



*Ce texte est une version provisoire.
Seule la version qui sera publiée dans
la Feuille fédérale fait foi.*

24.xxx

Message concernant un crédit d'engagement pour la mise en place d'un Swiss Government Cloud (SGC)

du ...

Monsieur le Président du Conseil national,
Madame la Présidente du Conseil des États,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons le projet d'un arrêté fédéral concernant un crédit d'engagement pour la mise en place d'un Swiss Government Cloud, en vous proposant de l'adopter.

Nous vous prions d'agréer, Monsieur le Président, Madame la Présidente, Mesdames, Messieurs, l'assurance de notre haute considération.

...

Au nom du Conseil fédéral suisse :

La présidente de la Confédération, Viola
Amherd
Le chancelier de la Confédération, Viktor
Rossi

Condensé

Par le présent message, le Conseil fédéral propose au Parlement d'approuver un crédit d'engagement de 246,9 millions de francs pour mettre en place le Swiss Government Cloud (SGC), soit une infrastructure hybride multi-cloud. Celle-ci est d'une importance capitale pour relever avec succès les futurs défis majeurs liés à la numérisation de la Confédération.

Contexte

Dans le cadre de ses efforts de numérisation, l'administration fédérale fait face à une demande croissante de solutions informatiques et à des exigences accrues en matière de performance, de fiabilité et de sécurité des infrastructures informatiques. Il s'ensuit que les services en nuage, élément clé de la transformation numérique, ne cessent de gagner en importance. C'est pourquoi, le 11 décembre 2020, le Conseil fédéral a adopté la stratégie d'informatique en nuage de l'administration fédérale pour poser les bases de leur utilisation.

Principal fournisseur de prestations informatiques de l'administration fédérale, l'Office fédéral de l'informatique et de la télécommunication (OFIT) doit lui aussi de mettre en œuvre cette stratégie. Or, son infrastructure en nuage (environnement système Atlantica) répond de moins en moins aux exigences de performance et sera bientôt obsolète. Compte tenu du faible degré d'industrialisation de la solution en nuage existante, les hausses de capacité destinées à répondre à la demande entraînent une forte augmentation des coûts d'exploitation. Il convient donc de mettre en place en temps opportun une infrastructure hybride multi-cloud appropriée qui permettra de relever les futurs défis majeurs de la transformation numérique.

Contenu du projet

Le Conseil fédéral prévoit de mettre en place le Swiss Government Cloud (SGC), une infrastructure hybride multi-cloud adaptée aux exigences et aux besoins de la Confédération. Le terme « hybride » signifie que le SGC combinera des services en nuage public de prestataires externes et des offres en nuage privé propres à l'administration fédérale. Des offres de plusieurs prestataires externes de services en nuage seront disponibles pour réduire les dépendances, d'où la précision « multi ». Le SGC permettra ainsi de couvrir la plupart des activités en nuage de l'administration fédérale grâce à une solution cohérente. Pour répondre à cet objectif, une approche globale a été choisie : outre la création de cette infrastructure, des investissements seront réalisés dans les domaines « formation, conseil et gouvernance », « processus commerciaux et d'exploitation », « cybersécurité » et « infrastructure réseau ». Cela permettra de garantir une mise en place et une utilisation ciblées, sûres et efficaces du SGC. S'ils sont intéressés, les cantons, les villes et les communes pourront eux aussi bénéficier de l'offre de celui-ci.

Le secrétaire général du Département fédéral des finances sera le mandant du programme SGC. Par ailleurs, il est prévu de mettre en place un comité responsable du programme et un comité spécialisé, composés de représentants des fournisseurs et des

bénéficiaires de prestations informatiques ainsi que de la Chancellerie fédérale (ChF, secteur Transformation numérique et gouvernance de l'informatique). Ces comités permettront de garantir la participation appropriée des fournisseurs de prestations et de la ChF ainsi que la prise en compte des besoins des bénéficiaires de prestations. Eu égard à l'ampleur et à la complexité du projet, une gestion solide et indépendante de la qualité et des risques sera également instaurée pour vérifier la qualité des travaux et pour recenser et évaluer les risques à tous les niveaux de responsabilité.

Le programme sera lancé en 2024. Quant à la réalisation, elle s'étendra de 2025 à 2032. À partir de 2027, la mise en place du SGC sera suffisamment avancée pour qu'il soit possible de lancer la migration des applications spécialisées à partir de l'environnement système Atlantica et du *cloud service broker* (CSB) de l'OFIT, l'objectif étant de terminer cette migration d'ici à la fin de l'année 2030.

Crédit d'engagement

Le crédit d'engagement sollicité s'élève à 246,9 millions de francs.

Ce crédit d'engagement comprend deux tranches : la première tranche, de 103,2 millions de francs pour les années 2025 à 2027, sera libérée par un arrêté fédéral de l'Assemblée fédérale. Le Conseil fédéral débloquera la seconde tranche, de 143,7 millions de francs pour les années 2028 à 2032, dès que les conditions nécessaires seront réunies.

Table des matières

Condensé	2
1 Contexte	6
1.1 Problématique, motif de la demande de crédit et intérêt du projet	6
1.2 Objectif et procédure	7
1.3 Relation avec le programme de la législature et avec le plan financier, ainsi qu’avec les stratégies du Conseil fédéral	8
1.4 Renonciation à la procédure de consultation	9
2 Contenu de l’arrêté de crédit	10
2.1 Proposition du Conseil fédéral, avec exposé des motifs	10
2.2 Description détaillée du projet	10
2.2.1 Mise en place de l’infrastructure hybride multi-cloud	10
2.2.1.1 Nuage public (<i>public cloud</i>)	11
2.2.1.2 Nuage public sur site (<i>public cloud on-prem</i>)	12
2.2.1.3 Nuage privé sur site (<i>private cloud on-prem</i>)	12
2.2.2 Développement de l’infrastructure réseau	13
2.2.3 Renforcement de la cybersécurité	14
2.2.3.1 Protection des données et sécurité de l’information	15
2.2.3.2 Défis liés à la cybersécurité	16
2.2.3.3 Objectif de la cybersécurité	17
2.2.3.4 Conformité informatique	18
2.2.4 Processus commerciaux et d’exploitation	18
2.2.4.1 Processus d’exploitation	19
2.2.4.2 Processus commerciaux	19
2.2.5 Formation, conseil et gouvernance	20
2.2.5.1 Offre de formation	20
2.2.5.2 Centre de compétence du SGC	21
2.2.5.3 Centre d’innovation	21
2.2.5.4 Gouvernance de l’informatique en nuage à l’échelle du SGC	21
2.3 Variantes étudiées pour la mise en place et la séquence	22
2.4 Analyse et identification des besoins	23
2.5 Risques	25
2.5.1 Contexte de l’évaluation des risques	25
2.5.2 Risque de ne pas atteindre les objectifs	25
2.5.3 Mesures pour atteindre les objectifs	26
2.5.4 Risque budgétaire	26
2.5.5 Mesures de respect des coûts et du budget	27
2.5.6 Risque de calendrier	27
2.5.7 Mesures de respect des délais	28
2.6 Structure du programme	29

2.7	Audit systématique	30
3	Conséquences	32
3.1	Conséquences pour la Confédération	32
3.1.1	Conséquences financières	32
3.1.1.1	Hypothèses retenues pour estimer les dépenses	32
3.1.1.2	Dépenses liées au programme	33
3.1.1.3	Crédit d'engagement	36
3.1.1.4	Dépenses d'exploitation après la conclusion du programme	37
3.1.1.5	Économies pendant le programme et après sa conclusion	37
3.1.1.6	Rentabilité	38
3.1.2	Conséquences en cas de non-réalisation	40
3.1.3	Coûts de la migration	41
3.1.4	Deuxième avis	42
3.2	Conséquences pour les cantons et les communes	42
4	Aspects juridiques	44
4.1	Constitutionnalité et légalité	44
4.2	Forme de l'acte à adopter	44
4.3	Assujettissement au frein aux dépenses	44
5	Liste des abréviations utilisées	45
6	Glossaire	47

Message

1 Contexte

1.1 Problématique, motif de la demande de crédit et intérêt du projet

L'Office fédéral de l'informatique et de la télécommunication (OFIT), qui est l'un des fournisseurs de prestations informatiques de l'administration fédérale, est chargé de mettre à la disposition de ses clients au sein de cette administration des systèmes informatiques sûrs, efficaces et conformes aux besoins et d'apporter un soutien fiable aux unités administratives dans l'exécution de leurs processus d'affaires numériques. Les conditions pour accomplir ce mandat ont sensiblement changé ces dernières années : les efforts croissants de numérisation de l'administration fédérale font augmenter la demande de prestations informatiques innovantes (p. ex. dans le domaine de l'intelligence artificielle) et les exigences en matière de performance, de fiabilité et de sécurité des infrastructures informatiques. L'utilisation de services en nuage, notamment, a gagné en importance dans ce contexte. En effet, l'environnement professionnel de l'administration fédérale se caractérise par une complexité et un dynamisme croissants. Malgré une pression accrue sur les coûts et le sévère manque de main-d'œuvre spécialisée, les unités administratives doivent pouvoir réagir aux exigences commerciales qui évoluent rapidement pour continuer d'accomplir leur mandat de prestations vis-à-vis du public. La transformation numérique est une nécessité. Grâce à leur standardisation élevée, à leur évolutivité, à leur grande fiabilité et à leur capacité d'innovation, les services en nuage sont propres à soutenir ce processus à un coût avantageux et à l'accélérer.

Le 11 décembre 2020¹, le Conseil fédéral a adopté la stratégie d'informatique en nuage de l'administration fédérale² pour créer les bases nécessaires à une utilisation sûre, efficace et ordonnée de la technologie en nuage. Cette stratégie prévoit une approche hybride multi-cloud : les unités administratives de la Confédération pourront faire appel à des infrastructures et services en nuage internes ou proposés par plusieurs prestataires externes et les combiner pour répondre au mieux aux exigences.

L'OFIT doit lui aussi de mettre en œuvre cette stratégie d'informatique en nuage, en tenant compte notamment des points suivants :

- Environnement système Atlantica : le nuage privé de l'OFIT, soit l'environnement système Atlantica, devra être remplacé dès 2027 pour des raisons techniques, car certains éléments arriveront à la fin de leur cycle de vie. De plus, compte tenu de la numérisation croissante de l'administration, l'infrastructure existante atteint ses limites en matière de capacités et de flexibilité ; elle ne permet plus de relever les défis liés au numérique. Il faut donc poser

¹ www.admin.ch > Documentation > Communiqués > Communiqués du Conseil fédéral > 11.12.2020 (état : 26.03.2024)

² www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Directives informatiques > Stratégies et stratégies partielles > SB020 – Stratégie d'informatique en nuage de l'administration fédérale (état : 26.03.2024)

de nouvelles fondations pour la réalisation des projets de numérisation sur le plan technique, tout en évitant une hausse considérable des coûts informatiques.

- Appel d'offres OMC 2007 : la base pour les acquisitions qui a été mise en place avec l'appel d'offres OMC 2007 et qui permet actuellement à l'administration fédérale d'acquérir des solutions en nuage public par l'intermédiaire du cloud service broker de l'OFIT (CSB-OFIT) sera à terme épuisée ou arrivera à échéance (vraisemblablement en 2026). Une solution de remplacement est donc nécessaire si l'administration fédérale entend mettre en œuvre sa stratégie hybride d'informatique en nuage.

Avec le projet Swiss Government Cloud (SGC), le Conseil fédéral prévoit dès lors de mettre en place une nouvelle infrastructure hybride multi-cloud adaptée aux exigences et aux besoins de la Confédération, qui associe plusieurs offres en nuage public et privé. Le SGC permettra ainsi de couvrir la plupart des activités en nuage grâce à une solution globale cohérente.

1.2 Objectif et procédure

Le SGC permettra de poursuivre la mise en œuvre de l'approche hybride multi-cloud prévue dans la stratégie d'informatique en nuage de l'administration fédérale. Toute la gamme de services en nuage, du nuage public jusqu'au nuage privé dans les centres de calcul de la Confédération (sur site), peut être acquise grâce à la même solution globale, la gouvernance du SGC garantissant que les produits exploités au sein de ce dernier s'intègrent aussi facilement que possible dans l'environnement système de la Confédération. Cela permettra de réduire les charges et d'investir de précieuses ressources dans la numérisation des processus d'affaires.

En outre, le SGC permettra à la Confédération de saisir les opportunités offertes par le numérique en proposant un accès économique à l'innovation. Grâce à des solutions appropriées basées sur des services en nuage, les bénéficiaires de prestations pourront réagir rapidement aux évolutions de leur environnement professionnel, ce qui renforcera la résilience numérique de l'administration fédérale. Des investissements réguliers contribueront à ce que le SGC réponde également à long terme aux besoins de la Confédération en matière de transformation numérique. S'ils sont intéressés, les cantons, les villes et les communes pourront eux aussi bénéficier de l'offre. En revanche, le SGC ne fournira aucune prestation au secteur privé.

La réalisation du projet débutera en 2025 pour s'achever en 2032. Les premiers résultats des mesures mises en place devraient être exploitables dès 2026. À partir de ce moment, les applications spécialisées nouvellement développées et celles qui devront être renouvelées seront réalisées autant que possible directement sur le SGC. Dès 2027, l'étendue de leurs fonctions utilisables de façon productive devrait permettre de lancer la migration des applications spécialisées depuis l'environnement système Atlantica et le CSB-OFIT, l'objectif étant de terminer cette migration d'ici la fin de l'année 2030, puis de démanteler l'environnement système Atlantica aussi rapidement que possible. Ces travaux de migration n'englobent cependant pas les systèmes et les

applications qui ne fonctionnent pas encore sur l'une des plateformes en nuage de l'OFIT (on parle dans ce cas de systèmes hérités). Il revient aux bénéficiaires de prestations de planifier ou de demander la modernisation de ces solutions. Le remplacement des systèmes hérités comporte un potentiel d'économie supplémentaire et sera examiné en priorité par le Conseil de la transformation numérique et de la gouvernance informatique de la Confédération en même temps que le SGC.

