Mandat du groupe spécialisé Cloud

Par le présent document, les auteurs demandent la création du **groupe spécialisé Cloud**. L'objectif en est d'élaborer des normes et/ou directives concrètes quant à l'utilisation des technologies d'informatique en nuage ou Cloud en Suisse.

L'analyse de potentiel réalisée a permis de mettre en évidence des besoins fondamentaux en normalisation dans le domaine du Cloud en Suisse. Dans le cadre de ses activités, le groupe spécialisé Cloud est appelé, en s'appuyant sur les normes internationales, à formuler concrètement les besoins en normes dans le domaine de l'informatique en nuage pour la cyberadministration. Il restera ensuite à élaborer de telles normes avec le concours des différents groupes d'intérêt de la population et de l'économie.

Contrôle des modifications, examen, approbation

Version	Date	Nom	Remarques (modifié, contrôlé, approuvé)
0.1	14.06.23	Jesko Mueller	Version de base avec premières contributions
0.2	11.08.23	Groupe de base	Adaptations selon Feedbacks groupe de base
0.3	31.08.23	Jesko Mueller	Adaptations selon Feedbacks groupe de base
1.0	29.11.23	Lorenz Frey-Eigenmann	Réception Comité directeur eCH

Table des matières

1 Situation de départ

Ce chapitre passe en revue les points forts et les points faibles dans le contexte actuel en matière de contenu eu égard aux normes et cadres déjà en place pour les projets d'informatique en nuage.

1.1 Points forts

L'enquête[1] menée dans le cadre de l'analyse de potentiel révèle que pour une grande majorité des personnes interrogées (89%), les besoins en normes dans le domaine de l'informatique en nuage en cyberadministration sont importants, une nette majorité (74%) se déclarant par ailleurs favorable à un alignement sur les normes internationales. À une très large majorité de 97%, ils jugent nécessaire la création d'un groupe spécialisé Cloud au sein de l'association eCH.

Qui plus est, l'étude «Swiss Cloud»[2] montre d'ores et déjà

- que si rien ne prouve qu'un «Swiss Cloud» sous la forme d'une infrastructure de droit public ne s'impose ni qu'il ne constitue un facteur de succès pour la Suisse,
- un label «Swiss Cloud» sous la forme de conditions-cadres et de lignes directrices appropriées visant à garantir une utilisation compétente et sûre des prestations du nuage informatique est vivement souhaité.

Des normes et documents auxiliaires appropriés peuvent aider à cet égard à pallier l'absence de conditions-cadres et de principes directeurs idoines (voir aussi 2.1 Objectifs).

1.2 Points faibles

Entre 2013 et 2016, un groupe spécialisé Cloud Computing[3] avait déjà produit deux documents de résultats, à savoir:

- Vue d'ensemble des certificats pertinents pour l'utilisation du Cloud, document auxiliaire, 2016
- Architecture de référence pour le Cloud, document auxiliaire, 2015

Du point de vue du contenu toutefois, l'analyse des potentiels a également démontré que les *Pain Points* (points faibles actuels) suivants pourraient être traités par des normes appropriées:

- Le trop peu de compréhension et de confiance dans les technologies d'informatique en nuage imputables à un défaut de fondements/ directives concernant par exemple les enjeux du Vendor Lock-In et l'absence de classification des données et d'affectation des données aux classes correspondantes par exemple. La perte d'autonomie, les dépendances préjudiciables et la sécurité des données en particulier suscitent des inquiétudes. Des inquiétudes qui bien souvent font également obstacle aux efforts déployés par les organismes publics en matière de numérisation.
- Hétérogénéité dans la maturité de l'adoption et de l'utilisation des technologies: certaines instances publiques (p. ex. cantons spécifiques) sont très avancées dans le domaine des technologies d'informatique en nuage, alors même que d'autres le taux d'adoption reste encore trop faible. Cette hétérogénéité marquée rend également difficile la coopération tant horizontale que verticale et s'oppose à toute orientation stratégique homogène aux différents niveaux (fédéral, cantonal, communal).

