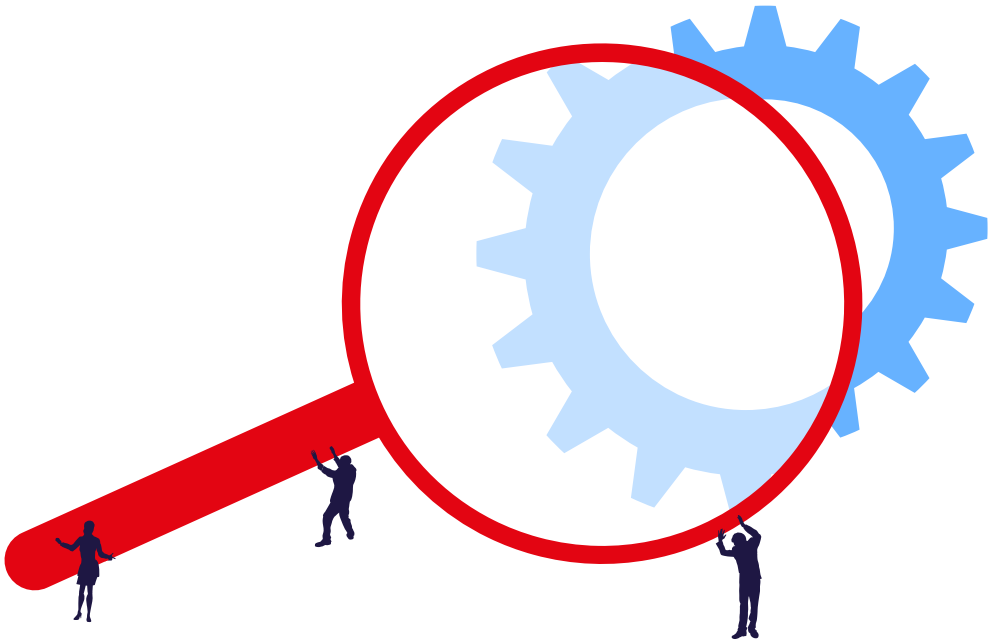
Digitale Verwaltung Schweiz
Administration numérique suisse
Amministrazione digitale Svizzera

Second Source

Étude mandatée par le groupe de travail
Cloud Governance et Workplace
de l'Administration numérique suisse



Avril 2025

ELCA ADVISORY

Second Source – Étude

Classification	aucune
Statut	approuvé pour utilisation
Direction du projet	Olaf Sparka, Erich Hofer
Version	1.0
Date	23 avril 2025
Mandant	Groupe de travail Cloud Governance et Workplace (ANS)
Auteur	ELCA Advisory

ELCA Informatik SA
Flurstrasse 62 | 8048 Zurich
Tél. +41 (0)44 456 32 11 | Fax +41 (0)44 456 32 00
www.elca.ch
Pully | Zürich | Genève | Bern | Basel | Rapperswil-Jona | Italy | Spain | Mauritius | Vietnam

Liste des modifications

Version	Date	Modification	Auteurs
0.1	Novembre 2024	Premier projet des chapitres 1 à 5	Luca Schädler, Nadine Tschichold
0.2	De décembre 2024 au 08.01.2025	Intégration des commentaires de la révision d'Olaf Sparka, compléments au chap. 5, introduction du chap. « Résumé » et des chap. 6 à 10	Luca Schädler, Nadine Tschichold
0.3	Du 9 au 30.01.2025	Intégration des commentaires de la révision concernant les chapitres 6 à 10 suite aux réunions du 09.12.2025 et du 27.01.2025 avec la direction de projet	Luca Schädler, Nadine Tschichold, direction de projet ANS
0.4	Du 30.01.2025 au 14.02.2025	Intégration des commentaires de la révision du groupe de travail et des partenaires d'entretien, et de leur évaluation avec la direction du projet.	Luca Schädler, Nadine Tschichold, direction de projet ANS
0.5	17.02.2025	Intégration des résultats de l'entretien de révision avec la direction de projet du 14.02.2025	Luca Schädler, Nadine Tschichold, direction de projet ANS
0.6	21.02.2025	Corrections linguistiques, envoi pour la révision par la direction opérationnelle de l'ANS	Luca Schädler, Nadine Tschichold
1.0	23.04.2025	Version finale	Nadine Tschichold

Avant-propos

La généralisation de la numérisation au sein de l'administration amène de plus en plus les autorités à se pencher sur des questions concrètes concernant les services en nuage et les aspects de sécurité liés à leur utilisation. Microsoft 365 constitue souvent la principale préoccupation : la plateforme est largement répandue et permet d'optimiser de nombreux processus. Ce type de services comporte toutefois de nouveaux risques, qu'il convient d'analyser et de gérer soigneusement, à l'instar de tous les autres outils informatiques.

Cette étude du groupe de travail Cloud Governance et Workplace aborde trois questions centrales auxquelles les administrations se trouvent confrontées eu égard à l'utilisation des services Microsoft en nuage.

L'étude a pour but de présenter la situation actuelle en toute neutralité et en toute objectivité, et de montrer de manière transparente les domaines qui nécessitent des mesures ciblées pour limiter les risques. Elle met également en évidence les domaines qui pourraient requérir des mesures plus complètes ou coordonnées.

L'étude renonce volontairement à une évaluation des solutions techniques et à une analyse de faisabilité approfondie. Les résultats présentés reposent sur les informations et les données de différents fournisseurs, sur une étude de la Haute école spécialisée bernoise, ainsi que sur l'expertise des auteurs de la présente étude. Ils ont pour but d'offrir une base objective et documentée en vue de travaux complémentaires.

Si la brève enquête menée lors de la diffusion de la présente étude révèle d'autres besoins, le groupe de travail étudiera l'opportunité de les intégrer dans un projet subséquent.

Résumé

La présente étude, réalisée par ELCA Advisory à la demande du groupe de travail « Cloud Governance et Workplace » de l'Administration numérique suisse (ANS), analyse les enjeux majeurs liés aux chances et aux défis découlant de la dépendance de l'administration publique par rapport aux logiciels propriétaires de Microsoft et aux services logiciels, notamment dans le domaine de la bureautique. L'analyse s'appuie sur des entretiens avec des représentants d'institutions publiques ainsi que sur une étude de marché réalisée par le biais de demandes d'information (*request for information*, RFI) adressées à des entreprises ayant leur siège en Suisse ou au sein de l'Union européenne (UE), afin d'assurer le respect de différents cadres juridiques et des exigences en matière de protection des données. L'évaluation et les conclusions de l'étude de marché, ainsi que la définition des prochaines étapes envisagées d'un point de vue technique (p. ex. au chapitre 9), sont le fruit d'une étroite collaboration entre le groupe de travail « Cloud Governance et Workplace » de l'ANS et ELCA Advisory. Les autres mesures recommandées ont quant à elles été élaborées par le groupe de travail de l'ANS, puis intégrées à l'étude.

Les conclusions d'ordre général concernant la souveraineté s'appliquent également à d'autres prestataires et services. Toutefois, la présente étude se concentre spécifiquement sur les services Microsoft 365, qui représentent un enjeu actuel et majeur pour les institutions publiques suisses.

Constats

1. **Grande variété de solutions envisageables**

   Le marché offre des produits intéressants dans le domaine de la bureautique. Des fournisseurs tels que VNCLagoon, InfoManiak, EGroupware et le Centre pour la Souveraineté Numérique (Zentrum Digitale Souveränität ou ZenDiS), détenu par des institutions publiques, travaillent au développement de solutions proposant la même diversité de fonctionnalités que les produits Microsoft. Des projets pilotes prometteurs, comme celui de la Chancellerie fédérale en Suisse, et des initiatives portées par des Länder en Allemagne (p. ex. Schleswig-Holstein), témoignent de l'approche innovante et de la détermination à renforcer la souveraineté numérique dans ce domaine. Ces projets offrent une base solide pour les développements futurs et offrent un éclairage précieux sur les solutions possibles.

2. **Renforcer la résilience au moyen de la gestion de la continuité des services informatiques (IT-SCM)**

   La présente étude montre qu'il existe dans certains domaines des options viables pour améliorer la résilience informatique. En ce qui concerne les conférences audio / vidéo et les services de messagerie électronique, il existe des solutions déployables rapidement si nécessaire, avec toutefois une réduction des fonctionnalités proposées. L'exploitation parallèle et la planification en amont permettent cependant d'augmenter sensiblement la réactivité en cas d'urgence. Même si leur implémentation engendre une charge de travail accrue et des coûts, elle renforce la souveraineté et assure le maintien des fonctions essentielles, également en situation de perturbation. L'étendue des mesures et leur mise en œuvre dépendent de la manière dont chaque institution gère les risques. C'est donc à ces dernières que revient la décision. S'agissant de la poursuite des aménagements et de l'optimisation des mesures, un échange, voire une collaboration coordonnée entre les institutions, serait judicieux.

3. **Transition stratégique et migration**

Si une institution souhaite cesser d'utiliser les services Microsoft et passer à une à une autre solution, elle doit prendre une décision stratégique et politique à ce sujet, être prête à supporter des coûts plus élevés, au moins à court terme, et effectuer une planification à long terme. Les projets pilotes menés jusqu'à présent le montrent : les chances de succès augmentent lorsque les institutions poursuivent des objectifs communs et que des organismes centraux tels qu'eOperations ou l'ANS coordonnent et pilotent les activités. Il conviendrait d'aborder les défis techniques, tels que la migration des applications spécialisées, par des approches coordonnées (p. ex. négociations avec les fournisseurs d'applications spécialisées utilisées dans plusieurs cantons) et des formations ciblées des utilisateurs, et de prendre en considération dès l'acquisition des facteurs comme l'interopérabilité et les normes ouvertes.

Les services actuellement disponibles et en cours de développement nécessitent des compromis et des adaptations sur les services informatiques et applications spécialisées existants, ce qui rend le changement particulièrement exigeant. Leur mise à disposition et la migration requièrent beaucoup de temps et de ressources. Avec l'intégration de nouveaux services de Microsoft (p. ex. Copilot, Power Platform), la transition devient de plus en plus complexe. En agissant de manière isolée, une institution publique devra mobiliser d'importantes ressources et s'expose à des risques élevés. Il convient en outre de ne pas sous-estimer les éventuelles résistances des utilisateurs et utilisatrices finaux par rapport à l'arrivée de services qui pourraient remplacer certaines applications maîtrisées et bien intégrées.

Évolutions positives et perspectives

La présente étude met en évidence les efforts substantiels déjà engagés en faveur de la souveraineté numérique de l'administration publique, ainsi que le travail que mènent de nombreuses institutions pour développer des solutions innovantes en ce sens. Des initiatives telles que le Swiss Government Cloud (SGC) ou la planification centralisée à laquelle s'attellent certains organismes publics démontrent l'existence d'une volonté et de la capacité de réduire la dépendance aux solutions individuelles, l'idée étant de développer des solutions flexibles et évolutives, qui répondent aux exigences des différentes institutions.

Conclusion

Le **renforcement de la souveraineté numérique** n'est pas un processus facile. Les approches ainsi que les actions menées actuellement montrent cependant qu'un tel changement, souhaité par de nombreuses institutions, est réalisable. Toutefois, le renforcement de la souveraineté numérique se traduit non seulement par des coûts d'exploitation plus élevés, mais aussi par une complexité opérationnelle croissante, ce qui renforce encore la nécessité d'une collaboration étroite entre la Confédération, les cantons et les communes ainsi qu'une coordination centralisée, afin de créer des solutions qui soient efficaces, durables et évolutives. Il convient en particulier d'éviter de se retrouver à nouveau en situation de dépendance et d'ouvrir des perspectives sur le long terme.

L'étude permet d'identifier quatre champs d'action principaux à prendre en compte dans le cadre de la transformation et du renforcement de la souveraineté numérique :

- Premièrement, il s'agit du remplacement technique d'applications existantes, de leur exploitation et de leur intégration fluide dans l'infrastructure informatique disponible, ce qui nécessite non seulement des solutions techniques, mais également une très bonne

compréhension des interactions entre les différents services ainsi qu'une intégration dans des applications spécialisées afin d'éviter les pannes ou les pertes de fonctionnalités.
- Deuxièmement, il convient d'examiner les évolutions des services Microsoft afin de pouvoir identifier s'il est opportun de les introduire ou s'il est préférable d'étendre des concepts déjà existants et permettant d'utiliser des solutions alternatives.
- Troisièmement, il est impératif de définir des standards communs (p. ex. les formats Office) pour garantir un développement uniforme et interopérable. Cette démarche est essentielle pour éviter que différents acteurs et utilisateurs ne travaillent dans des directions incompatibles, ce qui générerait à terme trop de complexité et des coûts plus élevés. L'existence de normes communes permet de surcroît une collaboration coordonnée et efficace.
- Quatrièmement se pose la question de l'exploitant, qu'il convient de clarifier d'un point de vue stratégique et à long terme. Le passage d'un prestataire privé à un autre ne résout pas le problème fondamental de la dépendance. En ce qui concerne les logiciels à code source ouvert (*open source software*, OSS), on ignore en outre à quoi pourrait ressembler un modèle d'exploitation pérenne qui garantirait non seulement la fonctionnalité, mais aussi la sécurité et la stabilité nécessaires. Des approches innovantes s'imposent pour assurer un fonctionnement et un développement durables et fiables.

Ces différents champs d'action soulignent la complexité des enjeux, mais offrent également des pistes claires pour une approche stratégique et coordonnée.

Les résultats de cette étude mettent en lumière le fait que les différentes administrations ne seront guère en mesure d'élaborer seules des solutions viables aptes à relever les défis exposés. La complexité des exigences techniques, organisationnelles et juridiques nécessite une collaboration étroite. Un regroupement des acteurs, idéalement au niveau national, voire supranational, par exemple en coopération avec l'UE, est essentiel pour créer des synergies, développer des normes et utiliser efficacement les ressources. Seule une approche coordonnée et globale permettra de parvenir à des solutions durables et souveraines à long terme.

Toutefois, une **solution d'urgence** n'impliquant ni conservation de données, ni migration, ni intégration permettrait de mettre en place et d'exploiter relativement facilement la plupart des services étudiés (même en mode veille). Chaque organisation doit évaluer pour elle-même l'utilité d'un tel environnement, qui garantit UNIQUEMENT une fonctionnalité minimale. Cette solution pourrait par exemple être utile pour des groupes spécialisés plus restreints comme les VIP, une organisation d'urgence, un état-major de crise, des responsables de la communication, etc., afin de pouvoir, avec certaines restrictions, poursuivre les opérations en situation d'urgence tout en limitant les dépenses supplémentaires.

