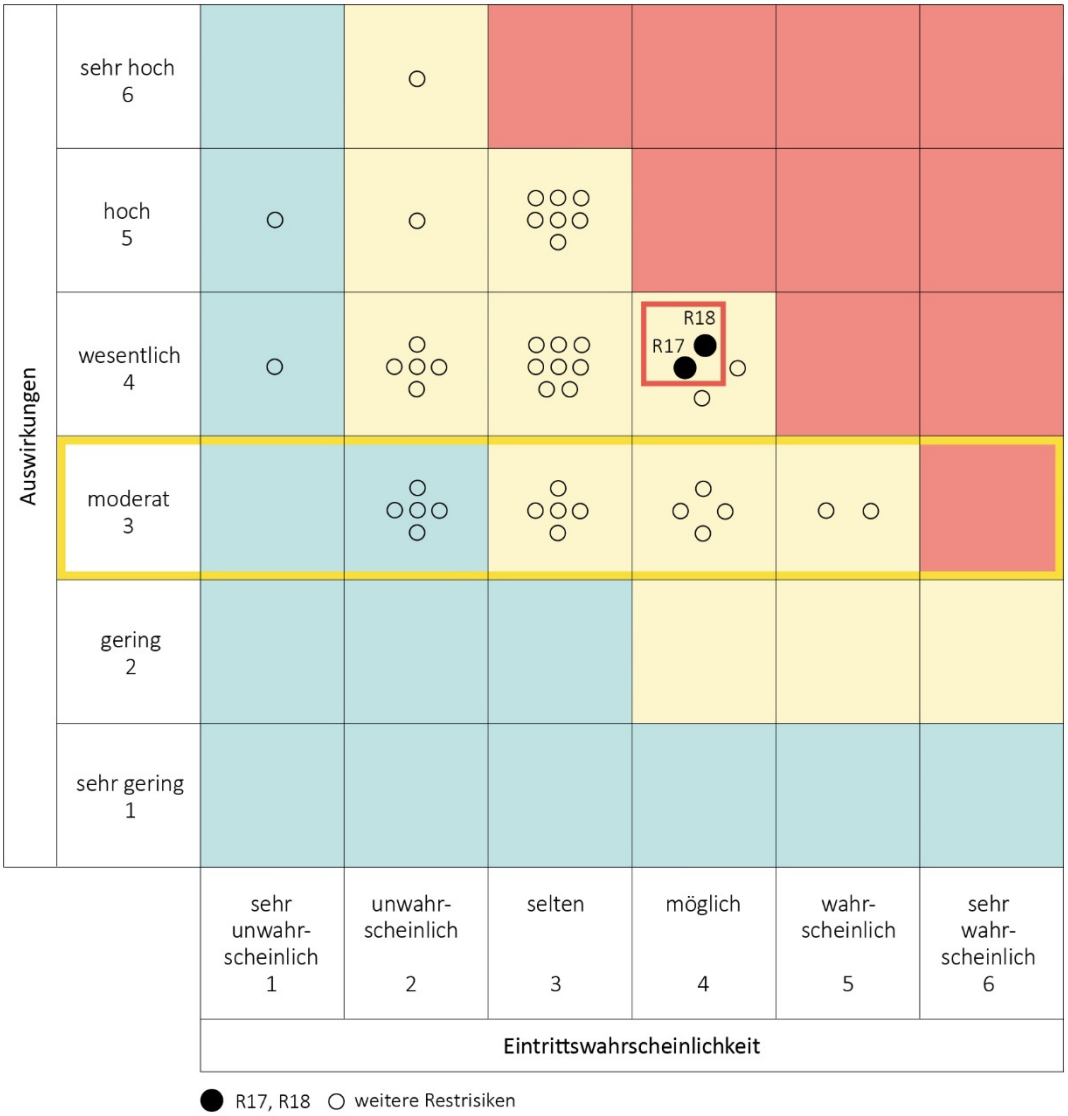

Abbildung 1: Die Restrisiken R17 und R18 in V0.7 des ISDS-Konzepts (rot umrandet), Darstellung: EFK

Beide liegen von ihrem Auswirkungsgrad her in der Analyse im ISDS-Konzept über der in der Berichterstattung erwähnten Einschätzung als «moderat», siehe gelb hervorgehobener Bereich in Abbildung 1. Die Einschätzung der betrieblichen Restrisiken in der Projektbeschreibung ist somit nicht gemäss der Bewertung im ISDS-Konzept wiedergegeben.

