Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF
Transformation numérique et gouvernance de l'informatique TNI

Initiative stratégique IS-4 « nuage hybride multi-cloud »

AR010 – Principes relatifs à l'informatique en nuage de l'administration fédérale

Directive concernant l'informatique de la Confédération avec renvois complémentaires et recommandations

Classification :	non classifié
Effet juridique:[1]	directive avec renvois complémentaires et recommandations
Type de directive:[2]	(AR) architecture
Domaine de planification:[3]	prestations numériques et informatiques de base pour l'ensemble de l'administration fédérale
Version:	1.0
Remplace:	pas de version antérieure
Statut:	final
Date de la décision / date de l'entrée en vigueur:	décision: date de la signature électronique entrée en vigueur: 1.10.2023
Autorité, base légale:	délégué à la transformation numérique et à la gouvernance de l'informatique (délégué TNI), conformément à l'art. 17, al. 1, de l'ordonnance du 25 novembre 2020 sur la transformation numérique et l'informatique (OTNI; RS *172.010.58*)
Langues:	document principal: allemand (original), français
Appendice:	aucun

[1] Concernant la forme de l'acte et le caractère contraignant, voir *Office fédéral de la justice, Guide de législation, 4ème édition entièrement révisée et complétée 2019*

[2] Selon *directives informatiques ChF*

[3] Domaines de planification selon *stratégie informatique de la Confédération 2020-2023 du 3 avril 2020 (SB000)*

Table des matières

1 Dispositions générales

La stratégie d'informatique en nuage de l'administration fédérale [1], adoptée par le Conseil fédéral le 11 décembre 2020, vise à faciliter l'utilisation des services en nuage. Conformément à sa stratégie, la Confédération utilise les services en nuage (privé et public) **de manière sûre, efficace et coordonnée**.

Conformément à sa stratégie, l'administration fédérale mise toujours sur ses propres centres de données et sur les nuages privés de la Confédération. Cette palette est complétée par les nuages publics de plusieurs fournisseurs. Cette **stratégie hybride**, qui combine nuages privés et nuages publics couvre particulièrement bien l'ensemble des exigences de l'administration, notamment pour ce qui est de la sécurité de l'information, de la protection des données, de la résilience, de l'innovation, de la fonctionnalité, de la criticité et du degré d'intégration optimal.

Le présent document comprend:

- trois nouvelles directives du secteur Transformation numérique et gouvernance de l'informatique (TNI) de la Chancellerie fédérale (ChF) pertinentes pour le nuage public (cf. ch. 4.1),
- des renvois à des documents pertinents dans ce domaine, élaborés par d'autres organes, et des recommandations du secteur TNI de la ChF (cf. ch. 4.2)

Il règle l'utilisation des services d'informatique en nuage public dans l'administration fédérale. Les présents principes visent à harmoniser les pratiques au sein de l'administration fédérale.

1.1 Objet

1. Les principes relatifs à l'informatique en nuage règlent l'utilisation des services en nuage public dans l'administration fédérale aux niveaux *Infrastructure as a Service* (IaaS) et *Platform as a Service* (PaaS).
2. Ils s'adressent aux fournisseurs de prestations, aux bénéficiaires de prestations et à leurs responsables d'applications, conformément au champ d'application.
3. Ils sont groupés par thème et décrits au ch. 4 (cf. Figure 1).

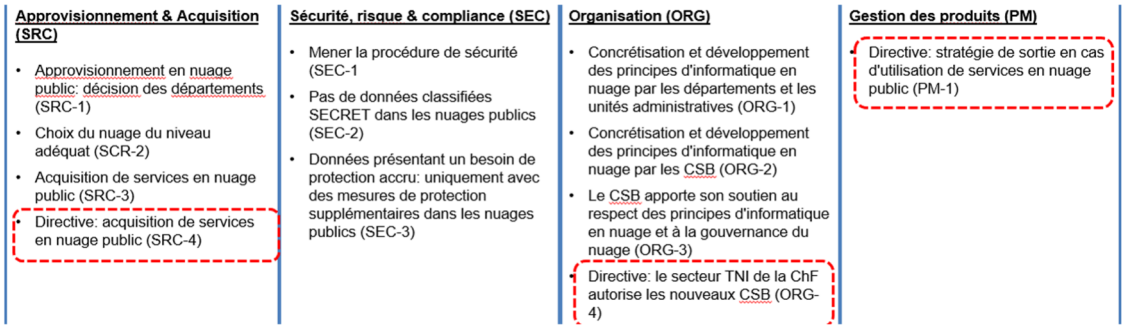

Figure 1: vue d'ensemble des principes de l'informatique en nuage de l'administration fédérale

Les principes encadrés en rouge SRC-4, ORG-4 et PM-1 sont des directives du secteur TNI et sont exposés au ch. 4.1. Les autres ont valeur de renvois à des documents complémentaires élaborés par d'autres organes, d'informations et de recommandations; ils sont groupés par thème au ch. 4.2.

1.2 Champ d'application

1. Le champ d'application du présent document correspond à celui de l'ordonnance sur la transformation numérique et l'informatique (OTNI); cf. art. 2 OTNI [2].
2. Les principes SRC-4, ORG-4 et PM-1 sont des directives du secteur TNI de la ChF et sont, en tant que telles, contraignants.

1.3 Buts des principes relatifs à l'informatique en nuage.

Les principes relatifs à l'informatique en nuage visent les objectifs suivants:

1. Les départements et les unités administratives utilisent les services infonuagiques selon des principes uniformes, dans la mesure où ces derniers sont des directives (contraignantes).
2. Les départements/ unités administratives sont assistés dans le choix du nuage de niveau adéquat pour leurs applications.
3. Les intermédiaires *(Cloud Service Brokers*; CSB) se fondent sur des principes uniformes.

Le présent document se concentre sur les questions de gouvernance. Il vise à répondre aux questions suivantes:

- Quels sont les différents niveaux de protection des données et de sécurité de l'information pour l'utilisation du nuage au sein de l'administration fédérale (ch. 2) ?
- Sur quelles bases se fondent les principes de l'informatique en nuage de l'administration fédérale (ch. 3) ?
- Quels sont les principes de l'informatique en nuage que le secteur TNI de la ChF édicte sous forme de directives contraignantes pour toute l'administration fédérale (ch. 4)?