Il convient toutefois de prendre en considération qu'une telle solution d'urgence devient extrêmement complexe et coûteuse dès lors qu'elle implique de conserver ou de synchroniser des données. Une telle mesure serait sans doute malgré tout nécessaire pour permettre à de grands groupes de collaborateurs de poursuivre leurs activités dans des conditions de fonctionnement efficaces et efficientes en situation d'urgence grâce au maintien des processus opérationnels essentiels. Chaque organisation doit donc déterminer, dans le cadre de sa gestion ordinaire des risques, les solutions dont elle a besoin en cas d'urgence et les solutions qu'elle veut et peut se permettre.

Délimitation

La présente étude vise clairement à dresser un état des lieux de la situation actuelle des administrations publiques eu égard aux solutions logicielles et services propriétaires. Elle adopte volontairement une approche globale, afin d'offrir une réelle vue d'ensemble. L'objectif n'était pas de comparer en détail la faisabilité technique ou les différentes solutions ni d'analyser de manière approfondie les raisons de certaines situations ou les options possibles. Il s'agissait au contraire de présenter aux administrations des pistes pour leur permettre d'élaborer des stratégies à long terme.

Table des matières

1 Introduction

L'administration publique suisse est consciente de la dépendance actuelle vis-à-vis des logiciels propriétaires, en particulier des services Microsoft. Cela concerne les solutions de bureautique, de collaboration et de communication telles que MS Office, SharePoint, Teams et Outlook ou Exchange. Le besoin croissant de souveraineté numérique suscite un intérêt grandissant pour les solutions logicielles qui offrent une indépendance à l'égard des fournisseurs individuels.

Le groupe de travail Cloud Governance et Workplace de l'Administration numérique suisse (ANS) a chargé les auteurs de la présente étude d'examiner quels logiciels à code source ouvert (*open source software*, OSS) pourraient constituer une solution de remplacement aux services Microsoft. L'objectif du mandat était d'identifier s'il existe des options crédibles et concrètement envisageables, qui permettraient de réduire la dépendance de l'administration à l'égard des services Microsoft. L'analyse concerne les OSS actuellement disponibles en Europe susceptibles de complètement remplacer les services Microsoft. Deux scénarios se présentent, l'un pour la gestion de la continuité des services informatiques (*IT service continuity management*, IT-SCM) et l'autre pour l'abandon des services Microsoft, qui pourrait être total ou partiel.

La présente étude vise à montrer dans quelle mesure les OSS répondent actuellement aux exigences de l'administration publique et pourraient contribuer à la souveraineté numérique de la Suisse. Les unités administratives en Suisse peuvent s'appuyer sur les résultats de l'étude pour développer leur stratégie de réduction progressive de la dépendance à l'égard des logiciels Microsoft et d'autres solutions propriétaires. Selon les informations reçues en vue de l'étude, l'objectif général pour les administrations est de réduire leur dépendance à l'égard des entreprises privées individuelles et de renforcer ainsi leur souveraineté numérique.

Définitions

La présente étude utilise la notion de « gestion de la continuité des services informatiques » (*IT service continuity management*, IT-SCM) pour mettre l'accent sur les mesures stratégiques visant à assurer la disponibilité des services informatiques en cas de perturbation ou de panne.

- La **gestion de la continuité des activités** (*business continuity management*, BCM) permet de garantir par la planification que l'administration pourra continuer à agir même en cas d'urgence ou de crise. L'objectif est de répondre à la question « De quelle manière pouvons-nous garantir la poursuite de notre travail, quoi qu'il arrive ? ». Par exemple, que faisons-nous en cas de panne totale d'un service informatique, d'incendie d'un bâtiment abritant des bureaux, de déclenchement d'une pandémie ou de survenance d'autres risques ?
- La **gestion de la continuité des services informatiques** (*IT service continuity management*, IT-SCM) fait partie de la BCM, mais concerne spécifiquement les services informatiques et vise à garantir le rétablissement rapide des services informatiques (p. ex. messagerie électronique, téléphonie) en cas de panne. La question qui se pose est « Comment nous assurons-nous que notre système informatique fonctionne même en cas de problème ? ». Par exemple, comment pouvons-nous remplacer temporairement un service informatique défaillant par un autre ?

L'**hypothèse retenue pour la présente étude** en cas de scénario IT-SCM, basée sur les résultats des entretiens menés, vise un rétablissement de la disponibilité des services informatiques en quelques jours (environ une semaine). La durée effective dépend toutefois de l'organisation, des services concernés et de la stratégie de gestion des risques.

2 Objectifs et portée de l'étude

Le projet Second Source a pour but de répondre à différentes questions fondamentales que chaque unité administrative du secteur public doit clarifier si elle souhaite utiliser les services Microsoft en nuage (services Microsoft 365, en particulier les produits de communication et de collaboration). L'étude s'efforce d'élaborer les réponses à ces questions de manière générale et centralisée, afin que toutes les unités administratives du secteur public (en particulier les cantons et les communes) puissent les reprendre et les adapter à leur situation spécifique, idéalement avec un minimum d'éléments supplémentaires à clarifier. L'étude se concentre sur l'examen des questions suivantes :

- Quelles sont les OSS disponibles aujourd'hui pour remplacer les services Microsoft ?
- Quelles sont les solutions permettant de soutenir les services Microsoft, notamment en présence d'un scénario IT-SCM ? Quelles sont les mesures à prendre dès maintenant pour disposer d'une bonne préparation en cas d'urgence ?
- Quelles sont les démarches à entreprendre aujourd'hui pour se préparer à une éventuelle cessation du contrat avec Microsoft (résiliation par l'administration elle-même ou par Microsoft) ?

L'étude a analysé et traité ces questions pour les services Microsoft figurant ci-dessous :

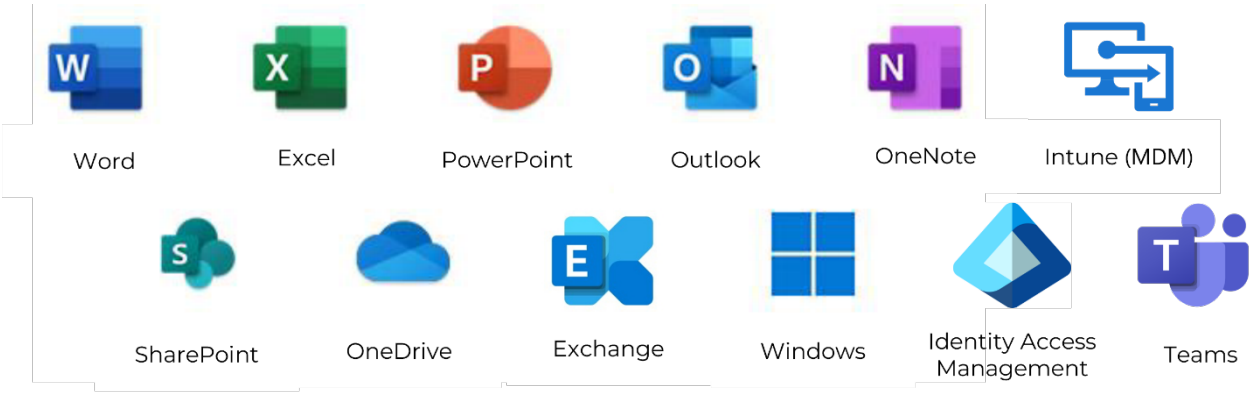


Illustration 1 : services Microsoft faisant l'objet de la présente étude

3 Déroulement et méthodologie

Nous avons opté pour une organisation de projet conforme à HERMES (voir Illustration 2).
Illustration 3 : échéances et activités durant la réalisation de l'étude

donne un aperçu de la planification ainsi que des différents jalons et des activités à chaque étape. La direction du projet et les auteurs de l'étude se sont rencontrés toutes les deux semaines durant l'ensemble de la durée du projet pour des réunions de coordination.

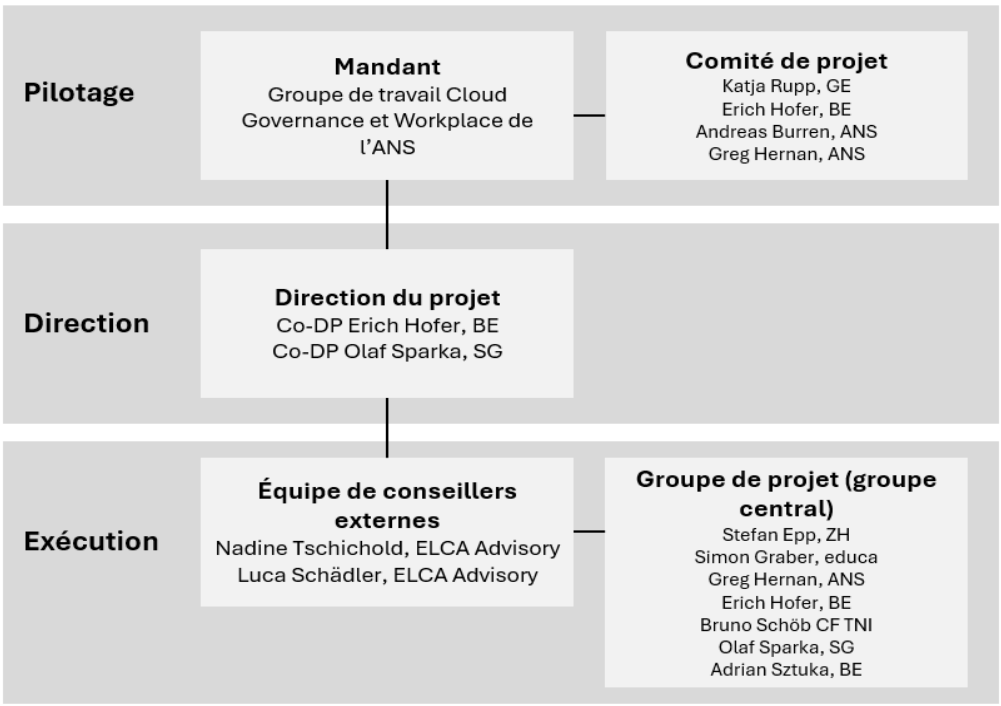


Illustration 2 : organisation du projet pour la réalisation de l'étude

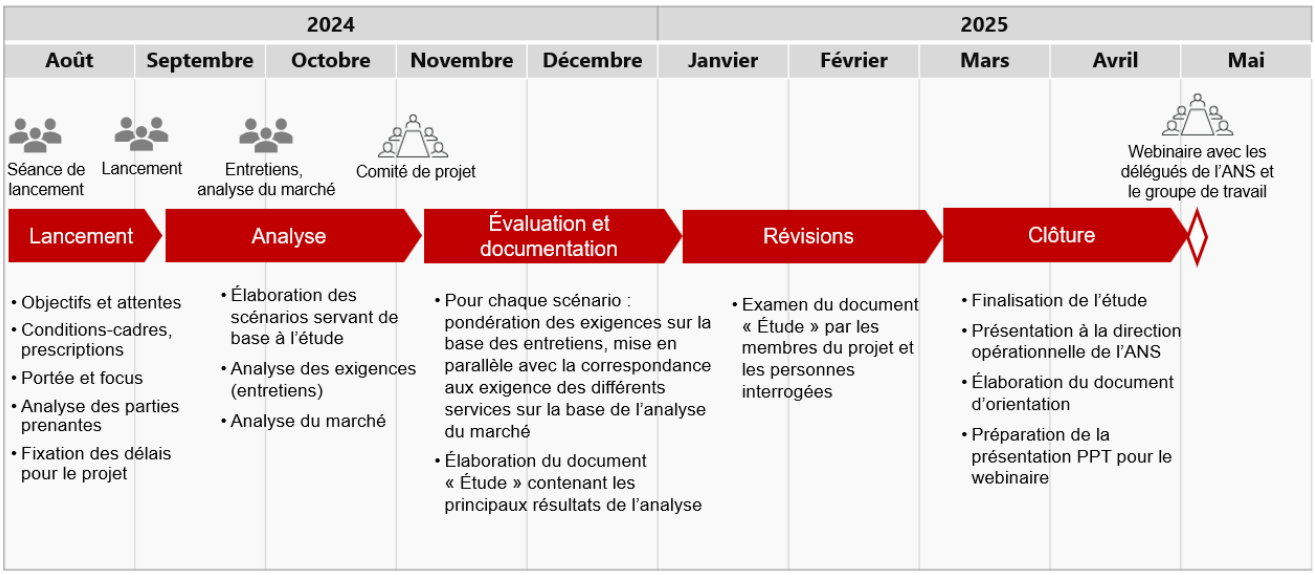


Illustration 3 : échéances et activités durant la réalisation de l'étude

L’étude s’est déroulée selon les étapes suivantes :

- **Identification de solutions** pour aménager l’architecture de manière à inclure des services alternatifs :
  ces solutions offrent différentes possibilités d’intégration des services à l’infrastructure informatique existante de l’administration (voir chap. 5).
- **Collecte des exigences requises** sur la base des deux scénarios (voir chap. 2), auprès de représentants d’unités administratives s’étant portées volontaires :
  la première étape a permis de recenser les exigences des administrations en termes de solutions. Nous avons mené des entretiens avec différents représentants de l’administration publique afin d’identifier les principaux besoins et les priorités. Pour bien comprendre les besoins, nous avons évalué les exigences de manière distincte pour les deux scénarios (IT-SCM et Exit, voir chap. 4) et les avons classées par ordre d’importance pour chacun des scénarios.
- **Étude de marché** au moyen d’un questionnaire écrit auprès de potentiels fournisseurs européens de suites de produits complètes et de prestataires de services individuels pour des solutions *frontend* et *backend* :
  nous avons invité les fournisseurs à évaluer la conformité de leurs solutions aux exigences spécifiques et à confirmer les informations générales disponibles sur leurs produits.
- **Comparaison des résultats de la collecte des exigences avec ceux de l’étude de marché** :
  lors de la dernière étape, nous avons comparé les résultats de la collecte des exigences aux résultats de l’étude de marché.

Délimitation

Il est important de préciser que l’étude ne contient pas de recommandations concrètes de mise en œuvre ni de solutions et qu’elle ne vérifie pas non plus la faisabilité technique des solutions. Elle n’évalue pas non plus les OSS et ne les compare pas. Au contraire, l’étude se limite à fournir une vue d’ensemble des solutions actuellement disponibles et à les comparer avec les exigences collectées dans le cadre des entretiens avec des représentants de différents cantons et communes.

4 Scénarios étudiés

Le présent chapitre décrit les deux scénarios à envisager, soit « IT-SCM » et « Exit ». Ils suivent des approches distinctes et fixent des priorités différentes eu égard aux exigences relatives aux logiciels (ouverts) envisageables.

