



LA TRANSITION VERS LE CLOUD

Mode d'emploi pour une évaluation
factuelle des risques

Résumé

Le passage au cloud est aujourd’hui un choix pertinent pour la plupart des entreprises, organisations et administrations publiques car grâce aux avancées technologiques le « nuage » est sûr et extrêmement utile. À la clé : des possibilités de développement et opportunités inédites.

Or, ce passage doit être réfléchi et anticipé. Comme pour tout projet, il y a divers risques qu’il s’agit d’identifier et d’évaluer. La décision pour le cloud doit donc reposer sur une rigoureuse évaluation de ces risques. Le présent document a pour vocation d’accompagner les organisations dans ce processus.

L’un des facteurs clés est par ailleurs la façon dont l’entreprise désireuse d’externaliser ses données va s’organiser, ce qui dépend aussi et surtout de sa taille et de l’envergure de son projet cloud. Une organisation claire des compétences et responsabilités, comprenant l’ensemble des départements spécialisés impliqués, est indispensable. C’est la base d’un processus décisionnel bien structuré permettant au besoin à l’échelon supérieur de prendre des décisions rapides.

La mise en place d’une solution cloud doit également prendre en compte le contexte réglementaire. La conformité, ou compliance en anglais, et la gouvernance sont également des enjeux importants pour tous les projets.

© (2021) Microsoft Corporation. All rights reserved. Microsoft, Windows and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational and discussion purposes only and represents the current view of Microsoft Corporation or any Microsoft Group affiliate as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment or binding offer or acceptance of any warranties, liabilities, wrongdoing etc. on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this document.

Sommaire

| | | |
|---|---|----|
| 1 | Le cloud, un facteur clé pour le succès de l'entreprise | 4 |
| 2 | Conformité : des dispositions claires pour faciliter le contrôle..... | 6 |
| 3 | L'assurance risque (risk assurance) | 10 |
| 4 | Le processus d'évaluation des risques..... | 14 |
| 5 | La gouvernance du cloud | 27 |

Figures

| | | |
|------------|---|----|
| Figure 1 | – Structure du document..... | 5 |
| Figure 2 | – Les principales exigences de conformité relatives aux données | 7 |
| Figure 3 | – Les données peuvent être soumises à différentes exigences de conformité en fonction de leur localisation, et la responsabilité pour les données peut être répartie entre plusieurs acteurs..... | 7 |
| Figure 4 | – Répartition de la responsabilité..... | 10 |
| Figure 5 | – Microsoft Assurance Framework..... | 13 |
| Figure 6 | – Appréciation et évaluation des risques..... | 14 |
| Figure 7 | – Les six étapes du processus de gestion des risques selon la norme ISO 31000 | 15 |
| Figure 8 | – Les niveaux de risque..... | 16 |
| Figure 9 | – Liste des risques potentiels pour la migration vers le cloud et l'utilisation des services cloud..... | 17 |
| Figure 10 | – Effet du risque – grille d'évaluation..... | 18 |
| Figure 11 | – Probabilité d'occurrence d'un risque : grille d'évaluation..... | 19 |
| Figure 12 | – Exemple de matrice d'évaluation des risques | 19 |
| Figure 13 | – Exemple de contrôle pour la gestion des autorisations d'accès..... | 22 |
| Figure 14 | – Intégration des contrôles du fournisseur de services cloud..... | 23 |
| Figure 15 | – Les éléments d'une option risque étudiée | 25 |
| Figure 15b | – Mix optimal de mesures contractuels, techniques et organisationnelles | 25 |
| Figure 16 | – Les risques évaluées, avant et après la mise en œuvre d'un ensemble de mesures d'atténuation | 26 |
| Figure 17 | – Harmonisation des structures de gouvernance du client et du fournisseur de services cloud..... | 29 |
| Figure 18 | – L'approche MVP pour l'élaboration de la gouvernance du cloud | 30 |

Avis de non-responsabilité

Ce document reprend les questions souvent posées par nos clients sur l'utilisation des solutions de cloud computing. Il devrait vous permettre de mieux comprendre les contextes techniques et juridiques impliqués par l'utilisation d'une solution d'informatique en nuage. Ce document n'inclut pas un examen spécifique de la situation juridique individuelle. Pour obtenir une évaluation juridique individuelle et définitive sur la recevabilité de l'utilisation des solutions Microsoft Cloud spécifique à votre cas, vous devrez donc recourir séparément à un conseil juridique.