[1] Voir l'analyse de potentiel; n=39, membres du groupe spécialisé dissous Cloud Computing.
[2] Rapport sur l'évaluation des besoins d'un nuage informatique suisse (Swiss Cloud), https://www.newsd.admin.ch/newsd/message/attachments/64462.pdf
[3] Ce groupe a ensuite été dissous, la faute notamment au peu d'évolution thématique, au départ de son instigateur, au déficit de représentants des instances publiques et à un potentiel de normes rigoureuses jugé trop modeste à l'époque.

- Redondance dans le développement de stratégies par chaque instance du fait de la définition de normes propres sur des thématiques qu'une norme centrale permettrait pourtant de clarifier une bonne fois pour toutes.
- En l'absence de règles, les fournisseurs/Hyperscalers ne proposent aucun service de cyberadministration adapté au contexte suisse. L'adoption de technologies s'en trouve freinée et le potentiel de renforcement du site technologique novateur qu'est la Suisse demeure inexploité.
- L'absence de normes uniformes en matière de sécurité informatique lors de l'utilisation du Cloud représente un risque pour la sécurité. Les organisations de moindre envergure, dont les ressources en la matière sont limitées, sont particulièrement vulnérables.

1.3 Évaluation

Le groupe spécialisé devrait avoir vocation à atténuer les points faibles précédemment évoqués en mettant à profit les moyens pertinents (nouvelles normes ou nouveaux outils p. ex), tout en tirant parti de la dynamique inhérente au marché (points forts). Il doit avoir pour principal objectif d'épauler les décideurs publics dans leurs projets en lien avec l'informatique en nuage. Par exemple, les redondances dans le développement de stratégies (point faible) pourraient être atténuées en élaborant des plans directeurs (sous forme de documents auxiliaires du groupe spécialisé Cloud par exemple) censés guider l'utilisation des normes internationales.

2 Objectifs et conditions limites

2.1 Objectifs

Le groupe spécialisé a pour finalité l'élaboration de normes et documents auxiliaires associés régissant l'utilisation de technologies d'informatique en nuage dans le domaine de la cyberadministration.

L'objectif ultime de ces normes est de renforcer la confiance dans les solutions d'informatique en nuage et d'aider les instances publiques à adopter les technologies de Cloud et à préserver leur souveraineté dans la fourniture de leurs services dans le cadre de l'utilisation de ces technologies. Le groupe spécialisé ambitionne donc, en déployant les moyens appropriés (notamment des normes et documents / outils connexes, etc.), d'apporter aux instances publiques la certitude qu'elles sont sur la bonne voie du point de vue technique, juridique et organisationnel et qu'elles peuvent instaurer leur propre gouvernance *au cours de la préparation*, *de la migration vers* et de *l'utilisation du Cloud*.

Le champ d'application est défini par référence aux modèles de livraison pour l'informatique en nuage suivant la stratégie d'informatique en nuage de l'administration fédérale[4] et concerne les modèles de livraison *Hybrid Multi-Cloud* tel qu'indiqué dans le graphique ci-dessous. Pour ce faire, les modèles de livraison des Clouds privés et des Clouds publics sont examinés plus avant et servent de cadre de référence.

Remarque: Même lorsque la stratégie d'informatique en nuage de l'administration fédérale est utilisée comme cadre de référence en vue de définir le champ d'application, le travail et les livrables du groupe spécialisé Cloud ne sont pas cantonnés à la Confédération et à ses instances. L'objectif visé est une utilisation à grande échelle dans l'ensemble du secteur public et au-delà, pour autant que cela soit pertinent.

[4] Stratégie d'informatique en nuage de l'administration fédérale, 11.12.2020 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-81568.html
«Le *Hybrid Multi-Cloud de l'administration fédérale* désigne l'approche visant à mettre à la disposition de l'administration fédérale suisse les prestations en nuage de ses propres fournisseurs de prestations et celles de différents fournisseurs de nuages publics en tant que services d'infrastructure et de plateforme abstraits.»