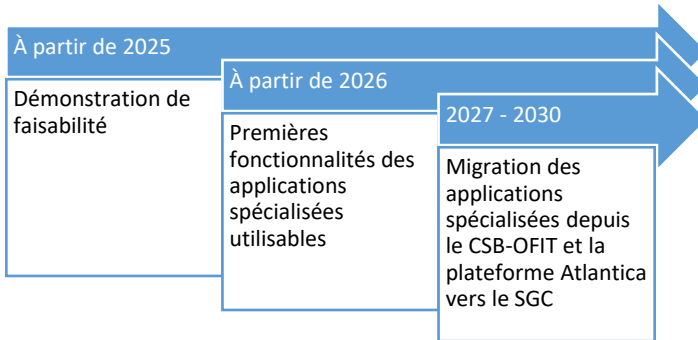


Illustration 1 : Calendrier de mise en place du SGC et de migration des applications spécialisées

Pendant la migration et jusqu'à la fin du projet en 2032, des travaux d'optimisation et de développement seront effectués sur le SGC afin de garantir l'adéquation aux besoins et le caractère innovant de la solution.

1.3 Relation avec le programme de la législation et avec le plan financier, ainsi qu'avec les stratégies du Conseil fédéral

Le SGC repose sur la stratégie d'informatique en nuage de l'administration fédérale, que le Conseil fédéral a adoptée le 11 décembre 2020. De plus, la mise en œuvre du projet est conforme aux plans concernant le réseau de centres de calcul (niveau III), à la stratégie « Réseaux de la Confédération »³ et aux principes de l'administration fédérale relatifs à l'informatique en nuage⁴.

Le SGC pose les bases nécessaires pour relever avec succès les futurs défis majeurs liés à la numérisation de l'administration fédérale. Soutenant la mise en œuvre de la

³ www.bk.admin.ch > Documentation > Communiqués > Stratégie « Réseaux de la Confédération » (état : 26.03.2024)

⁴ www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Directives informatiques > Architectures > AR010 – Principes relatifs à l'informatique en nuage (état : 26.03.2024)

stratégie « Administration fédérale numérique »⁵, ce projet contribue donc également à la stratégie « Administration numérique suisse 2024–2027 »⁶.

Dans le message du 24 janvier 2024 sur le programme de la législature 2023 à 2027⁷, le projet fait partie des affaires à traiter pour atteindre l'objectif 8 « La Confédération fournit ses prestations de manière efficace et promeut la transition numérique ».

1.4 Renonciation à la procédure de consultation

Le projet ne remplit aucune des conditions énoncées à l'art. 3, al. 1, de la loi du 18 mars 2005 sur la consultation (LCo)⁸. C'est pourquoi il ne fait pas l'objet d'une procédure de consultation

⁵ www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Administration numérique (état : 26.03.2024)

⁶ FF 2024 45

⁷ FF 2024 525

⁸ RS 172.061

2 Contenu de l'arrêté de crédit

2.1 Proposition du Conseil fédéral, avec exposé des motifs

Le projet de mise en place d'un SGC comprend des dépenses totales de 319,4 millions de francs entre 2024 et 2032 pour le programme (précision de l'estimation : $\pm 20\%$). L'OFIT y contribuera en fournissant, sur la même période, des prestations propres de l'ordre de 70,9 millions de francs. Aucun engagement pluriannuel ne sera pris en 2024, mais les coûts des travaux préparatoires, financés par l'OFIT, s'élèveront à 1,6 million de francs.

Par le présent message, le Conseil fédéral propose au Parlement d'approuver un crédit d'engagement de 246,9 millions de francs. L'arrêté fédéral prévoit en outre la libération d'une première tranche. Le Conseil fédéral décidera de la libération de la seconde tranche en fonction de l'avancement de la réalisation (cf. ch. 3.1.1.3 « Crédit d'engagement »). De plus, il pourra procéder à des transferts entre les tranches afin que les engagements découlant de dépenses supplémentaires attendues dans une tranche puissent être couverts par l'autre tranche le cas échéant.

2.2 Description détaillée du projet

La mise en place et l'utilisation ciblées et efficaces du SGC ainsi que la création de synergies nécessitent des travaux dans différents domaines, à savoir l'installation de l'infrastructure hybride multi-cloud (niveaux I et II a, II b et III) et des investissements en matière de « formation, conseil et gouvernance », « processus commerciaux et d'exploitation », « cybersécurité » et « infrastructure réseau » :

Illustration 2 : Présentation des champs d'action visés dans le cadre du projet de SGC et de la gestion générale du programme

Ces champs d'action sont présentés brièvement ci-après.

2.2.1 Mise en place de l'infrastructure hybride multi-cloud

Solution globale pour le traitement de la plupart des activités en nuage de l'administration fédérale, le SGC couvrira à l'avenir les niveaux I à III du modèle d'informatique en nuage du secteur Transformation numérique et gouvernance de l'informatique (secteur TNI) de la Chancellerie fédérale (Chf) (cf. Illustration 3), dans les domaines « Infrastructure en tant que service » (*Infrastructure as a Service* [IaaS]) et « Plateforme en tant que service » (*Platform as a Service* [PaaS]). Il constitue également une base pour les prestataires internes et externes en vue de la fourniture de solutions « Logiciel en tant que service » (*Software as a Service* [SaaS]) innovantes dans le nuage privé du SGC (niveau III) ou de leur acquisition dans le portefeuille de prestations des fournisseurs de nuages publics (niveaux I et II).

Entre 2027 et fin 2030, les solutions en nuage actuelles de l'OFIT (environnement système Atlantica et CSB-OFIT) seront remplacées par le SGC ou y seront transférées.

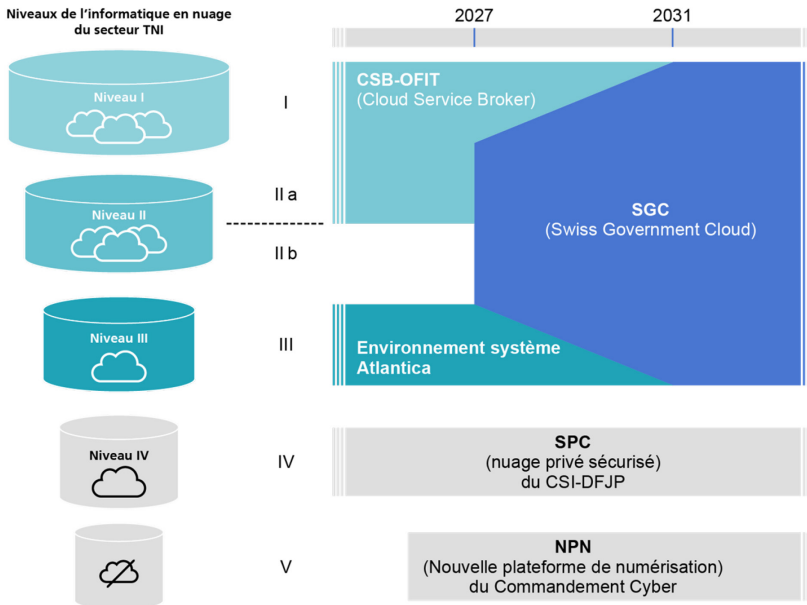


Illustration 3 : Le SGC dans le contexte du modèle d'informatique en nuage du secteur TNI

Pour le niveau IV du modèle d'informatique en nuage (nuage privé répondant à des contraintes spécifiques), les unités administratives peuvent utiliser le nuage privé sécurisé (*secure private cloud* [SPC]) du Centre de services informatiques du Département fédéral de justice et police (CSI-DFJP). Le Commandement Cyber gère la nouvelle plateforme de numérisation (NPN ; niveau V) pour les systèmes sensibles de l'armée et du Réseau national de sécurité.

Lors de l'utilisation de services en nuage, il convient de toujours déterminer quelles exigences en matière de protection des données, de sécurité de l'information, de souveraineté numérique, de fonctionnalité et d'efficacité des coûts sont prépondérantes. Solution tripartite, le SGC offre la flexibilité nécessaire pour répondre aux exigences et aux besoins divers des unités administratives.

2.2.1.1 Nuage public (*public cloud*)

La première partie de la solution comprend les services en nuage public que l'OFIT met à la disposition des bénéficiaires de prestations par l'intermédiaire de fournisseurs

établis. Elle correspond au niveau I (nuages publics standard) et à une partie du niveau II (niveau II a, soit les produits en nuage public avec des contraintes supplémentaires) du modèle du secteur TNI. Le nuage public se caractérise notamment par son évolutivité élevée et son vaste portefeuille de prestations novatrices.

L'utilisation de services en nuage public est intéressante d'un point de vue économique et technologique, car par comparaison avec les services en nuage privé, leurs coûts sont plus faibles et le portefeuille de prestations est sensiblement plus étendu. Le recours au nuage public est donc préconisé, dans le respect des obligations légales. Les fournisseurs de nuages publics doivent être en mesure de répondre aux exigences juridiques et techniques supplémentaires qui sont définies dans un cahier des charges.

Lorsque les unités administratives acquièrent des prestations en nuage public depuis le SGC, elles bénéficient de prestations préliminaires qui leur font gagner du temps et de l'argent. Elles profitent par exemple des acquisitions déjà réalisées par l'OFIT (en d'autres termes, elles ne doivent pas lancer leurs propres appels d'offres OMC) ainsi que de prestations préconfigurées et compatibles avec les services standard de la Confédération, tout en ayant la garantie que les exigences de la protection de base sont respectées.

2.2.1.2 Nuage public sur site (*public cloud on-prem*)

La deuxième partie, à savoir le nuage public sur site, couvre une partie du niveau II (niveau II b) du modèle du secteur TNI. En l'espèce, des solutions de fournisseurs établis de nuages publics sont exploitées dans les centres de calcul de la Confédération (exploitation sur site ou *on premise*). Les bénéficiaires de prestations peuvent ainsi tirer parti des avantages des services en nuage public sur site et, dans la mesure du possible, traiter les données là où elles sont générées (*edge computing*). Ce dernier point, notamment, revêt une grande importance pour les applications gourmandes en données, en particulier dans des secteurs d'avenir comme l'Internet des objets ou l'analyse de données : les temps de latence sont inférieurs à ceux des niveaux I et II a (nuage public), ce qui améliore la performance, décharge le réseau, et se répercute donc favorablement sur les coûts. Le niveau II b sera toutefois mis en place uniquement si une demande en ce sens est avérée, et les capacités ne seront augmentées que pour répondre à une demande explicite des clients.

2.2.1.3 Nuage privé sur site (*private cloud on-prem*)

La troisième partie du SGC englobe le nuage privé sur site, couvrant ainsi le niveau III du modèle du secteur TNI. Contrairement au nuage public, toute l'infrastructure en nuage est ici exploitée dans le réseau de centres de calcul de la Confédération. Conformément au modèle susmentionné, les données sont conservées et traitées exclusivement sur les propres systèmes de l'administration fédérale, dans ses centres de calcul, sur la base d'un produit standard pour les infrastructures en nuage et les plateformes. Si nécessaire, l'administration fédérale peut assurer seule l'exploitation du nuage privé sur site (exploitation autonome en cas de besoin).

2.2.2 Développement de l'infrastructure réseau

L'infrastructure réseau est un élément capital pour réussir la transformation numérique, car elle est le socle de toutes les prestations de l'infrastructure hybride multi-cloud actuelle et future de l'OFIT. L'infrastructure réseau de l'administration fédérale comprend des connexions directes à Internet et des raccordements dédiés aux fournisseurs de services en nuage public.

L'utilisation accrue de ces services dans le modèle hybride de l'informatique en nuage modifie également les exigences relatives à l'infrastructure réseau, tant pour les réseaux existants dans et entre les centres de calcul de l'administration fédérale que pour les deux connexions susmentionnées. Ces deux types de raccordement nécessitent des consolidations substantielles, que l'on peut résumer comme suit :

Augmentation des bandes passantes réseaux et amélioration de la disponibilité de l'infrastructure réseau

Le besoin en bande passante réseau augmente en raison de l'utilisation croissante des applications spécialisées de l'administration fédérale sur Internet, de l'intégration accrue des services de fournisseurs de nuages publics, d'une plus grande interconnexion numérique avec d'autres administrations en Suisse et à l'étranger et, de manière générale, d'une numérisation accrue de l'administration fédérale. Le trafic réseau se réoriente vers les prestataires externes, au détriment des centres de calcul sur site. Compte tenu de cette évolution, l'infrastructure réseau existante atteint parfois ses limites, par exemple pour traiter en temps réel les données vidéo dans le domaine douanier, analyser de grands volumes de données dans le nuage public ou rapatrier depuis celui-ci vers le réseau de la Confédération des données sauvegardées. Si l'administration fédérale poursuit sa transformation numérique, ce problème s'accroîtra : selon des données empiriques, le besoin en bande passante double actuellement tous les trois ans environ. Au vu des évolutions susmentionnées, l'OFIT estime que ce doublement pourrait même se produire tous les deux ans à l'avenir.