1 LE CLOUD, UN FACTEUR CLÉ POUR LE SUCCÈS DE L'ENTREPRISE

Le nombre d'entreprises misant sur des applications cloud ne cesse de croître. Grandes ou petites, elles sont toujours plus nombreuses à penser que le cloud, grâce à l'efficacité et la robustesse de ses processus, offre une base pour accélérer l'innovation. Le cloud permet d'externaliser différents processus de travail liés à la productivité, favorise la modernisation des environnements applicatifs existants et une approche client holistique au travers des canaux digitaux. C'est pourquoi même des entreprises réglementées telles que les instituts financiers sont aujourd'hui prêtes à traiter des données sensibles ou essentielles en cloud public. On observe une évolution similaire dans l'administration publique et le secteur de la santé où, à l'instar du secteur bancaire, la discrétion et la confidentialité font partie intégrante du modèle économique.

Aujourd'hui, même des services centrés sur le patient ou essentiels à l'activité concernée, donc des applications qui doivent répondre aux exigences les plus strictes en termes de sécurité et de conformité légale et réglementaire, sont gérés dans le cloud. La plupart des entreprises admettent qu'un cloud public opéré par un prestataire sérieux offre un niveau de sécurité au moins égal, sinon supérieur, à celui qu'elles sont en mesure d'assurer par elles-mêmes. De plus en plus de dirigeants d'entreprise et de conseils d'administration ont compris que les infrastructures basées sur le cloud sont un facteur clé pour assurer et pérenniser le succès de l'entreprise, et qu'elles jouent donc un rôle très important du point de vue stratégique.

Le cloud est sûr

Les doutes concernant la sécurité des données figuraient il n'y a pas si longtemps encore parmi les raisons principales pour ne pas utiliser le cloud. Si ces doutes sont aujourd'hui largement dissipés, c'est aussi et surtout grâce à l'essor général de la digitalisation et à la maturité de la technologie du cloud.

Mais malgré une technologie plus sûre et plus performante, il est encore aujourd'hui indispensable de bien planifier sa transition vers le cloud. Différents critères sont à prendre à compte, depuis le choix de la technologie jusqu'aux aspects culturels et organisationnels en passant par le respect d'exigences concrètes telles que les dispositions légales ou les réglementations spécifiques, par exemple liées à un secteur en particulier. On citera ici à titre d'exemple la loi suisse sur la protection des données, les circulaires de l'Autorité fédérale de surveillance des marchés financiers FINMA, ou encore la nécessité de protéger les données sensibles. Les développements à l'échelle internationale sont un autre facteur qui gagne en importance aujourd'hui pour l'évaluation de tout projet cloud spécifique, concrètement les discussions relatives à l'arrêt « Schrems II » ou la suppression de fait de l'accord « Privacy Shield » entre la Suisse et les États-Unis. Ces deux sujets concernent le cadre juridique des transferts internationaux de données, notamment en dehors de l'Europe ou vers des pays assurant un niveau de protection moindre.

Pas de passage au cloud sans une évaluation factuelle des risques

C'est un fait : tout projet cloud exige de soigneusement peser les opportunités et les risques, en particulier en ce qui concerne le besoin de protéger les applications et bases de données externalisées ou le respect des exigences juridiques et réglementaires pertinentes. Or, il ne s'agit pas seulement d'évaluer proprement les risques d'une externalisation vers le cloud mais aussi de les gérer en aval.

