eraneos

FOCUS

Utilisation du cloud dans l'environnement réglementé

De gauche à droite : **Christian Mauz**, Partner ; **Richard Hess**, responsable du numérique à l'ASB ; **Hanspeter Christ** ; **Cédric Moullet** ; **Adrian Anderegg**, Partner ; **Marc Raum**, Senior Manager ; **Thomas Vogt**, Senior Manager ; **Tom Schons**, Manager

Contexte

Le voyage vers le cloud dans l'environnement réglementé

On ne se pose plus la question de savoir si le cloud arrive. La décision a été prise il y a longtemps. Les fournisseurs de cloud ont fait leur devoir et ont créé les bases pour une utilisation sécurisée des services de cloud. Mais dans l'environnement réglementé, il existe des conditions-cadres différentes, qui doivent impérativement être prises en compte pour une mise en œuvre conforme des stratégies de cloud.
Christian Mauz

Le cloud est largement reconnu comme étant le pionnier central de la transformation numérique, y compris dans l'environnement réglementé. Mais les défis liés à l'utilisation du cloud sont variés. Que faut-il prendre en compte dans la stratégie de cloud ? Comment concevoir la gouvernance ? Quels rôles, processus et directives sont nécessaires pour une utilisation sécurisée et conforme du cloud ? Comment aborder la migration vers le cloud des applications qui étaient jusqu'ici exploitées au sein-même des infrastructures, et qu'est-ce que cela implique pour mon organisation et mon modèle d'exploitation ? La bonne nouvelle : de nombreux obstacles ont déjà été franchis par les précurseurs. Il n'est donc pas nécessaire de réinventer la roue. Le soutien des fournisseurs de cloud est aussi disponible, en particulier du côté des géants du web. Malgré tout, les organisations informatiques sont confrontées à une tâche colossale avec la transition vers le cloud. Dans le présent FOCUS, nous souhaitons vous transmettre quelques suggestions de réflexion dans le voyage vers le cloud.

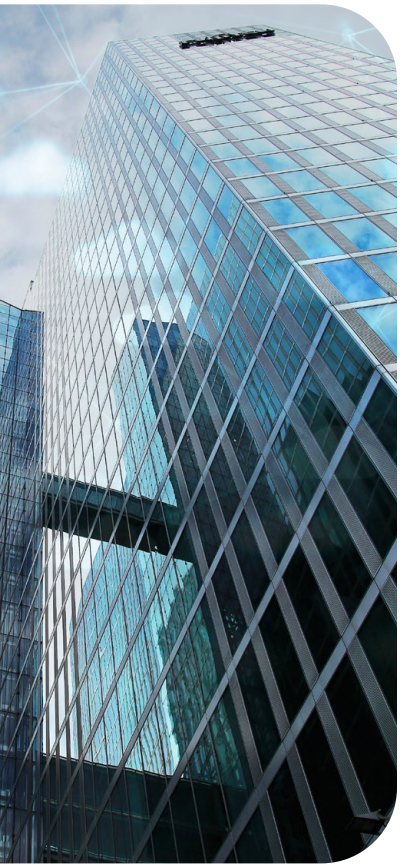
« En tant qu'instrument de la transformation numérique, le cloud est également central dans l'environnement réglementé et indispensable aux solutions informatiques modernes. »

Christian Mauz,
Partner

Dans ce contexte, la vaste initiative de cloud européenne, GAIA-X, qui vise à dissiper les réticences qui subsistent face au cloud, est passionnante. GAIA-X a été lancée par des représentants de l'économie, des sciences et de l'administration originaires d'Allemagne et de France en vue de développer, avec d'autres partenaires européens, des normes et règles pour une infrastructure de données de nouvelle génération. GAIA-X représente un écosystème numérique ouvert, transparent et sécurisé, dans lequel les données et services peuvent être rassemblés dans un environnement fiable, mis à disposition et utilisés communément. Dans ce contexte, le renforcement de la souveraineté numérique et des données constitue un élément central, afin de garantir aux utilisateurs le contrôle total sur les données enregistrées et traitées.

Nous vous souhaitons une lecture enrichissante.

Le cloud dans l'environnement réglementé – un voyage complexe



Dans l'environnement réglementé, il existe, parallèlement aux conditions-cadres légales en vigueur pour toutes les organisations, des normes et instructions supplémentaires ou renforcées. Celles-ci concernent de plus en plus les processus métiers numériques et définissent les conditions-cadres commerciales et techniques pour l'intégration et l'utilisation des services cloud. La transition vers le cloud s'accompagne d'un besoin de changement en termes de gouvernance et exige une modification volontaire de la culture.

Adrian Anderegg, Marc Raum, Thomas Vogt, Tom Schons

Les principaux moteurs de l'utilisation croissante des services de cloud (non limités à l'environnement réglementé) incluent :

- La collaboration virtuelle au sein des organisations ainsi qu'avec des partenaires externes, notamment dans les processus de communication et de collaboration
- La mise à disposition rapide et automatisée d'environnements
- La « capacité à la demande » pour absorber de manière flexible les pointes de charge et ne payer que l'utilisation effective
- Les propriétés non fonctionnelles de premier plan, comme les fonctions de sécurité à granularité fine ou les capacités de cybersécurité et de confidentialité
- Le développement et la disponibilité rapides de blocs de solution technologiques modernes
- Les prestataires fournissant les nouvelles solutions exclusivement en tant que services de cloud
- La focalisation de ses propres compétences à un niveau supérieur de la chaîne de valeur IT

Quels sont les défis, les obstacles et les risques ?

Dans son rapport sur l'« examen de la nécessité d'un Swiss Cloud[1] », la Confédération a identifié les conditions-cadres floues de l'utilisation des services de cloud public comme un obstacle majeur. Tandis que l'industrie financière a déjà élaboré les guides et directives correspondants pour l'utilisation du cloud, l'utilisation des services de cloud dans le secteur public est souvent empêchée par des lois sur la protection des données ainsi que par l'infraction pénale de la violation du secret de fonction (art. 320 CP).

Des directives de conformité existantes doivent être modifiées, par exemple dans l'ancrage contractuel du droit d'audit pour les contrats d'approvisionnement, car cela n'est souvent réalisable dans l'environnement de cloud public qu'en respectant des certifications spécialisées. Les directives et concepts de cybersécurité comme le concept de zones de réseau ou l'intégration de processus SIEM[2] existants doivent être réévalués et conçus pour les applications dans le cloud. La disponibilité des spécialistes du cloud constitue elle aussi un défi en raison de la « guerre des talents ». Il faut en outre tenir compte du risque de vendor lock-in, c'est-à-dire la dépendance à long terme à un seul fournisseur. En pratique, il faut beaucoup de connaissances et de discipline pour prendre des décisions techniques qui maintiennent les possibilités de changement durables sur le plan économique.