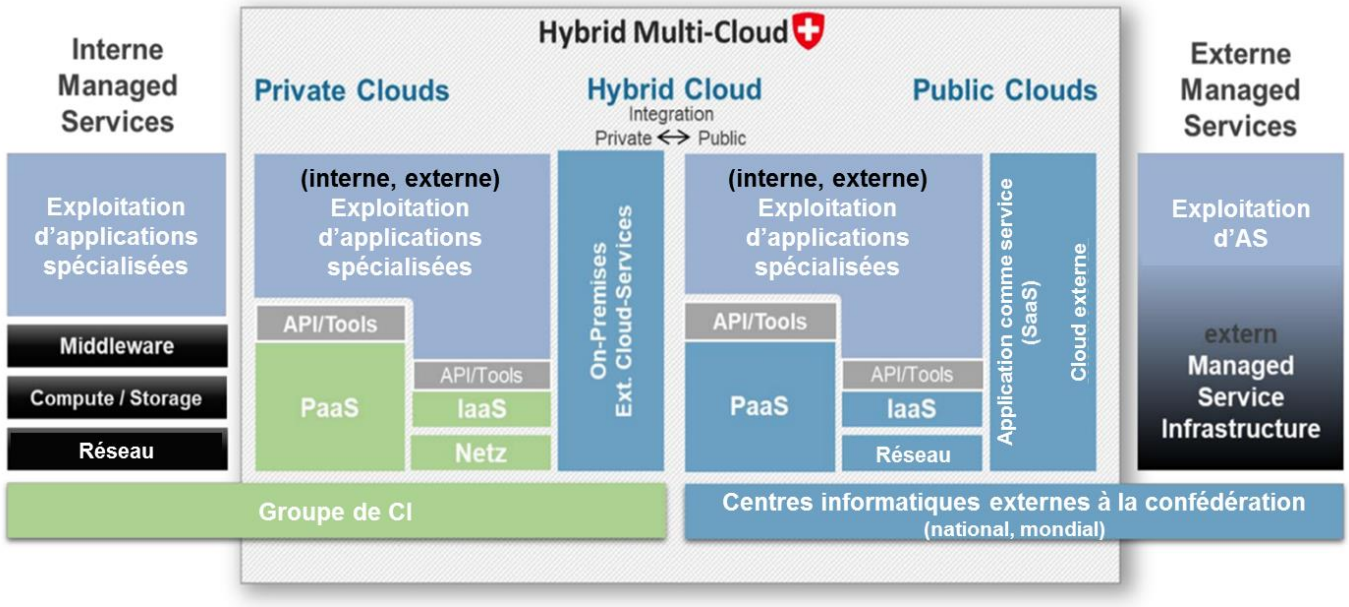

Figure 1: Modèles de livraison du Hybrid Multi-Cloud de la Confédération.

Le groupe spécialisé travaille donc sur des normes et documents auxiliaires propres à aider les utilisateurs des Private Clouds et Public Clouds. Leurs domaines thématiques incluent (sans pour autant forcément s'y limiter):

- Ecosystem: Aspects relatifs à l'obtention d'une vue d'ensemble et au contrôle nécessaire des services disponibles/utilisés dans l'écosystème Mult Cloud et leurs capacités d'intégration, ainsi que leurs dépendances les uns par rapport aux autres.
- Governance: Aspects du pilotage à toutes les phases du cycle de vie de l'organisation de l'informatique en nuage et des solutions de Cloud.
- Compliance: Aspects de conformité par rapport au mandat légal de l'organisation bénéficiaire et à d'autres exigences réglementaires.
- Finance: Aspects de la collecte d'informations, du calcul et de la gestion d'informations pertinentes sur le plan financier concernant l'informatique en nuage, y compris l'optimisation des coûts d'exploitation du Cloud. Voir aussi FinOps.

Les normes et documents auxiliaires prévus mettent en œuvre les aspects susmentionnés de façon modulaire, de sorte à permettre aux utilisateurs d'adapter les résultats à leur propre cas d'application.