2 Utilisation de l'informatique en nuage dans l'administration -(modèle des niveaux)

Plusieurs options d'approvisionnement s'offrent aux unités administratives qui souhaitent faire usage de services de nuages privés ou publics. Le modèle des niveaux de l'informatique en nuage favorise une compréhension commune de ces solutions. Il aide les unités administratives à choisir la solution qui leur convient le mieux.

Les différents niveaux Figure 2 se distinguent non seulement par leurs fonctionnalités, mais aussi par le type de données qui peuvent y être traitées. En général, plus le niveau est élevé, plus le besoin de protection des données est important.

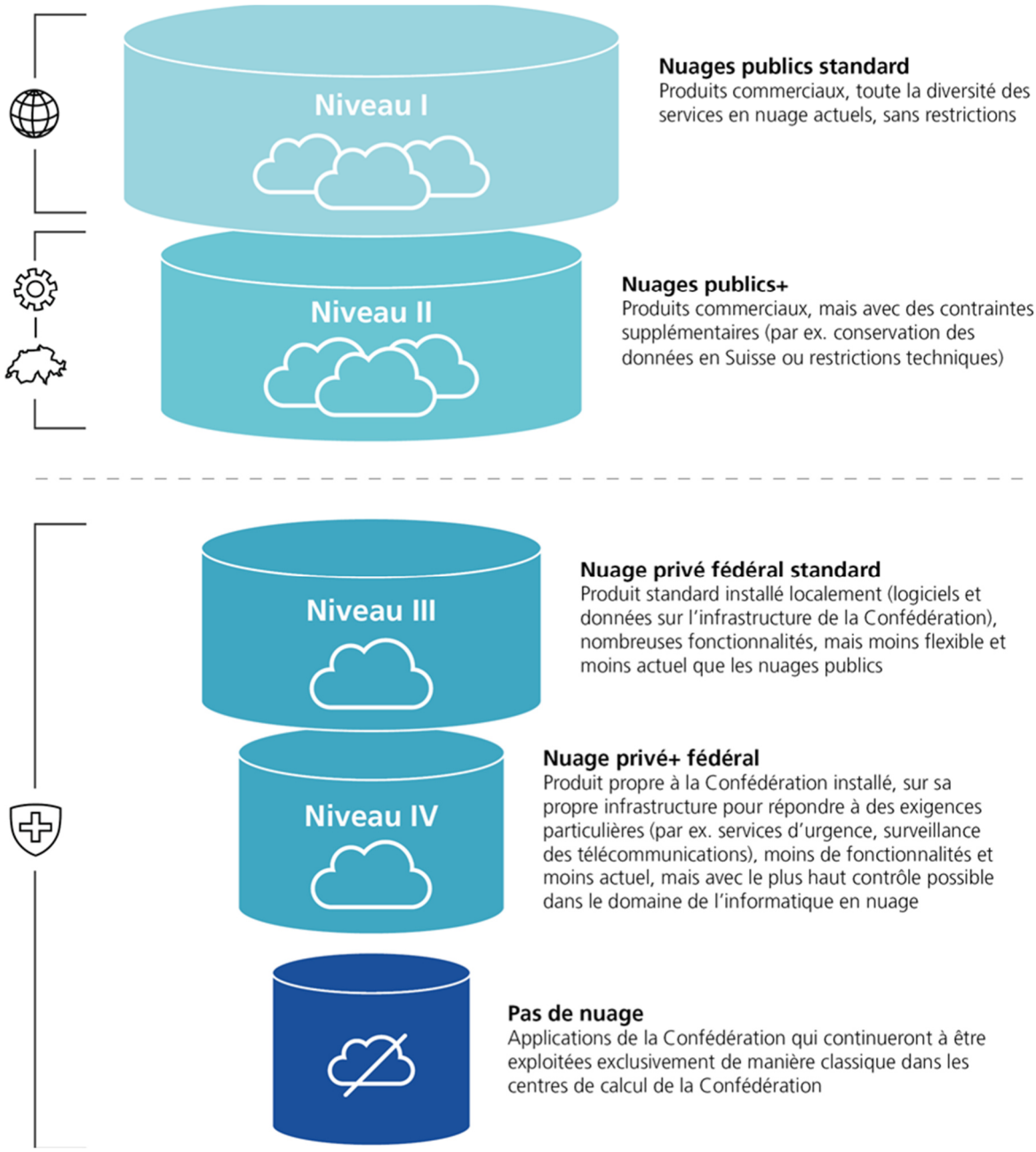

Figure 2: utilisation de l'informatique en nuage dans l'administration fédérale, présentation tirée du rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale » [3]

Lorsque l'administration fédérale utilise des services en nuage privé ou public, la souveraineté numérique, la sécurité de l'information et la protection des données sont cruciales. Les unités administratives doivent donc accorder la plus grande attention à ces aspects.

L'administration fédérale classifie les informations en fonction de leur besoin de protection dans les échelons suivants « interne», « confidentiel» ou « secret» (cf. art. 13 de la loi sur la sécurité de l'information [4]). Elle vérifie en outre si les informations contiennent des données personnelles, voire des données sensibles (cf. loi fédérale sur la protection des données [5]) ou si elles doivent être protégées pour d'autres motifs (lois spéciales, secret de fonction).

Le tableau suivant donne un aperçu sommaire de l'adéquation potentielle des niveaux de nuage Figure 2 pour certaines catégories de données:

Niveau	Conservation des données	Classification	Protection des données	Exigences en matière de souveraineté de l'État
I	monde entier	aucune	données non critiques, anonymes et/ou publiques qui ne sont pas pertinente pour la protection des données	aucune
II	par ex. UE/Suisse	«interne»	aucune donnée sensible	fondamentales
III	par ex. Swiss Government Cloud (3e pilier), OFIT	«interne»	aucune donnée sensible	élevées
IV	Par ex. Secure Private Cloud, DFJP	«confidentiel»	données sensibles	très élevées
	par ex. nouvelle plateforme de numérisation, DDPS	«secret»	données sensibles	maximales
Pas de nuage	Environnements qui ne reposent pas sur des technologies infonuagiques. Il s'agit d'applications qui continueront à être exploitées de manière classique dans les centres de calcul de la Confédération.			

Tableau 1: aperçu des niveaux d'informatique en nuage

Les explications relatives à l'adéquation potentielle des différents niveaux pour certaines catégories de données ont valeur purement indicative. Des différences par rapport aux informations du tableau 1 sont possibles dans les deux sens, par exemple lorsque la loi proscrit l'utilisation d'un certain niveau ou lorsque des mesures compensatoires sont mises en œuvre.