Les surcharges de l'infrastructure réseau depuis et vers les prestataires Internet affectent la stabilité et la fiabilité des prestations réseaux, entraînant le ralentissement, voire une interruption des applications spécialisées de la Confédération. Pour réduire ce risque, il est primordial de développer à temps l'infrastructure réseau depuis et vers les fournisseurs de services en nuage public et les connexions directes à Internet en vue d'une utilisation accrue des bandes passantes. En plus d'augmenter celles-ci, il convient d'améliorer la fiabilité grâce à du matériel supplémentaire performant. Les modifications de l'infrastructure réseau, y compris les extensions de bande passante, sont longues à réaliser et doivent être planifiées minutieusement.

Développement des infrastructures réseaux dans les centres de calcul de l'administration fédérale

Les infrastructures réseaux doivent être développées dans les centres de calcul de l'administration fédérale pour répondre au besoin supplémentaire qui découle d'une plus grande utilisation des prestations numériques.

Automatisation accrue du réseau et processus de facturation facilité conforme au principe de causalité dans les centres de calcul de l'administration fédérale

La mise à disposition plus rapide et plus économique des applications nécessite également une automatisation accrue du réseau sous-jacent. L'automatisation des tâches répétitives et des processus récurrents se traduit par une hausse considérable de la sécurité et de l'efficacité, car elle réduit le temps et les ressources alloués aux interventions manuelles. De plus, l'automatisation permet de réagir plus rapidement aux exigences changeantes et diminue la durée des possibles interruptions. Ce point est essentiel pour pouvoir réagir avec souplesse à de nouveaux projets, services ou technologies sans pour autant compromettre la performance du réseau. Le SGC permettra aux fournisseurs et aux bénéficiaires de prestations informatiques d'utiliser de manière flexible des services en nuage adaptés à leurs besoins. Les unités administratives ayant des besoins différents, il va de soi que les prestations utilisées et les bandes passantes nécessaires divergent également. Par conséquent, les travaux relatifs à l'infrastructure réseau seront l'occasion de mettre en place les conditions techniques requises pour une facturation transparente et conforme au principe de causalité des prestations réseaux utilisées tant sur le réseau de la Confédération que pour Internet. La possibilité de recenser et d'imputer précisément l'usage des ressources réseau facilitera l'établissement d'un budget précis et le contrôle des coûts. L'administration fédérale sera alors en mesure de gérer plus efficacement ses ressources financières.

Renforcement de la sécurité technique du réseau

Compte tenu du trafic réseau en hausse, il est indispensable de renforcer la sécurité technique du réseau pour s'assurer que les dispositifs mis en place peuvent supporter l'accroissement du volume de données. L'extension de l'infrastructure de sécurité garantit une protection efficace contre les menaces éventuelles et l'intégrité du réseau.

2.2.3 Renforcement de la cybersécurité

Les données seront davantage traitées en dehors des centres de calcul de l'administration fédérale à la suite de la mise en œuvre de la stratégie hybride multi-cloud. Leur protection doit donc être adaptée aux nouvelles circonstances. Les mesures prévues dans le cadre du SGC permettront de combler les lacunes éventuelles et d'exploiter les synergies potentielles, créant ainsi les conditions requises en vue de poursuivre la mise en œuvre de la cyberstratégie nationale⁹ et des obligations de l'administration fédérale en matière de sécurité de l'information¹⁰.

⁹ www.ncsc.admin.ch > Stratégie CSN (état : 26.03.2024)

¹⁰ www.ncsc.admin.ch > Documentation > Directives de sécurité informatique (état : 26.03.2024)

2.2.3.1 Protection des données et sécurité de l'information

Conformément à la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)¹¹, il convient de garantir une sécurité adéquate des données personnelles par rapport au risque encouru. À cette fin, la loi exige des mesures organisationnelles et techniques appropriées. On veillera à ce que le SGC remplisse les conditions voulues sur les plans technique et organisationnel pour satisfaire aux exigences de la LPD en matière de sécurité des données.

Pour s'assurer que le SGC répond à ces exigences, il sera appliqué la procédure de sécurité de l'Office fédéral de la cybersécurité¹². Les données à traiter ne pourront être transférées dans l'un des niveaux du SGC qu'après un examen au cas par cas réalisé par l'organe fédéral compétent, indiquant que le projet concerné et le traitement des données y relatives dans l'un des niveaux du SGC sont conformes à la loi. En l'espèce, il est essentiel d'examiner en détail le droit applicable au traitement des données concernées.

L'examen peut révéler que le traitement des données présente un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Dans ce cas, l'organe fédéral compétent doit procéder à une analyse d'impact relative à la protection des données personnelles (AIPD). Si, malgré les mesures prévues, l'AIPD confirme ce risque, il faut demander au Préposé fédéral à la protection des données et à la transparence (PFPDT) de prendre position.

Par conséquent, il n'est pas possible d'affecter automatiquement ou sur la base d'un schéma les données personnelles et les informations sensibles à l'un des niveaux de l'informatique en nuage. Le traitement de données personnelles dans un nuage public en particulier peut ne pas être autorisé, car il présente le risque que les prestataires, leur État d'origine ou des tiers accèdent aux données en question.

Selon la LPD, des données personnelles peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que l'État concerné dispose d'une législation assurant un niveau de protection adéquat ou que les conditions énoncées dans cette loi sont remplies. Là encore, la décision devra être prise au cas par cas.

La loi du 18 décembre 2020 sur la sécurité de l'information (LSI)¹³, l'ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI)¹⁴, l'ordonnance du 8 novembre 2023 sur les contrôles de sécurité relatifs aux personnes (OCSP)¹⁵, l'ordonnance du 8 novembre 2023 sur la procédure de sécurité relative aux entreprises (OPSEnt)¹⁶ et l'ordonnance du 19 octobre 2016 sur les systèmes de gestion des données

¹¹ RS 235.1

¹² www.ncsc.admin.ch > Documentation > Directives de sécurité informatique > Procédure de sécurité (état : 26.03.2024)

¹³ RS 128

¹⁴ RS 128.1

¹⁵ RS 128.31

¹⁶ RS 128.41

d'identification et les services d'annuaires de la Confédération (OIAM)¹⁷ visent à garantir la sécurité du traitement des informations relevant de la compétence de la Confédération et la sécurité de ses moyens techniques.

La LSI fixe les échelons de classification suivants : « interne », « confidentiel » et « secret ». Elle définit également les catégories de sécurité « protection de base », « protection élevée » et « protection très élevée », tous les moyens informatiques étant affectés à la catégorie de sécurité « protection de base », à moins qu'ils relèvent d'une catégorie de sécurité supérieure.

Le SGC est conçu de telle sorte que les informations relevant de la catégorie de sécurité « protection élevée » ou des catégories inférieures puissent être traitées en toute sécurité. En revanche, les informations de la catégorie de sécurité « protection très élevée » ne pourront pas y être traitées. Le SGC ne proposera donc aucune solution pour les données de l'échelon de classification « secret » visées par la LSI. Il couvre les niveaux I à III du modèle d'informatique en nuage du secteur TNI.

Les conditions techniques pour un traitement sûr des informations requérant une « protection élevée » ou plus faible sont réunies tant dans l'infrastructure en nuage sur site de la Confédération que chez les éventuels fournisseurs établis de nuages publics.

Les autorités et organisations concernées sont responsables de la sécurité de l'information. Les unités administratives évaluent régulièrement les risques inhérents aux objets à protéger, mettent en œuvre les mesures nécessaires et vérifient leurs effets. Le service compétent doit accepter expressément les risques résiduels constatés.

Fédéraliste, la gouvernance prévue dans la LSI et les ordonnances s'y rapportant incombe aux autorités et organisations concernées. Pour le SGC, il est néanmoins important de proposer des prestations aussi standardisées que possible pour permettre à la fois l'automatisation nécessaire et la création de synergies. Il est donc prévu de créer un centre de compétence du SGC, qui sera chargé de conseiller les bénéficiaires de prestations en conséquence, afin de contribuer à une utilisation économique des infrastructures en nuage.

2.2.3.2 Défis liés à la cybersécurité

La cybersécurité a pour but de protéger contre les abus et les dysfonctionnements les moyens informatiques utilisés pour accomplir les tâches prévues par la loi. Les défis qu'elle doit relever dans ce contexte ont cependant fondamentalement changé : auparavant, les systèmes informatiques étaient exploités de manière centralisée dans les centres de calcul, et les postes de travail se trouvaient dans les bâtiments de la Confédération. Or, la technologie permet désormais de travailler de n'importe où et d'accéder au réseau de la Confédération avec différents appareils, l'utilisation du nuage public gagnant lui aussi en importance.

Cette évolution a modifié les limites du périmètre de sécurité classique et requiert un ajustement des stratégies de cybersécurité. De nouvelles stratégies de défense doivent

¹⁷ RS 172.010.59

être élaborées en raison de la professionnalisation croissante des pirates informatiques, qui affinent régulièrement leurs méthodes (p. ex. grâce à l'intelligence artificielle). Grâce à leurs vastes mesures de sécurité et à leurs équipes internationales de sécurité, les fournisseurs de nuages publics sont en mesure de renforcer les infrastructures de sécurité de l'administration fédérale.

Il est important d'opérer une distinction entre la « sécurité du nuage » (responsabilité opérationnelle du fournisseur du nuage public) et la « sécurité au sein du nuage » (responsabilité opérationnelle du client). Un modèle de « responsabilité partagée » a été élaboré pour répartir les compétences entre ces deux domaines de responsabilité. Il définit qui est responsable de quelle partie de l'infrastructure et constitue dès lors l'élément central de la gouvernance pour exploiter les applications spécialisées. Cela décharge l'administration fédérale, qui peut ainsi se focaliser sur ses tâches principales.

2.2.3.3 Objectif de la cybersécurité

La cybersécurité vise à assurer la protection des informations et des données ainsi que le respect des prescriptions de l'administration fédérale. Pour répondre à ces objectifs, des mesures sont prises dans cinq sous-domaines sur la base du dispositif (*Cyber Security Framework*) établi par le *National Institute of Standards and Technology* (NIST)¹⁸. Ces sous-domaines sont présentés ci-après en mettant l'accent sur le SGC.

Identifier

Un inventaire fiable est nécessaire pour organiser la cybersécurité de manière professionnelle. Il doit pouvoir être mis à jour automatiquement, car le secteur informatique évolue rapidement. La mise en place du SGC étend considérablement cet inventaire, raison pour laquelle le champ d'action relatif à la cybersécurité comprend l'installation d'un outil visant à recenser automatiquement les logiciels utilisés et, le cas échéant, à détecter les failles de sécurité.

Protéger

Une fois que l'inventaire sera établi et à jour, il conviendra de mettre en place une protection appropriée fondée sur les risques. Dans le cadre du SGC, cela implique d'étendre les licences nécessaires pour les outils de protection afin de garantir partout la protection de base prescrite. De plus, un nouveau plan de protection devra être défini et mis en œuvre.

Par ailleurs, il importe de prévoir contractuellement non seulement la mise en œuvre des mesures prévues par l'OPSEnt, mais aussi la possibilité de mener des audits indépendants auprès des fournisseurs.

Détecter

¹⁸ [www.csrc.nist.gov > Glossary > Search > NIST Framework for Improving Critical Infrastructure Cybersecurity](https://www.csrc.nist.gov/Glossary/Search/NIST-Framework-for-Improving-Critical-Infrastructure-Cybersecurity) (état : 26.03.2024)

Les menaces générales et les méthodes d'attaque spécifiques étant en constante évolution dans le domaine de la cybersécurité, une protection absolue ne saurait être garantie. Il est donc primordial de mettre sur pied un système de détection performant : si un cybercriminel réussit à pénétrer dans l'infrastructure de l'administration fédérale, il faut identifier l'attaque aussi rapidement que possible pour en limiter les dommages. Pour ce faire, il convient d'étendre les mesures en vigueur et d'en mettre en place de nouvelles, la principale étant un outil de détection des comportements inhabituels sur le réseau. Dans le cadre du SGC, les équipements et les licences nécessaires seront acquis, et le personnel sera habilité à détecter des anomalies dans le trafic réseau et à prendre des contre-mesures.

Réagir

Lorsqu'une attaque de cybercriminel ou un malicieux a été détecté, il faut prendre des contre-mesures. En l'espèce, il est essentiel d'agir aussi rapidement que possible. C'est la raison pour laquelle une automatisation partielle des réponses aux attaques et aux malicieux sera introduite avec le SGC.

Restaurer

Après qu'une attaque ou un malicieux a été contré, il convient de tirer les enseignements pertinents de cet incident et de mettre à jour les outils de détection pour éviter que des procédés similaires n'atteignent leur but. Pour ce faire, il n'est pas prévu de prendre des mesures techniques supplémentaires dans le SGC, mais de renforcer les effectifs.

2.2.3.4 Conformité informatique

Lors de la mise en place des trois niveaux du SGC, il faudra veiller au respect des dispositions en matière de sécurité et de conformité. C'est pourquoi des règles de sécurité reconnues sur le plan international et un test strict de la conformité informatique seront mis en place. Pour répondre à cette exigence, il faudra recruter de nouveaux collaborateurs dotés des compétences nécessaires.

Certifié selon la norme ISO 27001, l'OFIT exploite depuis des années un système de management de la sécurité de l'information (SMSI) conforme à cette norme. En outre, sur mandat du Contrôle fédéral des finances (CDF), une société externe effectue chaque année l'audit selon la norme ISAE 3402 des applications qui sont pertinentes pour le compte d'État et gérées par l'OFIT. La LPD prévoit également une certification. Son SMSI étant certifié, l'OFIT remplit les conditions pour certifier la protection des données sur cette base. L'extension de la certification ISO 27001 au nuage public entraînera une hausse des charges de personnel. Le SGC ne tient cependant pas compte des charges supplémentaires induites par la nouvelle LPD, car celles-ci sont imputées aux applications concernées et donc aux bénéficiaires des prestations.