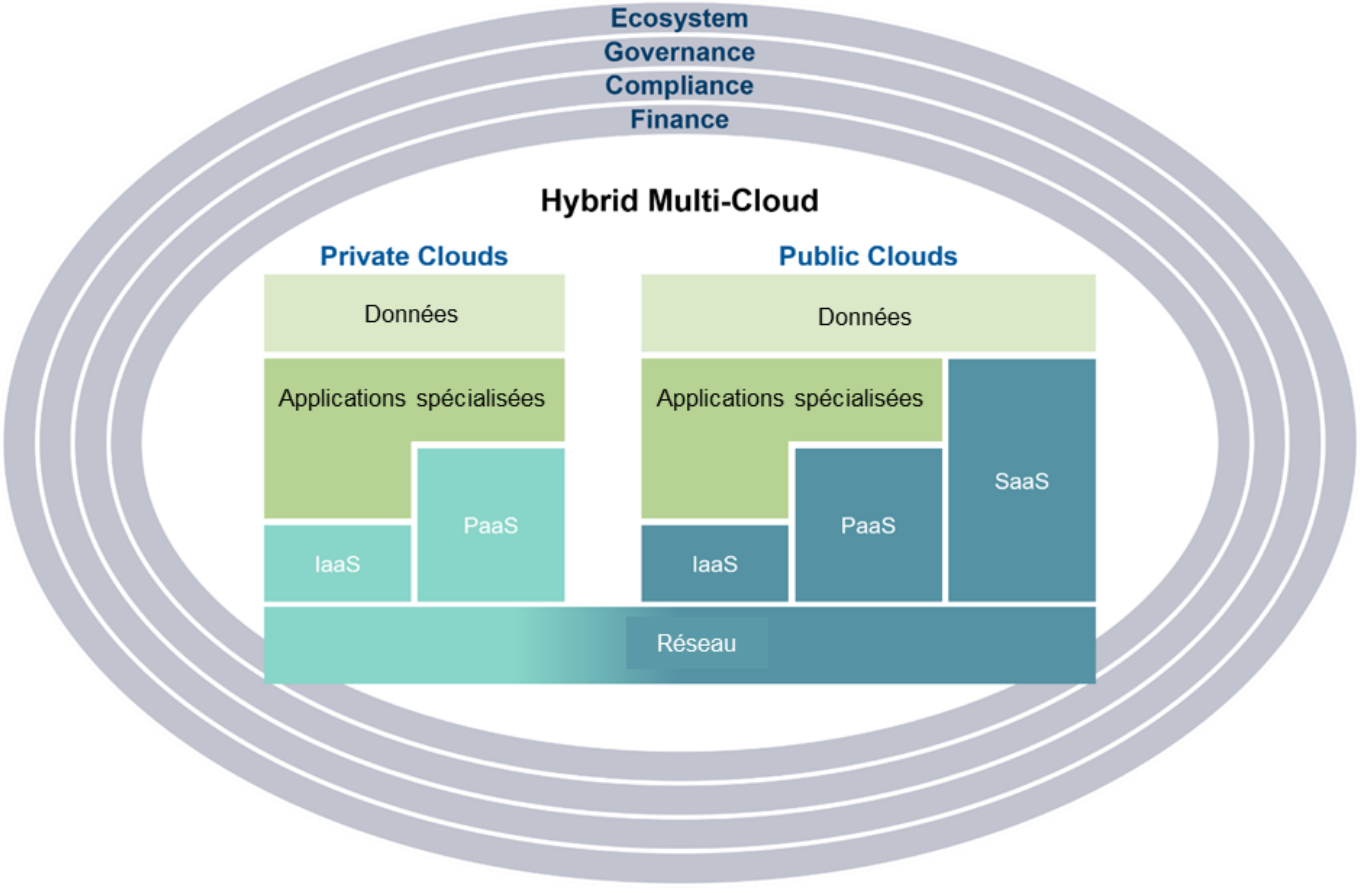

Figure 2: Périmètre prévu des résultats du groupe spécialisé

Le groupe spécialisé prendra également des mesures visant à promouvoir l'utilisation effective et efficace des résultats du groupe. Qui plus est, il a également vocation à servir de plateforme d'échange entre les différents groupes d'intérêt.

Le groupe spécialisé prendra des dispositions à cet effet:

- Développement, sélection et adaptation des normes
- Développement de documents auxiliaires destinés à permettre une utilisation efficace et efficiente des normes
- Mise à disposition et communication de normes et documents auxiliaires associés
- Promotion de l'échange entre les Stakeholders concernant l'utilisation la plus performante qui soit des normes.