L'unité administrative responsable vérifie notamment, pour chaque application, les bases légales pertinentes, le besoin de protection et les risques potentiels, conformément aux directives départementales. Se fondant sur les résultats de ces analyses, elle choisit l'option d'approvisionnement et le niveau d'informatique en nuage qui convient, avec les mesures de protection nécessaires.

La limite entre les différents niveaux n'est cependant pas strictement définie. Il se peut par

exemple qu'une application fonctionne en mode hybride sur des nuages de différents niveaux, avec des données sensibles stockées dans un nuage privé et des services qui utilisent des données non critiques proposés dans un nuage public. On notera toutefois que les solutions complexes entraînent des risques supplémentaires, tels qu'une mauvaise catégorisation des données.

3 Gouvernance du nuage et principes

Les principes de l'informatique en nuage reposent sur deux éléments:

1. La gouvernance du nuage définit comment la Confédération organise et pilote l'utilisation du nuage.
2. Les principes tirés de la stratégie d'informatique en nuage constituent la base des principes de l'informatique en nuage décrits au ch. 4.

Les bases et les principes essentiels de la stratégie d'informatique en nuage de l'administration fédérale [1] sont reproduits ci-après. Ils ont été adaptés conformément aux connaissances actuelles.

3.1 Gouvernance du nuage: interaction organisationnelle

Des mesures contractuelles, organisationnelles et techniques s'imposent afin que l'administration fédérale utilise les services en nuage public de manière sûre, efficace et ordonnée. La figure 3 illustre le modèle cible organisationnel.

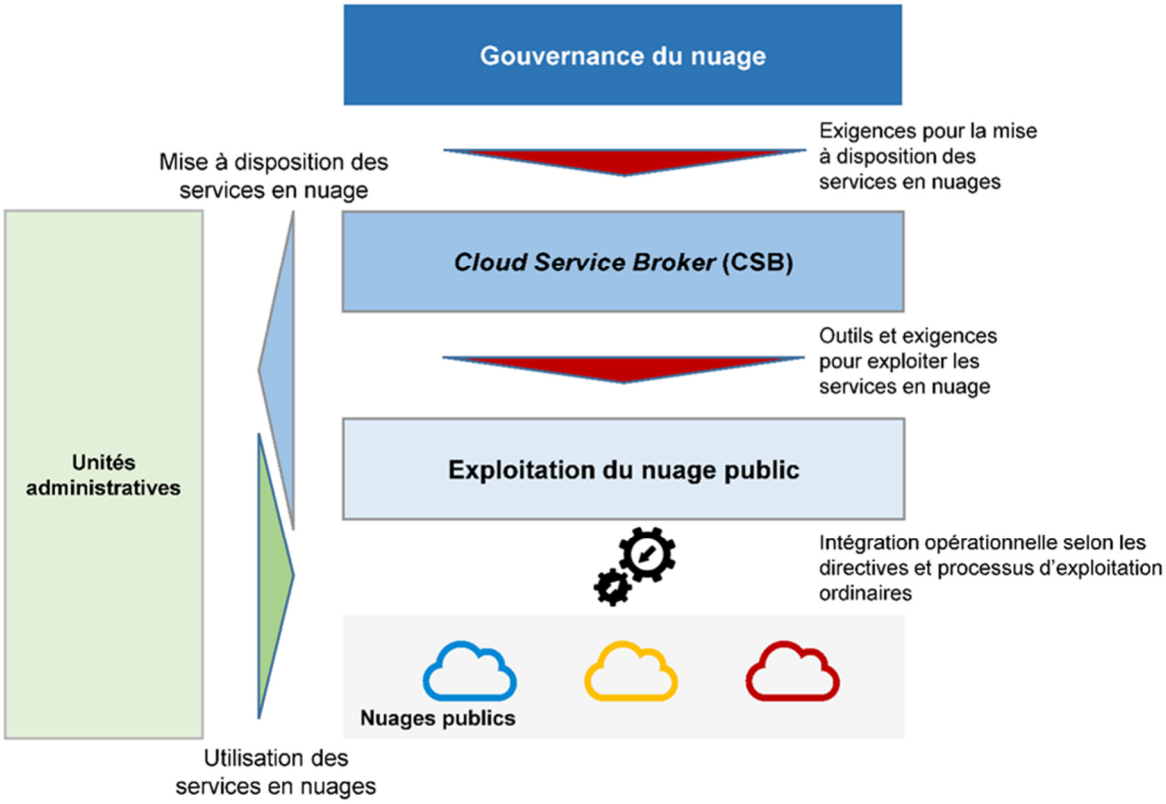

Figure 3: modèle cible organisationnel, fonctions pour la mise à disposition et l'utilisation de services en nuage public

Les fonctions représentées à la Figure 3 sont précisées ci-après:

- **Gouvernance du nuage:** le secteur TNI de la ChF définit les principes de l'informatique en nuage qui doivent être respectés lors de l'utilisation de services en nuage public et privé, et décide des exceptions éventuelles. Il met à disposition d'autres outils de manière centralisée. Les départements, la ChF et les CSB concrétisent et élargissent la gouvernance dans leur domaine de responsabilité.
- **Cloud Service Broker (CSB):** le CSB (ou intermédiaire dans la stratégie d'informatique en nuage) soutient les unités administratives dans l'utilisation ordonnée, sûre et efficace des services d'informatique en nuage public. Il peut concrétiser et élargir les principes relatifs à l'informatique en nuage dans son domaine de compétence. Il conseille sur le choix d'un nuage de niveau adéquat pour les applications. Il met en outre à disposition des environnements sécurisés (« zones d'atterrissage » [7]) pour les projets infonuagiques dans lesquels des applications peuvent être développées et exploitées. Le secteur TNI de la ChF définit les exigences applicables aux CSB dans leur cahier des charges, en accord avec le fournisseur de prestations.

  Le CSB complet de l'administration fédérale est l'Office fédéral de l'informatique et de la télécommunication (OFIT). Il existe en outre des CSB dédiés qui couvrent les besoins spécifiques de certains départements ou offices fédéraux ou des domaines spécialisés (par ex. Swisstopo, MétéoSuisse).
- **Exploitation du nuage public:** cette fonction est responsable de l'utilisation des services en nuage public, dans le cadre des processus d'exploitation internes ordinaires, pour des applications concrètes d'une unité administrative. Cette fonction assure l'exploitation pour les aspects qui dépassent l'exploitation technique des services en nuage par les fournisseurs de services en nuage public.