2.2.4 Processus commerciaux et d'exploitation

Le dynamisme croissant dans l'environnement numérique, en particulier en matière de nuages publics, requiert des solutions industrialisées et fortement automatisées

pour exploiter un environnement hybride multi-cloud (processus d'exploitation) et pour traiter les mandats (de la commande de services en nuage par les clients sur le portail de libre-service jusqu'à l'imputation complète et conforme au principe de causalité des prestations utilisées [processus commerciaux]). La chaîne des processus du champ d'action « Processus commerciaux et d'exploitation » sera donc automatisée dans son intégralité.

2.2.4.1 Processus d'exploitation

Des processus d'exploitation hautement automatisés garantissent une mise à disposition et une actualisation technique rapide et cohérente des infrastructures et des prestations, réduisent les incohérences et les erreurs, contribuent à un usage efficace des ressources existantes et à la désactivation automatique des ressources inutilisées et déchargent les spécialistes informatiques des tâches manuelles récurrentes.

Le SGC servira ainsi à mettre en place un nouveau modèle d'exploitation industrialisé qui permettra, d'une part, de réduire considérablement les ressources en personnel dédiées à l'exploitation des infrastructures et des plateformes. Les ressources ainsi libérées pourraient alors être affectées à des secteurs qui travaillent plus étroitement avec la clientèle (p. ex. le développement des applications spécialisées ou le conseil) et apportent une plus grande valeur ajoutée aux bénéficiaires de prestations. D'autre part, l'automatisation systématique des processus et la standardisation du catalogue de prestations permettront à long terme de réduire les coûts d'exploitation.

Afin qu'il soit socialement acceptable, ce changement interviendra dans le cadre de la future vague de départs à la retraite des baby-boomers (ces dix prochaines années, près d'un tiers des personnes travaillant à l'OFIT prendront leur retraite) ; les futurs retraités seront remplacés par des personnes dont le profil correspond aux exigences du nouveau modèle d'exploitation.

Modèle « Fournisseur de prestations informatiques pour un fournisseur de prestations informatiques »

Par ailleurs, les autres fournisseurs de prestations informatiques pourront également proposer des prestations à leurs clients au sein de la Confédération et à d'autres services de l'administration publique à partir du SGC. Celui-ci met à disposition un modèle « Fournisseur de prestations informatiques pour un fournisseur de prestations informatiques » grâce à des fonctionnalités techniques et à des mesures organisationnelles. Par conséquent, ses prestations ne devront pas nécessairement être acquises auprès de l'OFIT, mais pourront en principe l'être auprès de tous les fournisseurs de prestations informatiques de la Confédération, ce qui permettra de créer des synergies au sein de celle-ci.

2.2.4.2 Processus commerciaux

Dans le cadre du SGC, l'accent sera également mis sur les processus commerciaux afin d'automatiser l'intégralité de la chaîne des processus, l'objectif étant de réduire sensiblement la charge administrative des bénéficiaires de prestations et du personnel de l'OFIT. De plus, les bénéficiaires de prestations profiteront d'une transparence accrue.

Portail de libre-service

Grâce au SGC, les fournisseurs et les bénéficiaires de prestations informatiques pourront profiter des avantages des services en nuage en toute facilité. En effet, le SGC sera relié à un nouveau portail de libre-service de l'OFIT, dans lequel les bénéficiaires de prestations pourront commander et gérer de manière simple et centralisée leurs prestations sur les différentes plateformes en nuage. Cela permettra également de rendre l'utilisation du nuage plus sûre, plus efficace, plus agile et plus conviviale.

Rapports et décomptes des services en nuage (cockpit à 360 degrés)

La gestion de l'utilisation des ressources dans un environnement hybride multi-cloud nécessite une surveillance, un décompte et une facturation effectifs des services employés. Le portail de libre-service proposera donc un cockpit à 360 degrés qui fournira à tout moment aux unités administratives une vue d'ensemble de l'utilisation et des coûts de leurs ressources en nuage, ce qui leur permettra de les contrôler.

Dans ce cockpit, les unités administratives pourront suivre et évaluer de manière centralisée l'utilisation des ressources acquises auprès de différents fournisseurs de nuage. Des rapports transparents sur cette utilisation et ses coûts et des mécanismes intégrés de contrôle des coûts leur permettront d'analyser en détail les habitudes d'utilisation. Les unités administratives pourront ainsi garder un œil sur leurs dépenses, et planifier et optimiser l'usage de leurs ressources en nuage.

Intégration de processus commerciaux spécifiques pour le modèle « Fournisseur de prestations informatiques pour un fournisseur de prestations informatiques »

Le SGC mettra à disposition des interfaces et des fonctionnalités en vue de son intégration dans les processus commerciaux des fournisseurs de prestations informatiques qui proposent des services du SGC à leurs bénéficiaires de prestations sur la base du modèle « Fournisseur de prestations informatiques pour un fournisseur de prestations informatiques ». Ces fournisseurs pourront ainsi offrir eux aussi à leurs clients des rapports transparents et automatisés sur leur utilisation des services et une facturation conforme au principe de causalité.

2.2.5 Formation, conseil et gouvernance

Les unités administratives doivent pouvoir utiliser le SGC de manière sûre, efficace et ciblée. Dans le cadre du champ d'action « Formation, conseil et gouvernance », elles pourront, en cas de besoin, bénéficier d'un accompagnement de A à Z pour apprendre à utiliser l'environnement hybride multi-cloud. On s'assurera ainsi qu'elles tirent pleinement parti des avantages de l'environnement et des technologies connexes, tout en réduisant les risques potentiels.

2.2.5.1 Offre de formation

Le SGC introduira de nouvelles technologies, plateformes et prestations en nuage et de nouveaux processus dans l'administration fédérale. Une offre de formation de grande qualité baptisée « SGC Academy » sera proposée pour développer et consolider le savoir technique relatif au SGC, permettant ainsi au personnel d'acquérir les

connaissances et les compétences requises pour exploiter au mieux ces nouvelles possibilités. Les cours s’adresseront aux personnes assumant les rôles les plus divers pour aider de manière optimale les unités administratives à acquérir les connaissances nécessaires dans les domaines concernés, mais l’accent sera mis sur le perfectionnement des spécialistes informatiques.

2.2.5.2 Centre de compétence du SGC

Le centre de compétence du SGC conseillera, soutiendra et accompagnera les unités administratives intéressées dans l’élaboration et la mise en œuvre de leur stratégie d’informatique en nuage et des projets en découlant (p. ex. sélection des services en nuage appropriés ou présentation des meilleures pratiques). Les principaux thèmes seront la fonctionnalité et l’architecture de l’informatique en nuage, l’efficacité et le contrôle des coûts, la gouvernance de l’informatique en nuage et la souveraineté numérique. Ce centre aidera les unités intéressées à choisir le niveau adéquat du nuage ou à coordonner leurs acquisitions, contribuant ainsi de manière importante à une utilisation économique des trois niveaux du SGC.

2.2.5.3 Centre d’innovation

Il faut rendre les prestations et les concepts du SGC tangibles. En leur montrant comment faire progresser leur transformation numérique grâce au SGC, le centre d’innovation entend inspirer les bénéficiaires de prestations. Il contribuera ainsi à l’objectif stratégique du SGC, à savoir accélérer la numérisation de l’administration. Le centre d’innovation permet aux unités administratives et à d’autres services intéressés d’engager un dialogue ouvert sur des projets d’informatique en nuage qui ont été mis en œuvre avec succès, sur les nouvelles prestations innovantes disponibles (p. ex. dans le domaine de l’intelligence artificielle) et sur les bonnes pratiques.

2.2.5.4 Gouvernance de l’informatique en nuage à l’échelle du SGC

Conformément à la stratégie hybride multi-cloud de l’administration fédérale, les unités administratives pourront utiliser et combiner différents services en nuage qu’ils ont achetés ou qui ont été développés par la Confédération. Des mesures techniques, contractuelles, organisationnelles et relatives au personnel sont toutefois nécessaires pour garantir une utilisation sûre, ordonnée et efficace de ces services. Elles sont définies dans le cadre de la gouvernance de l’informatique en nuage.

Le secteur TNI de la ChF a défini dans les principes relatifs à l’informatique en nuage les règles fondamentales à prendre en compte lors de l’utilisation de services en nuage public ou privé. Sur cette base, la gouvernance de l’informatique en nuage à l’échelle du SGC garantit que l’ensemble des ressources et des services en nuage respectent des directives et des normes unifiées pour assurer une gestion cohérente des différents environnements en nuage et prévenir les incompatibilités. De plus, cette gouvernance permet de mettre en œuvre et d’imposer des directives et des mesures de sécurité à tous les échelons du SGC, garantissant ainsi une protection homogène contre les menaces. Ce faisant, elle contribue également au respect des exigences de conformité et des dispositions relatives à la protection des données. Dans le cadre du SGC, les fournisseurs de prestations informatiques peuvent utiliser des services préconfectionnés,

préconfigurés et compatibles avec les services standard de la Confédération pour élaborer et mettre en œuvre leurs solutions.

Dans un modèle hybride d'informatique en nuage, plusieurs environnements en nuage doivent pouvoir se combiner facilement les uns aux autres. La gouvernance générale de l'informatique en nuage englobe la mise en place de mécanismes d'interopérabilité des différentes offres en nuage du SGC permettant de passer aussi simplement que possible d'un fournisseur de nuages à un autre et d'un niveau du nuage à un autre (« stratégie de sortie »). La gouvernance de l'informatique en nuage à l'échelle du SGC contribue fortement à garantir la rentabilité à long terme du SGC en donnant la possibilité à la Confédération de réagir, par exemple, à une modification défavorable des conditions et de changer de fournisseur le cas échéant.

2.3 Variantes étudiées pour la mise en place et la séquence

Dans le cadre de la conception du SGC, plusieurs variantes ont été étudiées pour la mise en place séquentielle de l'infrastructure hybride multi-cloud et évaluées selon les critères suivants :

- réduction des coûts du fournisseur de prestations informatiques (FP), à savoir l'OFIT ;
- réduction des coûts du bénéficiaire de prestations (BP) ;
- charges liées à la migration ;
- sécurité de la planification ;
- amélioration de la stabilité opérationnelle ;
- mise à profit de la vague de départs à la retraite ;
- coûts liés à la mise en place et à l'exploitation en parallèle.

La variante qui a obtenu la meilleure évaluation est celle qui établit dès le début les bases de l'acquisition de l'ensemble des trois niveaux du SGC. Les niveaux I, II a et III seront ensuite mis en place en parallèle. Les niveaux II b et III seront d'abord mis en place avec les ressources d'infrastructure requises pour la migration, puis ajustés selon les besoins. Le niveau II b ne doit être mis en place que si des clients en font concrètement la demande. Sur la base de l'analyse des besoins, l'OFIT considère que les premiers bénéficiaires de prestations voudront profiter de cette offre à partir de 2029.

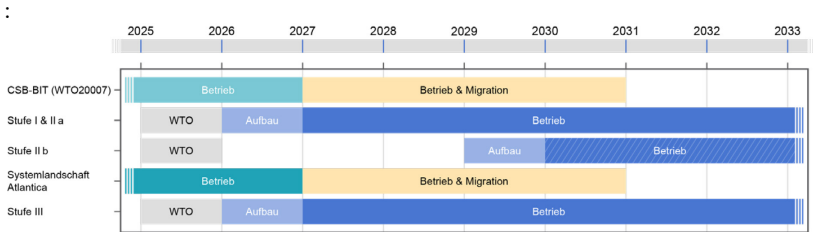


Illustration 44 : Calendrier pour la variante mise en place parallèle des niveaux I, II a et III

Cette façon de procéder permettra de réaliser d'importantes économies (cf. ch. 3.1.1.5 « Économies pendant le programme et après sa conclusion ») et d'améliorer fortement la stabilité opérationnelle grâce à une automatisation et une standardisation cohérente (voir aussi ch. 2.2.4 « Processus commerciaux et d'exploitation »). La sécurité de la planification des bénéficiaires de prestations et des autres fournisseurs de prestations informatiques de la Confédération sera par ailleurs assurée, puisque l'équipement technologique des niveaux du SGC sera défini suffisamment tôt. La planification de la migration vers les niveaux ainsi que celle des projets de cycle de vie des applications spécialisées vieillissantes devant être rapidement remplacées, notamment, s'en trouvera grandement simplifiée.

2.4 Analyse et identification des besoins

Le SGC implique de mettre en place une infrastructure hybride multi-cloud réalisée selon les exigences et besoins de la Confédération, et conforme à la stratégie d'informatique en nuage de celle-ci. Pour atteindre cet objectif, deux enquêtes ont été menées dans le cadre des travaux préparatoires relatifs au SGC.

L'analyse des besoins, qui a permis de définir les besoins et les exigences des unités administratives de l'administration fédérale et des Services du Parlement, offre une base cohérente au SGC. Les résultats servent à comprendre les exigences spécifiques des bénéficiaires de prestations en matière d'évolutivité, d'étendue des fonctions ainsi que de sécurité et de conformité de l'infrastructure. La suite de la planification du projet ainsi que l'appel d'offres public pour la mise en place du SGC s'appuient sur ces résultats. L'analyse montre que les unités administratives approuvent la mise en place d'une infrastructure hybride multi-cloud qui remplit les nombreuses exigences de la Confédération relatives à l'activité professionnelle, à la sécurité et aux aspects techniques.