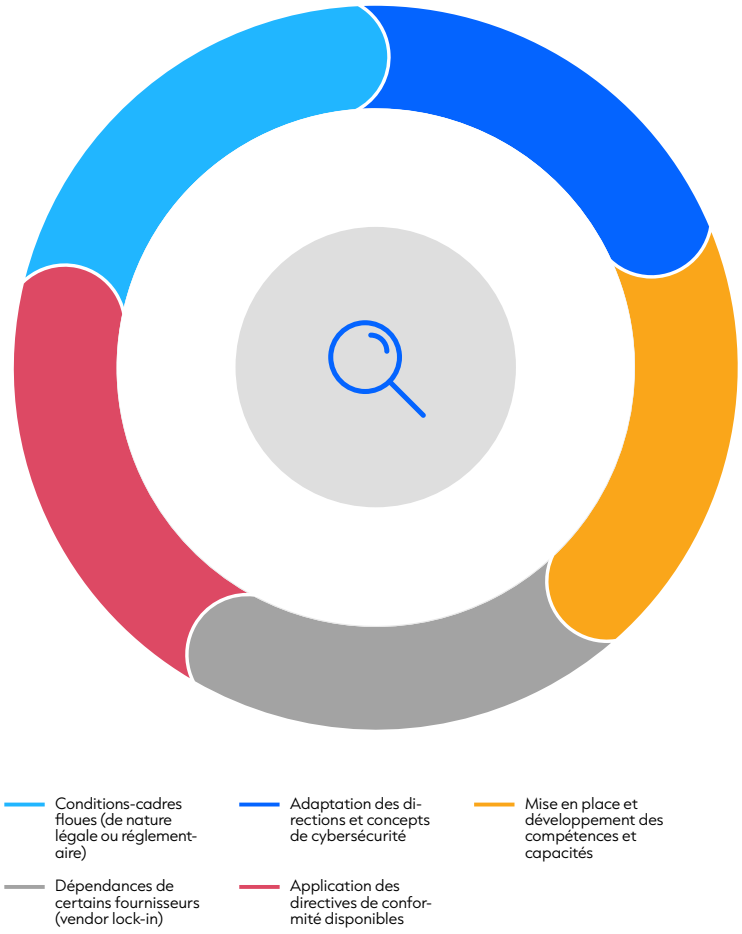


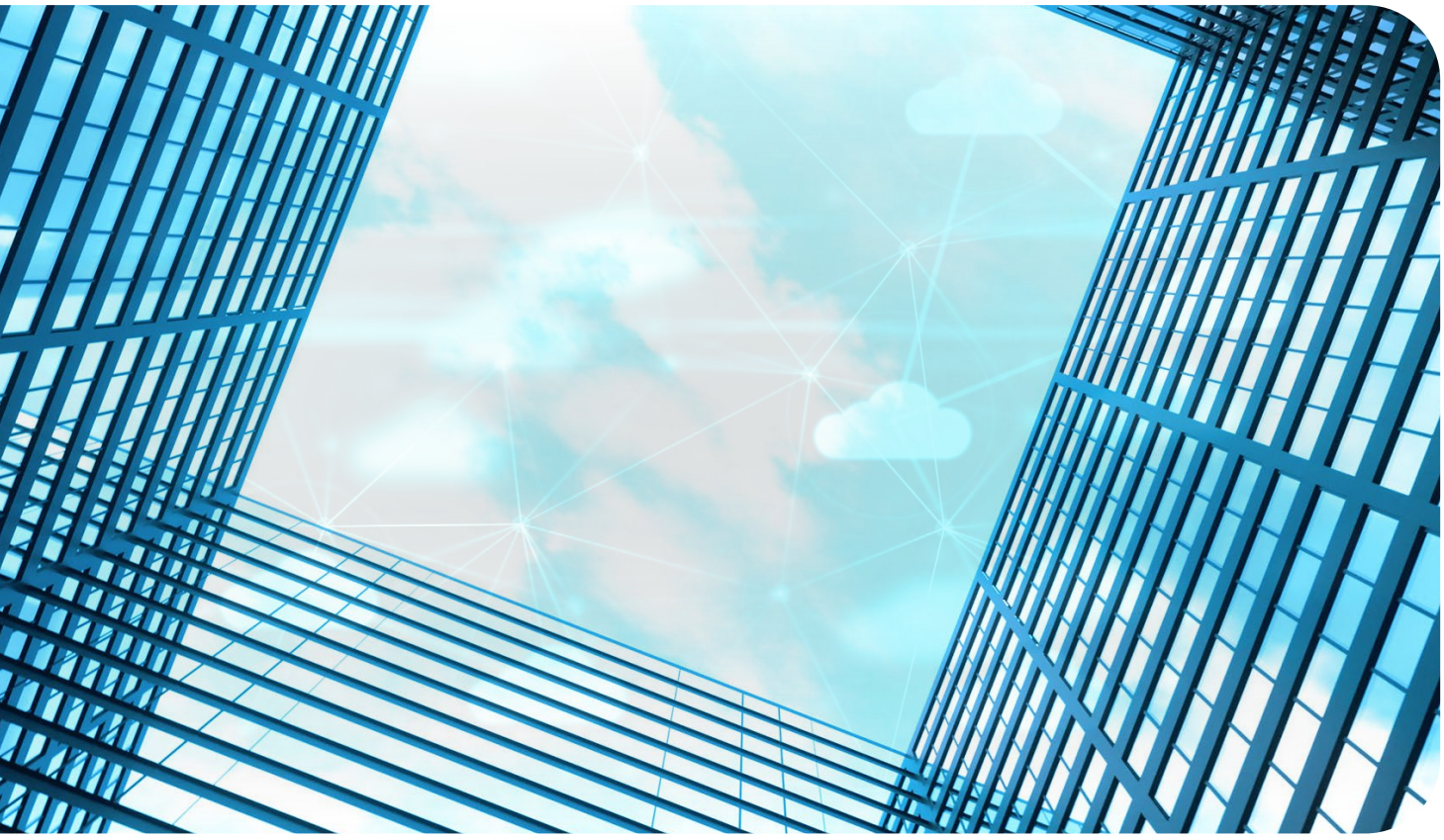
Illustration 1 : Obstacles critiques pour l'utilisation du cloud

1 https://www.newsd.admin.ch/newsd/message/attachments/64462.pdf

2 SIEM: Security Information and Event Management

Les éléments recommandés d'une stratégie de cloud

Une stratégie de cloud englobe une **vision** et une **mission** claires ainsi qu'un **objectif** de transition vers le cloud, qui aborde en particulier les aspects organisationnels concernant l'intégration dans la transformation numérique de l'ensemble de l'organisation. Les **principes d'utilisation du cloud** sont des bases de décision déterminantes. Les **risques liés à l'utilisation du cloud** doivent en outre être analysés et évalués, en tenant compte des recommandations du secteur (p. ex. guides sur le cloud de l'Association suisse des banquiers). Bien sûr, une **considération économique de l'utilisation du cloud** est elle aussi importante pour créer une base solide pour des changements à venir du point de vue de toute l'organisation informatique. D'autres aspects essentiels sont la définition de la future **gouvernance** et du **modèle d'exploitation visé**, incluant les conditions-cadres organisationnelles globales, la mise à disposition des capacités nécessaires et des éventuels modèles d'approvisionnement. Sur cette base, il s'agit d'organiser les étapes grossières ainsi que les services et comités de décision à impliquer pour **l'évaluation et l'acquisition des services de cloud**. Les **mesures de gestion de la continuité des activités** et les **directives** concernant la **possible stratégie de sortie** du cloud doivent également être déterminées. Pour finir, il convient de définir les initiatives de transition vers le cloud à appliquer dans le cadre d'une **feuille de route** élaborée sur plusieurs années. Cela impose de nombreuses exigences à l'équipe de direction, car les principes et modes de travail existants ainsi que l'organisation doivent être modifiés.



Mise en œuvre de la stratégie de cloud

Nous recommandons de répartir l'opérationnalisation et l'ancrage de la stratégie de cloud définie sur plusieurs phases avec différents points forts, qui sont planifiés et appliqués de manière intégrale. La base est constituée par la gouvernance de cloud, qui gère les conditions-cadres organisationnelles, ainsi que l'architecture de cloud globale. Cette dernière doit tenir compte de l'architecture d'entreprise existante et des dépendances technologiques avec les modules de solution en place. Une attention particulière doit être accordée à l'adaptation des architectures de sécurité TIC disponibles. Pour la migration concrète des applications vers le cloud, il est utile de réaliser une évaluation préalable des préparatifs pour déterminer l'état cible optimal de l'application et de la procédure de migration. Une procédure agile ou itérative s'offre généralement aux différentes procédures de migration vers le cloud afin de limiter les risques et collecter des expériences.