  Les unités administratives compétentes sont responsables de la mise à disposition contractuelle, conforme aux règles fédérales, de l'exploitation par des fournisseurs de prestations internes ou des prestataires externes.
- **Public Clouds**: cette fonction est responsable de l'exploitation des services infonuagiques. Ce rôle est assuré par les fournisseurs de nuages publics.

3.2 Principes

Les principes stratégiques constituent la base des principes relatifs à l'informatique en nuage décrits au ch. 4. Ils découlent de la stratégie d'informatique en nuage de l'administration fédérale [1] et ont été complétés ponctuellement.

Principe S-1: options d'approvisionnement stratégiques

L'administration fédérale dispose de plusieurs options d'approvisionnement: elle peut traiter et stocker des données et exploiter des applications dans les nuages publics de grands fournisseurs internationaux ou de fournisseurs locaux, dans des nuages communautaires, dans les nuages privés internes, dans les centres de calcul de la Confédération et dans les centres de calcul de partenaires d'externalisation classiques (utilisation de services gérés, externalisation de services d'exploitation, etc.).

Principe S-2: les options d'approvisionnement stratégiques se complètent, y compris sur le long terme

Pour différentes raisons (par ex. exigences légales, souveraineté numérique), à l'avenir certaines applications et données devront être exploitées ou traitées sur des infrastructures ou plateformes situées dans les centres de calcul de l'administration fédérale.

L'utilisation de nuages publics doit permettre aux unités administratives de l'administration fédérale d'accéder efficacement et rapidement aux solutions innovantes et aux technologies les plus récentes des fournisseurs de nuages publics, pour autant qu'aucune raison ne s'y oppose (par ex. exigences légales, besoin de protection des données ou préoccupations concernant la souveraineté des données).

Principe S-3: le choix d'une option d'approvisionnement, à l'exception des services standard, incombe aux départements, aux unités administratives devenues autonomes et à la Chancellerie fédérale

Les départements, les unités administratives devenues autonomes et la Chancellerie fédérale décident de manière décentralisée de la suite à donner aux demandes des bénéficiaires de prestations ou des unités administratives en ce qui concerne le choix de l'option d'approvisionnement pour des applications ou données, après consultation des fournisseurs de prestations concernés.

Principe O-1: gouvernance du nuage selon des principes communs

Les présents principes relatifs à l'informatique en nuage sont édictés par le secteur TNI de la ChF en vue d'une utilisation sûre, efficace et ordonnée des services en nuage public.

Les départements et les unités administratives peuvent concrétiser et compléter les principes et les recommandations du secteur TNI de la ChF dans leur domaine de compétence.

Principe D-1: introduction progressive du traitement des données dans les nuages publics

Même si le cadre juridique en vigueur offre éventuellement une plus grande latitude (cf. rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale » [3]), les unités administratives ont tout intérêt, dans un premier temps à ne traiter dans les nuages que des informations classifiées «interne» ou des données personnelles non sensibles.

Les informations faisant l'objet d'une classification supérieure, les données personnelles ou les données qui doivent être protégées pour d'autres raisons (par ex. lois spéciales) peuvent être stockées ou traitées dans des nuages publics pour autant que le droit en vigueur soit respecté, que les concepts de protection nécessaires soient établis et que les mesures définies dans le cas d'espèce soient mises en œuvre. La Conférence des secrétaires généraux (CSG), le délégué fédéral à la cybersécurité et le Préposé fédéral à la protection des données et à la transparence (PFPDT) doivent en être informés.

Les unités administratives sont tenues de procéder à une vérification de la conformité au droit (protection des données et obligations de garder le secret incluses, par ex. secret de fonction) et d'appliquer les procédures de sécurité pertinentes (cf. [3]) pour leurs données et leurs applications.

4 Principes-de l'informatique en nuage de l'administration fédérale

Le présent chapitre expose les principes d'informatique en nuage applicables à toute l'administration fédérale. Afin d'en faciliter la lecture, les principes sont catégorisés à la Figure 4. Aucun principe d'application générale n'a encore été défini dans les catégories ombrées.

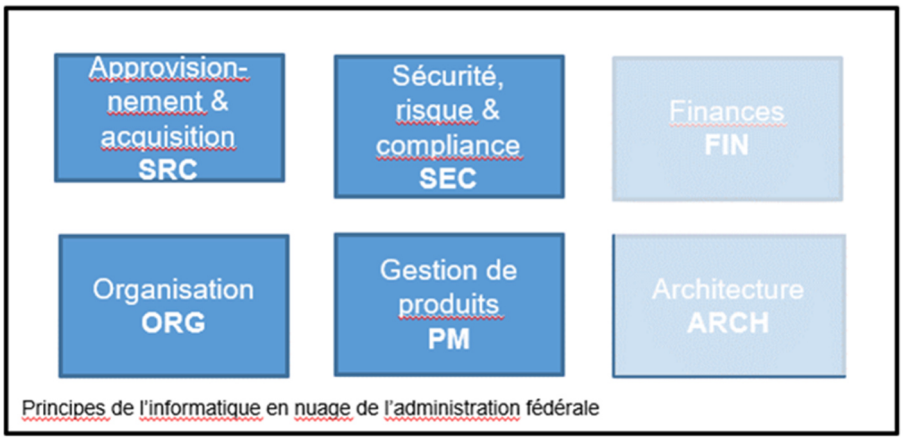

Figure 4: catégorisation des principes de l'informatique en nuage

Les principes de l'informatique en nuage applicables à toute l'administration fédérale sont élaborés et gérés de manière centralisée par le secteur TNI de la ChF. Le ch. 4.1 traite des directives (caractère contraignant). Les autres principes ont valeur de renvois à des documents élaborés par d'autres organes et pertinents dans le contexte nuagique, d'informations et de recommandations; ils sont groupés par thème au ch. 4.2.

Les départements, les unités administratives ou les CSB peuvent définir des principes spécifiques plus détaillés dans chaque catégorie. Ceux-ci ne sont pas mentionnés dans le présent document.

Les éléments plus détaillés ne concernant que les CSB sont décrits dans le cahier des charges CSB [8] (tâches, compétences et responsabilités).

4.1 Directives (caractère contraignant)

Les principes énoncés dans le présent chapitre ont valeur de directives (caractère contraignant).

