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

Audit de la mise en œuvre de la stratégie cloud

Chancellerie fédérale – secteur Transformation numérique et gouvernance de l'informatique, Office fédéral de l'informatique et de la télécommunication

CDF-23766 | Prises de position incluses | 11 avril 2024

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Contrôle fédéral des finances (CDF) Monbijoustrasse 45 3003 Berne Suisse
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	104.23766
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Table des matières

Audit de la mise en œuvre de la stratégie cloud

Chancellerie fédérale – secteur Transformation numérique et gouvernance de l'informatique, Office fédéral de l'informatique et de la télécommunication

L'essentiel en bref

L'informatique en nuage (« cloud computing ») est une composante importante de la transformation numérique de l'administration fédérale. Elle doit lui permettre de réaliser ses projets innovants de manière plus rapide, plus agile et à moindres coûts. Dans cette perspective, le Conseil fédéral a adopté en 2020 une stratégie d'informatique en nuage. Cette dernière définit les modalités d'approvisionnement possibles, notamment les nuages privés des prestataires internes de la Confédération, publics de fournisseurs externes, et combinés – hybrides. Elle souligne en particulier la nouvelle option des nuages publics. Enfin, elle propose un modèle organisationnel décrivant les rôles des différents intervenants pour la gouvernance, les intermédiaires (« Cloud Service Broker », CSB) et l'exploitation du nuage. La mise en œuvre de cette stratégie incombe au secteur Transformation numérique et gouvernance de l'informatique (Secteur TNI) de la Chancellerie fédérale.

Le Contrôle fédéral des finances (CDF) a examiné la mise en œuvre de cette stratégie. Il constate qu'une majorité de jalons ont été atteints, mais que quelques points ouverts subsistent. Le modèle de niveaux doit notamment être affiné et un cadre élaboré pour l'utilisation de services de type « Software as a Service » (solutions hébergées sur le cloud). Un processus réglant les améliorations des outils de travail et de meilleures possibilités pour l'échange d'expériences entre intervenants doivent aussi être mis en place.

Les jalons de la mise en œuvre sont définis, les travaux ne sont pas encore terminés

La stratégie d'informatique en nuage définit huit jalons s'étendant jusqu'en 2025 ainsi que le détail des produits à livrer. Une majorité de ces produits ont été élaborés, certains en retard, et quelques autres doivent encore être finalisés. Parmi les résultats particulièrement importants, le CDF relève l'établissement de contrats-cadres avec cinq fournisseurs de services de cloud public pour un total de 110 millions de francs. Le Secteur TNI a aussi mis au point différents documents fondamentaux, notamment un cadre juridique et des principes pour l'utilisation de services d'informatique en nuage public. Divers exemples et une première génération d'outils d'aide à la décision ont par ailleurs été élaborés.

Le cahier des charges du CSB et les clarifications à la procédure d'appel (en cours de validation) ainsi que la mise à jour de la stratégie pour le réseau de centres de calcul sont des éléments encore ouverts lors de l'audit. La mise en place du modèle-cible organisationnel se poursuit. L'Office fédéral de l'informatique et de la télécommunication (OFIT), dans son rôle de CSB, continue d'étendre sa palette de guides et d'aides à la mise en œuvre du nuage public à l'attention des bénéficiaires des prestations.

Le modèle des niveaux et les principes doivent être complétés, les risques et les chances sont globalement déterminés

Le modèle actuellement en vigueur décrit quatre niveaux d'informatique en nuage (deux pour le cloud public, deux pour le privé) et un niveau correspondant à l'exploitation classique dans des centres de calcul de la Confédération. Conçu comme une aide à l'orientation, il ne délimite pas nettement ces niveaux et ne définit pas clairement tous les critères d'adéquation pour le choix d'un niveau. Le Conseil fédéral a déjà demandé au Secteur TNI de clarifier le modèle et des extensions sont en cours.

Le CDF a relevé que les principes couvrent les prestations de type infrastructure et plateforme comme service (« IaaS » et « PaaS ») mais pas celles de type solution (« SaaS »), alors que ces dernières étaient aussi dans le périmètre de la stratégie. Le CDF a demandé au Secteur TNI d'élaborer un cadre pour l'utilisation des SaaS.

Il n'existe pas d'examen détaillé des chances et des risques pour chaque niveau du modèle, seulement pour le nuage public en général. Ces éléments forment toutefois une première base de travail suffisante pour les travaux – analyse des bases légales, des risques et de rentabilité – que les bénéficiaires des prestations doivent continuer de faire au sein de leurs projets cloud. Le Secteur TNI suit par ailleurs en permanence les évolutions des technologies et des aspects juridiques de l'utilisation de l'informatique en nuage.

Les intervenants sont suffisamment intégrés, mais les échanges d'expériences doivent être facilités

Les intervenants au processus de mise en œuvre de la stratégique d'informatique en nuage et leur rôle sont définis. Ils ont été suffisamment intégrés dans l'élaboration des résultats. Ceux-ci ont été validés par le délégué TNI.

En revanche, une plateforme d'échange des enseignements tirés lors des projets de mise en œuvre de l'informatique en nuage fait défaut. La courbe d'apprentissage est raide et les intervenants ont un degré de maturité inégal dans l'utilisation de ces technologies. Le CDF a demandé à l'OFIT en collaboration avec le Secteur TNI de mettre en place une telle plateforme d'échange. L'objectif est de diffuser les bonnes pratiques et éviter que certaines erreurs ne se répètent dans les projets.

La première génération d'outils de travail devra être complétée et un processus mis en place pour gérer les priorités des travaux

Le Secteur TNI et l'OFIT ont mis en place une première génération d'aides à la décision (guides, processus, grilles d'analyse, etc.) en vue de l'utilisation de services d'informatique en nuage. Cette palette est régulièrement complétée. L'accès aux documents n'est toutefois pas toujours aisé. De plus, des modèles ou des outils de travail manquent pour certaines étapes préconisées dans les principes.

Le CDF a relevé que certaines notions pour déterminer le niveau approprié du cloud étaient encore floues. Le Conseil fédéral doit d'ailleurs encore livrer des éclaircissements sur le point de la souveraineté numérique. Enfin, avec l'évolution des techniques et des aspects juridiques et la montée en compétence des intervenants, de nouveaux outils seront requis. Pour une mise en œuvre priorisée des outils et des améliorations les plus utiles, un processus dédié doit être mis en place.

Prüfung der Umsetzung der Cloud-Strategie

Bundeskanzlei – Bereich Digitale Transformation und IKT-Lenkung, Bundesamt für Informatik und Telekommunikation

Das Wesentliche in Kürze

Cloud-Computing ist ein wesentlicher Bestandteil der digitalen Transformation der Bundesverwaltung. Es soll der Bundesverwaltung ermöglichen, ihre innovativen Projekte schneller, agiler und kostengünstiger umzusetzen. Vor diesem Hintergrund hat der Bundesrat 2020 eine Cloud-Strategie verabschiedet. Darin sind die möglichen Beschaffungsmodalitäten festgelegt, darunter Private Clouds von bundesinternen Anbietern, Public Clouds von externen Anbietern sowie Hybrid Clouds, eine Kombination daraus. In der Strategie wird insbesondere die neue Option der Public Clouds hervorgehoben. Schliesslich enthält die Strategie ein organisatorisches Zielbild, in dem die Rollen der verschiedenen Beteiligten für die Governance, die Intermediäre («Cloud Service Broker», CSB) und den Cloud-Betrieb beschrieben sind. Für die Umsetzung dieser Strategie ist der Bereich Digitale Transformation und IKT-Lenkung (DTI-Bereich) der Bundeskanzlei zuständig.

Die Eidgenössische Finanzkontrolle (EFK) hat die Umsetzung dieser Strategie geprüft. Sie stellt fest, dass die meisten Meilensteine erreicht wurden, einige Punkte jedoch noch offen sind. So soll insbesondere das Stufenmodell verfeinert und ein Rahmen für die Nutzung von «Software as a Service»-Diensten (in der Cloud gehostete Lösungen) ausgearbeitet werden. Des Weiteren soll es einen Prozess für die Optimierung der Arbeitshilfen sowie bessere Möglichkeiten für den Erfahrungsaustausch unter den Beteiligten geben.

Die Meilensteine für die Umsetzung sind festgelegt, die Arbeiten aber noch nicht abgeschlossen

Die Cloud-Computing-Strategie definiert acht Meilensteine, die sich bis 2025 erstrecken, und die Einzelheiten der zu liefernden Produkte. Die meisten dieser Produkte wurden entwickelt, manche mit Verspätung, andere sind noch nicht ganz abgeschlossen. Zu den besonders wichtigen Ergebnissen zählt die EFK den Abschluss von Rahmenverträgen mit fünf Public-Cloud-Anbietern über insgesamt 110 Millionen Franken. Der DTI-Bereich hat ebenfalls verschiedene grundlegende Dokumente ausgearbeitet, insbesondere einen rechtlichen Rahmen und Grundsätze für die Nutzung von Public-Cloud-Diensten. Darüber hinaus wurden verschiedene Beispiele und eine erste Generation an Entscheidungshilfen erstellt.