C'est justement là qu'intervient le présent document. Il propose des pistes sur la manière d'aborder l'évaluation des risques et montre comment intégrer les exigences juridiques et réglementaires dans le cadre de contrôle d'une plateforme cloud afin d'en permettre une évaluation fiable. Il s'interroge sur les mesures organisationnelles, techniques ou contractuelles en place et sur leur aptitude à répondre avec efficacité aux exigences définies, comme par exemple d'empêcher tout accès non autorisé à des ensembles de données. Le sujet est donc la méthodologie de base d'une évaluation factuelle des risques et les différents aspects à prendre en compte.

Dans ce contexte, il est important de comprendre la stricte répartition des tâches entre le client et le fournisseur des services cloud. L'objectif est d'apporter au client un niveau de transparence et des preuves fiables qui lui permettent de juger en connaissance de cause et de faire des choix éclairés. Un principe s'applique dans tous les cas : c'est au client qu'incombe la responsabilité de l'appréciation finale. En re-

vanche, il est strictement interdit au fournisseur de services cloud de se prononcer sur la conformité juridique d'une implémentation spécifique.

Il en découle la deuxième vocation du présent document : servir de guide pour trouver rapidement les informations, rapports d'audit et illustrations techniques pertinentes, sachant notamment que de nombreux clients ne disposent pas d'un service juridique ou de gestion des risques dédié ayant les compétences essentielles requises.

Microsoft propose des services cloud à partir de centres de données basés en Suisse

Opérant en Suisse depuis plus de 30 ans, Microsoft dispose aujourd'hui d'un réseau de plus 4'600 entreprises partenaires ancrées localement et entretient un contact régulier et une relation de confiance avec les régulateurs et les autorités de surveillance. Toujours à l'écoute, nous nous efforçons de comprendre les appréhensions de nos clients pour mieux y répondre. C'est pourquoi Microsoft a décidé de proposer ses propres services cloud à partir de centres de données situés en Suisse et de stocker les données dormantes de certains services sur le territoire suisse. Il en va de même pour les avenants propres à un secteur spécifique, comme par exemple le Financial Services Amendment, l'avenant relatif aux services financiers dont bénéficient nos clients financiers suisses compte tenu des spécificités locales.

Ces deux initiatives sont pour nos clients des outils de contrôle supplémentaires pour tout ce qui concerne l'identification, l'évaluation et la gestion des risques éventuels. Elles s'inscrivent dans notre volonté d'aider le mieux possible les entreprises suisses à profiter des avantages du cloud hyperscale dans une approche tournée vers l'avenir et conforme à la réglementation. L'accueil largement favorable réservé à cette offre trouve son écho dans la liste grandissante d'entreprises suisses bénéficiant de services cloud à partir des centres de données locaux. Plus de la moitié d'entre elles sont issues de secteurs réglementés, à savoir le secteur financier, le secteur de la santé ou les pouvoirs publics.

Nous sommes conscients du fait que les thèmes à aborder dans le cadre d'une évaluation des risques peuvent être très complexes. Aussi avons-nous opté dans le cadre du présent document pour une représentation simplifiée pouvant être élargie en fonction des besoins. Aucune connaissance particulière n'est requise pour suivre nos explications des principes essentiels du cloud. Nous avons joint sous forme de modèles les formulaires types ou approches concernés.

Le cloud offre un grand nombre de possibilités. Le présent document ne pourra donc pas répondre à toutes les exigences. Un renvoi est fait vers d'autres documents importants.

Ce document se base sur le schéma suivant :