4.1.1 Approvisionnement & acquisition (SRC)

ID	Nom	Caractère contraignant[4]	Principe d'informatique en nuage
SRC-4	**DIRECTIVE: acquisition de services en nuage public**	**DOIT**	**S-1, O-1**
Dispositions L'unité administrative DOIT se procurer ses services en nuage public IaaS et PaaS par l'intermédiaire du CSB de son choix. Ce principe ne s'applique pas au modèle SaaS, aux offres ERP et à la bureautique.			
Commentaire Ce principe permet de canaliser les prestations et d'aider leurs bénéficiaires à respecter la gouvernance. Il permet d'organiser de manière ordonnée et efficace les achats pour les unités administratives et d'automatiser un maximum d'étapes pour le CSB.			
Niveaux de l'informatique en nuage Niveaux I et II			
Informations complémentaires Pour les définitions d'IaaS, de PaaS et de SaaS [9]: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf			

[4] Pour les mots-clés définissant le caractère contraignant, voir annexe B.

4.1.2 Organisation (ORG)

ID	Nom	Caractère contraignant	Principe d'informatique en nuage
ORG-4	**DIRECTIVE: le secteur TNI de la ChF autorise les nouveaux CSB**	**DOIT**	**O-1**
Dispositions Si une unité administrative souhaite assumer la fonction de CSB, elle DOIT adresser une proposition motivée au secteur TNI de la ChF. Celui-ci vérifie les motifs et le respect du cahier des charges CSB. Le cas échéant, le secteur TNI de la ChF approuve la proposition.			
Commentaire Le principe O-1 prévoit qu'il peut y avoir d'autres CSB en plus du CSB de l'administration fédérale. Une unité administrative doit remplir certaines conditions pour jouer le rôle de CSB. Celles-ci sont définies dans le cahier des charges CSB [8]. Celui-ci distingue le CSB de l'administration fédérale des CSB dédiés, lesquels doivent satisfaire à d'autres exigences. Si les conditions sont remplies et qu'il existe de bonnes raisons pour qu'une unité administrative assume la fonction de CSB, le secteur TNI de la ChF accepte la proposition par décision du délégué TNI, après avoir entendu le conseil TNI.			
Niveaux de l'informatique en nuage Niveaux I et II			
Informations complémentaires Cahier des charges CSB définissant les tâches, compétences et responsabilités du CSB [8]			

4.1.3 Gestion des produits (PM)

ID	Nom	Caractère contraignant	Principe d'informatique en nuage
PM-1	**Directive: stratégie de sortie en cas d'utilisation de services en nuage public**	**DOIT**	**-**

Dispositions

Afin de gérer en connaissance de cause et de contrôler les dépendances vis-à-vis des fournisseurs de services infonuagiques, l'unité administrative compétente DOIT définir une stratégie de sortie pour chaque projet (ou groupe d'applications) avec le soutien du CSB responsable. Celle-ci décrit comment une solution logicielle peut être transférée en temps utile sur une autre plateforme, un autre service ou une autre technologie. La stratégie de sortie DOIT être mise à jour en cas d'extension de l'application.

Commentaire

L'utilisation de services en nuage public génère des dépendances envers le fournisseur de services ou certaines technologies (effet *lock-in*).

Le présent principe vise à faire prendre conscience de la nécessité de penser aux dépendances et au *lock-in* possibles dès la conception d'une solution logicielle et avant d'utiliser des services infonuagiques. Cela permet d'anticiper les dépendances indésirées et de les atténuer dans la mesure du possible.

Selon le contexte, il peut être utile de formuler une stratégie de sortie commune pour un groupe d'applications (par ex. toutes les applications d'une unité administrative qui fonctionnent chez le même fournisseur).

Les dépendances envers des fournisseurs ou des technologies sont également possibles dans les environnements en nuage privé et hors des nuages.

Niveaux de l'informatique en nuage

Niveaux I et II

Informations complémentaires

Aucune

4.2 Recommandations et renvois à d'autres réglementations

Le présent chapitre expose, d'une part, des recommandations et, d'autre part, des principes qui trouvent leur origine ailleurs et dont l'applicabilité au contexte du nuage est expliquée par des renvois et des informations complémentaires.

4.2.1 Approvisionnement & acquisition (SRC)

ID	Nom	Principe d'informatique en nuage
SRC-1	**Modèle d'approvisionnement nuage public - décision des départements et de la ChF**	**S-1**
Dispositions L'utilisation de services en nuage public relève de la décision des départements, de la ChF ou des unités administratives devenues autonomes. Ce choix repose sur la stratégie d'approvisionnement informatique de la Confédération [10], les directives et les normes de la Confédération en matière d'interopérabilité, l'architecture d'entreprise de l'unité administrative, une évaluation des risques et une vérification de la conformité au droit.		
Commentaire La décision quant au choix de l'approvisionnement en services en nuage public est prise par analogie avec la décision relative à l'acquisition dans d'autres domaines d'approvisionnement (choix du nuage du niveau adéquat). Le pouvoir de décision correspond aux principes définis à l'art. 8 OTNI [2]. La vérification de la conformité au droit porte essentiellement sur la protection des données, la sécurité de l'information et les éventuelles obligations relatives au maintien du secret.		
Niveaux de l'informatique en nuage Tous les niveaux		
Informations complémentaires Art. 8 (Décision relative à l'acquisition de prestations) et 18 OTNI (Directives du chancelier de la Confédération sur des services standard avec obligation d'achat) [2]: https://www.fedlex.admin.ch/eli/cc/2020/988/fr Stratégie d'approvisionnement informatique de la Confédération [10]: https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/strategien-teilstrategien/sb017-ikt-strategie_sourcing.html Directives informatiques de la Confédération [11]: https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/alle-ikt-vorgaben.html		

ID	Nom	Principe d'informatique en nuage
SRC-2	**Évaluation préalable du nuage de niveau adéquat**	**S-2, D-1**

Dispositions

Avant l'acquisition ou avant la procédure d'appel et l'exploitation de services en nuage public, la conformité au droit (analyse des bases légales) doit être vérifiée et une analyse des besoins de protection, ainsi que, le cas échéant, une analyse des risques doivent être menées. Le cas échéant, une analyse d'impact relative à la protection des données doit être menée pour les données personnelles.