Das CSB-Pflichtenheft und die Klärung des Abrufverfahrens (Validierung läuft) sowie die Aktualisierung der Strategie für den Rechenzentren-Verbund sind Punkte, die zum Prüfungszeitpunkt noch offen waren. Die Einführung des organisatorischen Zielbilds setzt sich fort. Das Bundesamt für Informatik und Telekommunikation (BIT) baut in seiner Rolle als CSB seine Palette an Leitfäden und Hilfen zur Umsetzung der Public-Cloud für die Leistungsbezüger weiter aus.

Das Stufenmodell und die Grundsätze sind zu ergänzen, die Risiken und Chancen wurden grundsätzlich bestimmt

Das aktuelle Modell beschreibt vier Cloud-Stufen (zwei für die Public Cloud, zwei für die Private Cloud) und eine Stufe für den klassischen Betrieb in den bundeseigenen Rechenzentren. In dem als Orientierungshilfe entwickelten Modell sind diese Stufen nicht deutlich voneinander abgegrenzt und die Kriterien für die Auswahl einer Stufe nicht klar definiert. Der Bundesrat hat den DTI-Bereich bereits gebeten, das Modell zu präzisieren, Erweiterungen sind im Gange.

Die EFK stellt fest, dass die Grundsätze Infrastruktur- und Plattformdienste («IaaS» und «PaaS»), aber keine Lösungsdienste («SaaS») abdecken, obwohl Letztere auch im Strategieperimeter liegen. Die EFK hat den DTI-Bereich aufgefordert, einen Rahmen für die Nutzung von SaaS-Diensten auszuarbeiten.

Es existiert keine detaillierte Prüfung der Chancen und Risiken der einzelnen Modellstufen, sondern nur für die Public Cloud im Allgemeinen. Diese Elemente stellen jedoch eine erste Grundlage für die Arbeiten dar, die die Leistungsbezüger weiterhin in ihren Cloud-Projekten durchführen müssen (Analyse der Rechtsgrundlagen, Risiken und Rentabilität). Darüber hinaus verfolgt der DTI-Bereich kontinuierlich die Entwicklungen der Technologien und rechtlichen Aspekte der Cloud-Computing-Nutzung.

Die Beteiligten sind ausreichend eingebunden, der Erfahrungsaustausch soll aber erleichtert werden

Die an der Umsetzung der Cloud-Computing-Strategie beteiligten Akteure und ihre Rollen sind festgelegt. Sie wurden bei der Ausarbeitung der Ergebnisse ausreichend eingebunden. Die Ergebnisse wurden vom Delegierten DTI validiert.

Eine Plattform für den Austausch von Erkenntnissen aus den Projekten für die Umsetzung des Cloud-Computing fehlt dagegen. Die Lernkurve ist steil und die Beteiligten weisen bei der Nutzung dieser Technologien unterschiedliche Reifegrade auf. Die EFK hat das BIT aufgefordert, gemeinsam mit dem DTI-Bereich eine solche Plattform einzurichten. Ziel ist es, Best Practices zu verbreiten und zu verhindern, dass sich bestimmte Fehler in den Projekten wiederholen.

Die erste Generation an Arbeitshilfen muss ergänzt und ein Prozess für das Prioritätenmanagement der Arbeiten eingeführt werden

Der DTI-Bereich und das BIT haben für die Nutzung von Cloud-Diensten eine erste Generation an Entscheidungshilfen (Leitfäden, Prozesse, Analyseraster etc.) eingeführt. Diese werden regelmässig ergänzt. Die Dokumente sind jedoch nicht immer leicht zugänglich. Zudem fehlen für einige der in den Grundsätzen empfohlenen Schritte Vorlagen oder Arbeitshilfen.

Die EFK stellt fest, dass einige Begriffe zur Bestimmung der angemessenen Cloud-Stufe noch unklar sind. Ausserdem soll der Bundesrat die Frage der digitalen Souveränität noch klären. Schliesslich werden angesichts der Entwicklungen auf technischer und gesetzlicher Ebene und der zunehmenden Kompetenz der Beteiligten neue Arbeitshilfen erforderlich sein. Für eine vorrangige Umsetzung der nützlichsten Arbeitshilfen und Optimierungen soll ein entsprechender Prozess eingeführt werden.

Originaltext auf Französisch

Verifica dell'attuazione della strategia cloud

Settore Trasformazione digitale e governance delle TIC della Cancelleria federale e Ufficio federale dell'informatica e della telecomunicazione

L'essenziale in breve

La nuvola informatica («cloud computing») è una componente importante per la trasformazione digitale dell'Amministrazione federale. I cloud permettono di attuare progetti innovativi in maniera più rapida, agile e a basso costo. In tale prospettiva, nel 2020 il Consiglio federale ha adottato la strategia cloud della Confederazione. Quest'ultima definisce le possibili modalità di approvvigionamento, segnatamente i cloud privati di fornitori interni alla Confederazione, i cloud pubblici di fornitori esterni e i cloud combinati, ossia ibridi. In particolare, la strategia mette in evidenza la nuova opzione dei cloud pubblici. Propone infine un modello organizzativo che descrive i ruoli dei vari partecipanti nell'ambito della governance, gli intermediari («cloud service broker», CSB) e la gestione dei cloud. L'attuazione della strategia compete al Settore Trasformazione digitale e governance delle TIC (Settore TDT) della Cancelleria federale.

Il Controllo federale delle finanze (CDF) ha sottoposto a verifica l'attuazione della summenzionata strategia. Ha constatato che, sebbene le tappe siano in gran parte raggiunte, alcuni aspetti rimangono in sospeso. Ad esempio deve essere perfezionato il modello dei livelli, nonché predisposto un quadro per l'utilizzo dei servizi «Software as a Service» (SaaS, modello applicativo ospitato su cloud). Inoltre, è necessario realizzare un processo che disciplini l'ottimizzazione degli strumenti di lavoro, come pure le possibilità di scambio di esperienze tra i partecipanti.

Le tappe dell'attuazione sono definite, ma i lavori non sono ancora conclusi

La strategia cloud definisce otto tappe che durano fino al 2025 e, nel dettaglio, anche i prodotti che devono essere forniti. La maggior parte di essi è stata elaborata, benché in ritardo, mentre alcuni prodotti devono ancora essere finalizzati. Tra i risultati di particolare rilevanza, il CDF ha constatato la conclusione di contratti quadro con cinque fornitori di servizi di cloud pubblici, per un importo complessivo di 110 milioni di franchi. Il Settore TDT ha inoltre messo a punto diversi documenti fondamentali, ad esempio un quadro giuridico e una serie di principi per l'utilizzo di servizi nel cloud pubblico. Inoltre, sono stati sviluppati diversi esempi e la prima generazione di strumenti di lavoro, che fungono da supporto alle decisioni.

Il capitolato d'oneri del CSB, i chiarimenti relativi al bando (in corso di validazione) e l'aggiornamento della strategia per la rete dei centri di calcolo sono elementi che risultavano ancora in sospeso al momento della verifica. L'attuazione del modello organizzativo di riferimento avanza. Nel suo ruolo di CSB, l'Ufficio federale dell'informatica e della telecomunicazione (UFIT) continua ad ampliare la sua gamma di linee guida e documenti di aiuto per l'implementazione del cloud pubblico, che sono destinati ai beneficiari delle prestazioni.

Il modello dei livelli e i principi devono essere completati, i rischi e le opportunità sono generalmente definiti

Il modello vigente descrive quattro livelli di cloud (due per i cloud pubblici, due per i cloud privati) e un livello che corrisponde alla gestione classica nei centri di calcolo della Confederazione. Concepito quale ausilio orientativo, il modello non delimita nettamente questi livelli, né definisce in maniera esaustiva tutti i criteri di adeguamento per la scelta di un livello. Il Consiglio federale ha già chiesto al Settore TDT di chiarire il modello. Sono in corso degli ampliamenti.

Secondo il CDF, i principi coprono le prestazioni di servizi relative all'infrastruttura e alla piattaforma («IaaS» e «PaaS»), ma non le prestazioni di servizi («SaaS»), anche se queste ultime facevano parte della strategia. Il CDF ha chiesto al Settore TDT di allestire un piano per l'utilizzo delle SaaS.

Non esiste alcuna analisi dettagliata delle opportunità e dei rischi per ciascun livello del modello, cosa che viene fatta soltanto per il cloud pubblico. Questi elementi costituiscono tuttavia una prima base sufficiente per i lavori (analisi delle basi legali, dei rischi e della redditività) che i beneficiari delle prestazioni devono continuare a svolgere nell'ambito dei loro progetti in ambito cloud. Il Settore TDT segue peraltro costantemente l'evoluzione tecnologica e i cambiamenti in atto sul piano giuridico nell'utilizzo del «cloud computing».