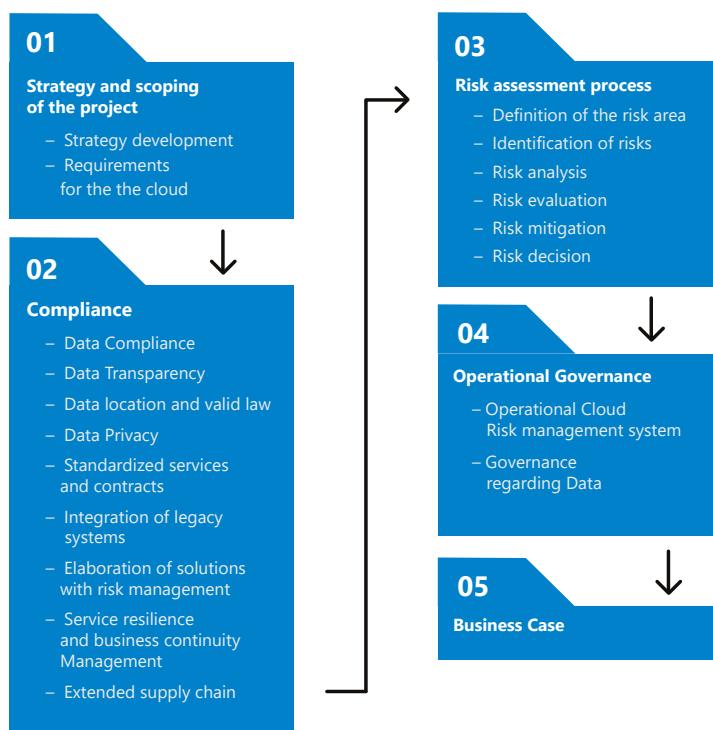


Figure 1 – Structure du document

2 CONFORMITÉ : DES DISPOSITIONS CLAIRES POUR FACILITER LE CONTRÔLE

Que veut dire conformité/compliance ?

La conformité désigne le respect, par les entreprises et leur personnel, de l'ensemble des dispositions légales et directives internes en vigueur. Mais elle signifie aussi que les entreprises contrôlent leurs fournisseurs et prestataires de services dans le cadre de leur chaîne d'approvisionnement de manière à assurer le respect de ces exigences.

La conformité en lien avec les données : un aperçu

Pour divers types de données, il y a des prescriptions de conformité à respecter. Le tableau ci-après donne un aperçu des principales dispositions :

| Type de données | Dispositions suisses | Loi |
|---|---|--|
| Données personnelles et données personnelles particulièrement sensibles | Preuve de la nécessité du traitement des données Mise en place d'une protection adéquate des données personnelles Information des personnes concernées du traitement et de la localisation des données Droit d'accès et droit d'effacement Minimisation des données et effacement | Loi fédérale sur la protection des données RGPD |
| Données bancaires | Preuve de la classification et de la protection spécifique des données des clients des banques Garantie que le régulateur puisse disposer en temps opportun des données relevant de son territoire et y accéder | LB Circulaires FINMA |
| Données financières du bilan et du compte de résultat | Obligation de conservation pour le bilan et le compte de résultat Obligation de fournir des renseignements et garantie que le régulateur puisse disposer en temps opportun des données relevant de son territoire et y accéder. | Olico CO |
| Données fiscales | Obligation de conservation pour les impôts et en particulier données liées à la TVA Obligation de fournir des renseignements et garantie que le régulateur puisse disposer en temps opportun des données relevant de son territoire et y accéder | LTVF |
| Données liées au contrôle à l'exportation | Collecte et stockage de données concernant des biens soumis au contrôle à l'exportation ou des composantes de ces biens (biens militaires ou à double usage, par exemple) Obligation de conservation, obligation de fournir des renseignements et garantie que le régulateur puisse disposer en temps opportun des données relevant de son territoire et y accéder | Loi sur le contrôle des biens |
| Données de produits | Collecte et stockage de données décrivant les processus d'élaboration et les composantes du produit ainsi que les tests réalisés Obligation de conservation | LSPro |

| Type de données | Dispositions suisses | Loi |
|---|--|------|
| Données de recherche | Collecte et stockage de données décrivant les contenus et procédures de recherche, les parties prenantes, les résultats, les tests réalisés ainsi que les résultats de ces tests Obligation de conservation, obligation de fournir des renseignements et garantie que le régulateur puisse disposer en temps opportun des données relevant de son territoire et y accéder | LERI |
| Données IP | Descriptions des informations de l'adresse IP et de son enregistrement Précision du lieu et du pays où l'adresse IP est allouée du point de vue fiscal | LDA |
| Données soumises au secret de fonction et professionnel | Données gérées par l'État et soumises au secret de fonction. Obligations de conservation, de fournir des renseignements et d'effacement. | CP |

Figure 2 – Les principales exigences de conformité relatives aux données

Les données doivent être analysées au regard des exigences de conformité qui les concernent, catégorisées en fonction de cette analyse puis traitées au moyen de mesures adéquates.