En fonction des résultats des vérifications et des analyses, les unités administratives ou les départements optent pour une solution nuage public (niveaux I et II), nuage privé fédéral (niveaux III et IV) ou renonce à tout nuage (cf. ch. 2). La responsabilité incombe à l'unité administrative concernée ou à son département.

Si des informations faisant l'objet d'une classification supérieure, des données personnelles ou des données qui doivent être protégées pour d'autres raisons (par ex. lois spéciales) sont traitées dans des nuages publics, la Conférence des secrétaires généraux (CSG), le délégué fédéral à la cybersécurité et le Préposé fédéral à la protection des données et à la transparence (PFPDT) doivent en être informés au préalable.

Commentaire

Ce principe décrit le processus de décision concernant l'option d'approvisionnement adéquate: nuage public ou privé et niveau approprié. Les analyses portant sur la cybersécurité se fondent sur les directives du Centre national pour la cybersécurité (NCSC) [12].

Pour des précisions concernant l'application de la procédure de sécurité, voir principe SEC-1.

Niveaux de l'informatique en nuage

Tous les niveaux

Informations complémentaires

Rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale » [3]: https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

Procédure de sécurité NCSC [12]: https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html

Méthode HERMES [13]: https://www.hermes.admin.ch/

ID	Nom	Principe d'informatique en nuage
SRC-3	**Acquisition de services en nuage public**	**S-1, S-2, S-3**

Dispositions

Chaque unité administrative doit commander ses services en nuage public selon le modèle Iaas ou PaaS, sur la base de l'appel d'offres OMC 20007.

Ce principe ne s'applique pas au modèle SaaS, aux offres ERP et au service standard bureautique. Il ne s'applique pas non plus aux offres d'entreprises tierces sur les marchés des fournisseurs de services en nuage public.

Le droit des marchés publics s'applique.

Commentaire

Si l'objet du marché n'est pas compris dans l'appel d'offres OMC 20007 ou si l'adjudicataire ne peut pas fournir les prestations demandées conformément à cet appel d'offres, une autre base légale doit être prévue.

Outre les SaaS, les offres ERP et la bureautique, les offres de sociétés tierces (c'est-à-dire celles qui ne font pas partie des adjudicataires de l'appel d'offres OMC) sur les marchés des adjudicataires ne font pas partie des prestations couvertes par l'appel d'offres OMC 20007.

Niveaux de l'informatique en nuage

Niveaux I et II

Informations complémentaires

Pour les définitions d'IaaS, de PaaS et de SaaS: [9]: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Loi fédérale sur les marchés publics (LMP) [14]: https://www.fedlex.admin.ch/eli/cc/2020/126/fr

Ordonnance sur les marchés publics (OMP) [15]: https://www.fedlex.admin.ch/eli/cc/2020/127/fr

4.2.2 Sécurité, risque et compliance (SEC)

ID	Nom	Principe d'informatique en nuage
SEC-1	**Mener la procédure de sécurité**	**D-1**

Dispositions

Les départements et leurs unités administratives sont tenus de procéder, pour leurs applications et leurs données, à une vérification de la conformité au droit (protection des données et, le cas échéant, obligations de garder le secret) et d'appliquer les procédures de sécurité pertinentes.

Avant l'acquisition, la procédure d'appel ou l'exploitation de services en nuage public une analyse des besoins de protection (Schuban) doit être menée.

Si l'analyse des besoins de protection révèle un besoin de protection accru, un concept de sécurité et de protection des informations (concept SIPD) avec analyse des risques doit être établi en plus de la documentation de la mise en œuvre de la protection informatique de base.

Le conseiller à la protection des données de l'unité administrative doit être consulté pour toute décision concernant l'externalisation de données personnelles dans un nuage et pour la conception de ce traitement (art. 26, al. 2, let. a, OPDo).

Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, l'unité administrative doit procéder à une analyse d'impact relative à la protection des données personnelles. Le guide du PFPDT sur les mesures techniques et organisationnelles de la protection des données [16] doit être consulté et on procédera, si nécessaire à une analyse d'impact relative à la protection des données personnelles.

Commentaire

Les directives du NCSC concernant la procédure de sécurité [12] doivent également être appliquées aux projets potentiels de nuage public.

Ce principe renvoie aux processus SCHUBAN établis et au concept SIPD et garantit la conformité des logiciels aux règles de la protection des informations. Ces processus couvrent l'analyse et la gestion des risques.

Le rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale » [3] et les listes de contrôle pertinentes servent d'assise à la vérification de la conformité au droit.

Niveaux de l'informatique en nuage

Tous les niveaux

Informations complémentaires

Page d'information sur l'informatique en nuage dans l'administration fédérale [17]: https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

Rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale » [3]: https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

Procédure de sécurité NCSC [12]: https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html

Méthode HERMES [13]: https://www.hermes.admin.ch/ PFPDT Guide relatif aux mesures techniques et organisationnelles de la protection des données [16]: https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/aDSG/guideTOM_fr.pdf.download.pdf/guideTOM_fr.pdf FF 2023 1882 - Directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale (Directives AIPD) [18]: https://www.fedlex.admin.ch/eli/fga/2023/1882/frfga/2023/1882/fr Instrument d'examen préalable des risques [19]: https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/info-bundesbehoerden.html

ID	Nom	Principe d'informatique en nuage
SEC-2	**Pas de données classifiées « secret » dans les nuages publics**	**D-1**
Dispositions Il est interdit de stocker et de traiter des données classifiées « secret » dans les nuages publics (niveaux I et II) et dans les nuages privés de niveau III.		
Commentaire L'unité administrative veille à ce que les données classifiées « secret » restent sous le contrôle exclusif de l'administration fédérale.		
Niveaux de l'informatique en nuage Niveaux I, II et III		
Informations complémentaires Rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale » [3]: https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html Loi sur la sécurité de l'information (LSI) [4]: https://www.fedlex.admin.ch/eli/fga/2020/2696/fr Ordonnance sur la sécurité de l'information (OSI) [20]		

ID	Nom	Principe d'informatique en nuage
SEC-3	**Données présentant un besoin de protection accru: uniquement avec des mesures de protection supplémentaires dans les nuages publics**	**D-1**

Dispositions

Des mesures contractuelles, techniques et organisationnelles de protection adéquates garantissant le respect du droit applicable doivent être prises pour traiter et stocker dans un nuage public des informations classifiées « interne » ou « confidentiel » ou des données couvertes par une obligation de garder le secret.