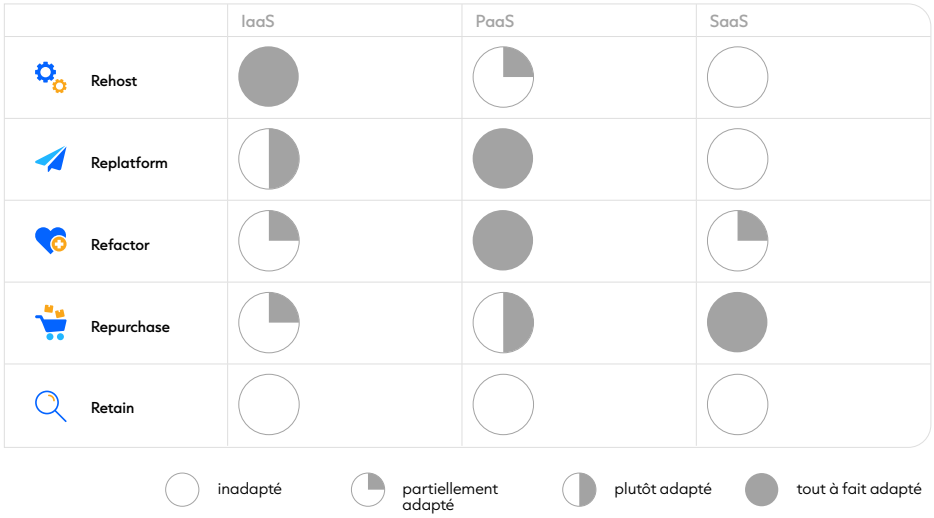


Illustration 2 : Stratégies standard pour la migration des applications

Illustration 3 : Stratégie standard de migration des applications

Le fournisseur de cloud public et l'environnement réglementé

Dans de nombreux domaines, les fournisseurs de cloud public proposent déjà de très bonnes conditions-cadres pour l'environnement réglementé. Souvent, l'emplacement géographique ou légal du stockage et du traitement des données est déterminant. Cet aspect est adressé par les emplacements des centres de calculs déjà disponibles ou annoncés en Suisse par les fournisseurs de cloud public. Ces fournisseurs proposent en outre une large sélection de certifications propres à la réglementation et à l'industrie.

Les disponibilités très élevées et les possibilités multiples pour les configurations redondantes des services sur les plateformes des géants du web sont attrayantes. En effet, les niveaux de service plus élevés n'impliquent pas d'investissements fixes supérieurs, car ils ne se répercutent que sur les coûts de service.

Les plateformes de cloud actuelles fournissent de plus en plus de services cloud spécifiques aux secteurs, par exemple sous forme de plans de configuration pour répondre aux exigences de conformité. Les concepts de cybersécurité existants peuvent également être largement développés dans le cadre des transitions vers le cloud et optimisés en termes d'efficacité.

Conclusion : Les services Cloud sont indispensables dans l'environnement réglementé.

Les services de cloud sont devenus indispensables dans l'environnement réglementé. Pour répondre aux attentes associées, il est toutefois important d'examiner en détail les décisions stratégiques ainsi que la conception et la mise en œuvre d'une transformation vers le cloud dans le contexte concerné et de tenir compte des conditions-cadres de l'organisation.

La base est constituée par la stratégie de cloud, qui crée les principes stratégiques à l'aide d'un objectif clair. Il convient de se pencher sur les risques en amont. Il faut aussi définir des directives claires concernant les aspects économiques et organisationnels de l'utilisation du cloud.

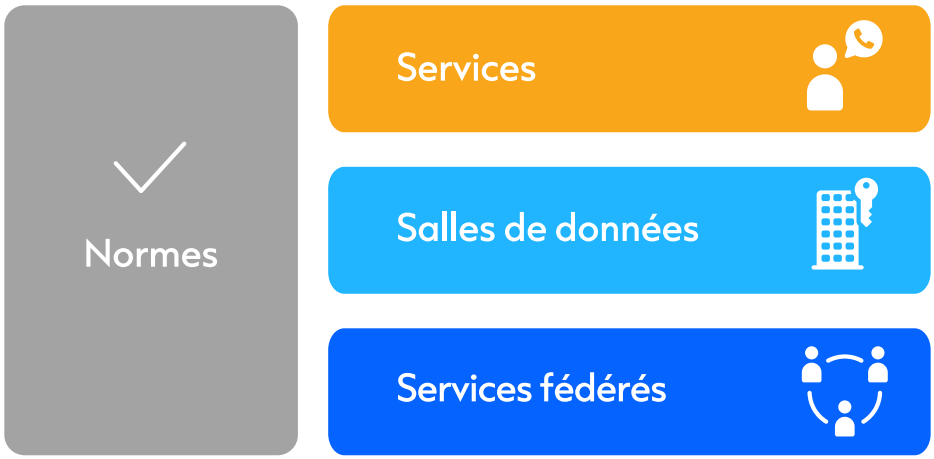
Dans la deuxième phase, il faut définir la gouvernance et l'architecture visée en termes de cloud. La migration vers le cloud se fait de préférence de manière itérative afin de mettre en place successivement les capacités nécessaires et de maîtriser les risques. Le développement rapide des services et modèles de cloud requiert le contrôle et le développement réguliers des conditions-cadres définies pour l'utilisation du cloud.

Eraneos soutient les organisations dans l'environnement réglementé avec son expertise et son expérience, tant dans l'élaboration de stratégies de cloud et de conceptions associées que dans la mise en œuvre de transformations vers le cloud.

Dans quelle mesure l'initiative GAIA-X peut-elle devenir significative ?

GAIA-X[3] est un projet européen de développement d'une infrastructure de données pour l'Europe, qui est non seulement performante et compétitive, mais aussi sécurisée et fiable. Actuellement, le projet est surtout porté par des représentants de l'économie, des sciences et de l'administration originaires d'Allemagne et de France, mais il reste ouvert à d'autres partenaires qui souhaiteraient participer. Il s'agit donc aussi d'un projet intéressant pour la Suisse, en tant que partenaire politique possédant des conceptions juridiques largement convergentes (p. ex. RGPD).

Le concept de GAIA-X est basé sur le niveau d'architecture supérieur sur des éléments « services fédérés », « salles de données » et « services », qui sont interopérables via des normes définies de manière commune. Chaque instance participante peut proposer et consommer des services basés sur GAIA-X. La standardisation permet non seulement de définir clairement les principes technologiques, mais aussi de mettre en œuvre de manière homogène les classes de qualité à respecter (critères de qualité des services). Grâce à ce concept, la dépendance à différents prestataires ou fournisseurs de cloud est en principe atténuée dans l'utilisation des services de cloud.



Même si GAIA-X offre encore peu d'utilité concrète, l'initiative pourrait apporter une contribution importante aux organisations réglementées à moyen terme avec ces approches. Il vaut donc la peine de suivre de près son évolution et de vérifier une éventuelle participation.

Illustration 4 : Le concept de GAIA-X

3 https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

Conformité à des normes de cybersécurité élevées dans le cloud

Le cloud permet aux entreprises d'augmenter leurs normes de cybersécurité et de les appliquer dès le départ de manière cohérente lors de la migration. Le passage à un environnement de cloud devrait notamment s'accompagner de gains de sécurité importants, notamment pour les PME, par rapport à leur infrastructure sur site existante. En effet, proportionnellement, elles profites davantage des fonctions de sécurité standardisées et des progrès techniques des fournisseurs que les grandes entreprises.

Mais quelle que soit la taille de l'entreprise, il faut veiller à quelques éléments importants pour l'organisation et l'utilisation sécurisées des solutions de cloud. Avant la migration vers le cloud, une (cyber)analyse détaillée des risques doit être effectuée, impliquant tous les acteurs pertinents au sein de l'entreprise. Selon l'appétence au risque, des mesures d'atténuation peuvent être définies à l'avance, intégrées dans les concepts (de sécurité) correspondants puis mises en œuvre. Bien sûr, il ne faut pas oublier pour autant une analyse continue des risques identifiés.