4.1 Scénario « IT-SCM »

Ce scénario se concentre sur la préparation à une indisponibilité inattendue des produits Microsoft (scénario d'urgence). Ce type de défaillance peut résulter d'incidents techniques imprévus, de changements politiques ou réglementaires ou de menaces pour la sécurité. L'IT-SCM vise à assurer la continuité et la stabilité des services informatiques critiques lors de la survenance d'une situation d'urgence de ce type. Il s'agit d'identifier les exigences qui ont une importance cruciale dans le cadre d'un scénario IT-SCM et que les produits de remplacement doivent donc impérativement respecter.

Ce scénario part du principe que des contraintes externes impliqueront de remplacer temporairement les services Microsoft dans des délais très serrés. La stratégie IT-SCM intervient donc pour garantir le bon fonctionnement des services informatiques critiques. De plus, le monde VUCA[*] dans lequel nous évoluons actuellement ne permet plus de se reposer sur l'existence de dispositions contractuelles. Les organisations doivent anticiper les risques et prendre les mesures qui s'imposent pour garantir la continuité des services informatiques, même dans des situations imprévues.

4.2 Scénario « Exit »

Ce scénario envisage une transition planifiée de l'utilisation des services Microsoft vers des solutions OSS. Il vise un remplacement progressif et structuré des services Microsoft afin de réduire la dépendance vis-à-vis des solutions logicielles propriétaires (notamment de Microsoft). L'intégration de Copilot dans différents services Microsoft ainsi que les problèmes de protection des données qui en découlent peuvent par exemple mener les institutions publiques à résilier ces services, si les nouvelles conditions deviennent incompatibles avec les exigences.

Ce scénario se concentre sur l'identification de produits appropriés qui répondent aux besoins spécifiques de l'administration publique. Étant donné que ce scénario ne présente pas de contraintes externes ni de délais serrés, il est possible de le planifier et de prévoir une mise en œuvre progressive. Toutefois, pour que les utilisateurs acceptent les solutions proposées, celles-ci devront offrir la même qualité que les services Microsoft actuels, ainsi que des fonctionnalités comparables, voire plus intéressantes, afin de répondre pleinement aux besoins de l'administration.

[*] L'acronyme VUCA signifie volatilité (*volatility*), incertitude (*uncertainty*), complexité (*complexity*) et ambiguïté (*ambiguity*). Il décrit les défis dynamiques et souvent imprévisibles auxquels se voient confrontés les entreprises et les dirigeants dans le monde moderne.

Remarque : si Microsoft devait résilier ses services, la plupart des institutions seraient confrontées à des difficultés extrêmes, car le délai de résiliation minimal est de six mois seulement. Il est donc important de définir en amont des mesures appropriées et de prendre des dispositions pour qu'un changement soit possible, même s'il implique des restrictions.

5 Options étudiées

Dans le cadre de cette étude, nous présentons trois options qui illustrent la manière dont l'architecture peut être conçue avec des OSS.

5.1 Variantes d'architecture

Les illustrations ci-après présentent les différentes options.

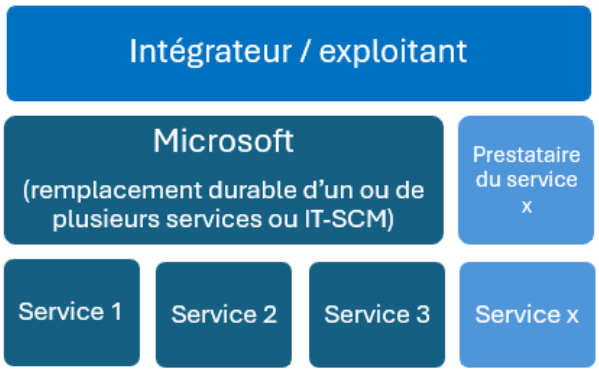


Illustration 4 : option 1 « Architecture hybride »

Architecture hybride :

analyse de produits individuels (en bleu clair) comme options de remplacement de certains services. Évaluation de la possibilité de les intégrer dans l'infrastructure informatique existante, par l'intermédiaire d'une entreprise tierce ou par des prestations de l'administration à l'interne.

Illustration 5 : option 2 « Architecture avec plusieurs fournisseurs »

Architecture avec plusieurs fournisseurs :

les services de différents prestataires couvrent toutes les fonctionnalités des services Microsoft. Ce scénario combine plusieurs solutions pour fournir les fonctionnalités requises. L'intégration de ces services peut se faire aussi bien par des fournisseurs externes que par des ressources internes.

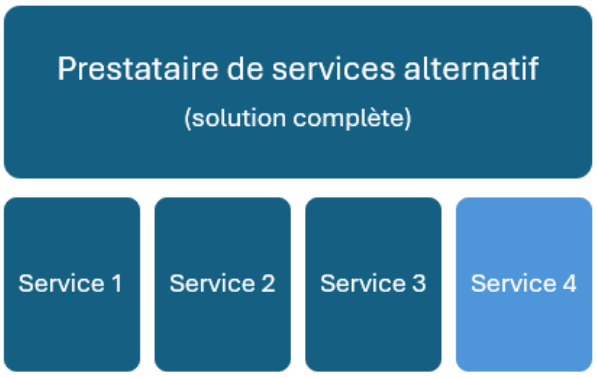


Illustration 6 : option 3 « Architecture avec un seul fournisseur »

Architecture avec un seul fournisseur :

un seul et même prestataire couvre toutes les fonctionnalités des services Microsoft. Si nécessaire, il peut également intégrer des services de prestataires tiers, mais en assume alors la responsabilité.

5.2 Comparaison des différentes options

Caractéristique / critère	Architecture hybride	Architecture avec plusieurs fournisseurs	Architecture avec un seul fournisseur
Nombre de fournisseurs	Un seul ou plusieurs	Plusieurs	Un seul
Responsabilité de l'intégration des produits	Responsabilité propre ou d'entreprises tierces (pas Microsoft)	Responsabilité propre ou d'entreprises tierces	Prestataire
Flexibilité et adaptabilité	Élevées, en raison du choix sélectif d'alternatives aux solutions Microsoft, restrictions possibles par l'intégrateur / l'exploitant	Très élevées, avec possibilité de choisir les meilleures solutions	Limitées, car tous les services proviennent d'un seul fournisseur
Charge de travail pour l'intégration	Moyenne à élevée, car l'intégration du service en question n'est pas effectuée par Microsoft	Très élevée, car intégration de plusieurs solutions	Faible, car le fournisseur livre la solution
Complexité	Moyenne, en raison du besoin d'intégration	Très élevée, car nécessite la coordination de nombreux fournisseurs et l'intégration individuelle de chaque solution	Faible, car centralisation de tous les services
Dépendance vis-à-vis du prestataire	Faible à moyenne grâce à une solution hybride	Faible, car diversification des prestataires	Très élevée, car prestataire unique
Évolutivité à long terme	Élevée, grâce à une adaptation et une intégration progressives	Très élevée, car possibilité d'intégrer de nouveaux prestataires de manière flexible	Moyenne, car le prestataire n'est potentiellement pas en mesure de couvrir toutes les exigences futures

Tableau 1 : comparaison des différentes options

Chaque architecture présente des avantages, qu'il convient de pondérer en fonction des objectifs stratégiques de l'organisation et de sa disposition à prendre des risques.

5.3 Critères pour le choix des options

Différents critères permettent d'évaluer les options envisagées.

Les principaux critères sont :

1. **Adéquation :** la solution ou l'architecture de service doit correspondre aux exigences et processus spécifiques de l'administration et être en mesure de faire preuve de flexibilité face aux changements légaux ou organisationnels.
2. **Coûts :** en plus des coûts d'acquisition, les coûts de maintenance, de licence et de support à long terme doivent être pris en considération, afin de garantir la rentabilité de la solution en termes de coût total de possession (*total cost of ownership*, TCO).
3. **Exigences techniques :** les produits utilisés doivent être stables, fiables et compatibles avec les systèmes existants et supporter les normes ouvertes afin de garantir l'interopérabilité et l'efficience.
4. **Évolutivité à long terme :** la conception de la solution doit permettre de répondre de manière flexible aux besoins futurs liés à l'augmentation du nombre d'utilisateurs et des volumes de données, ainsi qu'aux nouvelles exigences techniques sans devoir procéder à des changements majeurs.
5. **Ressources et connaissances disponibles :** la solution repose sur les ressources humaines et techniques disponibles, complétées au besoin par de la formation et un soutien externe, afin de garantir une exploitation fiable et la mise en œuvre des développements nécessaires.
6. **Convivialité :** une interface conviviale facilite l'accès, réduit les besoins en formation ainsi que les erreurs et améliore l'efficience.
7. **Acceptation par l'utilisateur :** un accueil favorable des collaborateurs renforce la productivité et simplifie l'intégration des nouvelles solutions.
8. **Sécurité :** des contrôles d'accès et des mécanismes de protection contre les cybermenaces sont nécessaires pour garantir la sécurité des données sensibles.
9. **Protection des données :** l'architecture doit respecter les règles de protection des données et offrir des mécanismes sûrs et transparents pour protéger les données personnelles.
10. **Souveraineté :** l'indépendance à l'égard des différents fournisseurs est essentielle pour préserver la souveraineté numérique et le contrôle sur les données et les systèmes.

6 Identification des exigences

Les auteurs ont mené des entretiens avec les administrations publiques afin d'obtenir une vue d'ensemble complète des exigences et d'évaluer leur pertinence en lien avec des solutions potentielles. Les personnes consultées ont en outre été invitées à évaluer séparément l'importance de ces exigences dans les deux scénarios envisagés (IT-SCM et Exit), afin de pouvoir traiter de manière ciblée les besoins tout en tenant compte de la pertinence des diverses exigences en fonction des scénarios.

6.1 Démarche

L'analyse des exigences s'est déroulée comme suit :

1. **Recensement des exigences applicables aux services Microsoft** : les exigences techniques applicables aux services Microsoft ont été établies sur la base de recherches documentaires. Les auteurs ont ensuite généralisé ces exigences et les ont résumées sous une forme moins technique afin de permettre leur évaluation du point de vue de la gestion.
2. **Définition des exigences applicables aux fournisseurs** : les auteurs ont défini une liste d'exigences afin de pouvoir prendre en compte dans l'étude les caractéristiques pertinentes des potentiels fournisseurs de solutions (voir chap. 7.5).
3. **Recrutement des participants à l'analyse des exigences** : l'appel à participer à l'analyse des exigences a été émis dans le cadre de la journée « Cloud et Workplace » de l'ANS du 29.08.2024durant laquelle ont été présentés les objectifs de l'étude, son déroulement et sa teneur. Un deuxième appel à participation est intervenu par courriel le 23.09.2024. Toutes les parties intéressées ayant répondu ont été incluses dans les entretiens (voir Tableau 2).
4. **Préparation et réalisation de l'analyse des exigences** : l'analyse des exigences a pris la forme d'entretiens en ligne. Les listes d'exigences (voir points 1 et 2), préalablement adressées aux répondants, ont été retournées remplies avant les entretiens. Ces derniers ont permis de discuter les exigences, d'en déterminer l'importance pour les personnes consultées et de recueillir leurs commentaires le cas échéant. Certaines exigences ont fait l'objet de discussions approfondies, notamment celles dont l'importance était perçue de manière particulièrement variable.
5. **Consolidation des résultats** : l'annexe A [1] présente les résultats des entretiens sous forme consolidée et indique l'importance des diverses exigences selon chaque répondant. Les auteurs ont résumé les commentaires émis durant les entretiens.

Parties prenantes	Inclusion dans le projet	Représentation	Entretiens
Administration numérique suisse	Mandant	Groupe de travail Cloud Governance et Workplace	Pas d'entretien, uniquement conception de l'analyse des exigences, y c. passage en revue de la liste d'exigences
Cantons	• Canton de Bâle-Ville • Canton des Grisons • Canton du Tessin • Canton de Genève • Canton d'Appenzell Rhodes-Extérieures	• Urs Bühler (BL) • Reto Rauch & Mirko Demarmels (GR) • Rudi Belotti (TI) • Katja Rupp (GE) • Christoph Schwalm (AR)	• 17.10.24 • 16.10.24 • 21.10.24 • 16.10.24 • 16.10.24
Communes	• Ville de Zurich	• Werner Kipfer (ville de ZH)	• 17.10.24

Tableau 2 : parties prenantes et personnes consultées

6.2 Contenu

L'analyse des exigences se répartit en plusieurs domaines thématiques, qui couvrent les exigences essentielles applicables aux services Microsoft considérés :

- **système d'exploitation** ;
- **IAM** (gestion des utilisateurs et LDAP) ;
- **bureautique** ;
- **messagerie** ;
- **stockage de données et collaboration** (p. ex. Teams, SharePoint) ;
- **communication** (p. ex. chat, audioconférences, vidéoconférences) ;
- **gestion des appareils mobiles** (MDM) ;
- **exigences indépendantes des solutions** (convivialité, UI, UX, etc.) ;
- **téléphonie** ;
- **bureautique RAS / VDI.**

6.3 Résultats des entretiens

Les résultats des entretiens recensés dans le tableau 2 ont été rassemblés dans un classeur Excel (voir annexe A [1]).

La première partie des entretiens servait à recueillir des informations sur des sujets d'ordre général. Le Tableau 3 contient un résumé des réponses à ces questions.

Dans la deuxième partie des entretiens, les répondants ont classé l'importance des exigences applicables aux divers services Microsoft. Les avis recueillis quant au délai dans lequel la solution doit devenir opérationnelle dans le scénario IT-SCM varient énormément. Certains mentionnent une période de deux semaines. D'autres estiment qu'un bref délai n'est guère réaliste et envisagent des périodes allant jusqu'à 48 mois, argumentant qu'une solution définitive nécessite d'être évaluée, intégrée et implémentée et qu'il faudrait y former l'ensemble des collaborateurs.

Les participants tendaient nettement à accorder une moins grande importance aux exigences en matière de fonctionnalités des services dans le scénario IT-SCM. Cela s'explique par le fait que, dans un tel scénario, les services informatiques doivent rester à disposition et que l'on accepte de faire des concessions sur certaines exigences. Certains participants ont également argumenté que, puisqu'il s'agit d'une phase de transition plutôt que d'une solution définitive, certaines exigences peuvent temporairement ne pas être respectées.

Dans le scénario Exit en revanche, la plupart des exigences étaient jugées comme très importantes. Cela se comprend puisqu'une solution ne satisfaisant pas aux exigences, ou qui ne propose qu'une partie des fonctionnalités requises, ne sera pas acceptée.