La règle s'applique également aux données personnelles et aux données sensibles si les clarifications révèlent un risque pour la personnalité des personnes concernées. Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement doit procéder au préalable à une analyse d'impact relative à la protection des données personnelles, conformément à l'art. 22, al. 1, de la loi fédérale du 25 septembre 2020 sur la protection des données (voir SEC-1).

Si le volume de l'externalisation et la nature des données externalisées présentent un risque élevé pour la souveraineté de l'État, on doit vérifier si des mesures adéquates permettent un traitement dans un nuage public.

Commentaire

L'analyse des besoins de protection permet de déterminer si une application contient ou génère des données classifiées ou des données personnelles.

Si, en l'espèce, des mesures contractuelles, techniques et organisationnelles de protection adéquates garantissent le respect du droit applicable, des données présentant un besoin de protection accru ou protégées par la législation sur la protection des données peuvent aussi être stockées et traitées dans un nuage public.

La procédure de sécurité NCSC [12] ou une analyse d'impact relative à la protection des données personnelles permet de vérifier si les mesures de protection envisagées sont suffisantes.

Les mesures techniques de protection actuelles comprennent notamment le cryptage lors du stockage, le cryptage des données en transit ou l'utilisation de technologies particulières (Bring Your Own Key, Hold Your Own Key, Confidential Computing, etc.).

Le stockage redondant (nuage public et centre de calcul de l'administration fédérale) permet par exemple d'assurer la souveraineté numérique en garantissant la disponibilité des données.

De telles mesures doivent être coordonnées avec le département compétent.

Niveaux de l'informatique en nuage

Niveaux I et II

Informations complémentaires
Rapport « Cadre juridique pour l'utilisation de services en nuage public au sein de l'administration fédérale [3]: https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html Procédure de sécurité NCSC [12]: https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html PFPDT Guide relatif aux mesures techniques et organisationnelles de la protection des données [16]: https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/aDSG/guideTOM_fr.pdf.download.pdf/guideTOM_fr.pdf

4.2.3 Organisation (ORG)

ID	Nom	Principe d'informatique en nuage
ORG-1	**Concrétisation et développement des principes d'informatique en nuage par les départements et les unités administratives**	**O-1**
Dispositions Les principes de l'informatique en nuage sont applicables à toute l'administration fédérale. Les départements et les unités administratives peuvent concrétiser ou compléter ces principes dans leur domaine de compétence, dans les limites du droit en vigueur.		
Commentaire Ce principe permet aux départements et aux unités administratives d'adapter librement les principes généraux à leurs spécificités. Ils peuvent notamment renforcer, préciser ou compléter les principes communs ou en ajouter de nouveaux.		
Niveaux de l'informatique en nuage Tous les niveaux		
Informations complémentaires Loi sur l'organisation du gouvernement et de l'administration (LOGA) [21]: https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/fr Ordonnance sur la transformation numérique et l'informatique (OTNI) [2]: https://www.fedlex.admin.ch/eli/cc/2020/988/fr		

ID	Nom	Principe d'informatique en nuage
ORG-2	**Concrétisation et développement des principes d'informatique en nuage par les CSB**	**O-1**
Dispositions Les CSB peuvent concrétiser ou compléter les principes d'informatique en nuage dans leur domaine de compétence. Les clients ont la possibilité d'influencer les adaptations des principes d'informatique en nuage par l'intermédiaire du CSB responsable. Ces adaptations ne s'appliquent qu'aux clients du CSB concerné.		
Commentaire Ce principe permet aux CSB d'adapter librement les principes généraux à leurs spécificités. Ils peuvent notamment renforcer, préciser ou compléter les principes communs ou en ajouter de nouveaux.		
Niveaux de l'informatique en nuage Niveaux I et II		
Informations complémentaires Loi sur l'organisation du gouvernement et de l'administration (LOGA) [21]: https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/fr Ordonnance sur la transformation numérique et l'informatique (OTNI) [2]: https://www.fedlex.admin.ch/eli/cc/2020/988/fr		

ID	Nom	Principe d'informatique en nuage
ORG-3	**Le CSB apporte son soutien au respect des principes d'informatique en nuage et à la gouvernance du nuage**	**O-1**
Dispositions Le CSB doit soutenir ses clients dans l'exercice de leur activités en relation avec le respect des principes d'informatique en nuage et de la gouvernance du nuage définie.		
Commentaire Ce principe formule l'une des tâches du CSB: il aide les départements et les unités administratives à respecter les principes d'informatique en nuage et les directives relatives à la gouvernance. L'unité administrative concernée demeure toutefois responsable du respect des principes et des directives.		
Niveaux de l'informatique en nuage Niveaux I et II		
Informations complémentaires Cahier des charges CSB définissant les tâches, compétences et responsabilités du CSB voir [8]		

5 Dispositions finales

5.1 Dispositions transitoires relatives aux directives SRC-4, ORG-4 et PM-1

Les applications réalisées avant l'entrée en vigueur de la présente directive peuvent continuer à fonctionner sans changement. Lors du prochain renouvellement ou de l'extension des fonctionnalités de l'application, les directives doivent être vérifiées et leur respect initialisé.

5.2 Respect des directives SRC-4, ORG-4 et PM-1

En vertu de l'art. 3 OTNI , les départements et la ChF sont responsables de l'application des directives dans leurs domaines de compétence respectifs.

5.3 Suivi

Le secteur TNI de la ChF vérifie l'actualité et l'adéquation des principes relatifs à l'utilisation de l'informatique en nuage au plus tard quatre ans après leur entrée en vigueur.

5.4 Entrée en vigueur des directives SRC-4, ORG-4 et PM-1

Les directives entrent en vigueur le 1er octobre 2023.