Puisqu'il est alors possible de les déplacer, les réflexions ci-dessus permettent de préciser les défis en termes de conformité :

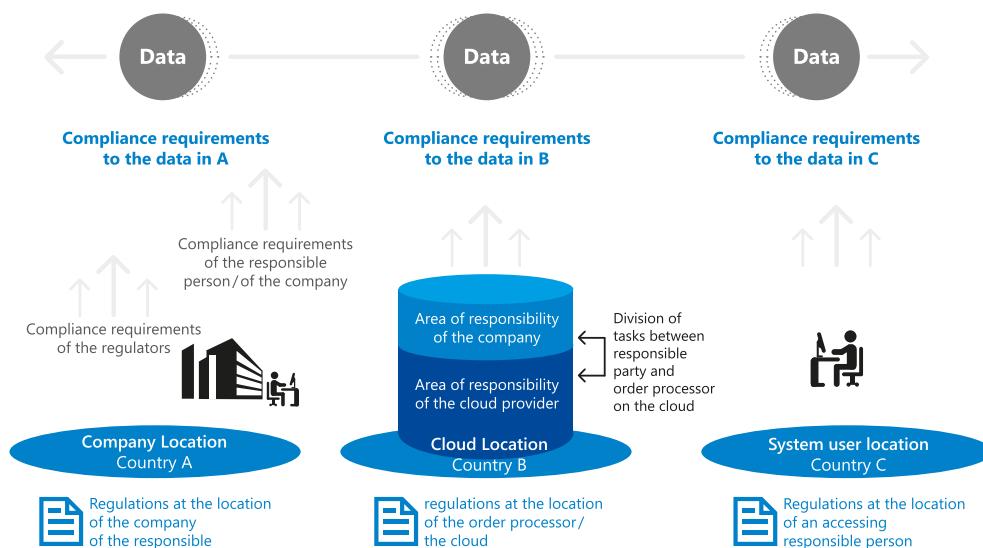


Figure 3 – Les données peuvent être soumises à différentes exigences de conformité en fonction de leur localisation, et la responsabilité pour les données peut être répartie entre plusieurs acteurs.

À titre d'illustration, on citera l'exemple d'une entreprise suisse qui déplace des données personnelles particulièrement sensibles de citoyens et citoyennes suisses dans le cloud au sein de la zone UE, par exemple dans les Pays-Bas. Les données y sont donc soumises à une protection adéquate comme c'est le cas en Suisse, à savoir au règlement européen sur la protection des données (RGPD). L'entreprise chiffre néanmoins ses données pour garantir qu'elles ne puissent être lues en cas de fuite de données. Elle assume donc la responsabilité de stocker les données chiffrées sur le cloud, d'y prévoir un système de basculement en cas de problème (failover) et de mettre en place une sauvegarde. De son côté, le prestataire de services cloud assume la responsabilité pour l'infrastructure, la cyberprotection des systèmes et la continuité du service conformément au SLA (service level agreement, ou accord sur les niveaux de services).

Enfin, le personnel de l'entreprise qui y est autorisé peut accéder aux données de partout dans le monde. Ce dernier point presuppose une sécurisation suffisante des terminaux de ces usagers (endpoint protection). Par ailleurs, ces usagers sont tenus, en vertu d'instructions données en ce sens, de ne pas accéder aux données depuis certains pays ni de les y télécharger localement si ces pays n'offrent pas une protection adéquate des données.

La transparence est importante

Il est impératif de documenter la conception de la solution cloud établie par les responsables sécurité et conformité du client, lors de sa mise en place et durant le fonctionnement qui s'ensuit. Toute modification ultérieure doit également être consignée. Sans une information détaillée sur la conception de la solution cloud et sur la manière dont différents contrôles de sécurité ont été implémentés, les responsables de la gestion des risques ne sont pas en mesure d'évaluer la sécurité du cloud. Microsoft offre dans le cadre de ses services la transparence détaillée requise sur la conservation et la gestion des données dans le cloud en accord avec les exigences de conformité.