2.2 Conditions limites

En règle générale, le groupe spécialisé ne remplacera pas les normes qui existent déjà sous une forme semblable. En particulier, l'élaboration des normes souhaitées implique de prendre en compte les normes internationales existantes. Sont notamment concernées:

- Normes ISO/IEC de la série 27000
- BSI Kriterienkatalog Cloud Computing C5 et documents affiliés, Allemagne
- IT Security Standard (IKSE), Estonie
- Federal Risk and Authorization Program (FedRamp), USA

- NIST Cybersecurity Framework (CSF) sowie NIST 800-52, USA
- ANSSI SecNumCloud, France
- European Cybersecurity Certification Scheme for Cloud Services (EUCS), EU

Qui plus est, les études / résultats suivantes devraient être pris en considération dans le contexte suisse:

- Stratégie d'informatique en nuage de l'administration fédérale, 2020[5]; Niveaux de l'informatique en nuage de l'administration fédérale 2022[6], Principes de l'administration fédérale en matière d'informatique en nuage 2023 (publication à venir)
- Cadre juridique pour l'utilisation de services de Public Cloud dans l'administration fédérale, 2022[7].
- Étude Swiss Cloud, 2020[8]
- «Étude d'opportunités Cloud souverain» et publication associées, 2023[9]
- Datenschutzbeauftragte des Kanton Zürichs, Neuer Leitfaden Nutzung externer Cloud-Dienste, 2022[10]
- Ville de Zurich, Rechtsgutachten von Laux Lawyers AG zur Rechtmässigkeit der Cloud-Nutzung, 2022[11]
- Canton de Berne, Risques résiduels dans le cadre de l'utilisation de M365[12]

L'élaboration des normes / outils implique de consulter des études et résultats supplémentaires. Nous nous abstenons à ce stade de répertorier explicitement l'ensemble des études et résultats connus.

2.3 Délimitation du projet

Les normes à élaborer ne doivent pas chercher à décider quelles applications / solutions peuvent ou ne peuvent pas «aller dans le Cloud». Les processus et procédures décisionnelles correspondants relèvent de la responsabilité de chaque instance. Au lieu de cela, les résultats du groupe spécialisé doivent rendre plus facile la «voie menant au Cloud» et aider les utilisateurs à prendre d'eux-mêmes les décisions y afférentes. Un principe qui s'applique, quel que soit le modèle de livraison à mettre en œuvre pour le service d'informatique en nuage.

---

[5] Stratégie d'informatique en nuage de l'administration fédérale, 11.12.2020 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-81568.html

[6] https://www.bk.admin.ch/dam/bk/de/dokumente/dti/themen/cloud/cloud-stufengrafik-pdf.pdf.download.pdf/Cloud-Stufen%20der%20Bundesverwaltung.pdf

[7] https://www.bk.admin.ch/dam/bk/de/dokumente/dti/themen/cloud/rechtsrahmen.pdf.download.pdf/Rechtlicher%20Rahmen%20f%C3%BCr%20die%20Nutzung%20von%20Public-Cloud-Diensten%20in%20der%20Bundesverwaltung%20(inkl.%20Anh%C3%A4nge%20A%20und%20B).pdf

[8] Rapport sur l'évaluation des besoins d'un nuage informatique suisse (Swiss Cloud), 12.2020, https://www.newsd.admin.ch/newsd/message/attachments/64462.pdf

[9] CLDN, 11.05.2023 https://cldn.ch/les-cantons-latins-veulent-renforcer-leur-action-concertee-pour-la-souverainete-numerique/

[10] Neuer Leitfaden Nutzung externer Cloud-Dienste, 30 032 022 https://datenschutz.ch/mitteilungen/2022/neuer-leitfaden-nutzung-externer-cloud-dienste

[11] Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale 31.08.2022 https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

[12] Risques résiduels dans le cadre de l'utilisation de M365, rapport au Conseil-exécutif BE, 07.06.23 https://www.rrgr-service.apps.be.ch/api/rr/documents/document/25fb10f9293d4ae0870c66a4c920c10e-332/29/Beilage-Bericht-28.06.2023-de.pdf

Exemple: les normes et documents auxiliaires mis à disposition peuvent assister une clinique à cet égard:

- avec quel type de données «aller dans le Cloud»,
- comment s'y prendre (procédure),
- comment se sécuriser (p. ex. par quelles mesures techniques, juridiques et/ou organisationnelles).