Annexes

A. Modifications par rapport à la version précédente

Version	Descriptif	Modifié le/par
0.1 – 0.8	Version initiale fondée sur la stratégie d'informatique en nuage, document de travail, élaboration des contenus	05.09.2022: 13.09.2022 D. Albisser, E. Dubach, S. Hüsemann
0.92	Intégration des commentaires E. Dubach, Markwalder, Stephan Brunner	15.09.2022: S. Hüsemann, D. Albisser
0.93	Intégration des résultats de la consultation	11.10.2022: S. Hüsemann, D. Albisser
0.94	Finalisation après la consultation	01.11.2022: S. Hüsemann, D. Albisser, R. Lichtsteiner, E. Dubach
0.95	Intégration des commentaires issus de la revue par Daniel Markwalder	08.11.2022: S. Hüsemann
0.96	Intégration des commentaires issus de la 2e consultation des offices	25.11.2022: S. Hüsemann, R. Lichtsteiner, E. Dubach
0.98	Adaptation du document aux directives architecturales Restructuration des chapitres, révision du texte, intégration des commentaires TNI Transformation et interopérabilité	24.01.2023: S. Hüsemann, E. Dubach, R. Lichtsteiner, S. Meyer, A. Spichiger
0.99	Intégration des résultats de la consultation interne ChF	02.02.2023: S. Hüsemann, E. Dubach, R. Lichtsteiner
1.0	Intégration des résultats de la consultation des offices et élimination des divergences	22.09.2023: N. Gammenthaler, S. Hüsemann, E. Dubach

B. Signification des mots-clés déterminant le caractère contraignant

Le caractère contraignant[5] des différentes dispositions de la présente directive est indiqué par les mots-clés suivants écrits en majuscules:

Mot-clé	Caractère contraignant
DOIT	La directive doit impérativement être respectée (sauf dérogation).
EST INTERDIT	L'option ne peut pas être choisie.

[5] Degrés du caractère contraignant selon *Request of Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF).* L'indication des degrés du caractère contraignant selon RFC 2119 est une pratique répandue dans la normalisation internationale.

PEUT	L'option est autorisée explicitement. Les utilisateurs décident s'ils veulent y recourir. Si la directive concerne une solution informatique, le fournisseur de la solution doit proposer cette option.
DOIT EN PRINCIPE	En règle générale, l'option doit être choisie. Il est toutefois possible de s'écarter de cette directive sans qu'une dérogation du secteur TNI ou du NCSC soit nécessaire, notamment si cette option ne permet plus de garantir la rentabilité ou la sécurité. Une justification écrite est cependant requise.
A LA POSSIBILITÉ DE	L'option est admise. Si la directive concerne une solution, le fournisseur de cette dernière décide s'il veut prendre en charge cette option.

C. Documents de référence

[1] Chancellerie fédérale, Transformation numérique et gouvernance de l'informatique SB020 — Stratégie d'informatique en nuage de l'administration fédérale

[2] Chancellerie fédérale (ChF), ordonnance sur la transformation numérique et l'informatique (OTNI), RS **172.010.58**

[3] Chancellerie fédérale (ChF), rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale »: https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html.

[4] Assemblée fédérale, loi sur la sécurité de l'information (LSI), RS **128**

[5] Assemblée fédérale, loi fédérale sur la protection des données (LPD), RS **235.1**

[6] Conseil fédéral, ordonnance concernant la protection des informations (OPrI), RS **510.411**

[7] IT-Business, 2022, Was ist eine Landing Zone? (it-business.de) [en allemand, consulté le 28.7.2023]

[8] Chancellerie fédérale (ChF), cahier des charges CSB [en cours de rédaction]

[9] National Institute of Standards and Technology (NIST), The NIST Definition of Cloud Computing, 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[10] Chancellerie fédérale (ChF), stratégie d'approvisionnement informatique de la Confédération 2018-2023,https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/strategien-teilstrategien/sb017-ikt-strategie_sourcing.html

[11] Chancellerie fédérale (ChF), directives informatiques, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/alle-ikt-vorgaben.html

[12] Centre national pour la cybersécurité (NCSC), Procédure de sécurité, 2022

[13] Chancellerie fédérale HERMES gestion de projet 5.1

[14] Assemblée fédérale, loi fédérale du 21 juin 2019 sur les marchés publics (LMP), RS **172.056.1**

[15] Conseil fédéral, ordonnance sur les marchés publics (OMP), RS **172.056.11**

[16] PFPDT Guide relatif aux mesures techniques et organisationnelles de la protection des données : https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/aDSG/guideTOM_fr.pdf.download.pdf/guideTOM_fr.pdf

[17] Chancellerie fédérale (ChF), Transformation numérique et gouvernance de l'informatique, informatique en nuage, 2022, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

[18] Conseil fédéral, Directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale (Directives AIPD), FF **2023** 1882 - [18]: https://www.fedlex.admin.ch/eli/fga/2023/1882/frfga/2023/1882/fr

[19] Office fédéral de la justice, instrument d'examen préalable des risques : https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/info-bundesbehoerden.html

[20] Conseil fédéral, ordonnance sur la sécurité de l'information (OSI), 2022 (entrée en vigueur : 1.1.2024).

[21] Assemblée fédérale, loi sur l'organisation du gouvernement et de l'administration (LOGA), RS **172.010**

[22] Cloudcomputing Insider, Cloud Governance, 2021, https://www.cloudcomputing-insider.de/was-ist-cloud-governance-a-990452/ [en allemand, consulté le 28.7.2023].

[23] Office fédéral de l'informatique et de la télécommunication (OFIT), Shared Responsibility Model, 2022 : https://confluence.bit.admin.ch/x/I5vzFw

D. Abréviations et glossaire

Terme/abréviation	Signification
ChF	Chancellerie fédérale
Gouvernance du nuage	La gouvernance du nuage vise à garantir l'utilisation judicieuse, sûre et conforme aux règles des services infonuagique. Elle se compose d'un ensemble de règles et de mesures organisationnelles et techniques qui concernent différents aspects de l'utilisation du nuage. [22]
CSB	Courtier de services en nuage
Conseil TNI	Conseil de la transformation numérique et de la gouvernance informatique de la Confédération

Terme/abréviation	**Signification**
TNI	Secteur Transformation numérique et gouvernance de l'informatique de la ChF
PFPDT	Préposé fédéral à la protection des données et à la transparence
CSG	Conférence des secrétaires généraux
ID	Identifiant
IaaS	*Infrastructure as a Service* ou infrastructure en tant que service
TIC	Technologies de l'information et de la communication
SIPD	Concept de sécurité de l'information et de protection des données
ITSM	Gestion des services informatiques
Zone d'atterrissage	Une zone d'atterrissage est un environnement sécurisé dans le nuage, auquel différents utilisateurs peuvent accéder. Elle permet de mettre à disposition et d'utiliser des applications et des charges de travail. Leur structure dépend des besoins de l'entreprise [7].
NCSC	Centre national pour la cybersécurité
PaaS	*Platform as a Service* ou plateforme en tant que service
SaaS	*Software as a service* ou logiciel en tant que service
Schuban	Analyse des besoins de protection