Parmi les principales difficultés du point de vue de la sécurité, figure l'utilisation de modèles de cloud hybrides, qui sera la norme au cours des prochaines années. Seules quelques entreprises migreront totalement dans un seul cloud. La plupart continueront d'exploiter une partie de leurs applications leur propre infrastructure ou migreront dans différents clouds. La sécurité de la solution globale est donc intimement liée aux concepts d'architecture (de sécurité) et à leur mise en œuvre. Le « modèle de responsabilité partagée », qui oblige les fournisseurs et utilisateurs de solutions de cloud à une limitation claire des responsabilités, provoque toutefois souvent la confusion chez les néophytes du cloud, suivie par une interprétation imprécise des responsabilités puis par des failles de sécurité (involontaires). De plus, la gestion des identités et des accès (IAM) ainsi que l'intégration de diverses identités de cloud et de leur gestion des autorisations deviendront de plus en plus complexes et exigeront un savoir-faire dédié. L'IAM et l'architecture de sécurité feront ainsi partie intégrante de la sécurisation des solutions de cloud. En conclusion, des aspects de sécurité classiques doivent aussi être examinés en détail, comme la surveillance des événements de sécurité et la détection de menaces, qui sont confrontés à de tout nouveaux défis en raison des structures décentralisées des modèles de cloud hybrides. Il est donc d'autant plus important de répondre clairement en amont aux questions comme : « Où enregistrer quels journaux à court/long terme ? Comment m'assurer que mon SIEM possède une vision globale ? Comment protéger la diversité des interfaces (API) de la manière la plus efficace possible ? »

C'est pourquoi il est recommandé de miser en principe sur des standards, approches et meilleures pratiques établis, comme ceux de la Cloud Security Alliance (CSA).

Le cloud dans l'industrie financière – un défi à plusieurs points de vue

L'industrie financière est soumise à des directives strictes en matière de réglementation, de conformité et de risque concernant la mise en œuvre des projets techniques et organisationnels. En raison du secret bancaire suisse, on conservait la plupart du temps un stockage des données en Suisse, l'externalisation à l'étranger étant jugée irréalisable. Faute de fournisseurs de cloud public présents sur le sol suisse, il ne restait que l'option d'un hébergement classique avec des fournisseurs suisses. Le développement de centres de calcul dans le cloud en Suisse a toutefois interrompu cette tendance et modifié le marché au profit de fournisseurs de cloud public étrangers, en particulier en raison de l'accord des fournisseurs de miser sur un stockage des données en Suisse.

Adrian Anderegg, Tom Schons

Autorité de surveillance compétente, la FINMA a publié la circulaire « 2018/3 Outsourcing » dès 2017, avant de la remanier à l'hiver 2020. Cette circulaire régit non seulement le cadre adapté à une externalisation classique vers des prestataires informatiques, mais a aussi des répercussions décisives sur l'utilisation de clouds publics. Comme l'interprétation correcte des différents paragraphes concernant le cloud est loin d'être évidente, l'Association suisse des banquiers a publié en été 2020 un «guide du cloud » avec les meilleurs pratiques. Toutefois, ce guide manque non seulement d'exemples concrets concernant les différentes solutions de cloud, mais aussi de recommandations techniques et organisationnelles concernant l'action et la mise en œuvre. Les établissements et leurs prestataires doivent combler les lacunes par eux-mêmes.

Aspects centraux et obstacles dans la mise en œuvre des solutions de cloud public

L'analyse des fonctions et données qu'un établissement externalise dans le cloud a des répercussions importantes sur l'applicabilité de l'externalisation « essentielle » ou « non essentielle ». Dans ce contexte, la répartition correcte selon la circulaire 2018/3 est essentielle. En pratique, l'interprétation en tant qu'« externalisation non essentielle », qui se transforme avec le temps en une « externalisation essentielle » en raison du développement continu des solutions de cloud, est risquée. Les établissements qui externalisent leur projet de cloud devraient accorder une attention particulière au risque accru d'une « shadow IT », par exemple alimentée par la fourniture et l'utilisation comparativement simples de solutions SaaS en dehors des structures informatiques centralisées.

Avec le développement des centres de calcul dans le cloud en Suisse, les grands fournisseurs s'opposent aux sceptiques de la souveraineté des données des fournisseurs de cloud étrangers suite au CLOUD Act américain et des « jugements Schrems ». En pratique, il faut continuer d'agir avec prudence, car des services et fonctions isolés continuent d'être assurés par les centres de données globaux. En cas de doute, les données sont « au repos » dans un centre de données suisses, mais parfois « en transit » à court terme

dans l'UE voire aux États-Unis. De plus, de nouveaux services et fonctionnalités sont souvent introduits ultérieurement dans les centres de données suisses. Une attention particulière doit aussi être accordée à la continuité des activités et à la reprise d'activité après catastrophe, car les géants du web sécurisent leurs clouds avec de multiples redondances, souvent au-delà des frontières nationales. Il est donc recommandé de vérifier précisément en amont à partir de quel pays les services et fonctionnalités sont fournis en cas normal et en cas d'urgence. Les connaissances acquises doivent être prises en compte en conséquence dans l'analyse des risques. Dans le contexte du CLOUD Act américain, la thématique de l'« accès légal » joue aussi un rôle central. Toutefois, selon les sources de données disponibles et les fournisseurs qui sont conscients de la force d'une telle intervention, ce risque est peu probable et peut être réduit à un niveau raisonnable par des mesures techniques, organisationnelles et contractuelles.

Il est essentiel que la décision stratégique d'externaliser les données commerciales, personnelles ou des clients vers un fournisseur de cloud soit prise sur une base solide. La procédure suivante est recommandée :

1 Établissement d'une analyse approfondie des risques, intégrant à la fois l'établissement et le fournisseur ainsi que les services et fonctions utilisés

2 Représentation des risques selon l'appétence au risque de la direction

3 Identification et mise en œuvre des mesures techniques, organisationnelles et contractuelles requises

4 Surveillance continue des risques identifiés et définition des contremesures pertinentes

Illustration 1 : Mise en oeuvre de solutions de cloud public

L'infrastructure informatique existante joue elle aussi un rôle important pour les établissements financiers. Les systèmes centraux des banques et assurances fonctionnent souvent sur des matériels très spécifiques, comme les macroordinateurs. Comme ces systèmes ont du mal à être virtualisés, il n'est pas question de migrer ces serveurs vers le cloud pour l'instant. En outre, la stabilité et la disponibilité de ces systèmes sont primordiales. Les concepts modernes comme le déploiement continu ne sont pas appliqués aux systèmes centraux jusqu'à maintenant, car même de petites erreurs logicielles peuvent avoir des répercussions majeures. Au moment du déploiement, la maturité doit déjà être très élevée. Dans ce contexte, un « produit minimum viable » (MVP) n'apporte généralement pas la maturité nécessaire à une utilisation productive.

Par conséquent, les établissements financiers possèdent une informatique à deux vitesses : avec des macroordinateurs et des mises à jour trimestrielles, assez lentes. Les avantages typiques d'une solution SaaS sont donc difficiles à exploiter. C'est pourquoi l'architecture des applications clés doit être redéfinie avant une migration vers le cloud. De nombreuses banques et assurances ainsi que leurs fournisseurs logiciels n'en sont qu'au tout début. De l'autre côté de l'informatique à deux vitesses, se trouvent les portails, les applis ou les applications d'analyse. Les avantages du cloud y sont particulièrement visibles, y compris dans l'environnement financier. De nouvelles technologies comme l'intelligence artificielle sont possibles avec ses propres logiciels ou matériels sans grand investissement. L'analyse de gros volumes de données en temps réel à l'aide de la performance de calcul du cloud permet des services de conseil innovants pour les clients ou l'automatisation de processus complexes concernant la conformité et le risque. Le développement et le test de nouvelles applications sont eux aussi possibles plus rapidement et plus efficacement. Les tests de charge et de performance peuvent être réalisés à bas prix avec des ressources de cloud temporaires. La flexibilité et l'agilité accélèrent la mise sur le marché.