Les normes et documents auxiliaires ne sont pas destinés en priorité:

- à supplanter les procédures de décision prédéfinies ou définies en interne,
- à dicter la collaboration avec les fournisseurs de services de Cloud ou à régir les opérations,
- à obtenir la certification de l'organisation ou des services de Cloud,
- à dégager des responsabilités.

3 Organisation et planification

3.1 Organisation du projet

L'organisation du projet exposée ici illustre la façon dont devrait être composé le groupe spécialisé Cloud lors de son lancement. Les futurs auteurs et co-auteurs des résultats du groupe spécialisé étant pour l'instant inconnus, les individus sont ici répartis en deux catégories: «membres actuels» et «nouveaux membres». Les groupes d'auteurs et de collaborateurs se réuniront par la suite.

3.1.1 Direction du projet / coordination générale

La ou les personnes ci-dessous seront chargées d'assurer la coordination générale du groupe spécialisé, ainsi que la communication avec l'eCH.

Organisation	Rôle au sein de l'organisation	Prénom	Nom

3.1.2 Membres actuels

Sous Auteurs, on trouve les membres actuels du groupe de base. Ces derniers sont par la suite appelés à devenir également membres du groupe spécialisé.

→ Tableau, voir annexe.

3.1.3 Nouveaux membres

Les membres ci-dessous ont été conviés par les membres actuels à participer et à coopérer dans le cadre du groupe spécialisé. Le groupe spécialisé devrait couvrir un éventail suffisamment large de groupes d'intérêt afin que:

- les normes et documents auxiliaires (résultats) élaborés couvrent les points de vue et les connaissances requises dans les différents domaines du secteur public et de l'économie dans un souci de pertinence, d'exactitude et d'exhaustivité technique comme en termes de contenu
- les résultats élaborés parlent aux groupes d'utilisateurs concernés et les aident

- les résultats élaborés reflètent les possibilités et compétences des prestataires de services concernés

Remarque: nombre de futurs membres ci-dessous du groupe spécialisé n'ont pas encore confirmé leur participation définitive.

→ Tableau, voir annexe.

3.2 Résultats attendus

Le groupe spécialisé prévoit de discuter des **résultats** suivants au sein du groupe spécialisé nouvellement constitué. Une fois la faisabilité et le potentiel constatés, le groupe spécialisé entreprendra d'élaborer ces résultats pour les soumettre au Comité d'experts.

Parmi les résultats, on trouve les **normes** suivantes:

Titre	Thème
Normes minimales Cloud	Normes minimales attendues devant être respectées et affichées par le fournisseur et l'utilisateur de services d'informatique en nuage (Hybrid Multi Cloud) (Doit/Devrait/Peut). Il s'agit notamment d'aspects tels que: • Technique et sécurité • Identity • Sécurité des informations / Privacy • Souveraineté • Organisation & Skill Management • Exit Strategies (Back-ups & Recoverability comprises) • Éléments juridiques[13] • Éléments contractuels[14] • Durabilité
(autres selon les besoins)	-

D'autres résultats pourront être proposés ultérieurement par des membres du groupe spécialisé.

Les **documents auxiliaires** suivants sont eux aussi inclus:

Titre	Thème
Cadre réglementaire & terminologie, normes et bases juridiques Cloud pertinentes	La terminologie, les normes et bases juridiques établies disponibles et pertinentes dans le contexte de l'informatique en nuage – à différents niveaux (macro vs micro, organisationnel vs technique). Elles peuvent servir de fondement à l'élaboration de «normes minimales de sécurité du Cloud» et y être différenciées. Le but est ici de s'abstenir de définir de nouvelles normes suisses

[13] par exemple: Exigences en matière de protection des données selon la LPD, compatibilité avec le RGPD, exigences de protection des secrets (secrets de fonction, secrets professionnels particuliers, secrets de fabrication et commerciaux), etc.
[14] par exemple: Éléments contractuels pour la collaboration avec les fournisseurs de services d'informatique en nuage.