Dans le cadre de l'identification des besoins, une enquête a été réalisée auprès des départements, des fournisseurs de prestations informatiques de la Confédération et des Services du Parlement pour savoir s'il était nécessaire d'introduire de manière planifiée un modèle « Fournisseur de prestations informatiques pour un fournisseur de

prestations informatiques » et pour identifier les exigences à remplir de leur point de vue à cet égard. L'enquête a révélé que tous approuvent l'introduction de ce modèle.

On a par ailleurs voulu estimer les besoins futurs, soit le volume d'acquisitions prévisionnel et sa répartition en pourcentage entre les différents niveaux d'informatique en nuage du SGC, pour établir, sur cette base, le volume d'achats des appels d'offres publics pour la mise en place du SGC, ainsi que vérifier l'estimation des coûts de la mise en place.

En résumé, les fournisseurs de prestations informatiques de la Confédération ont indiqué qu'en l'état actuel des choses, on pouvait s'attendre à ce que les acquisitions portent sur les volumes suivants en se basant sur les trois niveaux du SGC :

- applications spécialisées : 1027 ;
- machines virtuelles : 9413 ;
- conteneurs : 8200 ;
- mémoire : 108,9 pétaoctets ;
- cœurs de processeur : 19 868.

La répartition moyenne de l'utilisation de nuages par la Confédération se compose comme suit selon l'estimation actuelle des besoins futurs :

	Au moment de la migration en 2027	À la fin du programme en 2032
Niveau I et II a – nuage public	8 %	68 %
Niveau II b – nuage public sur site	0 %	10 %
Niveau III – nuage privé sur site	92 %	22 %

Tableau 1 : Répartition en pourcentage de l'utilisation prévisionnelle des niveaux de l'informatique en nuage

Le tableau montre que les fournisseurs de prestations informatiques prévoient un transfert relatif de leurs quantités de données du nuage privé vers le nuage public. Cela coïncide avec les estimations des gouvernements étrangers et de Gartner, cabinet spécialisé en études de marché, qui ont été interrogés dans le cadre des travaux préliminaires relatifs au SGC. Compte tenu de ce transfert, tous les niveaux du SGC seront conçus de manière évolutive. Le matériel nécessaire pour mettre en place les solutions sur site doit donc être obtenu dans le cadre d'un modèle de facturation selon l'utilisation effective (*Pay as You Use*) et pas acheté. On lira le tableau en tenant compte du fait que, selon des données empiriques, il y aura une forte croissance des volumes de données à tous les niveaux.

En raison de la modification constante de l'environnement des applications et des technologies ainsi que d'autres évolutions, il faut s'attendre à ce que les chiffres indiqués ci-dessus changent encore d'ici au début de la migration en 2027. L'OFIT mettra donc l'identification des besoins à jour chaque année pour que la taille de l'infrastructure évolutive du SGC mise en place corresponde aux besoins effectifs.

2.5 Risques

2.5.1 Contexte de l'évaluation des risques

L'évaluation des risques a été réalisée en considérant que le Parlement approuvera le crédit d'engagement pour le SGC puis le financement de ce projet.

L'évaluation se concentre sur les risques que le programme prend directement en compte, c'est-à-dire les tâches et objectifs non réalisés visés au ch. 2.1.

2.5.2 Risque de ne pas atteindre les objectifs

De manière générale : le risque de ne pas obtenir les résultats escomptés peut se réaliser lorsque les objectifs du programme définis à l'origine doivent être modifiés durant la mise en œuvre du projet, par exemple en raison de la rapidité de l'évolution technique, avec notamment l'intelligence artificielle ou la numérisation croissante de la vie quotidienne. Si les objectifs du programme sont adaptés pour pouvoir réagir à ce type d'évolutions, cela aura un effet direct sur les coûts et les délais de mise en œuvre.

Concrètement : il ne serait pas possible d'établir l'accès uniforme souhaité à l'ensemble du spectre des services d'informatique en nuage des niveaux I à III si la gouvernance informatique de l'administration fédérale optait pour une autre solution.

Sécurité et conformité : l'objectif est ici de fournir aux bonnes personnes les informations nécessaires au bon moment et sans qu'elles aient été modifiées, afin que les décisions puissent être prises de la manière la plus éclairée possible. Les attaques par rançongiciel, qui consistent à chiffrer des informations et menacer de publier les données volées, constituent actuellement la plus grande menace. Un autre objectif est de respecter les lois, les prescriptions et les conventions contractuelles.

Risques techniques : l'objectif est de mettre à disposition une infrastructure moderne et tournée vers l'avenir. Il existe un risque d'être pris de court par des innovations révolutionnaires et d'introduire de nouvelles technologies pouvant créer des problèmes de compatibilité pendant la durée du projet. Il s'agit également d'éviter au maximum les dettes techniques.

Risques de marché : le marché des nuages informatiques est volatil et se caractérise actuellement par la consolidation de différentes solutions techniques. Il résulte de cette situation le risque d'investir dans des solutions qui ne s'imposeront pas sur le marché et, donc, de se retrouver avec une dette technique. Autre aspect, la tendance des fournisseurs de nuages à proposer des offres verticales, c'est-à-dire à offrir de plus en plus des services adaptés à certains secteurs (p. ex. la santé ou l'industrie). Cette tendance s'observe aussi sur le segment de marché des administrations publiques. Si l'administration publique devait malgré tout miser sur des solutions personnalisées ou fortement adaptées à des besoins spécifiques plutôt que sur des solutions standard proposées par les fournisseurs de nuages, elle risquerait d'avoir à assumer des coûts élevés.

Risques d'acceptation : le SGC doit être conçu de manière à répondre aux exigences et aux besoins de l'administration publique. Dans le cas contraire, il existe un risque

que la solution mise en place dans le cadre du projet ne rencontre pas le degré d'acceptation nécessaire auprès des futurs utilisateurs. Il convient d'éviter d'éventuels mauvais investissements.

2.5.3 Mesures pour atteindre les objectifs

De manière générale : le programme SGC comporte différents axes d'action face à ce risque : la collaboration avec des hautes écoles et un cabinet spécialisé en analyses de marché renommé ; l'observation minutieuse du marché dans le domaine des nouvelles technologies ; et la gestion rigoureuse du changement.

Sécurité et conformité : aujourd'hui déjà, l'OFIT est certifié selon la norme ISO 27001 et dispose d'un système de contrôle complet. Par ailleurs, les applications pertinentes pour le compte d'État sont contrôlées chaque année par une entreprise mandatée par le CDF. L'OFIT réduit ainsi les risques liés à la sécurité de l'information. En outre, plus de 50 cyberchampions (collaborateurs internes à l'OFIT disposant d'une formation complémentaire en cybersécurité) garantissent le respect des prescriptions.

Risques techniques : en créant le poste de *chief technology officer*, dont le titulaire gère un radar technologique, l'OFIT a instauré les conditions permettant de réduire au minimum les risques techniques.

Risques de marché : ces risques sont réduits au minimum par l'exécution d'une évaluation approfondie des solutions possibles et la réalisation des acquisitions en fonction des résultats de celle-ci. Différents fournisseurs de nuages ont donc été interrogés au sujet de leur portefeuille de prestations actuel et futur. Depuis le début des travaux préparatoires correspondants, l'on s'attache à limiter autant que possible les risques liés à l'acquisition en entretenant un dialogue étroit avec les services d'achat de l'administration fédérale, qui se poursuivra dans le cadre du projet.

Risques d'acceptation : face aux risques d'acceptation, la gestion des parties prenantes constitue la principale mesure à appliquer. Le programme SGC met à disposition les ressources nécessaires au maintien d'un contact permanent avec les futurs utilisateurs, même après que les besoins ont été identifiés et analysés. Il est par ailleurs prévu de mettre en place un comité spécialisé au sein duquel les utilisateurs du SGC pourront évaluer les résultats du projet et faire en sorte que les retours correspondants soient directement pris en compte dans le programme (cf. ch. 2.6 « Structure du programme »).

2.5.4 Risque budgétaire

Il existe un risque budgétaire lorsque le programme dépasse le budget initialement fixé. Cela peut être dû à une budgétisation irréaliste ou insuffisamment détaillée durant la phase de planification du projet.

En dépit d'une planification minutieuse et détaillée du SGC, il est possible que le budget soit dépassé ou que les économies prennent trop de temps à être réalisées. Le premier cas de figure peut se produire par exemple lorsque les coûts de matériel informatique sont plus élevés que prévu en raison du renchérissement ou des progrès technologiques. Le risque de ne pas être en mesure d'effectuer les économies dans les délais peut par exemple se réaliser lorsque la plateforme en place est exploitée plus longtemps.

Puisque le processus d'acquisition n'a pas encore débuté, ni le portefeuille de services exact ni les modèles de prix correspondants ne sont connus. C'est pourquoi il existe actuellement un budget, mais pas encore d'analyse coûts-bénéfices.

2.5.5 Mesures de respect des coûts et du budget

Le programme SGC prend ces risques en compte d'une part en intégrant un supplément pour risque compris entre 15 % et 20 % permettant de couvrir les dépenses supplémentaires en cas d'évolution technologique ou de réalisation de risques liés à l'acquisition. L'estimation des coûts a été contrôlée par des tiers indépendants dans le cadre des travaux préparatoires relatifs au SGC (cf. ch. 3.1.4 « Deuxième avis ») et sera à nouveau contrôlée ainsi que mise à jour au plus tard pour la prochaine annonce des besoins en 2025, afin de s'assurer de la précision de la planification. D'autre part, les fournisseurs et les bénéficiaires de prestations informatiques doivent être impliqués suffisamment tôt pour réaliser les migrations sur la période prévue ainsi que les répartir le plus uniformément possible sur l'intervalle défini à cet effet.

Il convient en outre d'identifier des objectifs, des risques et des défis clairs par projet, de s'assurer de l'efficacité des manières de procéder, de réaliser des études de faisabilité et, si nécessaire, des démonstrations de faisabilité, qui testent la solution dans un cadre pratique et permettent de mieux prévoir les coûts du projet.

2.5.6 Risque de calendrier

Le risque de calendrier se réalise lorsque les tâches du programme durent plus longtemps que prévu initialement. Les retards par rapport au calendrier peuvent avoir des conséquences sur d'autres éléments tels que les coûts, le délai de réalisation ou la prestation dans son ensemble.

Concrètement : si les premières prestations n'étaient pas mises à disposition à compter de 2026 comme prévu, par exemple parce que le processus d'acquisition venait à prendre plus de temps qu'estimé, la migration prendrait du retard. Outre des risques relatifs à la sécurité, cela engendrerait des coûts supplémentaires, puisque l'environnement système Atlantica devrait être exploité plus longtemps.

Le respect du calendrier prévu pour les migrations des applications spécialisées vers le SGC sera déterminant. La sous-estimation de la charge de travail, le manque de ressources ou d'expertise, les décisions en suspens ou encore le départ de personnes clés, notamment, pourraient entraîner des retards. Les coûts augmenteraient en conséquence considérablement, car il faudrait alors exploiter plus longtemps que prévu l'ancienne infrastructure en nuage et la nouvelle en parallèle l'une de l'autre.

2.5.7 Mesures de respect des délais

Une mesure prioritaire consiste à surveiller avec une attention particulière les achats et les migrations des applications pour bien anticiper les écarts par rapport au calendrier. Une planification détaillée et régulièrement mise à jour permet de réduire au minimum le risque que de tels écarts se produisent. La planification des migrations débute à un stade précoce et s'effectue au moyen de ressources dédiées. L'objectif est de fournir en temps voulu aux bénéficiaires de prestations l'ensemble des informations pertinentes pour leur planification.

Par ailleurs, les différents projets sont réalisés de manière à respecter les délais de la façon la plus cohérente possible, en établissant des objectifs clairs, en adaptant régulièrement la planification des projets et des ressources, en surveillant de manière stricte si les jalons ont été atteints et en pilotant avec minutie les rapports de dépendance.

En outre, il est important de définir des processus décisionnels clairs et brefs ainsi que d'assurer une gestion des parties prenantes minutieuse et une communication adéquate. Aussi bien la communication que la gestion des parties prenantes seront donc confiées directement à la direction du programme, qui disposera des ressources voulues à cet effet.

Il existe enfin un risque que le degré d'acceptation du projet ne soit pas suffisant chez les futurs utilisateurs. Face à ce risque aussi, la gestion des parties prenantes constitue la principale mesure à appliquer. Le programme SGC met à disposition les ressources nécessaires au maintien d'un contact permanent avec les futurs utilisateurs, même après que les besoins ont été identifiés et analysés. Il est par ailleurs prévu de mettre en place un comité spécialisé au sein duquel les utilisateurs du SGC pourront évaluer les résultats du projet et faire en sorte que les retours correspondants soient directement pris en compte dans le programme (cf. ch. 2.6 « Structure du programme »).

2.6 Structure du programme

L'organisation du programme SGC respecte les prescriptions du Conseil fédéral sur la mise en œuvre des projets clés.

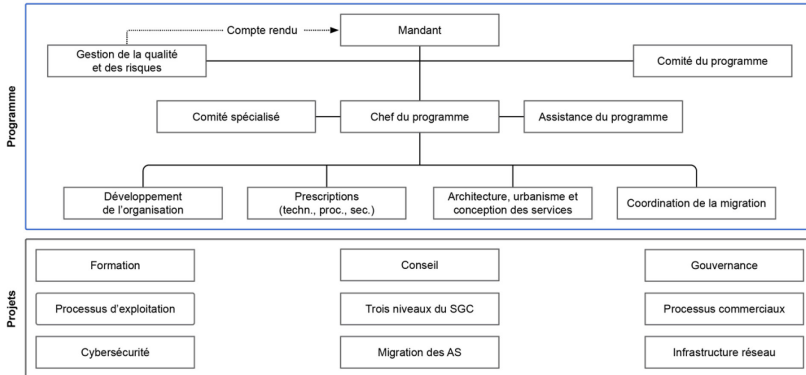


Illustration 5 : Représentation de la structure du programme SGC

Mandant

Le secrétaire général du DFF est le mandant du programme SGC.