Dans l'environnement financier, le cloud convient particulièrement aux thèmes qui permettent des développements agiles et éphémères, tandis que les systèmes centraux exploités par l'établissement lui-même restent sur l'infrastructure interne. Pour les applications de backoffice complexes, avec lesquelles un établissement peut moins se différencier, on observe toutefois une tendance à l'externalisation et à l'utilisation d'applications SaaS. Cela inclut par exemple le CRM, la comptabilité ou les applications de bureautique. La condition requise : des systèmes modulaires, sur lesquels les composants peuvent être développés rapidement, sans menacer la stabilité de l'ensemble du système. En outre, les interfaces compatibles au cloud, visant à relier les systèmes périphériques, sont d'une grande importance.

Conclusion : Les clouds publics peuvent jouer un rôle de plus en plus important dans le secteur financier

Les clouds publics peuvent être utilisés de manière renforcée dans l'environnement financier. Un cadre correspondant est fixé sur le plan réglementaire et les réflexions sur les risques permettent de définir des contremesures qui rendent supportables les risques associés. Il est important d'étudier la décision pour ou contre une externalisation spécifique du cloud avec l'attention requise, de la documenter avec une analyse des risques appropriée et d'appliquer la mise en œuvre sur la base de mesures adéquates. Cela fonctionne au mieux s'il existe une compréhension commune de l'avenir du cloud parmi les représentants du métier, de l'informatique, de la gestion, de la conformité et du droit au sein de l'établissement.

Les utilisateurs précoces parmi les établissements financiers suisses se trouvent déjà à la phase d'exploitation à l'heure actuelle et beaucoup d'autres à la phase de décision stratégique ou des réflexions relatives à la conception. Cela montre que les avantages des environnements de clouds publics sont de plus en plus identifiés et exploités par les établissements financiers suisses. Les établissements qui ne franchissent pas ce pas technologique et innovant en pâtiront à moyen ou long terme.

Le cloud dans l'environnement réglementé Entretien avec Richard Hess

→

« Il n'existe pas de monde sans risque. C'est pourquoi l'objectivation de la discussion sur le cloud est d'une importance capitale pour moi. »

Richard Hess, responsable du numérique à l'ASB

Comment décririez-vous votre rôle à l'ASB, Association suisse des banquiers ?
Richard Hess: J'assure la direction du secteur numérique depuis juillet 2020. Je dirais que ce rôle est varié, interdisciplinaire et enrichissant. Chaque jour est source d'étonnement et d'apprentissage. Au cœur de notre travail, se trouvent les questions et les défis qui naissent dans le contexte du numérique, à l'interface de la technologie et de la réglementation pour l'économie financière. Pour cela, nous élaborons avec nos membres les principes et les approches nécessaires en posant les bonnes questions, en impliquant les bons experts et en assurant la coordination des travaux correspondants dans les comités. Dans ce contexte, nous jouons aussi un rôle de passerelle entre l'industrie financière, les autorités et d'autres acteurs importants comme les grandes entreprises technologiques.

L'expérience montre toutefois que beaucoup des questions qui surgissent ne peuvent pas toujours être abordées à l'aide du schéma classique problème/solution. Aussi, il s'agit souvent d'identifier d'identifier à l'avance les opportunités des différentes tendances pour la place financière et de les accompagner activement du point de vue sectoriel, sans forcément trouver une solution concrète à chaque problème spécifique. Cela concerne par exemple l'open finance ou la tokenisation des actifs. L'objectif commun de toutes ces tâches est que nos membres trouvent en Suisse des conditions-cadres optimales, que nous favorisons en offrant une liberté d'action aux entreprises et en permettant l'innovation.

À l'heure actuelle, nous nous penchons en particulier sur les opportunités et les défis concernant l'open finance, l'intelligence artificielle responsable, l'identité électronique, les monnaies numériques (CBDC) ou les actifs numériques (Digital Assets) et DLT. Les différents aspects réglementaires de l'utilisation des services de cloud public par les banques font aussi partie de nos priorités. En 2019, nous avons déjà publié un guide à ce sujet pour nos membres au nom de l'ASB.

Selon vous, quelles sont les tendances relatives à l'utilisation des services de cloud ?
RH: Une étude publiée récemment par l'ASB sur « L'avenir du banking suisse en perspective » a clairement révélé que le cloud fait partie des ressources clés du futur. Les banques veulent utiliser des services de cloud et connaissent les avantages qui en découlent.

Selon les enseignements tirés de l'étude, le voyage vers le cloud dans le secteur financier est à l'heure actuelle encore largement centré sur l'infrastructure (IaaS, Infrastructure as a Service), tandis que, tandis que la capacité juridique, les applications, les intergiciels, les bases de données et les plateformes de développement restent souvent exploités dans la banque. Un coup d'œil sur l'avenir montre toutefois que le PaaS (Platform as a Service) et le SaaS (Software as a Service) prendront beaucoup d'importance. Le Banking as a Service est lui aussi activement appliqué. L'étude de la Confédération sur l'« examen de la nécessité d'un Swiss Cloud » est très utile dans ce contexte, car elle a déjà pu quantifier cette tendance.

Dans les bureaux, les banques ont déjà beaucoup de contacts avec le cloud public, par exemple en raison de l'utilisation croissante des outils de collaboration comme Microsoft Teams. Mais cela deviendra vraiment intéressant quand les banques migreront des volumes de travail complets de leurs domaines d'activité vers le cloud public.

Enfin, les activités des géants du web comme Microsoft et Google, qui gèrent aussi leurs propres centres de données en Suisse depuis 2018, contribuent aussi à ce que les banques s'intéressent davantage au cloud.

Quels sont les moteurs sous-jacents à l'utilisation croissante des services de cloud ?
RH: Je pense que l'environnement de marché et les besoins changeants des clients et clientes sont des moteurs essentiels. Les smartphones sont devenus incontournables dans notre quotidien. Parallèlement, les nouveaux compétiteurs et les banques concurrentes modifient les attentes des clientes et clients par rapport aux services financiers. La devise : rapidité, simplicité et sécurité. Pour pouvoir s'imposer face à cette concurrence, une mise sur le marché rapide est essentielle. Cela constitue un défi pour de nombreuses banques dotées de systèmes anciens. Dans ce contexte, le cloud peut permettre aux banques de répondre encore mieux aux besoins changeants des clients et clientes et devient ainsi un instrument utile pour les modèles commerciaux innovants. De plus, beaucoup des nouvelles technologies ne sont utilisables que via un cloud. Enfin, la pandémie du COVID-19 a encore accéléré la demande des banques pour les services de cloud, car, par exemple, la plupart des outils de collaboration en ligne ne sont disponibles que depuis le cloud en tant que SaaS.

Comment s'organisent la situation juridique et les conditions-cadres réglementaires concernant l'utilisation du cloud ?
RH: C'est certainement la question clé pour nous. Sur le fond, le principe actuel de réglementation neutre sur le plan technologique et basée sur des principes offre suffisamment de flexibilité en Suisse pour utiliser les services de cloud dans le cadre existant. Mais cela requiert une interprétation concrète des exigences légales et réglementaires en vigueur dans le contexte de cloud. Nous avons élaboré une série de recommandations à ce sujet avec notre guide sur le cloud. En ce sens, nous pensons que la base juridique actuelle est compréhensible et suffisamment réalisable. Cependant, il reste encore des points qui ne sont pas entièrement résolus. La gestion du devoir de publication des données des fournisseurs de cloud aux tiers, sur base du CLOUD Act américain, reste une question controversée sans réponse définitive, y compris parmi les experts. Un autre point important quant à la gestion du risque est le jugement « Schrems II ». Par conséquent, les banques doivent non seulement connaître leur fournisseur de cloud et ses sous-traitants, mais aussi savoir précisément où vont leurs données, où elles sont stockées, qui peut y accéder dans quel but et éventuellement les traiter.

Quel est le feedback de vos membres concernant le guide sur le cloud ?
RH: À notre connaissance, le guide est jugé utile par de nombreux membres et les aide dans leur mise en œuvre des stratégies de cloud. D'après nos membres, le guide permet aussi de cibler immédiatement les discussions sur les sujets centraux au sein des établissements et avec les fournisseurs de cloud. Cela nous réjouit, car c'est la raison pour laquelle nous l'avons rédigé. D'après moi, il a aussi contribué à en finir avec le dogme « non au cloud public » ou du moins à le relativiser et à rendre possible la discussion autour du cloud.