I partecipanti sono sufficientemente coinvolti, ma va promosso lo scambio di esperienze

I partecipanti al processo di attuazione della strategia cloud della Confederazione e i rispettivi ruoli sono definiti. I partecipanti sono stati sufficientemente coinvolti nell'elaborazione dei risultati, peraltro validati dal delegato TDT.

Manca tuttavia una piattaforma di scambio delle conoscenze acquisite nel quadro dei progetti di attuazione dei cloud. Vi sono notevoli sforzi da compiere nel processo di apprendimento e il grado di dimestichezza dei partecipanti nell'utilizzo di queste tecnologie non è omogeneo. Il CDF ha chiesto all'UFIT di realizzare una simile piattaforma di scambio in collaborazione con il Settore TDT. L'obiettivo è diffondere le buone pratiche ed evitare il reiterarsi di determinati errori nei progetti.

Occorre completare la prima generazione di strumenti di lavoro e realizzare un processo per gestire le priorità dei lavori

In vista dell'utilizzo dei servizi di «cloud computing», il Settore TDT e l'UFIT hanno realizzato una prima generazione di strumenti di supporto alle decisioni (linee guida, processi, liste di controllo ecc.), che viene regolarmente ampliata. Tuttavia, l'accesso ai documenti non è sempre facile. Inoltre, per alcune tappe mancano alcuni modelli o strumenti di lavoro formulati nei principi.

Il CDF ha appurato che alcuni concetti utilizzati per determinare il livello appropriato del cloud erano espressi in maniera astratta. Del resto, il Consiglio federale deve ancora fornire chiarimenti in merito alla sovranità digitale. Infine, con l'evoluzione tecnologica, i cambiamenti in atto sul piano giuridico e il rafforzamento delle competenze dei partecipanti saranno richiesti nuovi strumenti. Occorre dunque realizzare un processo specifico che definisca le priorità di attuazione degli strumenti e dei miglioramenti reputati indispensabili.

Testo originale in francese

Audit of the implementation of the cloud strategy

Federal Chancellery – Digital Transformation and ICT Steering Sector, Federal Office of Information Technology, Systems and Telecommunication

Key facts

Cloud computing is a key element of the Federal Administration's digital transformation. It should allow it to carry out innovative projects more rapidly, in a more agile manner and at lower cost. With this in mind, in 2020 the Federal Council adopted a cloud computing strategy. This sets out the possible details for service provision, specifically the Confederation's internal service providers' private clouds, external suppliers' external clouds and combined (hybrid) clouds. In particular, it underscores the new option of public clouds. Finally, it proposes an organisational model which describes the roles of the different stakeholders as regards governance, intermediaries (cloud service broker, CSB) and cloud operation. The Federal Chancellery's Digital Transformation and ICT Steering Sector (DTI) is responsible for implementing this strategy.

The Swiss Federal Audit Office (SFAO) audited the implementation of this strategy. It found that the majority of milestones had been reached, but that some points remained outstanding. In particular, the levels model needs to be refined and a framework developed for the use of software as a service (solutions hosted in the cloud). A process governing improvements to tools and better opportunities for stakeholders to exchange experiences also need to be put in place.

The milestones for implementation have been defined, but work is not yet finished

The cloud computing strategy defines eight milestones up to 2025, as well as the details of the products to be supplied. The majority of these products have been designed, some of them with a delay, and some others still need to be finalised. As particularly important findings, the SFAO noted among other things that framework contracts had been concluded with five public cloud service providers for a total of CHF 110 million. The DTI Sector has also drawn up different basic documents, especially a legal framework and the principles for using public cloud computing services. Various examples and a first-generation decision-making support tool have also been created.

The specifications for the CSB and the clarification of the appeals procedure (currently being validated), as well as the update of the strategy for the network of computer centres, were still outstanding at the time of the audit. The implementation of the target organisational model is ongoing. The Federal Office of Information Technology, Systems and Telecommunication (FOITT), in its role as CSB, continues to extend its range of public cloud guides and implementation aids aimed at service recipients.

The levels model and the principles need to be completed; the risks and opportunities have been defined overall

The currently applicable model describes four cloud computing levels (two for the public cloud, and two for the private cloud) and one level representing classical operation in the federal computer centres. Designed as an orientation aid, it does not clearly delineate the levels, nor does it clearly define all the criteria for choosing a level. The Federal Council has already requested the DTI Sector to clarify the model, and it is in the process of being expanded.

The SFAO found that the principles cover infrastructure as a service (IaaS) and platform as a service (PaaS), but not software as a service (SaaS), although the latter was included in the strategy. The SFAO has requested the DTI Sector to draw up a framework for the use of SaaS.

A detailed risk/reward analysis exists only for the public cloud in general, rather than for each level of the model. However, these elements form a sufficient working basis for the activities – assessment of the legal basis, risks and profitability – which the service recipients must continue to carry out within their cloud projects. In addition, the DTI Sector constantly monitors technological developments and the legal aspects of using cloud computing.

The stakeholders are sufficiently involved, but it must be made easier for them to exchange experiences

The stakeholders in the implementation process for the cloud computing strategy, and their roles, have been defined. They were sufficiently involved in the compilation of results. These results have been validated by the DTI delegate.

By contrast, there is no platform for exchanging the lessons learnt from cloud computing implementation projects. The learning curve is steep and the stakeholders have differing levels of maturity in using these technologies. The SFAO has requested the FOITT, together with the DTI Sector, to set up such an exchange platform. The aim is to share good practice and avoid certain errors being repeated in the projects.

The first generation of work tools should be completed and a process for managing work priorities should be put in place

The DTI Sector and the FOITT have implemented a first generation of decision-making aids (guides, processes, assessment grids, etc.) for using cloud computing services. This offering is regularly updated. However, access to documents is not always easy. Moreover, there is a lack of models or work tools for certain stages recommended in the principles.

The SFAO noted that some concepts for determining the appropriate cloud level are still unclear. In addition, the Federal Council still has to provide clarification on the question of digital sovereignty. Finally, developments in technologies and legal aspects, as well as the increasing skills of the stakeholders, will require new tools. A dedicated process needs to be put in place in order to prioritise implementation of the most useful tools and improvements.

Original text in French

Prises de position générales

Stellungnahme des Bereichs Digitale Transformation und IKT-Lenkung der Bundeskanzlei

Der Bereich DTI der BK dankt der EFK für die Prüfung und für die Gelegenheit der Stellungnahme. Wichtige Voraussetzungen für die Einführung von Public oder Private Clouds, sowie Hilfestellungen für Bezüger wurden erarbeitet und weitere sind in Arbeit. Die Umsetzung der Cloud-Strategie schreitet voran und wird innerhalb der Umsetzung der Digitalisierungsstrategie des Bundes nach SAFe umgesetzt. Da sich die Anforderungen bezüglich Cloud Adoption entwickeln, erlaubt diese agile Umsetzung den Stakeholdern eine laufende Priorisierung der Arbeiten.

Stellungnahme des Bundesamtes für Informatik und Telekommunikation

Das BIT verzichtet auf eine generelle Stellungnahme.

1 Mission et déroulement

1.1 Contexte

L'informatique en nuage (en anglais « cloud computing ») est un modèle et un ensemble de pratiques consistant à utiliser des ressources de calcul évolutives et accessibles à la demande sur un réseau pour stocker, gérer et traiter des données plutôt qu'un serveur local ou un ordinateur personnel. Ce modèle est un élément important de la transformation numérique de l'administration fédérale. Il doit permettre de mettre en œuvre de manière plus rapide, plus agile et à moindres coûts les projets innovants de l'administration, afin qu'elle puisse proposer des services efficaces aux entreprises et à la population.

Dans son édition 2020, le plan directeur de la stratégie informatique de la Confédération 2020–2023 décrit l'initiative stratégique 4 « Nuage hybride multi-cloud ». L'objectif était de mettre en œuvre une architecture combinant les propres infrastructures de calcul de la Confédération (« nuage privé ») et les plateformes de plusieurs fournisseurs de services cloud (« nuage public »). L'initiative vise aussi à développer le réseau de centres de calcul et à déployer à cet effet des plateformes numériques d'avenir spécialement conçues.

Dans le sillage du plan directeur, une stratégie d'informatique en nuage de l'administration fédérale a été élaborée. Le Conseil fédéral l'a adoptée en décembre 2020, posant ainsi les bases de l'utilisation des services en nuage. Entrée en vigueur au 1er janvier 2021, cette stratégie s'applique à l'administration fédérale centrale.