	là où des normes internationales généralement reconnues existent déjà (p. ex. ISO/IEC, UE).
Cloud Readiness Assessment	Cadre d'auto-évaluation de l'organisation concernant les aspects de technique, de procédure et d'organisation. L'organisation utilisatrice peut s'en servir pour évaluer les leviers sur lesquels travailler afin d'améliorer sa propre «Readiness» pour son propre Cloud Journey en termes de compétences existantes ou de processus définis par exemple.
Guides en matière d'informatique en nuage	On peut à ce stade imaginer différents documents auxiliaires de moindre ampleur et clos sur les thématiques suivantes: • Guide Cloud Journey dans l'environnement public (p. ex. arbres de décision, etc.) • Guide Objectifs d'affaires Cloud • Guide FinOps
(autres selon les besoins)	-

Les dates individuelles de dépôt des résultats respectifs ne sont pas connues à ce stade.

Les résultats devraient pouvoir être largement appliqués au sein des cercles d'utilisateurs pertinents du secteur public. Le public cible se concentre toutefois sur les décideurs du secteur public dans les projets concernés – par exemple:

- Chief Information Officer (CIO) / Chief Digitalization Officer (CDO) ou équivalent
- Chief Information Security Officer (CISO) ou équivalent
- Président(e)s de conseil municipal / secrétaires de commune
- Direction du projet / Achats / Requirements Engineering
- Enterprise Architects
- Préposé à la protection des données / DPO et service juridique / conseil juridique

Annexe A – Glossaire / abréviations

Terme	Description
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information, France
AWS	Amazon Web Services
BE	Berne
OFIT	Office fédéral de l'information et de la télécommunication
BS	Bâle
BSI	Bundesamt für Sicherheit in der Informationstechnik, Allemagne
CDO	Chief Digitalization Officer
CH	Confoederatio Helvetica / Suisse
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSF	NIST Cybersecurity Framework
DPO	Data Protection Officer
DFAE	Département fédéral des affaires étrangères
PFPDT	Préposé fédéral à la protection des données et à la transparence
DFJP	Département fédéral de la justice et de la police
EPFL	École Polytechnique Fédérale de Lausanne
EPFL	Eidgenössische Technische Hochschule (Zurich)
EU	European Union / Union européenne
EUCS	European Cybersecurity Certification Scheme for Cloud Services
BAC	Base d'aide au commandement
GE	Genf / Genève
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
SCI	IT Security Standard (IKSE), Estonie
ISC	Information Service Center
ISCeco	Information Service Center DEFR / «eco»
ISO	International Organization for Standardization
IT	Information Technology
LE	Fournisseur de prestations
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology, USA
OCSIN	Office Cantonal des Systèmes d'Information et du Numérique, Genève
SG	Saint-Gall
DETEC	Dépt. fédéral de l'Environnement, du Transport, de l'Énergie et de la Communication
UZH	Université de Zurich
VD	Waadt / Vaud
VZGV	Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute
ZH	Zurich

Annexe B – Membres

Membres actuels

Groupe	Organisation	Rôle au sein de l'organisation	Prénom	Nom
Confédération	Chancellerie fédérale	Architecte d'entreprise / experte en transformation numérique	Nina	Gammenthaler
Confédération / Cantons / Communes	Administration numérique Suisse	Coordinateur ICT	Gregorio	Hernan
Cantons	OCSIN GE	Architecte d'entreprise	Olivier	Baujard
Prestataires de services informatiques	Abraxas	Chief Operations Architect	Olaf	Sonderegger
	adesso	Team Tech Advisory	Jesko	Mueller
	adesso	Head CIO Advisory	Jean-Jacques	Pittet

Nouveaux membres

Remarque: la structure ci-dessous ne prétend pas proposer un «organigramme» exact, mais se veut plutôt une liste de personnes susceptibles d'être intéressées par une coopération avec le groupe spécialisé. Les membres peuvent s'impliquer de manière active, mais également en tant que simples membres passifs, en fonction de leurs souhaits et de leurs possibilités – ceci contribue aussi à l'objectif du groupe spécialisé consistant à recueillir un éventail d'opinions aussi large que possible et à diffuser dans les plus brefs délais les livrables aux instances concernées.