Avancement des travaux dans les unités organisationnelles	
Plans relatifs à l'évaluation ou au remplacement de Microsoft 365	Environ la moitié des personnes consultées est en train d'étudier des alternatives à Microsoft 365 ou prévoit de le faire. L'autre moitié ne voit pas de nécessité de compléter ou de remplacer Microsoft 365 par d'autres solutions.
Importance d'avoir des solutions pour atténuer la dépendance	Une majorité estime qu'il est « important » ou « en partie important » de développer des solutions afin d'atténuer la dépendance par rapport à Microsoft. Seule une minorité estime qu'il n'est pas nécessaire d'agir sur ce plan. Certains participants ont aussi mentionné que des membres de gouvernements cantonaux exigent l'élaboration d'une stratégie de type Exit en cas d'introduction de Microsoft 365 dans le canton.
Gestion de la continuité des services informatiques (*IT Service Continuity Management*, IT-SCM)	
Importance d'une stratégie IT-SCM en lien avec Microsoft 365	Une grande majorité reconnaît l'importance d'avoir une stratégie IT-SCM en lien avec Microsoft 365, même si le degré de maturité stratégique varie. Certains cantons ont déjà mis des stratégies en œuvre, d'autres n'en traitent que certains aspects.
Utilisation d'alternatives à Microsoft 365	Certains cantons emploient des alternatives afin d'atténuer les dépendances, p. ex. des logiciels ouverts. Le degré de satisfaction à l'égard de ces solutions varie. Les utilisateurs constatent souvent qu'elles n'équivalent pas à Microsoft en termes de catalogue de fonctionnalités ou de stabilité.

Stratégie Exit pour Microsoft 365	
Abandon de Microsoft 365	Seuls quelques-uns des participants ont élaboré des stratégies Exit concrètes ou envisagé de le faire. Il n'y a dans la plupart des cas pas d'options ou de partenaires définis qui pourraient prendre le relais de Microsoft 365. Il s'agit plutôt de compléter Microsoft 365 que de le remplacer entièrement.
Mesures politiques et réglementaires	
Initiatives en matière de souveraineté numérique	Des initiatives politiques visant à remettre en question la dépendance aux services Microsoft et à renforcer la souveraineté numérique ont été lancées dans quelques cantons et communes. Elles visent souvent à promouvoir plus fortement les logiciels ouverts ou à mettre en place de prescriptions réglementaires pour l'utilisation des services en nuage.
Mesures de renforcement de la souveraineté numérique	Certains cantons et communes misent de manière ciblée sur l'utilisation de logiciels ouverts. Ces derniers jouent toutefois globalement un rôle mineur. La plupart des mesures de renforcement de la souveraineté numérique en sont à leurs prémisses.
Mesures réglementaires en lien avec Microsoft 365	Bien que des mesures réglementaires et politiques en lien avec l'utilisation de Microsoft 365 aient été prises dans certains cas, leur gestion et leur mise en œuvre varient.

Tableau 3 : résumé des réponses aux questions d'ordre général

7 Analyse de marché

L'analyse de marché (voir l'annexe A [1]) a permis d'établir une vue d'ensemble de diverses solutions à code source ouvert pour remplacer les produits Microsoft.

7.1 Démarche

Une première étape a consisté, au moyen de recherches exhaustives sur Internet, à identifier les solutions ouvertes qui pourraient remplacer les services Microsoft et à établir une liste des divers fournisseurs ainsi que des services qu'ils proposent. En parallèle, les auteurs ont élaboré la liste des exigences applicables aux services Microsoft, qui a été mise au point avec des représentants de certains cantons et de certaines communes dans le cadre des entretiens.

Dans la seconde étape, une sélection de fournisseurs s'est vu adresser la liste d'exigences dans le cadre d'une demande d'information (r*equest for information* ; RFI) et a été invité à y répondre sous 3 semaines (du 30.10 au 18.11.2024). Le chapitre 7.3 présente en détail les critères et délimitations pour la sélection des entreprises.

Dans le cadre de l'analyse de marché structurée (voir l'annexe A [1]), les entreprises ont indiqué dans quelle mesure leurs services satisfont aux diverses exigences. Les auteurs ont mis ces indications en relation avec l'importance accordée aux exigences selon les entretiens effectués.

7.2 Structure de l'analyse de marché

L'analyse de marché repose sur un catalogue de questions structuré comme suit :

- **Catégories de produits :**
  - solutions complètes (suites) ;
  - solutions spécifiques pour le *backend* ;
  - solutions spécifiques pour le *frontend*.
- **Fonctionnalités :**
  - gestion des utilisateurs ;
  - services de bureautique et de messagerie intégrés ;
  - solutions de communication et de vidéoconférence ;
  - fonctions de collaboration (p. ex. gestion des documents, gestion de contenu, gestion des connaissances) ;
  - fonctions de messagerie instantanée ;
  - gestion des appareils mobiles (MDM) répondant aux exigences actuelles du travail.
- **Informations sur les fournisseurs :**
  - nom du produit ;
  - nom du fournisseur ;
  - adresse Internet ;
  - pays d'origine du fournisseur ;
  - disponibilité du code source du produit ;
  - modèles de mise à disposition (p. ex. SaaS ou sur site [*on-premises]*) ;
  - systèmes d'exploitation pris en charge.

7.3 Sélection des fournisseurs pour l'analyse de marché

Les auteurs ont utilisé les critères suivants pour sélectionner les entreprises interrogées dans le cadre de la demande d'information :

- offre de solution complète* ;
- logiciels à code source ouvert ;
- siège en Suisse ou dans l'UE.

Cette étude se concentre sur les suites (option 3 du chap. 5.1), autrement dit les produits complets et intégrés. Les autres variantes, basées sur des solutions individuelles, ont déjà été examinées dans les études de la Haute école spécialisée bernoise (voir les annexes [B1] et [B2]). Le *Land* allemand Schleswig-Holstein a élaboré une description détaillée de la stratégie pour le choix d'une telle approche ainsi qu'une variante de solution à plusieurs fournisseurs (voir l'annexe [B3]).

La présence du siège de l'entreprise en Suisse ou dans l'UE est importante, en particulier pour garantir le respect du cadre juridique spécifique et des exigences en matière de protection des données.

Le Tableau 4 présente les entreprises interrogées et leurs produits. Certaines d'entre elles n'ont pas répondu à la demande d'information (voir le tableau 4) et la qualité des renseignements fournis varie.

Entreprise	Produit	Réponse reçue le
Virtual Network Consult (VNC) AG	VNCLagoon	14.11.2024
ZenDiS GmbH	openDesk	04.02.2025
Infomaniak Group SA	kSuite	19.12.2024
EGroupware GmbH	EGroupWare	11.11.2024
Hostpoint AG	Solution de courriel et de bureautique	Aucune réponse reçue

Tableau 4 : liste des entreprises interrogées et de leurs produits

Le centre de souveraineté numérique (*Zentrum Digitale Souveränität*, ZenDiS GmbH) a répondu avec beaucoup de retard. L'entreprise est submergée de demandes, surtout en Allemagne, ce qui entraîne de longs délais de réaction.

Les entreprises Hostpoint et Unblu ont également été contactées dans le cadre de la demande d'information. Hostpoint n'a jamais répondu et Unblu a expressément indiqué ne pas souhaiter répondre.

7.4 Caractéristiques des services

Les services proposés doivent répondre aux exigences et réglementations spécifiques du secteur public tout en étant viables sur le plan économique à court et à long terme. Les principales caractéristiques à étudier incluent les suivantes :

- **Catalogue de fonctionnalités :** les solutions logicielles doivent satisfaire aux exigences actuelles et futures de l'administration publique et proposer les fonctionnalités de base des produits Microsoft.
- **Modèle de mise à disposition (Saas, sur site)** : les modèles SaaS sont évolutifs et permettent des implémentations rapides ; les modèles sur site offrent plus de contrôle, mais sont souvent plus onéreux.
- **Protection des données et sécurité de l'information (nuage privé / dédié)** : ces modèles de service offrent une sécurité élevée et respectent les normes en matière de conformité, p. ex. les lois sur la protection des données et la sécurité de l'information.
- **Code source ouvert** : il permet la transparence et l'indépendance, encourage les adaptations réalisées par la communauté *open source* et la souveraineté en matière de données.
- **Modèle de licence** : un modèle de licence clair est important pour pouvoir calculer les coûts de manière transparente et planifier un budget à long terme.
- **Prestations** : pour entrer en ligne de compte, l'offre doit impérativement inclure les prestations de services nécessaires, telles que l'intégration et la configuration des logiciels, des prestations de support et une assistance générale aux utilisateurs.
- **Coûts d'exploitation** : l'exploitation doit pouvoir être financée sur le long terme.
- **Modèle de contrat** : le contrat doit offrir une certaine flexibilité pour prévenir la dépendance et les coûts imprévus.

7.5 Caractéristiques des entreprises

Afin de pouvoir prendre une décision informée quant à l'utilisation de solutions informatiques, il faut non seulement analyser les produits, mais également évaluer les caractéristiques des fournisseurs potentiels. Celles-ci éclairent sur la capacité des entreprises proposant les solutions à garantir une collaboration durable et fiable, à répondre aux exigences à venir et à suivre l'évolution de la technologie.

Les caractéristiques pertinentes des fournisseurs comprennent les suivantes :

- **Siège de l'entreprise et projets** : le lieu où se trouve l'entreprise a des incidences sur la protection des données et la conformité. Les projets tels qu'un déménagement peuvent affecter le cadre juridique et la disponibilité des services.
- **Taille de l'entreprise** : la taille de l'entreprise renseigne sur les ressources à disposition pour faire évoluer les produits et services ainsi que pour le support.
- **Sécurité sur le marché** : la stabilité économique de l'entreprise est importante pour éviter les risques d'insolvabilité et les répercussions potentielles d'une telle situation sur la continuité des services.
- **Dépendance par rapport au fournisseur** : une trop grande dépendance peut devenir un facteur de risque capital. La possibilité d'influencer la conception des services et des solutions utilisés est un facteur important, qu'il convient de prendre en compte dans les négociations avec les fournisseurs.
- **Clientèle** : une base de clientèle importante et stable, comprenant idéalement des acteurs du secteur public, démontre que la solution a fait ses preuves en pratique et correspond aux exigences de l'administration.

Un autre facteur essentiel est la taille et le niveau d'activité de la communauté *open source*. Plus cette communauté est importante et partage des normes définies en commun, et plus les entreprises y participant activement sont nombreuses, moins le client est dépendant par rapport

à des fournisseurs spécifiques. Cela permet aux institutions publiques comme les cantons ou les communes d'obtenir des prestations de la part de plusieurs entreprises et de changer plus facilement de fournisseur si nécessaire.

7.6 Résultats de l'analyse de marché

Le tableau 5 ci-dessous résume les résultats de l'analyse de marché sur la base des retours des entreprises interrogées. Le degré auquel les solutions satisfont aux exigences posées résulte des indications des fournisseurs de solutions. Aucune vérification n'a été effectuée sur ce point.

Le tableau indique également le nombre d'exigences entièrement satisfaites par chaque groupe d'exigences.

Groupe d'exigences	Degré auquel les exigences sont satisfaites			
	EGroupware	VNCLagoon	kSuite	openDesk
Exigences indépendantes de la solution	**Majoritairement** (5 sur 9 entièrement)	**Presque entièrement** (8 sur 9 entièrement)	**Presque entièrement** (8 sur 9 entièrement)	**Presque entièrement** (7 sur 9 entièrement)
Bureautique	**Majoritairement** (3 sur 5 entièrement)	**Presque entièrement** (4 sur 5 entièrement)	**Presque entièrement** (4 sur 5 entièrement)	**Entièrement**
Messagerie (courriels)	**Majoritairement** (2 sur 4 entièrement)	**Entièrement**	**Presque entièrement** (3 sur 4 entièrement)	**Presque entièrement** (3 sur 4 entièrement)
Collaboration	**Majoritairement** (2 sur 4 entièrement)	**Entièrement**	**Entièrement**	**Entièrement**
Système d'exploitation	**En partie** (1 sur 4 entièrement, 3 en partie)	**Presque entièrement** (3 sur 4 entièrement)	**En partie** (1 sur 4 entièrement, 3 en partie)	**Majoritairement** (2 sur 4 entièrement)
Clients	**En partie** (0 sur 2 entièrement, 1 en partie)	**Majoritairement** (1 sur 2 entièrement)	**En partie** (0 sur 2 entièrement, 2 en partie)	**Majoritairement** (1 sur 2 entièrement)
IAM	**En partie** (1 sur 6 entièrement, 4 en partie)	**Entièrement**	**Entièrement**	**Presque entièrement** (5 sur 6 entièrement)
RAS / VDI **Accès à distance et virtualisation**	**En partie** (0 sur 2 entièrement, 2 en partie)	**Entièrement**	**En partie** (0 sur 2 entièrement, 1 en partie)	**En partie** (0 sur 2 entièrement, 1 en partie)

Groupe d'exigences	Degré auquel les exigences sont satisfaites			
	EGroupware	**VNCLagoon**	**kSuite**	**openDesk**
Gestion des appareils mobiles	**Néant**	**Entièrement**	**Entièrement**	**Ne fait pas partie d'openDesk**
Téléphonie	**En partie** (2 sur 7 entièrement, 3 en partie)	**Majoritairement** (3 sur 7 entièrement)	**En partie** (2 sur 7 entièrement)	**Ne fait pas partie d'openDesk**

Tableau 5 : degré auquel les exigences des divers groupes d'exigences sont satisfaites

Les résultats détaillés de l'analyse de marché se trouvent à l'annexe A [1], qui met en relation les exigences et leur importance, d'une part, et le degré auquel les différentes solutions y satisfont, d'autre part.

Bilan : aucune des entreprises interrogées ne propose une solution qui satisfasse entièrement à tous les groupes d'exigences. Il n'est donc pas possible, à l'heure actuelle, d'implémenter une solution complète sans compromis.

Observations côté client :

Du côté du client, la difficulté réside dans le fait que ce dernier privilégiera des solutions standardisées afin de réduire le travail nécessaire pour les adaptations individuelles et la personnalisation. Le but est de créer des solutions homogènes ne donnant pas lieu à une prolifération de versions différentes, pour diminuer la complexité dans la mise en œuvre et l'exploitation. Cela implique toutefois un travail de coordination plus important et la création de normes intercantonales (p. ex. normes eCH) afin de réduire le besoin d'adaptations spécifiques pour chaque canton.

Observations côté fournisseurs :

Du côté des fournisseurs, il s'agit de vérifier si ces derniers sont en mesure de traiter simultanément les exigences de plusieurs cantons et de mettre à disposition les ressources nécessaires pour le support et des projets d'implémentation. L'absence de normes intercantonales constitue un défi particulier : chaque canton demande des adaptations spécifiques, ce qui accroît considérablement la charge de travail des fournisseurs. Il faut garantir que les fournisseurs soient capables non seulement d'assurer la mise en œuvre technique, mais aussi qu'ils garantissent un support et une prise en charge fiables sur le long terme.