La stratégie définit un modèle cible de l'informatique en nuage à l'horizon 2025. Il comprend trois éléments principaux :

- Les modèles d'approvisionnement pour les prestations informatiques, notamment les nuages privés, hybrides, publics, de plusieurs fournisseurs, etc.
- Les options stratégiques en matière d'approvisionnement informatique, notamment la nouvelle option offerte par le nuage public.
- Un modèle organisationnel décrivant la manière dont l'administration fédérale devrait s'organiser par rapport aux fonctions requises : gouvernance du nuage, fonction d'intermédiaire, exploitation du nuage public par la Confédération et unités administratives jouant le rôle de bénéficiaires de prestations (BP).

Le Secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale (Secteur TNI) est en charge de la gouvernance du nuage. Il définit les principes à respecter lors de l'utilisation de services en nuage public et privé et les exceptions éventuelles. Il met aussi à disposition d'autres outils de travail (listes de contrôles, guides, directives, processus, etc.) de manière centralisée. L'intermédiaire (« cloud service broker », CSB) a pour tâche de soutenir les unités administratives dans l'utilisation de services d'informatique en nuage privé et public. Il conseille sur le choix d'un nuage de niveau adéquat. Le Conseil de la transformation numérique et de la gouvernance informatique (Conseil TNI) a désigné en juin 2022 l'Office fédéral de l'informatique et de la télécommunication (OFIT) comme CSB central de l'administration fédérale.

1.2 Objectif et questions d'audit

Dans cet audit, le Contrôle fédéral des finances (CDF) veut juger si les chances et les risques liés à l'utilisation des différents niveaux de l'informatique en nuage ont été identifiés et si les décisions fondamentales entourant son adoption ont été préparées et prises au niveau approprié. Il a approfondi en particulier les questions suivantes :

1. Y a-t-il un examen détaillé des chances et des risques pour chaque niveau de l'informatique en nuage ?
2. Cet examen a-t-il été évalué au niveau approprié et avalisé ?
3. Les outils de travail mis à disposition des bénéficiaires de prestations sont-ils appropriés, pour que ceux-ci puissent effectuer une estimation des risques et une analyse d'impact relative à la protection des données ?
4. Un plan de mise en œuvre de la stratégie cloud est-il défini et ce plan est-il tenu ?

Les questions liées aux achats publics effectués (appel d'offres, adjudication et procédures d'appel) dans le cadre de la mise en œuvre de la stratégie cloud n'ont en revanche pas été examinées.

Parallèlement à cet audit, le Center for Information Technology, Society and Law (ITSL) de la faculté de droit de l'Université de Zürich a procédé à une analyse des questions 2 et 3 sous un angle juridique et particulièrement du point de vue de la sécurité de l'information et de la protection des données. Les conclusions ont été intégrées dans le présent rapport.

1.3 Etendue de l'audit et principe

L'audit a été mené du 13 novembre au 22 décembre 2023 par André Stauffer (responsable de révision), Martin Scheid et Andreas Binggeli. Il a été conduit sous la responsabilité de Bernhard Hamberger. Le présent rapport ne prend pas en compte les développements ultérieurs à l'audit.

L'audit respecte les principes fondamentaux de l'audit de performance (International Standards of Supreme Audit Institutions).

1.4 Documentation et entretiens

Les informations nécessaires ont été fournies au CDF de manière exhaustive et compétente par le Secteur TNI et l'OFIT. Les documents ainsi que l'infrastructure requis ont été mis à disposition de l'équipe d'audit sans restriction.

1.5 Discussion finale

La discussion finale a eu lieu le 28 février 2024. Le Secteur TNI était représenté par la responsable du domaine Transformation et interopérabilité, l'OFIT par le directeur de l'office, le responsable du domaine Platform services et le business owner du Swiss Government Cloud. Pour le CDF, le responsable de mandats, le chef du centre de compétence, le responsable de révision et un expert en révision ont participé.

Le CDF remercie l'attitude coopérative et rappelle qu'il appartient aux directions d'office, respectivement aux secrétariats généraux de surveiller la mise en œuvre des recommandations.

CONTRÔLE FÉDÉRAL DES FINANCES

2 Définition des jalons de la stratégie et suivi

2.1 Les jalons sont définis

La stratégie d'informatique en nuage reprend, étend et détaille les étapes et les mesures décrites dans l'initiative stratégique 4 « nuage hybride multi-cloud » du plan directeur de 2020. Huit jalons sont définis et complétés par le détail des résultats à produire (voir ci-dessous). Les dates butoirs de ces jalons s'échelonnent de début 2021 à début 2025.

Pour la période dès janvier 2024, une nouvelle stratégie « Administration fédérale numérique » a été adoptée. Elle fixe les objectifs de la transformation numérique au sein de l'administration fédérale et définit les priorités permettant de les atteindre. Le nouvel objectif stratégique 15 reprend les éléments de l'initiative stratégique 4 de 2020 : *l'administration fédérale met à disposition des services en nuage public et privé, et la gouvernance relative à leur utilisation définit clairement les responsabilités.* Une concrétisation de cet objectif et l'agenda des mesures pour l'atteindre sont prévus dans le nouveau plan directeur 2024, attendu pour le printemps de cette année.

2.2 Les jalons sont majoritairement atteints, quelques points doivent encore être finalisés

Un suivi formel de la mise en œuvre des mesures de l'initiative stratégique 4 « Nuage hybride multi-cloud » est effectué au travers des plans directeurs édités chaque année. Il n'existe en revanche pas de rapport périodique formel du progrès de la mise en œuvre de la stratégie d'informatique en nuage. Le secteur TNI thématise toutefois les points ouverts dans le cadre de présentations à l'attention de divers groupements traitant de la numérisation (par exemple au Conseil de l'architecture de la Confédération ou au Conseil TNI).

Le CDF a analysé l'état de la mise en œuvre des jalons et des résultats associés par rapport au délai planifié (entre parenthèses ci-dessous) et note les points suivants :

J1 Contrats-cadres pour les nuages publics (3e trimestre 2021) :

Les résultats ont été produits, notamment l'appel d'offres « Public Clouds Confédération » (OMC-20007) et les cinq contrats-cadres conclus pour l'utilisation de nuages publics, les clarifications apportées à la procédure d'appel (le document était en cours de validation au moment de l'audit) ainsi que les principes relatifs à l'informatique en nuage de l'administration fédérale, entrés en vigueur en octobre 2023.

J2 Critères de l'approvisionnement informatique (4e trimestre 2021) :

Les critères et processus communs pour choisir l'option adéquate en matière d'approvisionnement informatique sont définis, de même que les mesures visant à surveiller l'évolution des coûts totaux au niveau fédéral.

J3 Orientation stratégique des centres de calcul et des nuages privés (fin 2021) :

La mise à jour de la stratégie pour le réseau de centres de calcul n'est pas terminée, une extension de délai à l'été 2025 a été demandée. Une proposition de portefeuille stratégique des infrastructures et plateformes souhaitées et de leur modèle d'exploitation est définie.

J4 Mise à jour de la stratégie d'informatique en nuage (fin 2021) :

Les résultats de l'étude de faisabilité Swiss Cloud et ceux découlant d'une éventuelle extension de l'admissibilité des données ont été incorporés dans les documents liés à la stratégie.

J5 Protection de l'information et des données, gestion des risques (2e trimestre 2021) :

Un rapport clarifiant les dispositions des normes légales et les règles internes qui portent sur l'utilisation de services en nuages publics a été édité (« Cadre juridique »). Une première génération d'aides décisionnelles (guides, listes de contrôles, directives et processus) a été produite.

J6 Nuages publics 2022 (1er trimestre 2022) :

Le modèle cible organisationnel est défini, sa mise en œuvre n'est toutefois pas achevée, les tâches, compétences et responsabilités du CSB n'étaient notamment pas encore validées au moment de l'audit. L'aptitude de l'administration fédérale à utiliser de manière sûre, efficace et ordonnée les services provenant de nuages publics n'était pas encore entièrement donnée, il y a trop peu d'expériences pour valider ce point. Le CSB met à disposition des prestations de conseil sur demande. Les principes d'un programme de formation pour développer les connaissances sont définis, mais les cours ne sont pas encore conçus.

J7 Gestion des coûts des services en nuage basés sur l'utilisation (1er trimestre 2022) :

Une première version des outils pour gérer et optimiser les coûts des services en nuage est disponible et doit permettre d'acquérir la capacité à budgétiser et à surveiller les dépenses.

J8 Modèle cible 2025 : modèle de nuages hybrides et multi-cloud (début 2025) :

La concrétisation de la vision de l'informatique en nuage et de la possibilité de combiner les services informatiques internes et dans un nuage public est en cours.

Appréciation

Le plan de mise en œuvre de la stratégie d'informatique en nuage est suffisamment défini.