L'objet du guide repose sur des recommandations qui peuvent servir aux banques et aux fournisseurs de cloud dans l'acquisition et l'application de services de cloud. Au total, quatre domaines sont abordés : aides au traitement des données, à la collaboration avec des sous-traitants, aux audits ainsi que gestion des ordonnances des auto-rités internationales quant à la publication des données. Des recommandations sont en particulier données sur les mesures techniques, organisationnelles et contractuelles concernant la protection des données et le respect du secret bancaire dans le cloud.

Selon vous, quels sont les principaux défis concernant la cybersécurité et la confidentialité dans l'adaptation du cloud ?
RH: Il est clair que la cybersécurité est de plus en plus importante, y compris dans le contexte de l'open banking (et de l'échange accru des données avec des tiers). Au niveau sectoriel, nous abordons ce sujet en participant, avec la Confédération, à la mise en place d'un centre de compétences pour la cybersécurité.

Dans le contexte du cloud, le lieu de stockage et la souveraineté des données sont également essentiels ; c'est-à-dire comment conserver la souveraineté sur mes données et imposer mes droits à ce sujet. La transparence est un aspect important dans ce contexte.

Comment évaluez-vous la disponibilité et le développement des capacités requises de vos membres concernant la mise en œuvre des projets de cloud ?
RH: Cela dépend de quels établissements nous parlons. On sait que les banques deviennent de plus en plus des entreprises technologiques. Selon les experts, la tendance est que les collaborateurs des banques doivent posséder à l'avenir davantage de compétences technologiques et inversement, les collaborateurs informatiques doivent en savoir plus sur le métier. La « guerre des talents » pour les compétences informatiques spécifiques, en particulier dans le domaine du cloud, est donc assurément perceptible aussi dans le domaine financier. Les banques sont en concurrence directe avec les entreprises technologiques et doivent se positionner en conséquence pour rester attrayantes en tant qu'employeur. Cela pourrait constituer un défi majeur pour les banques de petite et moyenne taille de gérer leur propre organisation informatique, qui puisse garder le rythme avec toutes les questions juridiques, techniques et liées aux risques. Des coopérations avec des fournisseurs tiers et la fragmentation de la chaîne de création de valeur seraient des orientations possibles. Nous nous efforçons ici de soutenir au mieux nos

membres dans la formation et le perfectionnement de leurs collaborateurs, par exemple par la coopération avec des plateformes de formation sélectionnées.

Où voyez-vous du potentiel supplémentaire concernant l'adaptation au cloud ?
RH: Un argument fort pour l'utilisation du cloud concerne l'intelligence artificielle (IA) et l'apprentissage automatique (AA). L'utilisation de l'IA et de l'AA offre de toutes nouvelles possibilités aux banques de préparer et de fournir de gros volumes de données de qualité. À cela s'ajoute la puissance de calcul disponible à la demande, qui peut être obtenue directement des géants du web, par exemple pour la gestion des transactions ou la détection des fraudes. Enfin, les aspects de sécurité sont une raison essentielle pour laquelle les banques décident de passer dans le cloud.

Selon votre expérience, quels sont les éléments pertinents d'une stratégie de cloud dans votre organisation/secteur ?
RH: Il convient ici de faire la distinction entre les banques nationales et les banques internationales, qui ont des contextes et des besoins différents. Les banques concentrées sur le marché national s'intéressent plutôt aux fournisseurs suisses et ont moins de stratégies complexes. L'expérience montre que les banques internationales se penchent en revanche sur ce sujet de manière beaucoup plus globale. Dans cet environnement, les stratégies de cloud sont souvent définies par la maison mère et déployées dans les différents pays.

La question qui revient toujours, quelle que soit la taille de la banque, est : le cloud est-il un sujet informatique ou métier ? Selon moi, la transition vers le cloud doit impérativement être considérée comme un projet stratégique et discutée au niveau de la direction. Les décisions pour ou contre le cloud et l'appétence au risque doivent être prises à ce niveau.

D'après des entretiens avec des représentants de la banque, il est important pour la mise en œuvre que le principe « cloud first » accompagne le processus de transforma-tion, qui s'étire généralement sur plusieurs années, tout au long du cycle de vie informatique. Cela requiert aussi une vision claire, des principes ainsi qu'une remise en question critique en cas de variations. Il ne faut pas négliger non plus les répercussions organisationnelles des migrations vers le cloud et impérativement en tenir compte.

Selon moi, les aspects réglementaires constituent un point essentiel pour la stratégie de cloud, en particulier dans le secteur financier. Comme indiqué, il s'agit de répondre à toutes les questions relatives au fournisseur de cloud et à ses sous-traitants dès le développement stratégique. Une réponse claire à la question « Qui peut accéder à quelles données, dans quel but, à quel moment et comment ? » est elle aussi essentielle du point de vue du risque. Il ne faut prendre une décision quant au fournisseur que lorsque tous les points cités ont été clarifiés.

Y a-t-il autre chose que vous aimeriez dire à nos lectrices et lecteurs ?
RH: Un monde sans risque n'existe pas. C'est pourquoi une approche objective de la discussion relative au cloud me semble essentielle. Cette étape ne signifie en aucun cas qu'une organisation passe d'un univers sans risque à un environnement ultra-risqué. Il existe une multitude de risques, y compris pour les applications qui sont exploitées en interne dans ses propres centres de calcul. Ce qu'il faut, c'est une approche basée sur le risque concernant les questions pertinentes relatives au cloud. Le cloud offre aux banques qui pèsent minutieusement les risques potentiels une belle occasion d'augmenter leur faculté d'innovation et leur compétitivité.

Notre ambition est de garantir que toutes les banques qui veulent migrer vers le cloud public puissent le faire. Nous sommes impatients de découvrir où ce voyage nous mènera dans les prochaines années. En effet, nous agissons ici dans un environnement très dynamique et en évolution rapide, qui soulève non seulement des questions techniques et réglementaires, mais aussi en dernier ressort des problématiques géopolitiques, qu'il convient de prendre en compte et de discuter.

Le cloud dans le secteur public - un impératif urgent avec un grand potentiel

Le secteur public englobe les organisations à tous les niveaux fédéraux, notamment l'administration publique, l'éducation et la recherche, les organisations de sécurité ainsi que les fournisseurs publics d'énergie, les entreprises publiques de transport et de logistique. En raison de son envergure, ce secteur pourrait devenir un poids lourd de la transition vers le cloud. Pourtant, son utilisation est encore très limitée à l'heure actuelle.

Marc Raum, Thomas Vogt

Le secteur public est soumis au principe de la légalité, énoncé à l'art. 5 al. 1 de la Constitution fédérale, qui impose que tout acte émanant d'une autorité se fonde sur une base légale. Dans ce contexte, les parlements et, dans le cadre réglementaire fixé, l'administration sous sa propre responsabilité, assurent en principe le rôle du législateur. Ainsi, de nombreuses directives sont disponibles sur la base des lois et des ordonnances. Leur interprétation concrète concernant les possibilités et limitations de l'utilisation du cloud est toutefois rarement claire. Les organes de surveillance publics, p. ex. pour la protection des données, se réfèrent certes aux risques, mais offrent rarement eux-mêmes des approches de solution.

L'utilisation des services de cloud est également un sujet politique pour le secteur public, notamment concernant la souveraineté des données dans le contexte international. En 2020, le gouvernement suisse s'est penché sur ce sujet, notamment avec son étude de faisabilité du « Swiss Cloud ». Celle-ci a révélé qu'il existe un besoin très limité voire inexistant d'infrastructure de cloud exploitée par la Confédération, mais un fort besoin de conditions-cadres claires quant à l'utilisation des services de cloud commerciaux. Pour la création de ces conditions-cadres, l'analyse des besoins estime qu'il appartient aux organes publics et notamment aux associations professionnelles et aux législateurs correspondants d'agir.