8 Aperçu des solutions Open Source alternatives à Microsoft

Question : quels logiciels ouverts actuellement disponibles peuvent remplacer les services Microsoft ?

Variante à fournisseur unique (architecture *single vendor*)

L'analyse de marché (voir le chap. 7) a montré qu'il existe en principe diverses solutions à code source ouvert à même de remplacer les services Microsoft. Cependant, aucune de ces alternatives ne couvre l'ensemble des fonctionnalités des services Microsoft correspondants. Certains fournisseurs se sont toutefois fixé comme objectif l'équivalence fonctionnelle entre leurs produits et l'offre Microsoft. On peut citer à titre d'exemple le ZenDiS, qui appartient entièrement à des institutions publiques allemandes. La Chancellerie fédérale a lancé le projet pilote « PoC BOSS » (étude de faisabilité d'un logiciel à code source ouvert pour la bureautique) afin d'évaluer l'adéquation et la performance des services proposés par ZenDis avec son produit openDesk.

Certains *Länder* allemands mènent également leurs propres initiatives, par exemple Schleswig-Holstein. La stratégie élaborée (voir l'annexe [B3]) consiste à remplacer les services Microsoft par des solutions à code source ouvert. Un projet de mise en œuvre de cette stratégie a déjà démarré.

Ces initiatives montrent clairement que, malgré les lacunes actuelles, des efforts accrus sont déployés pour renforcer la souveraineté numérique et mettre en place des solutions de remplacement.

Variante à plusieurs fournisseurs (architecture *multi vendor*) et variante hybride

Les études de la Haute école spécialisée bernoise (voir les annexes [B1] et [B2]) fournissent une vue d'ensemble des alternatives aux services Microsoft tels que les services d'annuaire, le stockage de données, la messagerie, la collaboration, le *webmail*, la bureautique en ligne, la synchronisation de données PIM et la communication (*unified communication*). Ces études révèlent aussi qu'il est impossible de satisfaire entièrement aux exigences pour tous les services. Il serait possible, en principe, d'optimiser la solution globale en jouant sur le catalogue de certains services, mais cela demanderait beaucoup de travail pour l'intégration et augmenterait les risques d'exploitation (voir le chap. 5.2).

Bilan : il n'existe actuellement sur le marché aucune solution à code source ouvert complète qui pourrait se substituer entièrement aux services Microsoft. Même les solutions spécifiques correspondant à des services Microsoft particuliers n'assurent pas entièrement la même fonctionnalité et leur implémentation demande un surcroît de travail considérable. Toutefois, le marché connaît actuellement une évolution dynamique que l'actualité politico-technique vient encore accélérer. Les initiatives du ZenDis et d'autres entreprises poursuivent des approches prometteuses en vue du développement, à long terme, d'alternatives souveraines et performantes aux services Microsoft, permettant de répondre aux besoins de manière durable.

Du côté du client, la difficulté consiste à ce que ce dernier privilégiera des solutions standardisées afin de réduire le travail nécessaire pour les adaptations individuelles. Le but est de créer des solutions homogènes ne donnant pas lieu à une prolifération de versions différentes, pour diminuer la complexité dans la mise en œuvre et l'exploitation. Cela suppose

également de créer des normes intercantonales (p. ex. normes eCH) pour réduire le besoin d'adaptations spécifiques pour chaque canton et assurer une meilleure acceptation.

Du côté des fournisseurs, il s'agit de vérifier si ces derniers sont en mesure de traiter simultanément les exigences de plusieurs cantons et de mettre à disposition les ressources nécessaires pour le support et des projets d'implémentation. Le faible niveau de normalisation entre les cantons constitue un obstacle important : chaque canton demande des adaptations spécifiques, ce qui accroît considérablement la charge de travail des fournisseurs. Il est donc important que les fournisseurs soient capables non seulement d'assurer la mise en œuvre technique, mais aussi qu'ils proposent un support fiable et une prise en charge continue sur le long terme afin de garantir une implémentation et une exploitation durables des solutions.

Un autre aspect à prendre en compte est l'existence et la mise à contribution d'une communauté *open source* correspondante. Idéalement, cet aspect serait géré conjointement par les fournisseurs et l'administration publique / des représentants des institutions publiques.

9 Continuité des services TI au moyen de solutions open source

Question : quelles sont les possibilités à disposition pour compléter les services Microsoft par des solutions à code source ouvert, en particulier dans le contexte d'une gestion de la continuité des services informatiques (IT-SCM) ?

La liste exemplative de services alternatifs n'est pas exhaustive et repose sur les résultats des études de la Haute école spécialisée bernoise (voir les annexes [B1] et [B2]). Les scénarios envisagés se rapportent principalement à la défaillance d'un service. Or, il est aussi possible que plusieurs services soient indisponibles simultanément, et ce point doit être pris en compte dans la planification.

Dans chaque cas IT-SCM, il appartient à l'équipe d'urgence de vérifier quels services sont concernés afin de pouvoir mettre en place des mesures appropriées pour rétablir l'exploitation.

Dans le cadre d'une stratégie IT-SCM, il est possible de compléter certains services Microsoft par des solutions à code source ouvert afin d'assurer la disponibilité et la résistance aux défaillances des services informatiques. Deux approches sont envisageables :

- **Exploitation en parallèle** : les services Microsoft et les solutions à code source ouvert sont exploités en parallèle, les données étant synchronisées en continu. Les deux solutions sont implémentées de manière qu'en cas de défaillance de l'une, l'autre puisse prendre le relais immédiatement ou en l'espace de quelques heures. Cette approche garantit une disponibilité continue des services et réduit la dépendance à l'égard d'un fournisseur unique.
- **Mise à disposition (*standby*)** : les services à code source ouvert sont mis à disposition de manière à pouvoir être activés en cas d'urgence, moyennant une certaine charge de travail. Il peut s'avérer nécessaire, en cas d'urgence, de travailler sans avoir accès à toutes les données ou de récupérer au préalable les données à partir d'un système de sauvegarde.

Le Tableau 6 fournit une vue d'ensemble des mesures IT-SCM. Les mesures à court terme sont celles pouvant être déployées en l'espace de quelques jours en cas de défaillance d'un service. Les mesures durables doivent avoir été mises en œuvre et intégrées au préalable afin de pouvoir être activées en cas de défaillance.

Service	Mesure IT-SCM à court terme	Mesure IT-SCM durable
Gestion des identités et des accès (IAM)	Aucune	Utilisation d'un méta-annuaire pour la gestion des identités des utilisateurs ou utilisation de plusieurs produits alternatifs pour les fonctionnalités d'Active Directory
Clients (panne du système d'exploitation)	Aucune	Mise à disposition d'un nombre limité de clients dotés de systèmes d'exploitation alternatifs

Service	Mesure IT-SCM à court terme	Mesure IT-SCM durable
Messagerie	Envoi / réception de nouveaux courriels dans un système alternatif	Exploitation parallèle d'un autre service de messagerie avec synchronisation des courriels
Gestion des appareils mobiles (MDM)	Aucune	Préparation de l'introduction d'un produit de MDM tiers indépendant
Gestion de système	Aucune	Impossible d'exploiter en parallèle un système alternatif Préparation de l'introduction d'un produit de gestion de système tiers indépendant
Services d'accès à distance / infrastructure de bureau virtuel (RAS / VDI)	Aucune	Abandon du travail à distance lors d'un scénario IT-SCM ou préparation de l'introduction d'un produit RAS / VDI tiers indépendant
Applications de bureautique	Utilisation de services de remplacement Condition : encore possible d'accéder aux données (données saisies locales)	Synchronisation des fichiers du nuage sur les clients
Collaboration et stockage des données	Utiliser des fichiers locaux Condition : les données sont disponibles dans des formats standardisés.	Configurer le système de manière qu'une copie locale des fichiers soit enregistrée sur le client
Communication (chat, audio / vidéo) sans téléphonie	Utilisation de services de remplacement	Service alternatif exploité durablement (canal de communication supplémentaire)
Téléphonie	Utilisation de services de remplacement (p. ex. aussi via téléphonie mobile) Condition : les données de contact sont encore disponibles	Déviation des appels sur les téléphones mobiles ; garantir la disponibilité des téléphones mobiles

Tableau 6 : vue d'ensemble des mesures IT-SCM

Les chapitres suivants décrivent les mesures IT-SCM possibles pour les divers services.

Bilan : des installations en parallèle peuvent compenser une défaillance de certains services Microsoft (p. ex. les courriels). Toutefois, un tel fonctionnement est en général très coûteux en ressources. De plus, il existe des services pour lesquels des installations en parallèle sont impossibles et une mise à disposition rapide de solutions de remplacement n'est guère réaliste (p. ex. MDM).

Une analyse approfondie basée sur la gestion des risques est décisive pour déterminer quels services sont essentiels pour les opérations, quels sont les risques en cas de défaillance, quelles sont les mesures à prendre et quelles concessions en termes de fonctionnalité sont acceptables. Il est impossible de couvrir l'ensemble des services sans restriction.

Il faut déterminer en amont les services et fonctionnalités devant impérativement être maintenus et les pertes de fonctionnalités tolérables. Cela implique aussi d'estimer dans quel délai les solutions de substitution doivent être à disposition et les ressources financières et temporelles qu'il est possible d'y affecter.

Un plan clair pour l'organisation et la formation du personnel, ainsi que pour la gestion des changements de manière globale, est indispensable pour pouvoir introduire et utiliser les solutions alternatives de manière efficiente. Pour permettre le maintien des activités également lors de situations exceptionnelles, il faut fixer l'ordre de priorité des services et définir les mesures sur la base des résultats des analyses en matière de gestion des risques.

9.1 Gestion des identités et des accès

Problématique :

La gestion des identités et des accès (*Identity & Access Management*, IAM) est essentielle pour gérer les accès aux systèmes et aux outils. En raison de ce rôle central, une panne du système IAM bloque l'accès à des applications et services importants, ce qui peut entraîner des conséquences graves pour l'exploitation.

En substance :

Des mesures sont déjà possibles pour réduire la dépendance par rapport à Active Directory (AD). Une option est d'utiliser un méta-annuaire d'un autre fournisseur exploité indépendamment d'AD qui reprend les fonctionnalités IAM. Cependant, s'affranchir entièrement de la dépendance par rapport à AD nécessite également le remplacement de ses autres fonctions (voir chap. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Prochaines étapes :

- Architecture spécifique aux cantons :
  un déploiement spécifique de l'architecture au niveau cantonal, qui vise à réduire au minimum la dépendance par rapport à AD et Entra ID (le pendant d'AD dans le nuage Microsoft), devrait garantir que les services IAM restent fonctionnels également en cas de défaillance d'AD ou d'Entra ID dans le cadre de scénarios IT-SCM.
- Analyse des services critiques :
  chaque unité organisationnelle devrait vérifier lesquels de ses services sont critiques, en particulier ceux accessibles via une authentification unique (*Single Sign-On*, SSO).

- Autres méthodes d'authentification :
  il faudrait déterminer, pour tous les services, s'il existe d'autres méthodes d'authentification possibles en cas de défaillance du SSO. Il faudrait ensuite tester les caractéristiques de sécurité de ces alternatives et leur adéquation pratique.
- Développement de stratégie :
  chaque institution devrait développer, sur la base des résultats de ces vérifications, une stratégie claire visant à assurer le fonctionnement des services critiques aussi en cas de défaillance.

Dans un environnement Microsoft, la gestion des identités et des accès passe par AD ou, dans le nuage Microsoft, par Entra ID. AD est un « annuaire » qui joue un rôle essentiel dans les réseaux Windows. Le service est également utilisé pour administrer les appareils et d'autres ressources réseau de manière centralisée.

Il n'existe aucune solution de substitution à Entra ID. En cas de défaillance, il ne sera plus possible d'accéder aux services en nuage de Microsoft.

En principe, il est possible de réduire la dépendance par rapport à AD pour ce qui est de la fonctionnalité IAM en recourant à un autre produit en tant que « méta-annuaire ». Les utilisateurs et les groupes, les mots de passe, l'authentification, le contrôle des accès et les autorisations seraient alors gérés dans ce méta-annuaire séparé et AD synchroniserait les données nécessaires. Cela entraînerait différents effets en fonction du scénario de défaillance :

- Défaillance du méta-annuaire : AD peut continuer à remplir les fonctions IAM avec les données à disposition, mais sans les actualiser (p. ex. à la suite de modifications des droits ou de mutations d'utilisateurs), afin d'éviter que les modifications ne soient écrasées lors de la réactivation du méta-annuaire.
- Défaillance d'AD : les services IAM demeurent disponibles. L'accès à l'ensemble des applications et services indépendants d'AD reste possible grâce au méta-annuaire.

Il n'est toutefois pas possible de mettre en œuvre une solution de ce type rapidement. Il faudrait concevoir, planifier et implémenter l'architecture de l'environnement d'exploitation en conséquence et le produit alternatif devrait fonctionner dans cet environnement en permanence. Cela occasionnerait des coûts supplémentaires de licence et d'exploitation pour ce service complémentaire et accroîtrait la complexité de l'architecture globale. De plus, cela engendrerait une nouvelle dépendance.

Les alternatives à code source ouvert à la fonction IAM d'AD sont plutôt limitées. Exemples :

- OpenLDAP est une implémentation à code source ouvert du protocole LDAP, qui propose un service d'annuaire ouvert pour la gestion des données d'utilisateurs, des groupes et d'autres ressources. Une intégration complète d'OpenLDAP nécessiterait toutefois des outils et extensions complémentaires, car les possibilités pour gérer des objets informatiques et des stratégies de groupe ne sont pas aussi complètes qu'avec AD.
- FreeIPA (*Identity, Policy, and Audit*) est une solution à code source ouvert pour la gestion des identités et des accès, axée sur les plateformes Linux et Unix. Elle repose sur des technologies comme LDAP, Kerberos et DNS et reflète bon nombre des fonctions d'AD. En revanche, FreeIPA est conçu principalement pour les environnements basés sur Linux / Unix. S'il est en principe possible de l'intégrer dans des environnements Windows, l'implémentation ne sera pas aussi aisée qu'avec AD.
- Univention Corporate Server (UCS) avec Nubus est une solution IAM à code source ouvert basée sur LDAP, Kerberos et SAML, qui permet d'administrer de manière centralisée les

utilisateurs et ressources et prend en charge les scénarios de nuages hybrides ainsi que l'intégration dans les environnements Linux et Windows. UCS ne propose toutefois pas toutes les fonctionnalités d'AD, notamment pour ce qui est des stratégies de groupe.
- D'autres solutions comme Red Hat Identity Management (idM) ou Okta sont conçus pour des environnements spécifiques (idM pour Linux, Okta pour la gestion d'identité dans le nuage). Ces solutions ne sont que partiellement adaptées au remplacement complet d'AD.
- Il faudrait encore examiner si AGOV (le service d'authentification des autorités suisses) pourrait être employé en tant que solution IAM complète au sein des institutions publiques.