Sur le plan de l'avancée des travaux, certains résultats définis dans les jalons de la stratégie ont été livrés en retard et quelques autres ne sont pas encore achevés. Les travaux étant encore en cours, le CDF renonce à émettre une recommandation sur ce point.

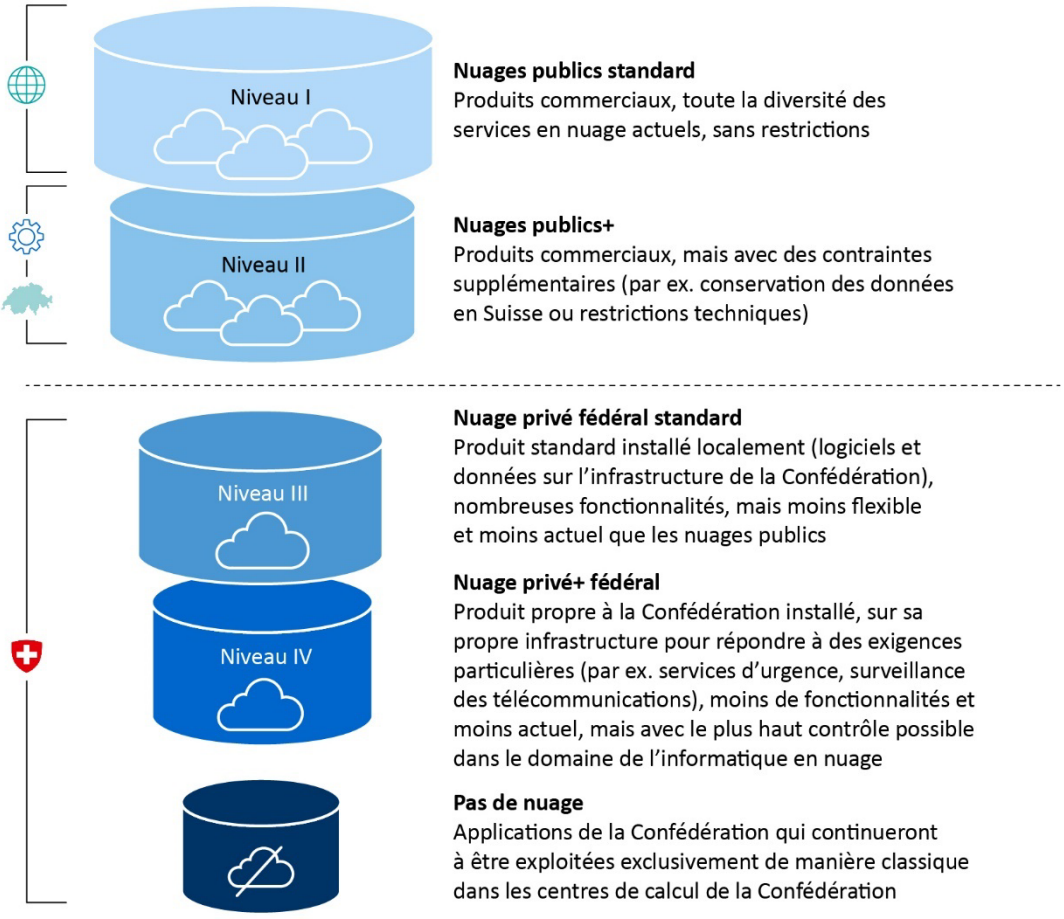
Un processus de suivi formel de l'avancée des travaux n'existe qu'au travers des plans directeurs de la stratégie informatique de la Confédération. Pour la stratégie d'informatique en nuage, un suivi interne au Secteur TNI est effectué. Les deux stratégies sont largement alignées, le CDF estime que le suivi au niveau de la stratégie informatique est suffisant en l'état. Il attend par ailleurs que l'état de la mise en œuvre de la stratégie d'informatique en nuage soit abordé dans le plan directeur 2024 de la nouvelle stratégie « Administration fédérale numérique ».

3 Niveaux de l'informatique en nuage, chances et risques

3.1 Les niveaux sont définis, le modèle doit être complété

Un modèle des niveaux de l'informatique en nuage est défini. Une version 1.0 de septembre 2022 est actuellement en vigueur, elle est reprise dans le cadre juridique pour l'utilisation de services d'informatique en nuage public et dans les principes relatifs à l'informatique en nuage. Quatre niveaux du cloud sont définis et un cinquième niveau correspondant à l'exploitation classique dans les centres de calcul de le Confédération est représenté. Des descriptions sommaires de chaque niveau sont données.

Le modèle décrit d'une part les nuages publics, exploités par des prestataires de services externes à la Confédération (« Cloud Service Providers », CSP) sans restrictions ou avec des contraintes supplémentaires (niveaux I et II). Il décrit d'autre part les nuages privés fédéraux standards et étendus (niveaux III et IV), dont les plateformes (Atlantica et Secure Private Cloud) sont déjà en service. Elles sont exploitées respectivement par l'OFIT et par le Centre de services informatiques CSI-DFJP sur leur propre infrastructure (« on premises »).



Infographie 1 : Modèle des différents niveaux de l'informatique en nuage de la Confédération (source : Secteur TNI de la Chancellerie fédérale, mise en forme par le CDF).

Les principes relatifs à l'informatique en nuage apportent diverses précisions quant aux modèles de livraison cloud admis. Ils s'appliquent par définition à l'utilisation des services en nuage public mettant à disposition des infrastructures (« Infrastructure as a Service », IaaS) ou fournissant en plus une palette d'intergiciels[1] et d'outils de développement (« Platform as a Service », PaaS). Ils ne couvrent en revanche pas les services de type SaaS (« Software as a Service », modèle de livraison mettant à disposition des logiciels applicatifs, par exemple SAP S/4HANA Cloud Public Edition).

Les plateformes définies dans le modèle de niveaux continuent d'évoluer. Les CSP externes et les prestataires internes de l'administration fédérale améliorent régulièrement leur offre d'informatique en nuage. A cet égard, la mise en place du « Swiss Government Cloud » (SGC) représente une des évolutions majeures projetées de l'infrastructure hybride multicloud. Elle vise à remplacer la plateforme Atlantica, qui arrivera en fin de vie en 2027, et à fournir un point d'entrée et une solution uniforme pour l'utilisation de services cloud des niveaux I à III. L'OFIT a été chargé de rédiger un message sur la mise en œuvre du SGC. Répondant à ces développements, des adaptations du modèle de niveaux sont en cours. Des versions modifiées du modèle circulent déjà. Des présentations de l'OFIT montrent notamment des propositions de niveaux cloud additionnels, des différenciations plus fines de certains niveaux et la position de l'éventuel futur SGC. Dans sa décision du 8 décembre 2023 sur le « Swiss Government Cloud », le Conseil fédéral a d'ailleurs chargé le Secteur TNI de concrétiser d'ici à fin 2024 les délimitations entre les niveaux du modèle d'informatique en nuage et d'examiner la pertinence de nouveaux niveaux.

Appréciation

Le modèle de niveaux de l'informatique en nuage de l'administration fédérale permet aux bénéficiaires de prestations de faire leurs premières réflexions sur les options à disposition. Il comporte encore certaines faiblesses : les niveaux ne sont pas toujours clairement délimités, par exemple entre les niveaux III et IV. De plus les prestations de type « Software as a Service » (SaaS) ne sont pas mentionnées, alors qu'elles figuraient dans les types d'approvisionnement possibles dans le modèle cible de la stratégie. Combinés à la circulation en parallèle de nouvelles versions du modèle, ces points peuvent provoquer une certaine confusion chez les bénéficiaires de prestations. Ils doivent être améliorés. Le Conseil fédéral a déjà demandé au Secteur TNI d'apporter des clarifications et d'examiner la pertinence d'une extension du modèle des niveaux. Le CDF estime qu'il faut par ailleurs élaborer un cadre pour la mise en œuvre des SaaS.

Recommandation 1 (Priorité 1)

Le CDF recommande au Secteur TNI de définir rapidement un cadre pour l'utilisation des services d'informatique en nuage de type « Software as a Service » (SaaS).

La recommandation est acceptée.

Prise de position du secteur TNI

SaaS beinhaltet eine grosse Fülle von Anwendungen auf allen Cloud Stufen, die als Dienstleistung der Cloud Provider bereitgestellt werden. Der grösste Handlungsbedarf besteht bei den in der Bundesverwaltung am breitesten eingesetzten SaaS Tools (insb. für agile, organisationsübergreifende Zusammenarbeit). Zur Steuerung der Nutzung dieser SaaS Tools hat

[1] Logiciels utilisé par des applications pour communiquer entre elles (angl. « middleware »).

DTI im Rahmen der Umsetzung der Strategie Digitale Bundesverwaltung eine überdepartementalen Arbeitsgruppe (CoP – Saas Tools) aufgebaut und wird weitergeführt. Der Fokus der Arbeiten liegt auf Identifikation der wichtigsten SaaS Tools für die Bundesverwaltung, sowie Hilfestellungen für deren Verwendung.