Jusqu'à maintenant, le secteur public a manqué l'occasion de créer une réglementation claire sur l'utilisation des services de cloud public. Des outils et offres pratiques pourraient sans problème voir le jour en collaboration avec les associations professionnelles.

Tendances et moteurs de l'utilisation du cloud dans le secteur public

Pour le secteur public, l'utilisation du cloud est particulièrement intéressante dans le domaine des applications, où les capacités du cloud offrent une valeur ajoutée directe et les conditions-cadres relatives au stockage et au traitement des données sont clairement définissables pour l'utilisation du cloud. Cela inclut par exemple :

- Portails et applications (ou applications mobiles) pour la fourniture directe de services pour la population et les entreprises privées
- Applications avec un besoin de ressources discontinu, qui doivent être rapidement évolutives
- Services qui doivent permettre un échange de données avec des acteurs externes (p. ex. services d'Open Government Data)
- Applications spécifiques, fournissant des capacités ,
  qui sont soumises à un développement technologique constant, par exemple les services dans les domaines de l'analyse des données, de l'apprentissage automatique ou de l'intelligence artificielle

Des exemples concrets de l'utilisation des services de cloud public dans le secteur public sont notamment la gestion et la fourniture des cartes de topographie suisse par swisstopo, l'application SwissCovid de l'Office fédéral de la santé publique (OFSP), les solutions de test et de développement pour le développement agile et l'utilisation de solutions de cloud dans la communication et la collaboration internes et globales dans de nombreux services publics.

« Mort à petit feu »

La voie vers l'utilisation des solutions de cloud par le secteur public est généralement très chaotique. Outre les conditions-cadres relatives à l'utilisation des services de cloud dans le secteur public qui sont floues, notamment au niveau politique, en particulier concernant la sécurité des informations et la protection des données, il faut surmonter un obstacle majeur : les marchés publics exigent rapidement un appel d'offres avec de nouveaux contrats pour les prestations qui nécessitent déjà une compréhension très précise des futurs modèles d'exploitation, des exigences de conformité et des besoins. Ces derniers impliquent à leur tour des principes d'architecture matures, en particulier dans le domaine de l'intégration, des réseaux et des systèmes de sécurité, pour que les services de cloud public puissent être utilisés efficacement. De nombreux petits services échouent face à ces conditions requises.

En raison de cette approche fragmentée, certains services ont du mal à atteindre le seuil de rentabilité pour assurer le financement requis en interne. Mais la situation s'améliore. Avec les CFF, la Poste et l'administration fédérale, trois grandes organisations ont décidé d'acquérir des services de cloud public. Ces expériences se révéleront précieuses, car elles serviront de modèles. Une démarche stratégiquement coordonnée est également nécessaire pour tirer parti des avantages des services de cloud.

Objectif possible de l'utilisation du cloud dans le secteur public

Comme base à une utilisation sécurisée, conforme et performante des services de cloud, les organisations du secteur public ont besoin d'un développement solide sur le plan politique et largement étayé par des principes stratégiques qui servent de glissières de sécurité pour l'intégration dans le cloud et son utilisation. Pour cela, il est recommandé de ne pas considérer le cloud séparément du point de vue organisationnel, mais comme une partie essentielle, voire l'instrument de la transformation numérique.

De notre point de vue, il existe essentiellement les éléments décisifs suivants pour une transition active et durable vers le cloud dans le secteur public :

- Rendre les expériences visibles
- Créer des principes orientés sur les applications dans le domaine de l'architecture, de la sécurité de l'information et de la protection des données
- Regrouper les besoins par une collaboration forma-lisée des différents services et principes d'approvi-sionnement flexibles, en tirant par exemple parti des potentiels de synergie via les fournisseurs de services informatiques
- Introduire des processus politiques et fixer un objectif avec des scénarios d'application ainsi qu'un planning ambitieux
- Passer à des approches agiles et itératives comme Scrum et SAFe, pour ancrer une culture d'apprentissage qui tolère les erreurs – dans ce contexte, contrôler et adapter constamment l'organisation
- Formation et perfectionnement des collaborateurs et collaboratrices concernant les capacités, modèles et technologies de cloud requis
- Établissement et collaboration dans les initiatives de cloud nationales et internationales pour le regroupement et le ciblage des expertises et des principes de décision dans le contexte de la transition vers le cloud dans le secteur public

Une approche possible pour donner l'élan nécessaire à l'utilisation du cloud dans le secteur public en Suisse consiste en une initiative ciblée et coordonnée sur ce sujet. Des exemples d'initiatives relatives au cloud dans le secteur public sont le G-Cloud du gouvernement britannique, le FedRamp du gouvernement américain, le cloud.gov.au du gouvernement australien ou le Government Commercial Cloud (GCC) de Singapour. Le G-Cloud du gouvernement britannique concerne principalement des conditions-cadres clairement définies pour faciliter l'acquisition de services de cloud. Le FedRamp du gouvernement américain va plus loin en fournissant un processus de certification qui assure une analyse des risques et de la sécurité des services de cloud. Cela permet de décider rapidement et clairement si et quels services de cloud peuvent être utilisés pour tel cas. Avec son initiative cloud.gov.au, le gouvernement australien a défini que les prestations TIC de l'administration

doivent être conçues pour être généralement compatibles au cloud. Le GCC du gouvernement de Singapour permet l'utilisation de services de cloud innovants pour les domaines d'application sensibles de l'administration.

Avec GAIA-X, l'Europe a lancé une grande initiative de cloud qui aborde des domaines similaires à ceux mentionnés ci-dessus, qui doit dans tous les cas être suivie aussi par le secteur public suisse. La capacité de GAIA-X de proposer ou d'identifier des services de cloud dans différentes classes de service peut être très utile pour l'utilisation du cloud dans le secteur public. Le rapport sur l'examen de la nécessité d'un Swiss Cloud du Conseil fédéral a également abordé cette orientation avec la recommandation de contrôle d'un système de certification pour les services de cloud.

S'agissant de la transformation vers le cloud dans son ensemble, le secteur public a encore du potentiel pour exploiter des synergies supplémentaires avec des coopérations entre les différents niveaux fédéraux et organisations. Comme de nombreuses questions relatives au cloud sont identiques dans les différentes organisations du secteur public, une collaboration ouverte et intensive est recommandée. L'élaboration commune de principes de décision solides qui font avancer la transformation vers le cloud et avec elle la transformation numérique dans son ensemble pour les différentes organisations est tout aussi importante.