Il est donc possible en théorie d'utiliser un service alternatif pour IAM, mais une activation rapide n'est pas réaliste. La solution devrait être exploitée en continu, soit en tant que complément, soit en tant que substitut à AD.

9.2 Applications de bureautique

Problématique :

Dans de nombreuses organisations, la disponibilité des applications de bureautique Microsoft Office est essentielle pour pouvoir traiter des documents. Une défaillance de ces applications peut ainsi fortement compromettre les processus de travail. De plus, certaines applications spécialisées recourent aux fonctions d'Office.

En substance :

Bien que des alternatives à Microsoft Office existent, elles présentent des problèmes de compatibilité et des déficits de fonctionnalité. Dans un scénario IT-SCM, les produits alternatifs pourraient être utilisés malgré les restrictions. Il ne sera toutefois pas possible de remplacer rapidement les fonctions d'Office dans les applications spécialisées. Dans le scénario IT-SCM, il faudrait renoncer à l'utilisation de ces fonctions dans les applications spécialisées, voire à toute utilisation de ces applications. Pour éviter de créer de nouvelles dépendances, il faudrait vérifier, à chaque publication d'une nouvelle version de l'offre Microsoft, quelles nouvelles fonctions il convient d'introduire.

Prochaines étapes :

- convenir pour les documents d'une norme ouverte commune à toutes les institutions publiques au sens d'une norme eCH (p. ex. format Open Document) ;
- examiner les options de remplacement de Microsoft Office ;
- concevoir les modèles de documents Office de façon simple afin qu'ils puissent être utilisés aussi dans les produits de bureautique alternatifs ;
- éviter en général les fonctions complexes telles que les macros dans les documents ;
- étudier les possibilités d'utiliser les applications spécialisées sans fonctionnalités Office ;
- configurer Microsoft 365 pour qu'il enregistre systématiquement les fichiers en local sur les clients, afin d'en garantir la disponibilité dans le cadre d'un scénario IT-SCM.

Si les applications Microsoft Office devaient ne plus être disponibles, il existe plusieurs solutions permettant de traiter les fichiers Office (p. ex. les fichiers Word, Excel ou PowerPoint). Les exemples de suites à code source ouvert incluent OnlyOffice, LibreOffice et OpenOffice. Une autre

option est Softmaker Office, surtout grâce à sa bonne compatibilité. Ce logiciel est toutefois sujet à licence et non ouvert.

Toutes les variantes nécessitent de mettre les services à disposition sur un serveur. Il faudrait donc les exploiter continuellement, en parallèle à Microsoft Office, pour qu'ils puissent rapidement prendre le relais dans une situation d'IT-SCM.

Il existe également des substituts disponibles dans le nuage, sans installation sur des serveurs, dont des solutions à code source ouvert comme Collabora, OnlyOffice et des services commerciaux comme Google Workspace, utilisable au moyen d'un compte utilisateur chez Google. Un tel service commercial de Google peut représenter une option pour un casIT-SCM. Toutefois, le passage à un autre service commercial entraînerait les mêmes défis que l'utilisation des services Microsoft, notamment en matière de protection des données.

Cependant, toutes les alternatives à Microsoft Office présentent des restrictions en termes de compatibilité avec les fichiers Microsoft (souvent au format Open XML). S'il est possible en règle générale d'importer et de traiter les fichiers Microsoft au sein d'autres produits, l'opération inverse pose souvent plus de problèmes (surtout pour les fonctions supplémentaires comme les commentaires, le suivi des modifications, etc.). Pour les fonctions avancées comme les macros et les formules complexes, la comptabilité est généralement perdue. Il faut en outre vérifier si les produits alternatifs permettent d'utiliser les modèles de documents existants.

Dans une situation IT-SCM, il est crucial que l'accès aux fichiers demeure garanti. Pour cela, Microsoft 365 doit être configuré de manière à les enregistrer systématiquement sur les clients en plus du nuage. Cela permet d'accéder aux données en local et de les traiter dans un service web, pour autant que le client fonctionne encore et qu'il soit encore possible d'accéder à Internet.

Un autre défi est la gestion des fonctions de MS Office dans les applications spécialisées (p. ex. générer des documents). Dans le scénario IT-SCM, des mesures à court terme sont impossibles, car il faudrait implémenter des adaptations dans les applications spécialisées concernées. Dans certains cas, ces applications peuvent être utilisées sans les fonctions MS Office ; dans le reste de cas, il faudrait renoncer à leur utilisation.

9.3 Messagerie

Problématique :

Une défaillance du service de messagerie de Microsoft affecte non seulement la communication par courriel, mais aussi la gestion des calendriers et des contacts. Faute d'accès aux calendriers et aux contacts, il est impossible d'agender des discussions ou de coordonner des délais, ce qui entraîne des retards et nuit à l'efficience du travail. Dans les organisations publiques, cela complique la communication interne et externe et compromet la productivité ainsi que la confiance prêtée à l'organisation.

En substance :

Plusieurs possibilités existent dans l'éventualité d'une défaillance du service de messagerie de Microsoft : utiliser un service de substitution et utiliser les données locales d'Outlook pour une communication restreinte, exploiter un autre service de messagerie en parallèle ou recourir à la duplication (*mirroring*).

Prochaines étapes :

- évaluer de manière détaillée les variantes évoquées compte tenu de thématiques comme les courriels de groupe, les filtres antispam, la prise en charge des étiquettes (p. ex.

confidentiel, public) et leur traitement, l'intégration des applications spécialisées, l'infrastructure centrale du système de messagerie (*backbone*) ;
- vérifier si une solution de substitution pourrait être basée exclusivement sur navigateur ou si elle doit aussi être disponible hors ligne, ce qui nécessiterait de l'installer sur les clients ;
- tester la solution retenue de manière détaillée au moyen d'une installation pilote.

En cas de défaillance du service de messagerie, il est possible de recourir à un autre service que celui de Microsoft. Il faudra décider si ce service doit être à la disposition de tous les utilisateurs ou non.

Les variantes suivantes existent s'agissant des services de messagerie :

Variante 1) La variante la plus simple consiste à **mettre à disposition des comptes de messagerie vides** d'un fournisseur tiers.

- Dans le scénario IT-SCM, il faut dévier les courriels entrants vers le fournisseur tiers (la solution concrète dépend de l'emplacement où est exploité le *backbone*, p. ex. un service de déviation de Swisscom).
- Deux variantes existent pour l'envoi de courriels :
  - Le client Outlook est disponible et il contient l'ensemble des courriels, adresses, entrées de calendrier, etc., sur le terminal local, car la synchronisation avec le nuage était activée en permanence (état des données à la dernière synchronisation avant la défaillance). Dans ce cas, il est possible d'utiliser le service d'un fournisseur tiers. Les données nécessaires (p. ex., adresses de courrier électronique) et les anciens messages ne seront disponibles que dans le client Outlook local, mais pourront être utilisés manuellement pour maintenir la correspondance par courriel.
  - Le client Outlook n'est pas disponible ou ne contient aucune donnée, car celles-ci n'étaient enregistrées que dans le nuage. Dans ce cas aussi, il est possible de recourir à un service de messagerie d'un fournisseur tiers. En revanche, les possibilités seront fortement limitées faute de données d'adresses et d'historique des messages. Si les utilisateurs enregistrent des copies d'archivage des courriels en local, celles-ci donnent accès à une quantité restreinte de données.

Variante 2) La deuxième variante consiste à **mettre à disposition un environnement de messagerie parallèle d'un fournisseur tiers**. Les courriels sont systématiquement envoyés aux deux adresses. Le point important est que le contenu du carnet d'adresses soit également disponible dans le service de substitution. Remarques :

- Les courriels de l'environnement de substitution seraient tous visibles dans la boîte de réception. Les dossiers définis par les utilisateurs dans Outlook ne seraient pas reproduits.
- Ce deuxième environnement devrait avoir une certaine capacité (comme l'environnement de production Exchange), avec les coûts correspondants. Il faudrait définir des règles de suppression des courriels dans l'environnement de substitution (p. ex. tous les courriels remontant à plus de 12 mois) afin d'assurer la capacité nécessaire.

Variante 3) La troisième variante est un **service de *mirroring***, qui consiste à synchroniser constamment sur une plateforme secondaire tout le contenu de la boîte de réception, y compris les dossiers et le carnet d'adresses, à l'aide d'un outil spécifique (p. ex. Quest). En cas de défaillance du service de courriel, les utilisateurs peuvent travailler comme d'habitude dans l'environnement alternatif. Les fonctions de calendrier seraient aussi disponibles. Cette solution est la plus confortable pour les utilisateurs, mais elle est lourde à opérer et onéreuse. Dans un scénario IT-SCM, il faut maintenir la duplication et dévier les courriels entrants sur le service alternatif. La remigration dans l'environnement standard à l'issue de la situation IT-SCM nécessite une planification soigneuse et devrait être pratiquée au moyen d'exercices.

9.4 Stockage de données et collaboration

Problématique :

Teams et SharePoint proposent de nombreuses fonctionnalités qui forment la base pour la collaboration au quotidien dans la plupart des institutions.

En substance :

Il est possible de remplacer SharePoint pour le stockage de données dans le scénario IT-SCM. Pour que les données soient disponibles en local sur le PC, la synchronisation doit être activée dans SharePoint. Dans ce cas, les données sont automatiquement enregistrées en local et restent à disposition au cas où SharePoint devient inaccessible. En outre, il faudrait au préalable enregistrer les données les plus importantes en cas d'urgence (p. ex. classeurs de crise) dans un stockage alternatif et les maintenir à jour afin qu'elles soient disponibles de manière centralisée dans un scénario IT-SCM.

Il n'existe pas de solutions à code source ouvert substituables rapidement aux autres fonctions de SharePoint (p. ex. implémentation de flux de travail).

Il est possible de remplacer rapidement Microsoft Teams par un autre service de collaboration, mais il faut garder à l'esprit que les conversations et d'autres données ne seront plus accessibles et que les données figurant dans le service de remplacement ne pourront pas être transférées dans Teams.

Prochaines étapes :

- vérifier si les lignes directrices de l'organisation autorisent l'enregistrement de copies des données en local sur les clients ;
- mettre les données pertinentes en situation IT-SCM à disposition sur un stockage alternatif ;
- garantir les accès aux groupes d'utilisateurs concernés ;
- tester la transition de Teams vers un service de stockage ou de collaboration alternatif et former le personnel afin de prévenir les complications en situation IT-SCM.

9.4.1 Stockage de données dans SharePoint

L'option de synchronisation doit être activée en permanence dans SharePoint afin de maintenir l'accès aux données dans un scénario IT-SCM. Dans ce cas, les documents sont enregistrés en local sur le client et synchronisés automatiquement, c'est-à-dire que chaque modification apportée aux fichiers (y compris hors ligne) est reproduite (dès que les fichiers sont à nouveau accessibles en ligne). Ainsi, les fichiers seraient disponibles en local sur les terminaux et utilisables

hors ligne dans un scénario IT-SCM. Il faut toutefois vérifier au préalable si les lignes directrices de l'organisation autorisent l'enregistrement de copies locales sur les clients.

Les utilisateurs pourraient par exemple échanger des fichiers entre eux par courriel. Cela permettrait au moins de collaborer sur un fichier à plusieurs de manière séquentielle.

Il serait aussi possible d'assurer l'échange de fichiers entre utilisateurs et la collaboration sur des documents au moyen d'une plateforme à code source ouvert (p. ex. Nextcloud) si une telle solution est mise à disposition dans le contexte d'un scénario IT-SCM. Les utilisateurs pourraient travailler en simultané sur les fichiers dans des solutions bureautiques comme Collabora ou OnlyOffice. Nextcloud propose aussi la synchronisation des fichiers sur les clients locaux. Les fichiers modifiés dans l'intervalle seraient ainsi automatiquement synchronisés dès que SharePoint redeviendrait accessible. La compatibilité complète de ces documents avec Microsoft Office n'est toutefois pas garantie.

SharePoint est également intégré à Teams en tant que stockage de données. Cette fonctionnalité de Teams ne fonctionnera plus en cas de défaillance de SharePoint.

Il faudrait enregistrer au préalable les données les plus importantes en cas d'urgence (p. ex. classeurs de crise) dans un stockage alternatif afin qu'elles soient disponibles de manière centralisée dans un scénario IT-SCM. Il faut impérativement veiller (par des mesures organisationnelles et techniques) à ce que ces données soient maintenues à jour.

9.4.2 Mise à disposition d'informations et collaboration SharePoint

SharePoint est souvent employé pour mettre à disposition des informations sur des sites web (notamment dans le cadre de de l'implémentation d'Intranet). On l'utilise également pour la collaboration dans le cadre de projets (p. ex. gestion des tâches). Une autre fonctionnalité populaire est l'automatisation de flux de travail.

Il existe des plateformes à code source ouvert comme Nextcloud qui proposent des fonctionnalités similaires. Dans le cas d'un scénario IT-SCM, il n'est toutefois pas possible de mettre à disposition l'environnement SharePoint sur une autre plateforme sans passer par une migration qui demanderait passablement de travail.

9.5 Communication (chat, audio / vidéo, sans téléphonie)

Teams est utilisé entre autres pour la communication par chat, audioconférence et vidéoconférence. Pour les fonctions de SharePoint intégrées à Teams, voir le chapitre 9.4. Il est en principe possible, dans un scénario IT-SCM, de proposer rapidement des alternatives à code source ouvert aux utilisateurs (p. ex. Matrix, Jitsi Meet ou Rocket.Chat). Bien que n'offrant pas le même éventail de fonctionnalités que Teams, ces solutions sont suffisantes dans un tel cas.

Il est possible d'exporter l'historique des discussions de Teams, mais pas de les importer sur les plateformes alternatives.

Les salles de conférence dotées d'une identité Teams doivent être reconfigurées manuellement, ce qui n'est pas envisageable dans un scénario IT-SCM.