Excursus : contrats-cadres pour le nuage public et durée de vie des applications

Dans le contexte du marché public OMC-20007, les durées des accords-cadres sont limitées au 31 août 2026. Selon ses termes, une reconduction n'est pas prévue. Or, les applications de l'administration fédérale ont en général des durées de vie plus longues que celle prévue par les contrats avec les CSP. De plus, l'OFIT, dans son rôle de CSB, développe de nombreuses fonctionnalités pour assurer l'intégration des services cloud et des applications, par exemple l'automatisation et le contrôle de l'accès aux services. Ces développements ont un coût. Enfin, les BP peuvent être amenés à utiliser des fonctionnalités spécifiques de l'hébergement sur la plateforme du CSP. Ces éléments font que la sortie d'une application d'une plateforme cloud à l'échéance du contrat de prestations, la conclusion d'un contrat avec un nouveau prestataire et la relocalisation sur une autre plateforme sont compliquées et coûteuses. La question se pose donc de savoir si les durées typiquement définies dans les contrats d'approvisionnement sont judicieuses dans le cas de prestations d'informatique en nuage.

A l'échéance du marché public OMC-20007, faudra-t-il donc faire un nouvel appel d'offres et conclure de nouveaux contrats pour des services cloud et encourir d'importants coûts de migration des applications sur les nouvelles plateformes ? Au moment de l'audit, le Secteur TNI étudiait de manière approfondie les possibilités en collaboration avec les spécialistes de l'Office fédéral des constructions et de la logistique.

3.2 La description des chances et l'aperçu des risques sont des bases de travail suffisantes

La stratégie d'informatique en nuage décrit de manière globale les avantages escomptés de l'utilisation du cloud. Des objectifs, tels que le soutien à la transformation numérique de l'administration fédérale, l'amélioration de l'agilité, l'innovation, la robustesse et la flexibilité des plateformes ainsi que la diminution des coûts de certains services informatiques, sont poursuivis. Il n'existe toutefois pas de description plus détaillée et par niveau des chances de l'informatique en nuage.

Le cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale (août 2022) vise à clarifier les questions juridiques fondamentales pour l'approvisionnement des prestations cloud et à créer une compréhension juridique uniforme. Il veut montrer quels sont les moyens pour évaluer l'admissibilité des projets dans le domaine et servir à l'analyse des bases légales. En annexe à ce cadre, le Secteur TNI a édité un aperçu des risques et des mesures d'atténuation liés à ce type de plateformes. 22 risques sont décrits et répartis en quatre catégories (conformité, continuité des activités, politique et technique). Les mesures d'atténuation possibles, contractuelles, organisationnelles ou techniques, sont aussi mentionnées. Pour les services concernés par la procédure de marché public OMC 20007, des mesures additionnelles sont définies au travers des clauses des contrats-cadres, l'aperçu précise que ceux-ci garantissent un standard minimal. Il n'existe par contre pas de description détaillée et par niveau des risques liés à l'utilisation

de l'informatique en nuage. Selon le modèle de fonctionnement défini, les BP doivent effectuer une analyse de risque sur la base de leur projet concret et déterminer les mesures d'atténuation nécessaires.

Appréciation

Il n'existe pas d'examen détaillé des chances et des risques pour chaque niveau du modèle, mais seulement pour le nuage public en général. Pour les prestations du nuage privé, les chances et les risques restent en grande partie similaires à ceux de l'informatique fédérale classique (plateformes des fournisseurs de prestations internes). Pour le CDF, ces éléments forment une première base de travail suffisante pour les analyses de rentabilisation (« business cases »), des bases légales et de risques que les BP doivent continuer de faire dans le cadre de leurs projets. L'évolution de la technologie et des aspects juridiques continue d'être sur le radar du Secteur TNI et diverses clarifications sont prévues. Le CDF ne formule donc pas de recommandation.

Excursus : données personnelles hébergées à l'étranger, l'incertitude juridique subsiste

Le cadre juridique édité par le Secteur TNI présente de manière descriptive les domaines juridiques qui peuvent être importants pour les projets cloud, notamment la protection des données, le secret de fonction et la sécurité de l'information. Ces domaines sont à la croisée de développements techniques et politiques continus. Un important risque lié à la dépendance d'environnements juridiques à l'étranger existe en la matière. Les scénarios selon lesquels des autorités étrangères pourraient accéder aux données d'applications de l'administration fédérale hébergées sur des plateformes de nuage public peuvent poser problème. Les juristes continuent de débattre sur la possibilité d'adopter une approche basée sur les risques et de les ramener à un niveau acceptable par des mesures appropriées.

De plus, la question de l'adéquation du niveau de protection assuré par des CSP ayant leur siège aux Etats-Unis pour des données personnelles provenant d'applications suisses continue d'agiter les esprits. En juillet 2023, la Commission européenne adoptait le « EU-U.S. Data Privacy Framework » (cadre de protection des données) et reconnaissait l'adéquation des Etats-Unis pour le transfert de données personnelles européennes. Un cadre similaire entre la Suisse et les Etats-Unis est défini (« Swiss-U.S. Data Privacy Framework »), mais n'est toujours pas formellement entré en vigueur, alors que le cadre européen pourrait être renvoyé devant la Cour de justice de l'UE.

Le Secteur TNI a reconnu le caractère dynamique du domaine et souligne que le document déterminant le cadre juridique est évolutif et sera régulièrement mis à jour et complété.

3.3 Les parties prenantes sont suffisamment intégrées dans les définitions mais doivent mieux partager leurs expériences

Répartition des rôles

Les principes relatifs à l'informatique en nuage décrivent les rôles définis dans la mise en œuvre de la stratégie cloud. La gouvernance incombe au Secteur TNI qui définit les principes de l'utilisation de cette technologie, décide des éventuelles exceptions et met à disposition d'autres outils de manière centralisée. Le délégué TNI décide de l'entrée en vigueur de ces éléments. Les départements, la Chancellerie fédérale et les CSB peuvent concrétiser

et élargir la gouvernance dans leur domaine de responsabilité. En cas de désaccord entre les intervenants, le processus de règlement des différends tel que le prévoit l'article 19 de l'Ordonnance sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale s'applique.[2] Le Préposé fédéral à la protection des données et de la transparence (PFPDT) et le Conseil TNI ont des rôles consultatifs.

Le rôle de CSB centralisé de la Confédération est assuré par l'OFIT. Celui de l'exploitation du nuage public (au sens de la responsabilité de l'utilisation des services en nuage public) est du ressort des unités administratives. Les départements sont responsables du choix de l'option d'approvisionnement pour son utilisation par les unités administratives dans leur rôle de BP. Une description formelle des rôles des parties prenantes dans l'élaboration des documents et des outils de travail, de type matrice RACI, n'est toutefois pas disponible.

Validation des documents fondamentaux

Les modèles de niveaux, les avantages escomptés et les risques du cloud dans l'administration fédérale sont consignés respectivement dans les principes relatifs à l'informatique en nuage, la stratégie d'informatique en nuage et dans le cadre juridique pour l'utilisation de services informatiques en nuage. Ces documents fondamentaux ont été validés de la manière suivante :

- Stratégie : approuvée par le Conseil fédéral en décembre 2020
- Cadre juridique et annexes : intégration de remarques du PFPDT et de la Chancellerie fédérale, consultation des offices, prise de connaissance par la Conférence des secrétaires généraux. Validation en août 2022
- Principes : 3 rondes de consultation avec les offices dès l'automne 2022 ont abouti à la rédaction de la version finale, une divergence subsiste avec le PFPDT. Mise en vigueur par le délégué TNI en octobre 2023.

Pour les autres documents et les outils de travail, le délégué TNI décide de leur mise en vigueur, après consultation de diverses parties prenantes. Par exemple, le cahier des charges du CSB a été présenté au Conseil TNI et passera devant la Conférence des secrétaires généraux.

Un apprentissage est en cours dans la réalisation de solutions basées sur l'informatique en nuage, autant pour le Secteur TNI que pour les bénéficiaires et fournisseurs internes de prestations. Au moment de l'audit, quelques projets de mise en œuvre de ces technologies au sein de l'administration fédérale étaient en cours ou déjà achevés comme par exemple les projets RZplus à MétéoSuisse[3] et CEBA de la Chancellerie fédérale[4] ou la boutique en ligne MySwissMap de swisstopo. Des échanges d'expériences ont lieu entre certains intervenants et l'OFIT a mis en place des canaux d'information et de questions-réponses. Il n'y a toutefois pas de plateforme d'échange permettant de partager systématiquement entre parties prenantes les enseignements des projets de mise en œuvre de l'informatique en nuage.

---

2 RS 172.010.58.

3 « Audit du projet TNI clé RZplus – Sécurisation de la puissance de calcul » (n° d'audit 23623), disponible sur le site Internet du CDF.