Beurteilung

Die Projektleitung beurteilt zwei wesentliche Risiko-Komplexe und gibt diese in der Berichterstattung per 31. Dezember 2022 wieder. Dies sind zum einen die operativen Projektrisiken, welche möglicherweise einer erfolgreichen Einführung des Projektes entgegenstehen. Zum anderen sind dies die Restrisiken, die sich im produktiven Betrieb der Lösung nach Anwendung aller vorgesehenen Sicherheitsmassnahmen ergeben. Diese Aufteilung ist sinnvoll.

Zu bemängeln ist, dass die Top-Projektrisiken in der Berichterstattung per 31. Dezember 2022 von den im Cockpit IKT geführten Top-Risiken abweichen und mit abweichenden Risikowerten bewertet wurden.

In der Offenlegung der betrieblichen Restrisiken fehlt eine durchgängige Transparenz.

Die EFK anerkennt, dass das ISDS-Konzept auf die Einführung des Projektes CEBA hin noch finalisiert werden wird und inkl. der darin ausgeführten Restrisiken noch formell abzunehmen ist. Der im Rahmen der Prüfung vorgelegte Entwurf stellt somit einen Zwischenstand dar. Es handelt sich hierbei jedoch teils um inhärente Risiken eines Cloud-Vorhabens, wie z. B. eine nachrichtendienstliche Ausspähung, Verlust der digitalen Souveränität oder unberechtigte Zugriffe auf vertrauliche Daten, die nicht vollständig beseitigt werden können und daher letztendlich akzeptiert werden müssen.

Wichtig für die Weiterentwicklung des ISDS-Konzepts bleibt daher, dass eine abgestimmte gemeinsame Sicht auf die Risiken, die möglichen Massnahmen sowie die Restrisiken hergestellt werden kann. Das ISDS-Konzept muss als Resultat ein für die Bundesverwaltung insgesamt tragbares Risiko-Niveau ausweisen. Die Einschätzung, ob ein Restrisiko tragbar ist, muss nach Berücksichtigung der technisch und organisatorisch möglichen Massnahmen zur Risikominderung erfolgen. Eine Einführung der Lösung darf erst erfolgen, wenn die organisatorischen und technischen Massnahmen zur Risikominderung wirksam eingeführt sind.

Empfehlung 7 (Priorität 2)

Die EFK empfiehlt dem Bereich DTI, die Einschätzung der Top-Projektrisiken in der Berichterstattung an den Bundesrat und an das Parlament konsistent zu den projektinternen Arbeitspapieren bzw. dem Cockpit IKT zu rapportieren.

Die Empfehlung ist akzeptiert.

Stellungnahme des Bereiches DTI der Bundeskanzlei

Das Zielpublikum ist unterschiedlich, deshalb sind die Texte zu den Risiken unterschiedlich. Die Risikowerte werden jedoch konsistent gehalten (konkret werden die Risikowerte in den IKT-Schlüsselprojektreportings identisch zum Cockpit berichtet).

Die im IKT-Cockpit rapportierten Projektrisiken werden regelmässig und zeitgleich abgeglichen mit dem Schlüsselprojektbericht. Die Qualitätskontrolle wird in Zukunft vermehrt auf die Konsistenz achten.

Empfehlung 8 (Priorität 1)

Die EFK empfiehlt dem Bereich DTI sicherzustellen, dass mit der Finalisierung des ISDS Konzepts die Vollständigkeit der Risiken überprüft wird und ein mit den späteren Nutzern abgestimmtes Risikoverständnis besteht. Die Restrisiken müssen auf der angemessenen Hierarchiestufe freigegeben werden. Im Falle von signifikanten Veränderungen sind die GSK und der Bundesratsausschuss Digitalisierung über die finalen Bewertungen der betrieblichen Restrisiken zu informieren.

Die Empfehlung ist akzeptiert.

Stellungnahme des Bereiches DTI der Bundeskanzlei

Das ISDS Konzept wurde finalisiert und unterzeichnet.

Die Restrisiken werden vom Bundeskanzler und vom Leiter DTI übernommen.