9.5.1 Déploiement rapide d'un service de communication

En cas de défaillance de Microsoft Teams, il est possible de déployer rapidement un service de communication à code source ouvert. Ces substituts présentent toutefois d'importantes

restrictions et ne sont pas équivalents à Teams (p. ex. faute d'intégration au système IAM). Les variantes pour une utilisation à court terme sont les suivantes :

- **Le client Microsoft Teams est disponible et il contient l'historique des discussions et les données de configuration, enregistrées en local sur le terminal.**

  Dans ce cas, des solutions à code source ouvert comme **Big Blue Bottom**, **Matrix** ou **Jitsi Meet** permettent de maintenir la communication par chat et vidéoconférence. Les historiques de discussions et les conversations ne seront accessibles que dans le client Teams et ne pourront pas être transposés dans la solution de remplacement, mais les utilisateurs pourront consulter les informations dans Teams et, si nécessaire, les reporter manuellement.
  Cette variante permet de maintenir la communication en temps réel, mais pas d'assurer l'intégration avec les autres services Microsoft (p. ex. SharePoint) ni de poursuivre les conversations menées dans Microsoft Teams. En outre, elle implique la mise en place d'un nouvel environnement avec des liens et une configuration distincts pour les vidéoconférences et la communication en groupes.
  À l'issue de la situation IT-SCM, il faudrait réintégrer toutes les conversations dans Microsoft Teams, ce qui n'est possible que de manière restreinte par des moyens manuels. Cette variante s'accompagne donc de nombreux désavantages en pratique.

- **Le client Microsoft Teams n'est pas disponible ou ne contient aucune donnée.**

  Dans ce cas, il est également possible de recourir à une solution comme **Big Blue Button**, **Matrix** ou **Jitsi Meet**, mais l'utilisation sera fortement restreinte faute d'historique des discussions et de données de configuration. Les utilisateurs pourront lancer de nouvelles conversations et vidéoconférences par le biais de la nouvelle plateforme, mais n'auront pas accès à l'historique, aux structures de groupe et aux listes de contacts.
  Les utilisateurs qui ont enregistré localement des notes ou des documents avec des informations importantes en matière de communication pourront les utiliser pour faciliter la transition. La fonctionnalité de la solution alternative restera néanmoins restreinte, car il ne sera pas possible d'utiliser entièrement l'infrastructure existante et les contacts de l'environnement Microsoft.

Les deux variantes permettent de maintenir temporairement la communication, mais sont assorties de restrictions pour tout ce qui va au-delà de la pure communication audio et vidéo. La perte de l'historique des discussions et l'absence d'intégration aux systèmes existants impliquent certaines difficultés. De plus, un travail manuel est nécessaire dans le cas où il faut assurer la traçabilité des communications au retour dans l'environnement Microsoft à l'issue de la situation IT-SCM.

9.5.2 Exploitation d'un service de communication en parallèle

L'exploitation en parallèle d'une solution de communications unifiées peut présenter des avantages, par exemple pour des scénarios d'utilisation ou des niveaux de confidentialité différents. Il existe plusieurs alternatives efficientes à Microsoft Teams implémentables rapidement, surtout s'il est possible de renoncer à une intégration complète et à l'historique des discussions. Des solutions de vidéoconférence ou des canaux de communication efficaces sont également à disposition.

Une exploitation parallèle exige un examen, car elle est associée à une certaine charge administrative. Il faut notamment :

- configurer et maintenir deux systèmes simultanément ;
- administrer deux profils d'utilisateur et structures d'autorisations, ce qui peut donner lieu à des droits d'accès incohérents et engendrer des failles de sécurité ;
- surmonter les défis techniques liés à la synchronisation et à la migration fiables des données (telles que les messages et les procès-verbaux d'appels) si cela est nécessaire et souhaité.

De plus, les collaborateurs doivent s'approprier un autre outil de communication et le deuxième système donne lieu à des coûts de licence supplémentaires.

9.6 Téléphonie avec Teams

Problématique :

La joignabilité par téléphone se heurt à des défis, surtout dans l'éventualité de pannes du réseau fixe et de l'infrastructure téléphonique centrale. Cela concerne aussi bien la communication interne que les appels extérieurs des partenaires et clients. Il faut préparer des scénarios de panne et mettre en place des canaux de communication de substitution.

En substance :

L'infrastructure de communication doit être conçue de manière que les services et personnes importants restent joignables en cas de panne du réseau fixe ou des solutions de téléphonie centrales. Cette préparation nécessite des téléphones mobiles de service, la téléphonie par IP et des solutions redondantes.

Prochaines étapes :

- Examiner la mise à disposition de téléphones mobiles de service :
  il faut déterminer quels collaborateurs disposent déjà d'un téléphone mobile de service et lesquels devraient en être équipés en plus afin de garantir qu'ils soient joignables.
- Utilisation de téléphones IP :
  il faut vérifier dans quelle mesure des téléphones IP entrent en ligne de compte comme alternatives pour assurer que les principaux numéros de l'organisation restent joignables.
- Mise en place d'infrastructures redondantes :
  il faut analyser s'il est possible d'exploiter en parallèle une infrastructure redondante afin de garantir une communication ininterrompue en cas de panne.

Les réflexions exposées dans ce chapitre partent du principe que l'administration utilise une instance de Teams intégrant la téléphonie. Autrement dit, la plupart des utilisateurs utilisent un numéro fixe et reçoivent les appels dans Teams, mais une centrale séparée gère le numéro principal et les centres d'appel, etc. Les auteurs admettent en outre que les appels sont acheminés vers la centrale, un centre d'appels ou Teams par un opérateur de téléphonie (p. ex. Swisscom) et ne parviennent pas directement à Microsoft.

Pour garantir la continuité de la capacité de communication, il est essentiel de mettre à disposition des alternatives pour divers scénarios de panne des systèmes de téléphonie. Les mesures suivantes fournissent une vue d'ensemble structurée des actions possibles dans trois domaines majeurs : les numéros fixes, le numéro principal et la centrale téléphonique.

9.6.1 Ligne fixe

Il est possible de configurer le service de l'opérateur de téléphonie mentionné de manière qu'un appel soit dévié sur un autre numéro si un numéro fixe particulier n'est pas joignable.

- **Déviation sur des téléphones mobiles :**

  Ce genre de déviation centrale permet à tous les collaborateurs dotés de téléphones mobiles de service de rester joignables sur ces derniers. Il faut que la déviation puisse être activée rapidement et de manière automatisée, ou qu'elle soit active aussi en temps normal. Un rappel depuis le téléphone mobile de service ne serait toutefois plus associé au numéro fixe.

- **Utilisation de solutions d'audioconférence / vidéoconférence :**

  Il est possible, moyennant des coûts de licence supplémentaires, de configurer des solutions comme **Matrix**, **Zoom**, **Webex** ou **Jitsi Meet** de manière qu'elles soient joignables via le réseau de téléphonie public, soit via les numéros fixes existants, soit par d'autres numéros à définir librement. Dans ce dernier cas, il ne serait pas possible d'utiliser le numéro fixe initial pour le rappel.

9.6.2 Numéro principal (joignabilité centrale)

Dans le contexte décrit ci-dessus, le numéro principal est exploité par une centrale téléphonique qui ne passe pas par Teams et ne serait donc pas concernée en cas de défaillance de Microsoft. La transmission interne des appels serait néanmoins entravée en raison de la rupture du canal de communication entre le numéro principal et le numéro de la personne à joindre au sein de l'administration.

- **Utilisation de téléphones IP** ou de *softphones* (logiciels de téléphonie) :

  En cas de panne du réseau fixe, il est possible d'utiliser des téléphones IP afin d'assurer que le numéro principal reste joignable au moyen d'une connexion Internet. Ces appareils devraient être connectés de manière redondante à des réseaux distincts afin de garantir une disponibilité élevée.

- **Appareils mobiles de secours :**

  La déviation du numéro principal sur un numéro mobile central ou plusieurs appareils mobiles permet à l'organisation de rester joignable.

9.6.3 Centrale téléphonique (*call center*)

Deux alternatives principales existent pour les centrales téléphoniques (*call centers*) :

- **Solutions indépendantes pour les organisations critiques (p. ex. organisations d'intervention d'urgence) :**

  Des produits indépendants de Microsoft et éprouvés sont à disposition pour les organisations ayant des contraintes élevées en matière de sécurité et de disponibilité. **Tetrapol** ou **TETRA**, par exemple, sont des systèmes de communication spécialisés qui restent fonctionnels même en cas de défaillance totale d'Internet.

- **Utilisation de solutions à code source ouvert :**

  Des plateformes à code source ouvert comme **Asterisk** proposent des alternatives flexibles et personnalisables pour une infrastructure de téléphonie centrale. Ces solutions peuvent fonctionner sur des serveurs redondants afin d'accroître la résistance aux défaillances.

9.7 Système d'exploitation des clients

Problématique :

En cas de défaillance du système d'exploitation des clients, les terminaux deviennent inutilisables.

En substance :

Des solutions à court terme comme le fait d'utiliser son propre ordinateur ou la mise à disposition de clients parallèles dotés de systèmes d'exploitation alternatifs (p. ex. Linux), ou encore l'utilisation d'appareils mobiles équipés d'iOS ou d'Android, peuvent constituer des options d'urgence. Elles nécessitent toutefois une planification détaillée et pourraient ne pas être réalisables si les utilisateurs sont nombreux. Une défaillance du système d'exploitation impose un remplacement rapide ou l'utilisation de solutions de bureau dans le nuage pour pouvoir reprendre le travail dès que possible.

Prochaines étapes :

Planification détaillée et test des solutions possibles : bureau dans le nuage, mise à disposition de clients préinstallés avec un système d'exploitation alternatif comme Linux. En complément, tests complets des périphériques tels qu'imprimantes, scanners et lecteurs de carte et mise en place de services centraux pour les solutions d'impression et de scan en tenant compte des contraintes en matière de sécurité et de protection des données.

9.7.1 Solutions à court terme

En situation de crise, il n'est guère possible de mettre à disposition des ordinateurs de remplacement en grand nombre. Pour cette raison, la possibilité de recourir à des solutions de bureau dans le nuage (VDI, voir chap. 9.8.3), par exemple à partir de l'ordinateur personnel, est indiquée en cas de défaillance du système d'exploitation Microsoft sur les clients. Ces solutions permettent d'accéder à un système d'exploitation entièrement virtuel en passant par un navigateur ou des protocoles de type Citrix. Il n'existe pas de « systèmes d'exploitation en nuage » au sens traditionnel, qui pourraient faire office de système d'exploitation à code source ouvert à part entière. Il s'agit plutôt de plateformes en nuage (comme OpenStack, OpenNebula et Cloud-init) et de technologies de conteneurs et de virtualisation (comme Docker, Kubernetes et CoreOS) qui permettent d'exploiter et d'optimiser des infrastructures en nuage.

Ce genre d'utilisation nécessite toutefois une planification détaillée et une réglementation contractuelle. Si un grand nombre d'utilisateurs accède simultanément à une solution de bureau dans le nuage, le fournisseur risque de ne pas avoir suffisamment de capacités.

Outre la solution de bureau en tant que tel, il faut également intégrer et pouvoir utiliser les périphériques tels qu'imprimantes, scanners et lecteurs de carte afin d'assurer une pleine capacité de travail. Ces appareils devraient être intégrés soit par le biais d'interfaces standardisées comme USB, soit par le biais de protocoles réseau (p. ex. IPP pour les imprimantes), soit par des protocoles de bureau à distance. Un fonctionnement impeccable des lecteurs de carte est indispensable pour certaines applications, comme les procédures d'authentification sécurisée au moyen de cartes à puce.

9.7.2 Mise à disposition clients avec système d'exploitation alternatif

Il serait envisageable de mettre durablement à disposition un certain nombre de clients dotés d'un système d'exploitation alternatif (p. ex. Linux, peu gourmand en ressources et donc également exploitable sur des terminaux plus anciens) en parallèle à Microsoft. Des appareils Android seraient également une variante envisageable, bien qu'avec un éventail de fonctionnalités restreint. Ces substituts seraient employés en cas de défaillance totale du système d'exploitation Microsoft. Une installation avec des PC Windows virtuels serait aussi possible pour le cas où la défaillance touche uniquement l'infrastructure de l'organisation. Dans les deux variantes, il faudrait un certain nombre de terminaux préinstallés dont il s'agirait de maintenir la configuration à jour. Une solution de ce type serait coûteuse en ressources et ne permettrait de couvrir qu'un nombre restreint d'utilisateurs, avec des fonctionnalités limitées. Divers fournisseurs de services en nuage proposent des modèles évolutifs permettant d'accroître rapidement les capacités au besoin. Rien ne permet toutefois de savoir si ces promesses seraient tenues dans l'éventualité où l'ensemble ou partie de la clientèle seraient touchés en même temps.

9.8 Solutions d'accès à distance / télétravail

Problématique :

Les possibilités d'accès à distance et de télétravail facilitent l'entretien à distance de systèmes, le soutien à distance aux utilisateurs et le télétravail des collaborateurs. Une défaillance de ces solutions implique notamment des pertes de productivité et de flexibilité.

En substance :

Il existe des alternatives aussi bien commerciales qu'à code source ouvert aux services Microsoft correspondants, mais les activer dans de courts délais engendrerait une charge de travail considérable. Les exploiter en parallèle ne serait guère judicieux non plus.

Prochaines étapes :

Examiner l'utilisation de solutions de remplacement (produits à code source ouvert ou commerciaux) sur la base d'une analyse des exigences.

9.8.1 Service d'accès à distance

Microsoft Remote Desktop permet d'accéder à un bureau à distance ou à une machine virtuelle via Internet afin de pouvoir utiliser les applications et les fichiers ainsi que les ressources réseau. Ce service est généralement utilisé à des fins de recherche d'erreurs et de résolution de problèmes. Il repose sur le Remote Desktop Protocol (RDP), un protocole à code source ouvert

développé par Microsoft. Puisque le RDP est documenté publiquement, il est depuis longtemps la cible des pirates, qui ont identifié et exploité plusieurs failles de sécurité. On trouve désormais sur le marché plusieurs alternatives au RDP, aussi bien commerciales (p. ex. TeamViewer, AnyDesk) qu'à code source ouvert (p. ex. NoMachine), dont plusieurs offrent beaucoup plus de possibilités, selon les besoins spécifiques.

Une de ces solutions est envisageable si le but est d'atténuer la dépendance par rapport au protocole de Microsoft.

9.8.2 Réseau privé virtuel (VPN)

Un VPN (*Virtual Private Network*, réseau privé virtuel) crée une connexion chiffrée (tunnel) entre l'appareil de l'utilisateur et le réseau de l'entreprise via le réseau Internet public. Les VPN permettent donc aux collaborateurs d'accéder en toute sécurité au réseau de leur entreprise. Il y a plusieurs pendants à code source ouvert aux solutions VPN de Microsoft, comme OpenVPN, WireGuard, SoftEther VPN, Pritunl (basé sur OpenVPN et WireGuard), ou StrongSwan.