4 « Audit du projet TNI clé Cloud Enabling Bureautique (CEBA) » (n° d'audit 23740), disponible sur le site Internet du CDF.

Appréciation

Pour les documents fondamentaux liés à la mise en œuvre de la stratégie d'informatique en nuage, les intervenants ont été suffisamment intégrés et ont pu livrer leurs commentaires. Les décisions de mise en vigueur ont été formellement prises au niveau approprié. Pour les outils de travail, malgré l'absence d'une description formelle complète des rôles des parties prenantes (matrice RACI), les processus de consultation sont suffisants et les commentaires peuvent être récoltés.

Par contre, une plateforme d'échange permettant de partager systématiquement les enseignements des projets de mise en œuvre d'informatique en nuage fait défaut. La courbe d'apprentissage est raide et les BP doivent fournir un travail important. Au vu du degré inégal de maturité des intervenants, le risque existe que certaines erreurs se répètent dans les projets ou que les bonnes pratiques ne se diffusent pas suffisamment. Cette lacune doit être corrigée.

Recommandation 2 (Priorité 2)

Le CDF recommande à l'OFIT en collaboration avec le Secteur TNI de mettre en place une plateforme d'échange des expériences des parties impliquées dans la mise en œuvre de l'informatique en nuage.

La recommandation est acceptée.

Prise de position de l'OFIT

Das BIT versteht hinter dieser Empfehlung die Absicht der EFK, eine Community of Practice zum Bezug von Cloudleistungen einzurichten (eine allfällige Einholung von Feedbacks zugunsten der Anpassung der Strategie würde das BIT als Aufgabe des Bereichs DTI verorten). In der Annahme, dass Ersteres zutrifft, akzeptiert das BIT die Empfehlung und wird die Form sowie Art des Austauschs dieser Community of Practice zugunsten eines Erfahrungsaufbaus der LB und LE zu diesem Thema definieren, dann initiieren und moderieren. Das BIT gedenkt dies bis Ende 2026 umzusetzen. Weil der Bezug von Public Cloud Services vor der Inbetriebnahme von SGC geringer ausfallen wird als danach und aus Kapazitätsgründen zugunsten des Aufbaus der SGC erachtet das BIT diesen Termin als realistisch und sinnvoll. Bis dahin wird das BIT die mit seinen Kunden gemachten Erfahrungen jeweils bei den nächsten Kundenprojekten einfliessen lassen.

4 Mise à disposition des outils de travail

4.1 Une multitude d'outils de travail sont déjà disponibles…

Le Secteur TNI a élaboré différents outils de travail (aides à la décision, guides, listes de contrôle, descriptions de processus, etc.) dans le sillage des documents fondamentaux liés à la stratégie d'informatique en nuage. Ils sont accessibles sur la page Web du Secteur TNI. En complément au cadre juridique, des annexes donnent ainsi un aperçu des risques et des mesures liées à l'utilisation du cloud ou fournissent une liste de questions permettant une évaluation de l'opportunité d'un passage à cette technologie (« liste de contrôle »). Des exemples d'utilisation pour chaque niveau du modèle de l'informatique en nuage sont aussi brièvement décrits.

Le document décrivant les principes relatifs à l'informatique en nuage énumère les bases de l'utilisation de cette technologie. Il livre un aperçu de l'adéquation potentielle des niveaux du nuage selon les catégories de données et les exigences en termes de souveraineté. Il énonce aussi les directives régissant cette utilisation, expose des recommandations et fait référence à des réglementations édictées dans d'autres cadres (par exemple Office fédéral de la cybersécurité pour les exigences concernant la procédure de sécurité). Ces principes concernent tant des questions d'approvisionnement et d'acquisition que de sécurité, d'organisation et de gestion des produits. Une foire aux questions a été éditée et au moment de l'audit, une description du cahier des charges du CSB était en cours de validation. Au chapitre des approvisionnements, une description de la procédure d'appel et des modèles de cahier des charges et des contrats-cadres sont disponibles.

L'OFIT, dans son rôle de CSB, met à disposition toute une panoplie d'aides et d'informations sur l'utilisation de l'informatique en nuage. D'une part, des composantes techniques facilitant l'intégration des applications fédérales avec les plateformes cloud publiques des cinq CSP adjudicataires sont en cours de mise en place. D'autre part, de nombreux guides, listes d'activités et documents sont publiés sur un espace de l'outil Confluence de l'OFIT et accessibles pour les BP. Ces aides ne couvrent pas encore toutes les plateformes cloud publiques disponibles à la Confédération, les priorités de travail suivent la demande. Enfin, l'OFIT a organisé un service d'heure des questions, au sein duquel des spécialistes répondent aux questions des BP au sujet de leur projet cloud. Ce service est toutefois suspendu pour l'instant, faute de demande suffisante.

En tant qu'exploitants des plateformes d'informatique en nuage privées de la Confédération, tant l'OFIT que le CSI-DFJP mettent à disposition des BP de nombreuses informations sur les modalités de l'utilisation du cloud privé des niveaux III et IV (architecture, sécurité, etc.).

Enfin, certaines aides sont éditées par d'autres unités administratives, par exemple les modèles nécessaires à l'analyse d'impact sur la protection des données (examen préalable des risques, guide et « check-list ») de l'Office fédéral de la justice, ou le guide relatif aux mesures techniques et organisationnelles de la protection des données du PFPDT.

Sur un plan formel, les outils de travail ne sont pas systématiquement munis des indications de leur version ou de leur date de mise en vigueur. Ces mentions apparaissent parfois sur le lien qui donne accès au document, mais manquent souvent dans les documents mêmes.

Appréciation

Les outils de travail mis à disposition constituent un pas dans la bonne direction permettant aux bénéficiaires des prestations d'évaluer les opportunités, l'adéquation et les risques d'une solution de type cloud pour leurs besoins informatiques et leurs applications. Des outils additionnels sont aussi régulièrement mis à disposition. Sur le plan de la systématique, cette première génération comporte toutefois quelques lacunes. Les accès aux outils de travail sont éparpillés dans une collection de liens publiés sur les pages web de plusieurs unités administratives ou dans des documents. La recherche de l'outil approprié par les bénéficiaires de prestations n'en est pas facilitée. De plus, l'absence de la version et de la date de validité sur certains outils de travail peut causer des confusions dans les projets des BP quant au contrôle des versions documentaires utilisées.

Recommandation 3 (Priorité 3)

Le CDF recommande au Secteur TNI d'améliorer l'organisation de la collection de liens permettant l'accès aux documents et aux outils de travail afin de faciliter les recherches des bénéficiaires de prestations. Le Secteur TNI veillera aussi à ce que les documents publiés soient systématiquement munis des indications de leur validité (version et date).

La recommandation est acceptée.

Prise de position du secteur TNI

Die erarbeiteten Dokumente und Hilfestellungen werden auf Intranet und nach Möglichkeit auch immer auf dem Internet publiziert. Dies ist bereits der Fall (siehe: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html). Wir werden prüfen, wie die Information besser auffindbar darstellen können und Version und Datum der Dokumente durchgehend sichtbar machen.

4.2 Des compléments sont nécessaires

Sur le plan matériel, certains outils de travail manquent par rapport aux directives et recommandations décrites dans les principes ou ne sont pas encore aboutis :

- Directive sur l'acquisition de services en nuage public : pas d'indications sur la marche à suivre pour le modèle SaaS (voir chapitre 3.1)
- Le cahier des charges des CSB est en cours de validation
- Directive sur la stratégie de sortie en cas d'utilisation de service en nuage public : pas d'outil de travail disponible
- Recommandation sur l'évaluation préalable du nuage de niveau adéquat : dans les principes, un tableau décrit la pertinence d'un niveau en fonction d'exigences de classification des données[5], de protection des données[6] et de souveraineté. Le tableau n'indique toutefois pas clairement comment traiter les cas où les critères pointeraient pour la même application vers des niveaux de nuage différents. La notion de souveraineté n'est par ailleurs pas définie concrètement. Sur ce point, une

[5] Au sens de la loi fédérale sur la sécurité de l'information, RS 128.

[6] Au sens de la loi fédérale sur la protection des données, RS 235.1, d'autres lois ou du secret de fonction.

clarification est en cours. Dans sa réponse au postulat Z'graggen « Stratégie Souveraineté numérique de la Suisse »[7] du 14 décembre 2022, le Conseil fédéral s'est en effet engagé à rendre un rapport jusqu'à fin 2024, qui devra notamment définir le concept de « souveraineté numérique ».