Comité du programme

Afin de garantir la bonne participation des bénéficiaires de prestations et du secteur TNI de la ChF ainsi que la bonne prise en compte de leurs besoins, un comité du programme sera mis en place.

Gestion de la qualité et des risques

Du fait de l'ampleur et de la complexité technique du projet, le Conseil fédéral exige la mise en place d'une gestion de la qualité et des risques solide et indépendante, chargée de contrôler la qualité des travaux ainsi que de gérer les risques à tous les niveaux de responsabilité. La gestion de la qualité et des risques devra adresser ses recommandations directement au mandant.

Chef du programme

Le chef du programme aidera le mandant à mettre en œuvre le SGC ; il dirige et contrôle les travaux au niveau du programme, coordonne les relations de dépendance, consolide les rapports et la communication. Le chef du programme doit déjà avoir mis en œuvre avec succès des programmes de même ampleur et d'un niveau de complexité similaire dans l'environnement de l'administration fédérale.

Assistance du programme

L'assistance du programme aidera la direction du programme sur les questions relatives à l'organisation, à l'administration et aux autres éléments de la gestion du programme. Cela comprend :

- la communication ;
- le contrôle de gestion ;
- les questions financières ;
- les questions juridiques ;
- les achats ;
- le *project management office* ;
- la gestion du personnel.

L'assistance du programme apportera aussi son aide aux directions de projets en fonction de la situation.

Comité spécialisé

Afin de garantir la bonne participation des fournisseurs de prestations et du secteur TNI de la ChF ainsi que la bonne prise en compte de leurs besoins, un comité spécialisé sera mis en place. Les membres de ce comité spécialisé devront aider la direction du programme à évaluer les résultats.

Pilotage du programme

Le pilotage du programme comprend des tâches de direction spécialisée et de coordination spécifiques au programme, afin de garantir une gouvernance et un pilotage englobant l'ensemble des projets :

- développement de l'organisation : gestion du changement de l'organisation, c'est-à-dire transformation au sein de l'OFIT ;
- prescriptions : prescriptions applicables à l'ensemble des projets en matière de technologies, de processus, de sécurité, etc. ;
- urbanisme, architecture et conception des services : responsabilité spécialisée du produit d'ensemble SGC avec ses prestations de marché ;
- coordination de la migration : coordination des tâches de migration avec les clients concernés et au sein de l'OFIT.

Projets

Plusieurs projets seront élaborés sur la base des cinq champs d'action du SGC

2.7 Audit systématique

Le programme SGC a été qualifié de projet clé de l'administration fédérale en raison des ressources qu'il requiert, de son importance stratégique, de sa complexité et des risques qu'il représente (selon l'art. 20 de l'ordonnance du 25 novembre 2020 sur la

transformation numérique et l'informatique¹⁹). Il convient donc d'appliquer un processus d'audit étoffé. En vertu du mandat qui lui est attribué par la loi du 28 juin 1967 sur le Contrôle des finances²⁰, le CDF effectue des audits périodiques de tous les projets clés.

¹⁹ RS 172.010.58
²⁰ RS 614.0

3 Conséquences

3.1 Conséquences pour la Confédération

La mise en œuvre du SGC aura des effets aussi bien sur le plan financier qu'en matière de ressources humaines pour la Confédération. Le chapitre suivant les détaille.

3.1.1 Conséquences financières

3.1.1.1 Hypothèses retenues pour estimer les dépenses

Les dépenses ont été estimées selon les hypothèses suivantes :

- la plupart des prestations concernent uniquement la Confédération et l'estimation des coûts ne contient pas d'extension aux cantons ;
- la durée du programme SGC sera de 9 ans ;
- les travaux de mise en place seront suffisamment avancés d'ici à 2027 pour que le SGC puisse remplacer l'environnement système Atlantica ;
- les niveaux d'informatique en nuage II b et III reposent sur un modèle de facturation selon l'utilisation effective du matériel (*Pay as You Use*) ;
- la durée de la migration des systèmes en place vers le SGC sera de maximum 4 ans ;
- il n'est pas prévu d'édicter de nouvelles directives ou réglementations clés ;
- les ressources financières et humaines nécessaires pour réaliser le projet sont disponibles ;
- le marché ne connaîtra aucune évolution fondamentale ;
- la mise en place du niveau II b est prévue à partir de 2029, mais ne sera effectuée que si un client en a concrètement besoin.

L'estimation du renchérissement repose ainsi sur les prévisions relatives à l'indice suisse des prix à la consommation (IPC) selon les valeurs économiques de référence pour la planification financière et selon les perspectives à moyen terme de décembre 2023 :

En %	2024	2025	2026	2027	2028	2029	2030	2031	2032	ØΔ	ØΔ
										2024-2028	2029-2032
Augmentation selon l'IPC	1,9	1,1	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,2	1,0

Tableau 2 : Prévisions concernant l'IPC

3.1.1.2 Dépenses liées au programme

En 2022 et 2023, les travaux préparatoires ont représenté en tout environ 2,3 millions de francs, dont 2,2 millions de francs de prestations propres sous forme de ressources en personnel. Les travaux préparatoires comprennent la garantie du financement, la préparation des appels d'offres OMC, la mise en place de l'organisation spécialisée ainsi que des tâches de conception. Ces dépenses ne sont pas prises en compte dans les dépenses liées au programme.

Le remplacement nécessaire de l'environnement système Atlantica impose de migrer les applications spécialisées concernées des clients dans le cadre de projets propres, indépendamment de la création ou pas du SGC. Les dépenses relatives à cette migration seront supportées par les clients et ne sont donc pas non plus intégrées dans les dépenses liées au programme.

Des dépenses sont prévues en 2024 pour la phase de lancement. Entre 2025 et 2032, les dépenses liées au programme sont celles provenant de la gestion du programme, des travaux de mise en place et de l'exploitation parallèle. Les dépenses totales prévues pour la période de 2024 à 2032 s'élèveront à 319,4 millions de francs. Les détails sur les hypothèses retenues pour établir les estimations des dépenses se trouvent au ch. 3.1.1.1 « Hypothèses retenues pour estimer les dépenses ».

Parmi les dépenses uniques liées au programme, l'OFIT fournit pour 70,9 millions de francs de prestations propres sous forme de ressources en personnel, à quoi viennent s'ajouter 20,6 millions de francs de fonds propres.

Le tableau 3 indique la répartition des dépenses entre les champs d'action décrits précédemment (avec $\pm 20\%$ de marge d'erreur) :

En millions de francs	2024	2025	2026	2027	2028	2029	2030	2031	2032	Total
Mise en place de l'infrastructure hybride multi-cloud	0,5	2,3	15,4	27,1	24,0	20,9	15,1	9,7	5,1	120,1
↳ Nuage public	0,1	0,2	1,1	2,0	1,7	1,0	0,6	0,3	0,1	7,1
↳ Nuage public sur site	0,0	0,0	0,0	0,0	0,0	2,4	0,9	0,7	0,5	4,5
↳ Nuage privé sur site	0,4	2,1	14,3	25,1	22,3	17,5	13,6	8,7	4,5	108,5
Infrastructure réseau	0,0	4,2	2,9	4,3	3,2	2,7	2,1	1,3	1,5	22,2
↳ Augmentation de la bande passante	0,0	0,0	0,0	2,0	2,2	1,9	1,5	0,9	0,4	8,9
↳ Développement et renouvellement	0,0	4,2	2,9	2,3	1,0	0,8	0,6	0,4	1,1	13,3
Cybersécurité	0,8	3,5	6,4	10,2	9,4	6,9	3,8	1,5	0,0	42,5
↳ Identifier	0,0	0,5	0,4	0,7	0,5	0,4	0,2	0,1	0,0	2,8
↳ Protéger	0,5	0,4	2,7	5,6	5,9	4,4	2,6	1,4	0,0	23,5
↳ Détecter	0,3	2,0	2,4	3,6	2,8	2,0	1,0	0,0	0,0	14,1
↳ Réagir	0,0	0,6	0,8	0,2	0,1	0,1	0,0	0,0	0,0	1,8
↳ Restaurer	0,0	0,0	0,1	0,1	0,1	0,0	0,0	0,0	0,0	0,3
Processus commerciaux et d'exploitation	0,2	1,3	3,0	6,6	4,8	2,9	1,4	0,9	0,5	21,6
Formation, conseil et gouvernance	0,9	2,8	5,5	4,8	4,0	2,5	1,2	0,4	0,1	22,2
Gestion du programme	2,9	3,7	7,3	7,6	8,1	6,9	4,0	2,7	2,3	45,5

Dépenses liées au programme (réserves non comprises)	5,3	17,8	40,5	60,6	53,5	42,8	27,6	16,5	9,5	274,1
Réserves	0,0	0,0	6,1	9,1	10,7	8,6	5,6	3,3	1,9	45,3
Dépenses liées au programme (y c. réserves)	5,3	17,8	46,6	69,7	64,2	51,4	33,2	19,8	11,4	319,4
Dont prestations propres sous forme de ressources en personnel	3,7	7,4	12,0	11,5	10,4	8,3	8,6	5,9	3,1	70,9
Dont dépenses en 2024	1,6	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	1,6
Crédit d'engagement	0,0	10,4	34,6	58,2	53,8	43,1	24,6	13,9	8,3	246,9

Tableau 3 : Dépenses liées au programme par champ d'action

Les ressources nécessaires durant la mise en place du SGC jusqu'en 2027 ne font qu'augmenter avant de se stabiliser au cours des trois premières années de la phase de migration puis de fortement diminuer vers la fin du programme. La raison en est qu'au fur et à mesure de l'avancement du projet, les dépenses liées au programme diminuent tandis que les dépenses d'exploitation augmentent. Ces dernières ne nécessitent pas de financement supplémentaire et ne sont pas couvertes par le crédit d'engagement. Même après l'achèvement du projet, des investissements seront réalisés dans le développement du SGC. Les moyens nécessaires à cet effet seront financés par le biais de l'exploitation.

Les dépenses liées au programme par champ d'action sont expliquées plus en détail ci-après.

- Mise en place de l'infrastructure hybride multi-cloud : ce poste contient les dépenses pour la mise en place du nuage public (7,1 millions de francs), du nuage public sur site (4,5 millions de francs) et du nuage privé sur site (108,5 millions de francs). Pour ce dernier, l'acquisition, l'installation et l'exploitation constituent le plus gros bloc de dépenses, avec environ 50 millions de francs. Les charges d'élaboration d'un portefeuille de services (19,5 millions de francs), d'essai des différents composants et processus (11 millions de francs) ainsi que d'aide à la migration (12,9 millions de francs) sont d'autres blocs de dépenses majeurs.
- Infrastructure réseau : ce poste contient l'extension des bandes passantes de l'accès à Internet et aux fournisseurs de prestations d'informatique en nuage (8,9 millions de francs) ainsi que l'extension et la modernisation des réseaux (13,3 millions de francs). Ce dernier point comprend notamment l'amélioration de la sécurité du réseau et de la fiabilité.
- Cybersécurité : les dépenses sont réparties entre les domaines identifier, protéger, détecter, réagir et restaurer décrits au ch. 2.2.3.3 Objectif de la cybersécurité. La mise en œuvre du concept « Zero Trust » (18,4 millions de francs), la garantie de la capacité de détection (10,4 millions de francs) et la gestion des vulnérabilités (2,4 millions de francs) constituent les principaux blocs de dépenses.

- Formation, conseil et gouvernance : ce poste de dépenses contient la conception et la réalisation des formations, la mise en place du centre d'innovation, la création du centre de compétence SGC ainsi que l'établissement de la gouvernance de l'informatique en nuage à l'échelle du SGC.
- Processus commerciaux et d'exploitation : ce poste contient les dépenses pour la numérisation des chaînes de processus, pour l'installation d'une plateforme clients centrale ainsi que pour la mise en œuvre d'un cockpit et d'interfaces.
- Gestion du programme : ce poste comprend les dépenses de personnel pour la planification et la coordination spécialisées et techniques globales, les assistances du programme, la mise en œuvre des mesures relatives au changement, la direction du personnel et la gestion des parties prenantes.

Conséquences sur l'état du personnel entre 2024 et 2032

Le projet peut être mis en œuvre avec les ressources humaines dont dispose actuellement l'OFIT.

L'objectif est de pouvoir réaliser le plus rapidement possible de nombreuses tâches liées au SGC avec le personnel interne à l'OFIT. C'est pourquoi, dès la période 2024-2029, jusqu'à 50 équivalents plein temps (EPT) doivent être transférés progressivement vers l'organisation du SGC. Parallèlement à la mise en place du SGC, les systèmes de l'environnement Atlantica devront toujours être exploités (cf. tableau 4 dans « Assistance pour l'exploitation »). Afin de pouvoir supporter cette charge multiple et combler le vide laissé par le déplacement de personnel interne, il faudra faire appel à du personnel externe supplémentaire au cours de ces années.

Selon la planification, de plus en plus de systèmes de l'environnement Atlantica pourront être désactivés après la migration des applications spécialisées et des prestations vers le SGC. Les ressources en personnel alors libérées seront progressivement transférées dans l'organisation du SGC et les EPT externes libérés seront supprimés.