Die Restrisiken und das ISDS-Konzept wurden am 30. Januar 2024 dem DRB zur Stellungnahme unterbreitet. Anschliessend wurde die GSK über die Diskussion und den Entscheid aufgrund der Positionen im DRB zum Rollout von CEBA informiert und auf die Möglichkeit zur Eskalation in die GSK aufmerksam gemacht. Kein Departement hat von der Möglichkeit der Eskalation Gebrauch gemacht. Der Bundesrat wurde am 14. Februar 2024 über die Einführung von M365 informiert.

Anhang 1: Rechtsgrundlagen und weitere Dokumente

Rechtstexte
Regierungs- und Verwaltungsorganisationsgesetz (RVOG) vom 21. März 1997, SR 172.010
Regierungs- und Verwaltungsorganisationsverordnung (RVOV) vom 1. Juli 2022, SR 172.010.1
Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (Verordnung über die digitale Transformation und die Informatik, VDTI) vom 25.11.2020, SR 172.010.58
Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung) vom 1. April 2020, SR 172.010.441
Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020, SR 235.1
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967, SR 614.0
Botschaften
23.007 – Botschaft über den Nachtrag Ib zum Voranschlag 2023 vom 29. März 2023
Weisungen
Weisungen über die Risikopolitik des Bundes vom 24. September 2010, BBI 2010 6549
W007 – Weisungen des Bundesrates zu den IKT-Projekten in der Bundesverwaltung und zum IKT-Portfolio des Bundes
SB008 – IKT-Teilstrategie Büroautomation Bund (BA Bund) 2021–2024
SB020 – Cloud-Strategie der Bundesverwaltung
Si001 – IKT-Grundschutz in der Bundesverwaltung
Si004 – Regelung der Zugriffe auf Ressourcen im Internet (Web Proxy Richtlinie BV)
P035 – Umgang mit Anforderungen und Vorgaben zur Bundesinformatik
P038 – Berichterstattung über die DTI-Schlüsselprojekte des Bundes
P051 – Weisungen zum Informatikcontrolling in der Bundesverwaltung

Anhang 2: Abkürzungen

BA	Büroautomation
BBL	Bundesamt für Bauten und Logistik
BIT	Bundesamt für Informatik und Telekommunikation
CEBA	Projekt «Cloud-Enabling Büroautomation»
DLV	Dienstleistungsvereinbarung
DRB	Digitalisierungsrat des Bundes
DSFA	Datenschutz-Folgenabschätzung
DTI	Bereich für Digitale Transformation und IKT-Lenkung der Bundeskanzlei
EBT	Projekt «Evolution BA-Technologie»
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFK	Eidgenössische Finanzkontrolle
EPA	Eidgenössisches Personalamt
GSK	Generalsekretärenkonferenz
ISB	Informatiksteuerungsorgan des Bundes
IT-EDA	Informatik EDA
LE	Leistungserbringer
M365	Microsoft 365, vormals Microsoft Office 365
nDSG	Bundesgesetz über den Datenschutz
OSS	Open Source Software
PA	Projektausschuss
Schuban	Schutzbedarfsanalyse
SD	Standarddienst

SLA	Service Level Agreement
TP	Teilprojekt
VK	Verpflichtungskredit

Anhang 3: Glossar

CLOUD Act	Clarifying Lawful Overseas Use of Data Act Der CLOUD Act ist ein seit 2018 bestehendes US-amerikanisches Gesetz zum Zugriff der US-Behörden auf gespeicherte Daten im Internet. Das Gesetz verpflichtet amerikanische Internet-Firmen und IT-Dienstleister, US-Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt.
HERMES	eCH-0054: HERMES Projektmanagement-Methode 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.
ISDS-Konzept	Informationssicherheits- und Datenschutz-Konzept Das ISDS-Konzept bildet die Grundlage für die Festlegung der Massnahmen für die Informationssicherheit und den Datenschutz. Es zeigt die Restrisiken auf, die mit dem Betrieb eines IT-Systems und der Organisation verbunden sind. Es beschreibt das Notfallkonzept.
On-Premises	Engl. «vor Ort» Die Bezeichnung «On-Premises» (kurz auch «On-Prem») wird verwendet, um ein Lizenz- und Nutzungsmodell für Software zu beschreiben. Software «On-Premises» zu betreiben, heisst, diese auf eigenen Servern zu installieren und zu hosten.
SD-BA	Standarddienst Büroautomation Die Büroautomation unterstützt die Verwaltungstätigkeit mit geeigneten IKT-Mitteln, wie den Arbeitsplatzsystemen inkl. zugehöriger Kommunikations- und Kollaborationsservices.

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).