- Renvoi à la directive sur la procédure de sécurité : pour déterminer les risques résiduels dans le cas de l'utilisation de nuage public, les BP doivent connaitre les mesures de sécurité mises en place avec le CSP. Ces mesures sont documentées dans les contrats-cadres. Or, dans les premiers projets de nuage public, l'accès à ces documents était traité de manière très restrictive, si bien que les spécialistes de la sécurité n'avaient pas toutes les informations nécessaires. Le Secteur TNI a entretemps précisé les modalités de l'accès aux contrats-cadres, qui est désormais possible sous conditions auprès du secrétariat général du département concerné. Ce point est documenté dans la foire aux questions de l'informatique en nuage.

De nombreux outils de travail additionnels sont pensables. Au fur et à mesure de leurs expériences, les intervenants vont venir avec de nouvelles idées. Un processus formel de gestion des exigences et de priorisation des travaux en la matière n'est toutefois pas en place.

Appréciation

Des modèles ou des outils de travail font défaut pour certains points des principes (par exemple stratégie de sortie). Afin de favoriser un traitement homogène de l'évaluation des solutions cloud, ces lacunes devront être comblées. Par ailleurs, des ambiguïtés subsistent dans cette première livraison des outils de travail, notamment pour l'évaluation du type de nuage approprié. Différents travaux sont prévus pour préciser le modèle des niveaux et la notion de souveraineté numérique, qui est centrale pour le choix entre nuages publics et privés. Enfin, avec la montée en compétence des intervenants à la mise en œuvre de l'informatique en nuage, des nouveaux outils de travail seront requis.

Un travail conséquent sera sans doute nécessaire pour traiter ces points. Pour une mise en œuvre priorisée des nouveaux outils les plus utiles et des améliorations, un processus de gestion des exigences doit être mis en place.

Recommandation 4 (Priorité 1)

Le CDF recommande au Secteur TNI de mettre en place une organisation et un processus afin d'identifier les outils de travail manquants ou les améliorations nécessaires pour la mise en œuvre des principes, directives et recommandations et de prioriser les activités correctives en collaboration avec les différentes parties prenantes.

La recommandation est acceptée.

Prise de position du secteur TNI

Die Erarbeitung der Hilfsmittel und Instrumente wird im Rahmen der Strategieumsetzung der Strategie Digitale Bundesverwaltung nach SAFe festgesetzt. Die sich stetig entwickelnden Anforderungen bezüglich Einsatz von Clouds werden durch diese agile Methode von den eng eingebundenen Stakeholdern iterativ priorisiert. Diese Arbeiten werden auch personell verstärkt.

[7] Postulat 22.4411.

Annexe 1 : Bases légales et stratégies

Textes législatifs
Loi fédérale sur la sécurité de l'information au sein de la Confédération (LSI) du 18 décembre 2020, RS 128
Ordonnance sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale (OTNI) du 25 novembre 2020, RS 172.010.58
Loi fédérale sur la protection des données (LPD) du 25 septembre 2020, RS 235.1
Interventions parlementaires
22.4411 – Stratégie Souveraineté numérique de la Suisse, Postulat de Heidi Z'graggen, Conseil des Etats, 14.12.2022
Stratégies
Stratégie « Administration fédérale numérique », 12 décembre 2023, Chancellerie fédérale
Stratégie d'informatique en nuage, 11 décembre 2020, Unité de pilotage informatique de la Confédération
Stratégie informatique de la Confédération 2020–2023, 3 avril 2020, Conseil fédéral

Annexe 2 : Abréviations

BP	Bénéficiaire de prestations
CDF	Contrôle fédéral des finances
ChF	Chancellerie fédérale
CSI-DFJP	Centre de services informatiques du Département fédéral de justice et police
ITSL	Center for Information Technology, Society and Law de l'Université de Zurich
OFIT	Office fédéral de l'informatique et de la télécommunication
PFPDT	Préposé fédéral à la protection de données et de la transparence
Secteur TNI	Secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale

Annexe 3 : Glossaire

Atlantica	Plateforme cloud exploitée par l'OFIT dans ses propres centres de calcul (niveau III du modèle d'informatique en nuage).
CEBA (projet)	Projet de la Chancellerie fédérale visant à faire de Microsoft 365, la version en nuage des services Microsoft, un nouvel outil standard de l'administration fédérale.
Cloud Service Broker (CSB)	Fonction d'intermédiaire qui crée les conditions nécessaires pour que les services en nuage public puissent être utilisés, intégrés et exploités dans l'environnement de l'administration fédérale conformément aux exigences définies.
Cloud Service Provider (CSP)	Fournisseur de services cloud, entreprise qui fournit des ressources de calcul évolutives et accessibles à la demande sur un réseau, par exemple via des services de calcul, de stockage, d'infrastructure, de plateformes et d'applications basée sur le cloud.
Confluence	Logiciel de travail collaboratif utilisé à l'OFIT pour la documentation, le partage et le suivi des tâches.
Conseil de l'architecture de la Confédération	Organe spécialisé dans lequel les bénéficiaires et les fournisseurs de prestations discutent des objets concernant l'architecture d'entreprise et décident des prescriptions à fixer en la matière.
Conseil de la transformation numérique et de la gouvernance informatique (Conseil TNI)	Organe interdépartemental qui conseille le délégué TNI et les unités administratives dans le cadre de la coordination interdépartementale de la transformation numérique et de la gouvernance informatique.
EU-U.S. Data Privacy Framework	Cadre de protection des données entre l'Union européenne (UE) et les Etats-Unis qui doit régler l'échange et la protection accordée par des fournisseurs cloud américains aux données provenant de l'UE. Ce cadre pourrait être renvoyé devant la Cour de justice de l'UE.
Infrastructure as a Service (IaaS)	Modèle d'informatique en nuage selon lequel des infrastructures de calcul évolutives sont mises à disposition à la demande en tant que services sur Internet. Le fournisseur cloud gère le matériel, les couches de virtualisation, le stockage, les réseaux.
Informatique en nuage (Cloud computing)	Modèle et ensemble de pratiques consistant à utiliser des ressources de calcul évolutives et accessibles à la demande sur un réseau pour stocker, gérer et traiter des données plutôt qu'un serveur local ou un ordinateur personnel.

Intergiciel	Logiciel utilisé par les applications pour communiquer entre elles (angl. « middleware »).
Nuage hybride multi-cloud	Architecture-cible de l'informatique en nuage de l'administration, se basant sur une combinaison des propres infrastructures de calcul de la Confédération (« nuage privé ») et les plateformes de plusieurs fournisseurs de service cloud (« nuage public »).
OMC-20007	Procédure de marché public « Public Cloud Confédération » pour la fourniture de services cloud publics.
On Premises	Sur place, se dit d'une infrastructure informatique exploitée dans les propres centres de calcul d'une organisation.
Platform as a Service (PaaS)	Modèle d'informatique en nuage selon lequel des plateformes sont mises à disposition à la demande en tant que services sur Internet. En plus du matériel et de l'infrastructure, le fournisseur cloud gère les logiciels de base (systèmes d'exploitation, moteurs de bases de données, etc.).
RACI (matrice)	Matrice des responsabilités. Elle indique les rôles et responsabilités des intervenants pour des processus et activités, selon qu'ils sont réalisateurs, approbateurs, consultés ou informés.
RZPlus (projet)	Projet de sécurisation de la puissance de calcul de MétéoSuisse.
Secure Private Cloud	Plateforme cloud exploitée par le CSI-DFJP dans ses propres centres de calcul (niveau IV du modèle d'informatique en nuage).
Software as a Service (SaaS)	Modèle d'informatique en nuage selon lequel des logiciels sont mis à disposition à la demande en tant que services sur Internet. Le fournisseur cloud gère l'ensemble des couches techniques, de l'infrastructure jusqu'à la solution applicative.
Swiss Cloud	Initiative en vue de l'évaluation des besoins, de la conception, de la nécessité et de la faisabilité d'une solution étatique d'informatique en nuage. Le rapport publié en décembre 2020 concluait que la nécessité d'un « Swiss Cloud » sous forme d'une infrastructure technique indépendante de droit public n'était pas démontrée.
Swiss Government Cloud (SGC)	Projet de l'OFIT visant à mettre en place une infrastructure multi-cloud hybride adaptée aux besoins de l'administration fédérale.
Swiss-U.S. Data Privacy Framework	Cadre de protection des données entre la Suisse et les Etats-Unis qui doit régler l'échange et la protection accordée par des fournisseurs cloud américains aux données provenant de Suisse. Ce cadre n'était pas entré en vigueur au moment de l'audit.

Priorités des recommandations

Le Contrôle fédéral des finances priorise ses recommandations sur la base de risques définis (1 = élevés, 2 = moyens, 3 = faibles). Comme risques, on peut citer par exemple les cas de projets non-rentables, d'infractions contre la légalité ou la régularité, de responsabilité et de dommages de réputation. Les effets et la probabilité de survenance sont ainsi considérés. Cette appréciation se fonde sur les objets d'audit spécifiques (relatif) et non sur l'importance pour l'ensemble de l'administration fédérale (absolu).