En équivalents plein temps (EPT)	2024	2025	2026	2027	2028	2029	2030	2031	2032
Besoin interne	17,8	35,0	50,0	50,0	50,0	50,0	70,0	75,0	80,0
Besoin externe	2,1	10,2	42,6	77,7	77,6	67,4	33,9	23,0	15,2
Assistance pour le programme	1,3	9,4	23,9	45,6	45,9	36,9	27,7	23,0	15,2
Assistance pour l'exploitation	0,8	0,8	18,7	32,1	31,7	30,5	6,2	0,0	0,0
Besoin total (réserves non incluses)	19,9	45,2	92,6	127,7	127,6	117,4	103,9	98,0	95,2
Réserves	0,0	0,0	13,9	19,2	25,5	23,5	20,8	19,6	19,0
Besoin total (y c. réserves)	19,9	45,2	106,5	146,9	153,2	140,9	124,7	117,6	

Tableau 4 : Besoin en personnel

Le SGC doit permettre d'établir un nouveau modèle d'exploitation offrant à l'OFIT la possibilité de réduire ses ressources en personnel dans le domaine de l'exploitation de l'infrastructure et des plateformes. Le personnel interne ainsi libéré (l'OFIT table

actuellement sur 100 EPT) pourra alors, par exemple, être redéployé pour renforcer des domaines offrant des prestations de proximité ou remplacer du personnel externe. Cela permettra de réaliser des économies et de réduire la dépendance vis-à-vis des fournisseurs externes.

Réserves

Les réserves indiquées s’expliquent par les éventuelles dépenses supplémentaires qui pourraient être occasionnées par l’adaptation au progrès technologique, les risques liés aux achats et les retards sur le calendrier.

Les réserves ont été fixées à 15 % sur la période 2026-2027 et à 20 % sur la période 2028-2032, du fait de la mise en œuvre plus éloignée dans le temps et du niveau d’incertitude alors nécessairement plus élevé.

Les réserves ne doivent pas être entièrement financées à l’avance. Si certains risques viennent à apparaître, les ressources supplémentaires éventuellement nécessaires seront demandées au Parlement par l’intermédiaire du budget annuel ou de ses suppléments.

En millions de francs	2024	2025	2026	2027	2028	2029	2030	2031	2032	Total
Réserves du programme	0,0	0,0	6,1	9,1	10,7	8,6	5,6	3,3	1,9	45,3

Tableau 5 : Réserves

3.1.1.3 Crédit d’engagement

Le crédit d’engagement pour les engagements financiers envers des tiers s’élève à 246,9 millions de francs. Il sera octroyé en deux tranches : la première tranche de 103,2 millions de francs sera octroyée par l’Assemblée fédérale avec l’arrêté fédéral. La seconde tranche de 143,7 millions de francs sera octroyée par le Conseil fédéral dès que les conditions suivantes seront remplies :

- le SGC est prêt à remplacer l’environnement système Atlantica en 2027 ;
- l’équipe indépendante chargée de la gestion de la qualité et des risques a confirmé le respect des exigences en matière de sécurité ainsi que de conformité, et le mandant du programme a validé la mise en production.

Le Conseil fédéral peut opérer des transferts entre les tranches du crédit d’engagement octroyées de sorte que, le cas échéant, des engagements pour des dépenses supplémentaires attendues dans une tranche puissent être compensés par l’autre.

Les ressources sont affectées sous réserve des demandes et décisions annuelles relatives aux crédits des organes compétents de la Confédération en matière de budget et de plan financier.

En millions de francs	2025	2026	2027	2028	2029	2030	2031	2032	Total
-----------------------	------	------	------	------	------	------	------	------	-------

Crédit d'engagement 1 ^{re} tranche	10,4	34,6	58,2	0,0	0,0	0,0	0,0	0,0	103,2
Crédit d'engagement 2 ^e tranche	0,0	0,0	0,0	53,8	43,1	24,6	13,9	8,3	143,7
Total du crédit d'engagement	10,4	34,6	58,2	53,8	43,1	24,6	13,9	8,3	246,9

Tableau 6 : Crédit d'engagement

3.1.1.4 Dépenses d'exploitation après la conclusion du programme

Les dépenses d'exploitation annuelles de l'OFIT après la conclusion du programme (à partir de 2033) s'élèveront à 64,1 millions de francs selon l'estimation actuelle. Les économies réalisées doivent permettre de réduire les dépenses d'exploitation de l'OFIT (voir à ce sujet le ch. 3.1.1.5 « Économies pendant le programme et après sa conclusion »).

3.1.1.5 Économies pendant le programme et après sa conclusion

Dans l'ensemble, environ 241,2 millions de francs d'économies peuvent être réalisés sur les coûts internes pendant la durée du programme et en partie redéployés sur le SGC. Après déduction des dépenses d'exploitation de 179,5 millions de francs, il en résulte donc une économie attendue de 61,7 millions de francs sur la durée du programme.

Les dépenses d'exploitation annuelles de l'OFIT après la conclusion du programme (à partir de 2033) s'élèveront à 64,1 millions de francs selon l'estimation actuelle. Puisque la réduction interne des coûts sera à ce moment-là de 88 millions de francs par an, il est prévu de pouvoir économiser 23,9 millions de francs par an au niveau de l'exploitation au sein de l'OFIT.

Les extensions dans les domaines de la cybersécurité, de l'infrastructure réseau ainsi que des processus commerciaux et d'exploitation génèrent d'autres coûts d'exploitation récurrents. Puisque ces travaux doivent aussi être réalisés sans le SGC, les coûts d'exploitation augmenteraient de toute façon. Le SGC permet cependant de réaliser des économies au niveau de l'exploitation grâce au remplacement de l'environnement système Atlantica et à l'internalisation des ressources. Il est ainsi possible d'éviter de générer des coûts d'exploitation supplémentaires ou de réduire les coûts d'exploitation futurs.

Les économies suivantes devraient donc pouvoir être réalisées pendant le programme et après sa conclusion :

En millions de francs	Total sur l'ensemble du programme 2024-2032	Par an après la conclu- sion du programme (à partir de 2033)
Estimation des dépenses d'exploitation	179,5	64,1
Réduction interne des coûts OFIT	-241,2	-88,0
Économies attendues	-61,7	-23,9

Tableau 7 : Économies

La mise en œuvre du programme entraîne au sein de l'OFIT la réduction suivante des coûts :

- Remplacement de l'environnement système Atlantica : le SGC doit être en mesure de remplacer l'environnement système Atlantica fin 2027. La migration vers le SGC supprimera les coûts liés à l'environnement système Atlantica. On suppose qu'il est possible de migrer un quart des applications spécialisées vers le SGC par an sur la période 2028-2030. Le dernier quart sera migré en 2031. L'environnement système Atlantica pourra ensuite être abandonné.
- Ressources en personnel internes : le personnel interne pour le SGC sera transféré depuis d'autres domaines de l'OFIT sans être remplacé, ce qui signifie que le SGC ne requerra pas de personnel interne supplémentaire (cf. ch. 3.1.1.2 « Dépenses liées au programme entre 2024 et 2032 »).
- Internalisation des ressources : l'automatisation des processus et la standardisation du catalogue des prestations dans le secteur consacré aux plateformes et aux infrastructures permettent ici de supprimer jusqu'à 100 postes en interne, pour les redéployer dans le développement interne. Avec ce transfert, 100 postes externes pourront être supprimés dans le domaine du développement une fois le programme terminé.

Les réductions de coûts de 241,2 ou 88 millions de francs sont réparties comme suit :

En %	Total sur l'ensemble du programme 2024-2032	Par an après la conclu- sion du programme (à partir de 2033)
Remplacement de l'environnement système Atlantica	55	46
Ressources humaines internes	16	16
Internalisation des ressources	29	38

Tableau 8 : Réduction interne des coûts OFIT

3.1.1.6 Rentabilité

La rentabilité du SGC est garantie au travers des aspects suivants :

- *Prise en compte des exigences commerciales de la Confédération* : dans le cadre des travaux préparatoires, l'identification des besoins auprès des fournisseurs de prestations informatiques de la Confédération et auprès des Services du Parlement ainsi que l'analyse des besoins auprès des bénéficiaires de prestations ont posé les fondements permettant d'adapter le SGC de manière cohérente aux exigences commerciales et de fournir les prestations nécessaires pour relever les prochains défis liés au numérique.

- *Prudence dans la conception et l'estimation des coûts* : afin de permettre une estimation sérieuse de la rentabilité, d'une part, une analyse complète de la structure des coûts de l'environnement système Atlantica a été réalisée, d'autre part, l'OFIT a évalué sa stratégie dans le cadre d'échanges d'expérience réalisés avec des gouvernements d'autres pays. Par ailleurs, des entretiens avec des fournisseurs de nuages publics ont permis de s'assurer que le SGC était un projet porteur d'avenir. La cohérence de l'estimation des coûts a été contrôlée par un expert indépendant.
- *Avantages en termes de coûts par rapport à la situation actuelle* : les calculs montrent que les coûts en cas de maintien de la situation actuelle seraient supérieurs de plus de 150 millions de francs aux dépenses totales induites par le SGC (voir ch. 3.1.2 « Conséquences en cas de non-réalisation »).
- *Gouvernance transversale* : une gouvernance transversale de l'informatique en nuage permettra de pouvoir passer le plus simplement possible d'un prestataire d'informatique en nuage à l'autre et d'un niveau d'informatique en nuage à l'autre.
- *Coordination de l'achat de prestations d'informatique en nuage* : le centre de compétence conseillera les unités administratives intéressées lors du choix du bon niveau d'informatique en nuage ou aidera à coordonner leur achat et contribuera ainsi de manière importante à ce que les trois niveaux du SGC soient utilisés de manière rentable.
- *Création de synergies grâce au modèle « Fournisseur de prestations informatiques pour un fournisseur de prestations informatiques »* : le SGC sera conçu de sorte à pouvoir être utilisé par tous les fournisseurs de prestations informatiques de la Confédération et de produire des synergies pour l'activité de masse de l'administration fédérale dans le domaine de l'informatique en nuage.
- *Fourniture de prestations prêtes à l'emploi* : dans le cadre du SGC, les bénéficiaires de prestations profiteront de prestations prêtes à l'emploi et déjà compatibles avec les services standard de la Confédération, auxquelles ils pourront recourir lors de la conception et de la mise en œuvre de leurs solutions.
- *Fort degré d'évolutivité* : le SGC à proprement parler ainsi que les prestations mises à disposition posséderont un fort degré d'évolutivité. Il sera ainsi possible de réagir rapidement et avec flexibilité (en grande partie de manière automatisée) aux évolutions des exigences en matière de capacités. Grâce au modèle de facturation selon l'utilisation effective (*Pay as You Use*) prévu, les coûts ne concerneront que les prestations effectivement perçues. Les fluctuations de recettes dues à la variation des volumes d'achat pourront ainsi être compensées en grande partie.
- *Modèle d'exploitation industrialisé* : le SGC introduira un nouveau modèle d'exploitation industrialisé. L'automatisation cohérente des processus et la standardisation du catalogue des prestations permettront de réduire à long terme les coûts d'exploitation.

- *Contrôle et transparence des coûts* : un suivi efficace des coûts liés à l'informatique en nuage pourra être effectué en recourant à des outils et à des tableaux de bord, par exemple sous forme de cockpit à 360°. Les coûts inutiles pourront par ailleurs être ainsi facilement identifiés et supprimés.
- *Conseil et formation* : le conseil et la formation donneront la capacité aux bénéficiaires de prestations et aux fournisseurs de prestations informatiques de la Confédération d'utiliser de manière rentable les infrastructures d'informatique en nuage du SGC.
- *Création des conditions pour remplacer les applications héritées* : le SGC posera les bases de la modernisation ou du remplacement des anciennes applications, dont l'exploitation génère souvent des coûts considérables. Des projets correspondants doivent être lancés par les bénéficiaires de prestations.
- *Octroi annuel des ressources* : il est prévu que l'octroi des ressources au SGC soit approuvé annuellement par le mandat sur la base d'une planification de l'OFIT et d'une identification des besoins mise à jour chaque année. Les parties évolutives de l'infrastructure du SGC ne seront ainsi mises en place que si le besoin est avéré et cela garantit que les moyens soient alloués de manière optimale au vu des coûts, des bénéfices et des risques.

3.1.2 Conséquences en cas de non-réalisation

Pour bien mettre en évidence ce que cela coûterait de ne rien changer, les coûts de l'environnement système Atlantica actuellement en place et du CSB OFIT ont été estimés sur la période 2024-2032, afin de pouvoir les mettre en regard des coûts de la réalisation du SGC. L'estimation se base sur une prévision de croissance annuelle plutôt conservatrice de 5 %, ainsi que sur un niveau de renchérissement conforme à l'indice suisse des prix à la consommation (cf. ch. 3.1.1.1 « Hypothèses retenues pour estimer les dépenses »). Afin d'offrir un tableau complet des coûts, les investissements nécessaires liés aux autres champs d'action du SGC (tels que la cybersécurité ou l'extension de l'infrastructure réseau) qui seraient effectués même si le projet SGC n'était pas réalisé ont aussi été pris en compte. Comme pour l'estimation des coûts du SGC au ch. 3.1.1.2 « Dépenses liées au programme », un supplément pour risque de 15 % sur la période 2026-2027 et de 20 % sur la période 2028-2032 a été inclus. Le supplément pour risque lié à l'environnement système Atlantica et au CSB de l'OFIT sert avant tout à couvrir les coûts d'investissement supplémentaires qui pourraient être occasionnés en cas de maintien de cette solution. Concernant les autres postes, le supplément pour risque sert à compenser les éventuelles charges supplémentaires résultant du progrès technologique et des risques liés aux achats.