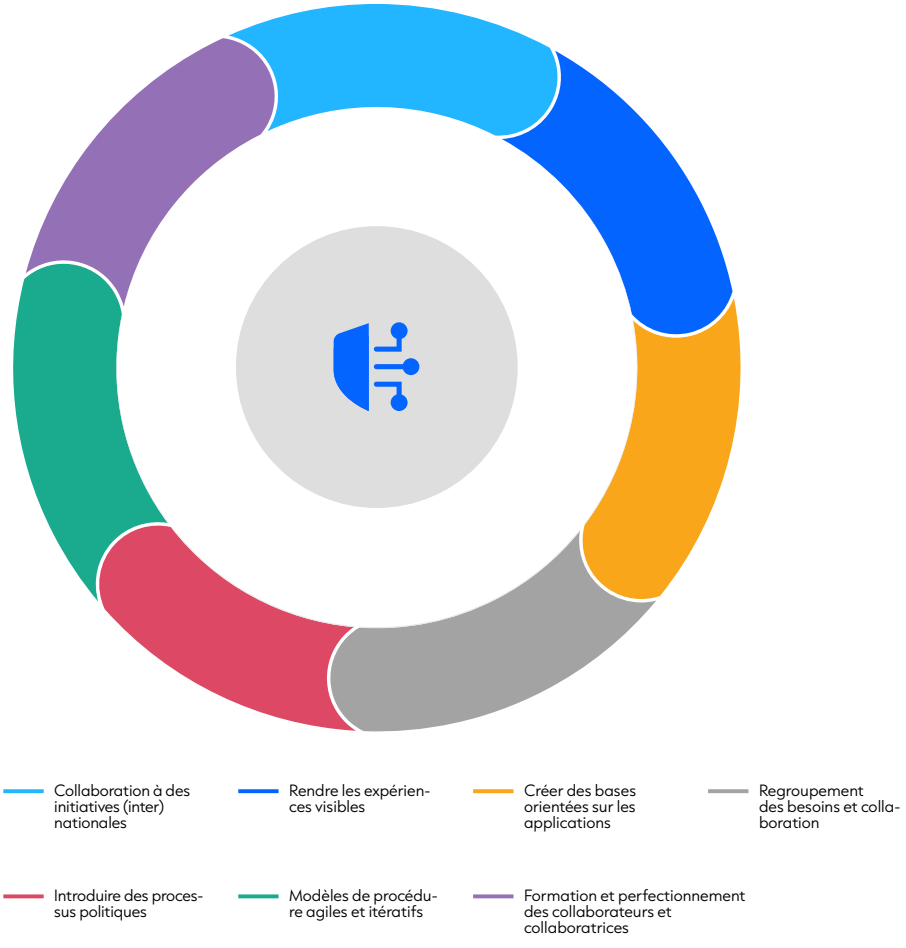


Illustration 1 : Éléments recommandés pour une transition réussie vers le cloud
1 https://www.newsd.admin.ch/newsd/message/attachments/64462.pdf

Pionnier en Suisse dans l'utilisation des services de cloud public

→

« Notre voyage dans le cloud nous a conduits d'une infrastructure exploitée sur site à une architecture hybride puis aujourd'hui à une mise en œuvre du portail géographique largement basée sur le cloud. »

Hanspeter Christ Diplômé de l'EPF de Zurich en tant qu'ingénieur géomètre, Hanspeter Christ travaille depuis 2000 à l'Office fédéral de topographie swisstopo. Chez swisstopo, il s'occupe depuis 2004 de la conception, du développement et de l'exploitation d'infrastructures de données géographiques composées principalement de modules open source. Dès 2008, il a collecté les premières expériences dans l'utilisation des services de cloud public et fait avancer en première ligne les années suivantes la conception du cloud et la migration de l'ensemble de l'infrastructure de données géographiques de la Confédération dans le cloud public.

« En 2008, nous avions une demande urgente des clients pour l'utilisation du matériel cartographique numérique de swisstopo. Si nous avions acquis et intégré notre propre infrastructure selon l'approche traditionnelle, le matériel requis n'aurait même pas été disponible à la date de mise en ligne souhaitée. »

Les moteurs de l'utilisation du cloud chez swisstopo étaient le besoin d'une infrastructure flexible qui s'adapte le mieux possible aux besoins de l'utilisation du portail géographique ainsi que des services de cartographie extrêmement évolutifs. La transition vers le cloud de swisstopo englobait d'abord la migration vers une architecture hybride, utilisant à la fois des ressources internes et des ressources du cloud public. À l'étape suivante, l'architecture du portail géographique a été développée pour en faire aujourd'hui une infrastructure largement basée sur le cloud.

Ce processus marque aussi notre nouvelle approche :

« Nous ne définissons pas d'infrastructures et architectures souhaitées sur le papier, mais suivons le marché en nous concentrant de manière ciblée sur les « fruits mûrs » dotés d'un fort potentiel. »

Recommandations pour les organisations publiques concernant les migrations dans le cloud public

- Les avantages des capacités du cloud ne peuvent pas être exploités au maximum avec la seule migration des machines virtuelles dans le cloud public (lift and shift). L'utilisation des modèles de solution de cloud optimisés (par exemple avec des architectures microservice) permet de tirer parti de potentiels nettement plus importants. Les services propres aux fournisseurs imposent des limites à de nombreuses organisations d'utilisateurs, compliquant une migration ultérieure. Dans ce contexte, les principes d'architecture standardisés contribuent à garantir des décisions durables.

- Une culture d'expérimentation productive avec les nouvelles technologies permet de réaliser des gains d'efficacité élevés dans le développement et l'exploitation des solutions informatiques. Les modes de travail agiles, comme SAFe, qui mettent la recherche de nouvelles approches au programme quotidien avec des sprints d'innovation et de planification, conviennent très bien pour cela.

« Le développement des capacités nécessaires des collaborateurs dans le do-maine du cloud aux différents postes d'une organisation est un facteur de réussite essentiel pour une adaptation performante, sécurisée et durable des services de cloud public. »

Cédric Moullet a étudié à l'EPFL et est titulaire d'un MBA de la Haute école de gestion de Fribourg et d'un CAS en intelligence artificielle de la Haute école spécialisée de Berne. Il a débuté sa carrière professionnelle à l'EPF de Zurich. Il a ensuite travaillé pour le développeur logiciel américain Autodesk et l'entreprise open source Camptocamp, qui l'a conduit chez swisstopo puis à l'Office fédéral de l'informatique et de la télécommunication (OFIT). Il y a dirigé le développement de l'application SwissCovid et du certificat Covid. Depuis le 1er septembre 2021, Cédric Moullet est responsable du service Numérisation & IT au Club alpin suisse (CAS).

Cédric a pu se servir des expériences spécialisées dans le cloud acquises chez swisstopo, où il était responsable du développement du portail géographique, dans la conception des applications SwissCovid et certificat Covid pendant la crise du coronavirus. On s'attendait à un très grand nombre d'accès, mais les centres de calcul propres n'étaient pas dimensionnés pour cela. Parallèlement, il était essentiel que les citoyennes et citoyens aient confiance enz la solution. Ces défis ont été surmontés grâce à une approche hybride : un réseau de diffusion de contenu (RDC) gère les accès de manière flexible. Les fonctions de base du back-end ont été fournies dans les propres centres de calcul. De plus, le code a été mis à disposition en open source et est soumis à un test public de sécurité pour que chacun puisse se convaincre de son fonctionnement. Le service RDC avait en outre l'avantage d'être facilement intégrable, ce qui a accéléré la mise à disposition de la solution. Le transfert de connaissances entre les spécialistes eux-mêmes a été très rapide. Il fallait décider si les adresses IP des utilisatrices et utilisateurs afficheraient des données personnelles, car celles-ci, combinées au CovidCode, permettent par exemple de déduire si quelqu'un est malade.

Mais selon l'expérience de Cédric, la technologie n'est qu'un élément de la sécurité :

« Le maillon faible est souvent l'individu. Le passage dans le cloud renforce ces risques. »

Recommandations pour les organisations publiques concernant les migrations dans le cloud public

- L'accès à un groupe d'experts aide à concevoir correctement et à réaliser rapidement les solutions liées au cloud. L'objectif devrait consister à habiliter les collaborateurs et collaboratrices internes par des transferts de connaissances et de responsabilités.
- Il faut cultiver activement la sécurité et la confiance. Pour cela, les architectures sécurisées et une grande transparence (p. ex. via l'open source et les audits) sont des éléments importants.

eraneos

Experienced in a wide range of industries

Eraneos Group est un groupe international de conseil en gestion et en technologie qui fournit des services allant de la stratégie à la mise en œuvre. Il est issu de l'alliance de Ginkgo Management Consulting, Quint Group et AWK Group, annoncée en 2021. Le groupe est au service de clients sur trois continents, où un mil-lier de professionnels dévoués et hautement qualifiés travaillent conjointement pour libérer le plein poten-tiel du monde digital. Les services comprennent le développement de modè-les d'affaires numériques, l'ana-lyse de données, la cybersécurité, le sourcing, le conseil en informatique et la gestion de projets de trans-formation complexes. Le groupe Eraneos est établi en Suisse, en Allemagne, au Luxembourg, en Espagne, aux Pays-Bas, en Chine, à Singapour et aux États-Unis. En 2021, il a réalisé un chiffre d'affaires de près de 200 millions d'euros.

Contact us >

Our offices >

Visit our website >