Ces solutions peuvent être utilisées pour atténuer la dépendance par rapport à Microsoft. Il n'est toutefois pas possible de les implémenter rapidement, tant pour des raisons administratives (nécessité de configurer les profils d'utilisateurs, d'organiser les certificats nécessaires, de communiquer et de former les utilisateurs à la nouvelle solution, etc.) qu'à cause des difficultés techniques (compatibilité avec l'infrastructure existante).

9.8.3 Infrastructure de bureau virtuel (VDI)

Une VDI (*Virtual Desktop Infrastructure*, infrastructure de bureau virtuel) héberge des environnements de postes de travail sur des serveurs centraux. Les utilisateurs accèdent à ces environnements virtuels via Internet. Cela permet de proposer un environnement homogène à tous les utilisateurs. La solution de Microsoft s'appelle Azure Virtual Desktop.

Il existe plusieurs alternatives à code source ouvert à la solution VDI de Microsoft, comme Promox VE, XCP-ng (basé sur XenServer de Citrix) ou Apache CloudStack. Toutefois, ces solutions présentent diverses restrictions en termes de fonctionnalités par rapport aux solutions commerciales spécialisées. Pour cette raison, s'il s'agissait d'atténuer la dépendance par rapport à Microsoft, il faudrait plutôt envisager des solutions commerciales, p. ex. Citrix ou VMWare.

9.9 Gestion de système

Dans l'environnement Microsoft, la gestion de système, par exemple la gestion des clients et des serveurs, se fait avec AD et Intune.

Variante sur site : s'il s'agit d'atténuer, voire d'éliminer la dépendance par rapport à Microsoft, il serait possible d'utiliser un produit tout à fait différent, à l'instar d'Univention Corporate Server (UCS), un système d'exploitation serveur comportant une gestion intégrée des identités et de l'infrastructure pour l'administration centralisée et multiplateforme de serveurs, services, clients, bureaux et utilisateurs, ainsi que des ordinateurs virtualisés fonctionnant sur UCS. D'autres alternatives sur site à code source ouvert, comme Samba ou FleetDM, conviennent plutôt aux organisations de moindre envergure.

Variante dans le cloud : Intune, une solution en nuage de Microsoft, est utilisé pour la gestion des correctifs et des mises à jour des clients. Des outils basés sur le nuage comme SaltStack, Ansible ou Puppet pourraient être étudiés à titre de solutions de remplacement à code source ouvert.

Il faudrait examiner dans quelle mesure ces solutions à code source ouvert peuvent être utilisées pour la gestion de système (que ce soit sur site ou dans le nuage). Les activer rapidement dans un scénario IT-SCM n'est toutefois guère réaliste. Exploiter plusieurs solutions en parallèle est associé à des risques importants : le fonctionnement des clients pourrait être compromis en cas de corruption des systèmes ou les deux programmes de gestion pourraient s'entraver mutuellement. Les erreurs affectant les outils de gestion de système (que ce soit sur site ou dans le nuage) peuvent entraîner des conséquences sérieuses, qui pourraient aller jusqu'à la nécessité de réinitialiser l'ensemble des clients.

9.10 Gestion des appareils mobiles (MDM)

Problématique :

En cas de panne du système de MDM, il n'est plus possible de gérer efficacement les appareils mobiles. Des fonctions de sécurité importantes comme le verrouillage à distance ou la suppression du contenu des appareils en cas de perte ou de vol deviennent indisponibles. De plus, il n'est pas possible de mettre en œuvre les directives de sécurité sur les appareils, ce qui entraîne des risques considérables.

En substance :

Il existe des alternatives, aussi bien commerciales qu'à code source ouvert, au système MDM de Microsoft, mais leurs fonctions et capacités sont limitées. Ces services ne permettent notamment pas de garantir la sécurité des données, c'est-à-dire de mettre en œuvre sur les appareils mobiles les règles liées à la classification des données (confidentiel, interne, etc.).

Prochaines étapes :

Continuer à observer le marché jusqu'à ce que de nouvelles solutions soient disponibles pour la MDM.

Une défaillance du système de MDM peut provoquer de graves problèmes de sécurité et de productivité. Des plans d'urgence, des mesures de sécurité correspondantes et une restauration rapide du système sont essentiels pour réduire ces risques au minimum.

Les principales conséquences d'une telle défaillance sont des risques de sécurité :

- Sans MDM, il est impossible de bloquer les appareils perdus ou volés ou de supprimer leur contenu à distance
- Les collaborateurs peuvent installer n'importe quelle application, qu'elle soit ou non conforme aux directives de sécurité. Ils peuvent télécharger des applications ou fichiers non sécurisés, ce qui peut entraîner des infections par des maliciels.
- Sans MDM, il est difficile de s'assurer que tous les appareils et fichiers sont chiffrés.
- Les appareils peuvent se connecter à des réseaux wifi non sécurisés, ce qui augmente la vulnérabilité aux attaques.

La solution de MDM de Microsoft (Intune) peut être remplacée par des solutions commerciales (p. ex. Citrix) et à code source ouvert. Les options à code source ouvert conviennent plutôt pour des organisations de moindre envergure. Elles ne proposent pas les mêmes fonctionnalités, notamment en termes de sécurité des données. La solution de Microsoft permet de garantir que les règles de classification des données (confidentiel, interne, etc.) sont mises en œuvre aussi sur les appareils mobiles. Les solutions de remplacement n'offrent pas cette fonctionnalité de manière entièrement intégrée.

De plus, il n'est pas possible d'exploiter en parallèle des services MDM, car les appareils mobiles doivent être gérés par un seul système. Il serait possible de préparer et de mettre en place une nouvelle solution en guise de préparation à une défaillance du service de MDM de Microsoft. En situation IT-SCM, il faudrait transitionner rapidement vers la solution de remplacement avec le concours des utilisateurs. L'appareil est toutefois sans protection durant la reconfiguration et les utilisateurs pourraient installer n'importe quelle application ou partager des données sensibles avec des personnes non autorisées.

10 Open source alternative à Microsoft dans le cadre stratégie Exit

Question : quelles mesures peut-on déjà prendre actuellement pour se préparer à une potentielle résiliation de contrat, que ce soit de la part de l'administration ou de la part de Microsoft ?

Il est possible de répondre à cette question au moyen d'une analyse du marché : **il n'y a pas d'option entièrement équivalente à Microsoft**. Chaque solution disponible nécessiterait des compromis et devrait être adaptée à l'infrastructure informatique existante. Quitter l'écosystème Microsoft nécessiterait donc une décision stratégique et politique et serait très difficilement réalisable pour une administration publique isolée.

Cependant, les mesures IT-SCM mentionnées au chapitre 9 peuvent aussi permettre de se préparer à la résiliation du contrat avec Microsoft.

Autres difficultés :

- La mise à disposition de services autres que ceux de Microsoft et la transition vers ces services seraient extrêmement laborieuses et demanderaient énormément de temps et de ressources. Pour assurer une transition sans heurts, il faudrait concevoir les solutions de remplacement en détail, les tester au moyen d'installations pilotes (preuve de faisabilité) et, dans la plupart des cas, les installer en parallèle à l'infrastructure Microsoft. Une institution publique se lançant seule dans une telle entreprise s'exposerait à des risques considérables dans le contexte actuel, marqué par l'absence de normes intercantonales (eCH) et de fournisseurs appropriés. Un abandon planifié de Microsoft devrait donc idéalement être coordonné par un service central (p. ex. l'ANS ou eOperations) afin de pouvoir établir les conditions nécessaires à une mise en œuvre réussie (normes eCH, etc.).
- En cas d'abandon total des services Microsoft, il faudrait débarrasser entièrement toutes les applications spécialisées de ces services (p. ex. traiter ou générer des documents Office à partir des applications spécialisées). Les charges et les travaux correspondants incomberaient aux institutions, car les applications spécialisées sont en général très spécifiques. En revanche, s'agissant des applications spécialisées basées sur des logiciels standard spécifiques et utilisées dans plusieurs cantons, il faudrait effectuer les adaptations dans le cadre d'une démarche coordonnée (p. ex. négociations communes et centralisées avec les fournisseurs d'applications spécialisées).
- Il faut tenir compte des aspects relevant du droit des marchés publics, aussi bien dans le cas d'une institution opérant seule que dans le cas d'une solution commune. Une démarche coordonnée peut aider à trouver des solutions cohérentes et à éviter les doublons. Des projets d'acquisition communs offrent en outre une meilleure position de négociation face aux fournisseurs potentiels.
- Les risques les plus élémentaires concernent les aspects opérationnels. À l'heure actuelle, les fournisseurs de solutions à code source ouvert sont plutôt des entreprises de petite taille. Si tous les cantons, voire toutes les institutions publiques de Suisse, souhaitent bénéficier en même temps de l'offre de prestations de la même entreprise, celle-ci ne sera probablement pas en mesure de développer suffisamment ses capacités en temps opportun. Les institutions courent en outre le risque de dépendre d'une petite société. Une approche nouvelle est requise pour surmonter ces difficultés. Une variante possible serait de développer et d'utiliser une prestation publique, telle que le Swiss Government Cloud, complétée par une approche à plusieurs fournisseurs. Un tel fonctionnement permettrait de ne pas simplement reporter la

relation de dépendance actuelle sur un autre fournisseur. Il serait aussi possible de viser une solution avec une grande entreprise disposant d'une capacité suffisante et au bénéfice d'une garantie de l'État pour assurer la stabilité et la fiabilité à long terme.

Bilan : la mise à disposition de services autres que ceux de Microsoft et la transition à ces services seraient extrêmement laborieuse et demanderaient énormément de temps et de ressources. Compte tenu de la complexité de l'opération et des défis financiers et organisationnels, il n'est guère envisageable pour une ou quelques institutions publiques de se lancer dans cette entreprise par elles-mêmes.

Les résultats de l'étude montrent que des administrations isolées ne seront guère en mesure de développer par leurs propres soins des solutions viables aux défis décrits. La complexité des exigences techniques, organisationnelles et juridiques nécessite une collaboration rapprochée. Un rapprochement des acteurs, idéalement au niveau national et même international, par exemple en coopération avec l'UE, est décisif pour créer des synergies, développer des normes et utiliser les ressources de manière efficiente. Seule une approche coordonnée et globale permettra de mettre en œuvre des solutions durables et souveraines sur le long terme.

Annexe

[1] Annexe A : analyse des exigences, analyse de marché, entretiens avec les administrations publiques et enquête auprès des fournisseurs potentiels *(document Excel, bien lisible en ligne)*

Appendices

[B1] *Studie zu Open Source Alternativen von Microsoft Services und Produkten in der Schweizerischen Bundesverwaltung* : Backend-Services; Haute école spécialisée bernoise ; version 1.8 de février 2024 [uniquement en allemand]

[B2] *Studie zu Open Source Alternativen von Microsoft Services und Produkten in der Schweizerischen Bundesverwaltung:* Frontend-Services (Client-Anwendungen) ; Haute école spécialisée bernoise ; version 1.0 de février 2024 [uniquement en allemand]

[B3] *Die Open Innovation und Open Source Strategie des Landes Schleswig-Holstein* ; chancellerie d'État du Land Schleswig-Holstein ; version 1.0 du 20.11.2024 [uniquement en allemand]

Glossaire

Terme	Description / explication
Active Directory (AD)	Service d'annuaire de Microsoft pour la gestion centralisée des utilisateurs, groupes, ordinateurs et autres ressources au sein d'un réseau
***Business Continuity Management* (BCM)**	Stratégies et mesures visant à assurer la continuité des opérations en cas d'urgence ou de crise
Cloud Governance	Lignes directrices et procédures pour le pilotage, la gestion et le contrôle des services en nuage au sein d'une organisation
Copilot (Microsoft)	Outil d'assistance basé sur l'intelligence artificielle intégré aux services Microsoft, qui soutient les utilisateurs dans diverses tâches
Souveraineté numérique	La capacité d'une organisation ou d'un État à contrôler ses infrastructures et ses données numériques de manière indépendante et autonome
Administration numérique suisse (ANS)	Organisation de collaboration visant à assurer l'efficacité du pilotage et de la coordination stratégiques des activités menées par la Confédération, les cantons et les communes en lien avec la transformation numérique https://www.administration-numerique-suisse.ch/fr
Normes eCH	Normes dans le domaine de la cyberadministration, promues, développées et adoptées par l'association eCH (https://www.ech.ch/fr). Ces normes visent à une collaboration électronique efficace entre les autorités, les entreprises et les personnes privées.

Terme	Description / explication
eOperations Suisse	Organisation pour l'acquisition, le développement et l'exploitation en commun de solutions TIC pour les prestations de cyberadministration de la Confédération, des cantons et des communes
***Identity and Access Management* (IAM)**	Système de gestion des identités numériques et des droits d'accès au sein d'une infrastructure informatique
Interopérabilité	La capacité de systèmes, organisations ou applications différents à fonctionner ensemble et à échanger des données sans heurts
***IT Service Continuity Management* (IT-SCM)**	Mesures visant à assurer la disponibilité des services informatiques en cas de défaillances ou de pannes
***Request for Information* (RFI)**	Démarche permettant d'obtenir une vue d'ensemble du marché au moyen de demandes de renseignements aux fournisseurs / prestataires potentiels
Microsoft 365 (M365)	Suite d'applications de productivité et de collaboration basées sur le nuage, qui comprend Office, Teams, SharePoint et Exchange
***Mobile Device Management* (MDM)**	Système permettant de gérer et sécuriser de manière centralisée les terminaux mobiles dans des entreprises ou des institutions publiques
Format Office	Formats standardisés pour les applications bureautiques, p. ex. Microsoft Open XML (.docx, .xlsx, .pptx) et Open Document Format (ODF).
***Open Document Format* (ODF)**	Un format de document ouvert et libre faisant office d'alternative aux formats propriétaires tels qu'Open XML de Microsoft. ODF est notamment pris en charge par les suites de bureautique à code source ouvert comme LibreOffice, OpenOffice et OnlyOffice. Le format est reconnu en Suisse en tant que norme eCH 0031.
***Open source software* (OSS)**	Logiciel dont le code source est accessible au public et que la communauté peut continuer à développer
Swiss Government Cloud (SGC)	Une nouvelle infrastructure en nuage capable de répondre aux exigences et aux besoins de l'administration fédérale. Le projet durera de 2025 à 2032. https://www.bit.admin.ch/fr/sgc-fr
***Total Cost of Ownership* (TCO)**	Coût total d'un investissement sur l'ensemble de son cycle de vie, de l'acquisition à l'élimination en passant par l'exploitation et la maintenance
***Virtual Desktop Infrastructure* (VDI)**	Infrastructure TIC permettant aux utilisateurs d'accéder aux ressources TIC d'une entreprise à partir de n'importe quel appareil