Les calculs montrent que les dépenses en cas de maintien de la situation actuelle, soit 688,1 millions de francs (dépenses de programme et d'exploitation), seraient supérieures de plus de 150 millions de francs aux dépenses totales cumulées du SGC jusqu'à la fin de 2032. Les économies potentielles décrites au ch. 3.1.1.5 « Économies pendant le programme et après sa conclusion » ne seraient par ailleurs pas ou que partiellement réalisées si le SGC n'était pas mis en place.

3.1.3 Coûts de la migration

Dans le cadre du projet, toutes les applications spécialisées fonctionnant jusqu'à présent dans l'environnement système Atlantica doivent être migrées vers le niveau correspondant du SGC. Dans la plupart des cas, il sera possible de transférer les applications spécialisées existantes de l'infrastructure d'informatique en nuage actuelle vers la nouvelle sans qu'aucune modification architecturale ne doive être effectuée sur les applications, ce qui signifie que tous les services nécessaires seront à disposition au terme de la migration, sans changements. La présente estimation des coûts de la migration a été réalisée en se fondant sur ce scénario. Les bénéficiaires de prestations sont cependant invités à intégrer les modifications liées au cycle de vie de leurs applications spécialisées durant la migration pour que celles-ci soient techniquement à jour lorsqu'elles auront été transférées. Les coûts liés à la migration technique s'en trouveront réduits.

Les coûts de la migration de chaque application spécialisée dépendent de sa complexité, du nombre d'environnements d'exploitation et d'autres facteurs qui se reflètent dans les coûts d'exploitation annuels que l'OFIT facture aux bénéficiaires de prestations correspondants.

Sur la base de la comptabilité de l'ensemble des coûts d'exploitation de l'OFIT de septembre 2023 et de l'expérience tirée des projets de cycle de vie déjà menés qui contiennent aussi une migration vers une nouvelle plateforme, l'OFIT a calculé un facteur des coûts de la migration qui s'élève à 35 % des coûts d'exploitation annuels. Les systèmes et les applications qui ne sont pas encore exploités sur une des plateformes d'informatique en nuage de l'OFIT (systèmes hérités) ne sont pas inclus dans l'estimation des coûts de la migration. Il revient aux bénéficiaires de prestations de planifier ou de demander la modernisation de ces solutions. Le remplacement des systèmes hérités comporte un potentiel d'économie supplémentaire et sera examiné en priorité par le Conseil de la transformation numérique et de la gouvernance informatique de la Confédération en même temps que le SGC.

Il en résulte dans l'ensemble des coûts de la migration d'un montant de 74 millions de francs, avec une marge d'erreur de +/- 20 %. Cette marge est liée à la durée de la planification : entre le moment de l'estimation (fin 2023) et le moment de la migration (à partir de 2027), aussi bien le paysage technologique sur le marché que la gamme d'applications des bénéficiaires de prestations sont destinés à évoluer. Étant donné que l'acquisition n'a pas encore eu lieu, la plateforme cible de la migration n'est toujours pas connue et il n'est donc pas possible pour le moment d'estimer les coûts de la migration avec précision. Les coûts effectifs de la migration pourraient donc être supérieurs aux estimations.

C'est pourquoi il est prévu, dans le cadre de la mise en œuvre du projet, d'analyser en détail les coûts de la migration par application spécialisée et d'en informer les bénéficiaires de prestations concernés en temps utile.

3.1.4 Deuxième avis

La conception du SGC repose sur une vaste enquête : outre des entretiens approfondis avec les fournisseurs d'informatique en nuage nationaux et internationaux pour sonder leurs offres, des échanges d'expérience ont été organisés avec d'autres pays (Allemagne, Italie, Singapour, Autriche, Croatie, Danemark, Pays-Bas, Grande-Bretagne), afin de pouvoir profiter des enseignements qu'ils ont pu tirer quant aux opportunités, problèmes et risques potentiels.

L'OFIT a aussi recueilli plusieurs autres avis :

- Concernant les objectifs stratégiques et le plan de mise en œuvre du SGC, ils ont confirmé que la stratégie suit les ambitions de nombreux autres organismes gouvernementaux et qu'un bon équilibre entre investissement et résultat a été trouvé, et aussi que la solution a été conçue de manière évolutive et pertinente sur le plan économique.
- Concernant l'estimation des dépenses liées au programme et des coûts de la migration, ils ont confirmé que l'estimation des dépenses liées au programme est probante et cohérente, et aussi que l'estimation des dépenses liées à la migration est fondée et adéquate compte tenu des données disponibles.

3.2 Conséquences pour les cantons et les communes

Des cantons, des villes et des communes souhaiteraient aussi pouvoir compter davantage sur les prestations d'informatique en nuage pour mettre en œuvre leurs projets de numérisation. Un certain nombre ne dispose cependant pas des ressources suffisantes pour mettre en place et exploiter de manière rentable leurs propres infrastructures d'informatique en nuage. C'est pourquoi les sept cantons membres de la Conférence latine des directrices et directeurs du numérique ont fait part à l'OFIT et dans une lettre datée du 2 mai 2023 adressée à la cheffe du DFF de leur grand intérêt pour une utilisation partagée du SGC.

Pour que la numérisation de l'administration publique réussisse, il est nécessaire que les unités administratives, de l'ensemble des niveaux fédéraux, soient davantage interconnectées. Le Conseil fédéral salue donc l'intérêt des cantons et souhaiterait par conséquent leur donner aussi la possibilité d'utiliser le SGC : bien que le SGC soit avant tout conçu pour les besoins de la Confédération, sa structure technique permettra également aux cantons, aux villes et aux communes de l'utiliser à l'avenir le cas échéant.

Concernant l'évolutivité du SGC, des études sont en cours pour définir les conditions juridiques dans lesquelles le SGC pourrait aussi fournir des prestations aux cantons, aux villes et aux communes et s'il est nécessaire de légiférer à cet effet. Ces études n'ont toujours pas livré de résultats.

Les cantons, les villes et les communes devront payer pour une éventuelle utilisation partagée du SGC. Le SGC sera toutefois mis en place au sein de l'administration fédérale et en premier lieu à l'intention de la Confédération. Il n'est donc pas prévu que les cantons, les villes et les communes participent aux coûts de mise en place. C'est

pourquoi ils n'ont pas pris part à l'identification et à l'analyse des besoins mentionnées dans le document. Il est toutefois prévu de continuer à communiquer ouvertement avec les cantons. Aujourd'hui déjà, une collaboration étroite avec l'ANS est mise en place dans le cadre de la priorité « Favoriser la mise en place de services publics capables de fonctionner dans le nuage informatique » de la stratégie « Administration numérique suisse 2024–2027 ».

4 Aspects juridiques

4.1 Constitutionnalité et légalité

Le présent projet repose sur la compétence générale de la Confédération de prendre les mesures nécessaires à l'accomplissement de ses tâches. La compétence de l'Assemblée fédérale pour le présent arrêté de crédit découle de l'art. 167 de la Constitution (Cst.)²¹.

4.2 Forme de l'acte à adopter

Conformément à l'art. 163, al. 2, Cst. et 25, al. 2, de la loi sur le Parlement²², l'acte à adopter revêt la forme de l'arrêté fédéral simple (qui n'est pas sujet au référendum).

4.3 Assujettissement au frein aux dépenses

L'art. 1 du présent arrêté fédéral est soumis au frein aux dépenses selon l'art. 159, al. 3, let. b, Cst., puisqu'il prévoit une dépense unique de plus de 20 millions de francs. Par conséquent, le crédit d'engagement de 246,9 millions de francs doit être adopté par les Chambres fédérales à la majorité des membres de chaque chambre.

²¹ RS 101

²² RS 172.10

5 Liste des abréviations utilisées

Abréviation	Signification
BP	Bénéficiaire de prestations
CC SGC	Centre de compétence SGC
CDF	Contrôle fédéral des finances
ChF	Chancellerie fédérale
CoP	Communauté de pratique (<i>community of practice</i>)
CSB	<i>Cloud service broker</i>
Cst.	Constitution fédérale
DFF	Département fédéral des finances
DFJP	Département fédéral de justice et police
FP	Fournisseur de prestations
IaaS	Infrastructure en tant que service (<i>Infrastructure as a Service</i>)
ISAE	<i>International Standard on Assurance Engagements</i>
ISMS	Système de gestion de la sécurité de l'information
LParl	Loi sur le Parlement
LPD	Loi fédérale sur la protection des données
LSI	Loi sur la sécurité de l'information
NIST	<i>National Institute of Standards and Technology</i>
OFCS	Office fédéral de la cybersécurité
OFIT	Office fédéral de l'informatique et de la télécommunication
PaaS	Plateforme en tant que service (<i>Platform as a Service</i>)
PFPDT	Préposé fédéral à la protection des données et à la transparence
RS	Recueil systématique du droit fédéral
SaaS	Logiciel en tant que service (<i>Software as a Service</i>)
SAP	<i>Systemanalyse Programmentwicklung</i> (entreprise de logiciels)

SGC	Swiss Government Cloud
TI	Technologies de l'information
TIC	Technologies de l'information et de la communication
TNI	Transformation numérique et gouvernance de l'informatique

6 Glossaire

Terme	Signification
Approche hybride multi-cloud	Une approche hybride multi-cloud implique l'utilisation de services en nuage public et de services en nuage privé et permet de les combiner. Le préfixe « multi » signifie que les services en nuage de plusieurs fournisseurs de nuages publics sont à disposition.
<i>Cloud service broker</i>	Un <i>cloud service broker</i> (CSB) crée les conditions nécessaires pour que les services en nuage public puissent être utilisés au sein de l'administration et pour qu'ils puissent être intégrés et exploités dans l'environnement informatique de l'administration fédérale conformément aux exigences définies. Pour ce faire, le CSB met à disposition des moyens auxiliaires (outils, prestations, expertise, mécanismes de contrôle) pour l'utilisation de services en nuage (public) selon les principes définis.
Environnement système Atlantica	Pour l'OFIT, l'environnement système Atlantica regroupe toutes les plateformes d'informatique en nuage sur site qu'il exploite dans le domaine IaaS et PaaS. En 2023, il s'agissait de la plateforme IaaS basée sur VM acquise par l'intermédiaire de l'appel d'offres OMC 1434 (Cumulus), de la plateforme IaaS Serverbazar basée sur VM développée par l'OFIT et de la plateforme PaaS Red Hat Openshift basée sur conteneurs mise en place par le programme AMBOSS. Le terme englobe par ailleurs l'ensemble des services et prestations (de marché) proposés par l'OFIT pour les plateformes indiquées.
Facturation selon l'utilisation effective	Ce modèle permet aux clients de payer seulement les prestations ou les ressources qu'ils ont effectivement utilisées. Contrairement à ce qu'il se passe lors d'un achat, les clients ne se voient pas facturer séparément les coûts liés au cycle de vie, car l'entretien et le renouvellement de l'offre incombent au fournisseur et sont inclus dans les prix.
Infrastructure en tant que service	L'infrastructure en tant que service (IaaS) est un modèle d'informatique en nuage qui permet aux entreprises de louer des infrastructures telles qu'une puissance de calcul, un espace de stockage ou des ressources réseau auprès d'un fournisseur de services en nuage plutôt que d'exploiter du matériel et une infrastructure physique sur site.

Logiciel en tant que service	Le logiciel en tant que service (SaaS) est un modèle de l'informatique en nuage qui permet aux fournisseurs de services en nuage de mettre à disposition des applications logicielles dans le nuage et de les exploiter. Plutôt que d'installer les logiciels et d'assurer leur maintenance sur les ordinateurs en local ou sur des serveurs, les utilisateurs peuvent accéder aux applications par Internet et les utiliser.
Nuage privé	Le nuage privé est un environnement en nuage déployé et exploité dans un réseau interne fermé, à savoir dans les centres de calcul de l'administration fédérale dans le cas du SGC. Les données seront ainsi stockées dans les centres de calcul.
Nuage public	Le nuage public est un environnement en nuage qui est mis à disposition par un fournisseur de nuage externe. Les données ne sont pas publiques, mais sont stockées sur la plateforme d'un fournisseur de nuage externe.
Plateforme en tant que service	La plateforme en tant que service (PaaS) est un modèle de l'informatique en nuage qui permet aux entreprises de louer une plateforme auprès d'un fournisseur de services en nuage afin de développer des applications, de les tester et de les mettre à disposition. À l'inverse du modèle d'IaaS, qui met uniquement à disposition l'infrastructure, le modèle PaaS fournit aussi les services nécessaires pour développer et exploiter les applications, par exemple des bases de données ou des plateformes de conteneurs.
Prestation entièrement gérée	Une prestation entièrement gérée comprend la mise à disposition, la mise à jour, la configuration initiale, l'assistance et la surveillance de la prestation concernée.
Souveraineté numérique	Par souveraineté numérique on entend notamment : <ul style="list-style-type: none"> • Souveraineté des informations et des données : le propriétaire contrôle ses données (personnelles ou non) ainsi que leur collecte, leur stockage, leur traitement et leur transmission. • Autonomie opérationnelle ou d'exploitation : il s'agit de la durée au cours de laquelle l'OFIT peut assurer l'exploitation de systèmes et applications existants avec son propre personnel, soit sans avoir recours aux services de partenaires externes à l'administration fédérale.
Sur site	Sur site signifie que la solution est exploitée dans les centres de calcul de l'administration fédérale.

Swiss Government Cloud	Le SGC est une infrastructure en nuage adaptée aux exigences et aux besoins de la Confédération qui permettra d'accéder à des prestations tant en nuage public qu'en nuage privé.
---------------------------	---