Choisir soigneusement la localisation des données et la loi applicable

La loi du pays dans lequel les données seront gérées est de prime importance. Le centre de données cloud pouvant se trouver dans un autre pays que le siège social du client, la loi applicable peut diverger de celle en vigueur dans le pays du client.

La plupart des services Microsoft Azure permettent au client de choisir parmi les pays dans lesquels le groupe opère ses centres de données celui dans lequel les données dormantes seront stockées. Le client doit impérativement savoir quelle loi s'applique à son contrat. L'évaluation et le choix par le client de la loi applicable doivent donc systématiquement précéder le recours aux services cloud.

Réaliser l'analyse d'impact relative à la protection des données

Les prescriptions telles que le RGPD / General Data Protection Regulation (GDPR) garantissent un haut niveau de contrôle sur le traitement des données à caractère personnel des individus. Pour garantir un traitement sûr des données à caractère personnel et protéger la vie privée des individus, il est primordial que les responsables des données ainsi que les responsables du traitement des données respectent ce règlement.

À l'heure d'évaluer un service cloud, il est tout aussi indispensable de réaliser une analyse d'impact relative à la protection des données (Data Protection Impact Assessment, DPIA) que de s'assurer que le système répond à l'exigence de protection de la vie privée dès la conception, ou « privacy by design ». Lors d'une analyse des risques du cloud, nous recommandons de commencer par la lecture de ce [guide RGPD simplifié](#). Notre [Centre de gestion de la confidentialité \(Trust Center\)](#) offre en outre un aperçu détaillé du RGPD, un aperçu des solutions RGPD intégrées dans chaque produit Microsoft, une FAQ RGPD et diverses ressources sur le RGPD tels que des livres blancs ou des vidéos.

Les services et contrats standardisés sont la règle

Les plateformes cloud se nourrissent de synergies impossibles à atteindre sans une standardisation systématique. La plupart des approches et solutions techniques ainsi que les conditions contractuelles y afférentes se présentent de ce fait sous une forme rigoureusement standardisée. Des avenants sont prévus pour les secteurs ayant des exigences spécifiques, comme l'avenant relatif aux services financiers (« Financial Services Amendment ») ou celui sur le secret professionnel (« Professional Secrecy Amendment »).

La standardisation des solutions techniques et des contrats fait la distinction entre contrats de services cloud d'une part et contrats d'externalisation plus traditionnels d'autre part, ces derniers étant personnalisables grâce à l'intégration de solutions techniques sur mesure.

Intégration de systèmes hérités (« legacy »)

L'intégration dans le cloud de systèmes hérités pose un certain nombre de défis, tant pour la migration que pour l'utilisation simultanée de solutions locales et cloud. Ces défis portent principalement sur les modalités de l'authentification et des autorisations d'accès ainsi que des flux de données entre les environnements cloud et locaux dans le cadre de l'utilisation simultanée (pendant la transition, par exemple).

Microsoft dispose de l'expérience, des outils et des ressources nécessaires pour soutenir les clients dans l'élaboration de scénarios de migration capables de répondre à ces défis. Pour la mise en place de services cloud, Microsoft propose par ailleurs un support direct via « Microsoft FastTrack » et ses partenaires pour la migration. C'est un soutien pour les clients qui s'est révélé très utile par le passé.

Élaboration de solutions avec l'équipe gestion des risques

Le modèle du cloud computing implique de transférer une partie de la gestion et de l'utilisation des services informatiques au fournisseur de services cloud. Le client doit vérifier si les exigences en matière de sécurité et de contrôle proposées par le fournisseur sont conformes aux directives internes du client.

Les différences de conception des systèmes de contrôle mis en place par les fournisseurs de services cloud et les clients peuvent donner lieu à des failles obligeant le client à recourir à des scénarios alternatifs pour minimiser les risques ou à renoncer à certaines mesures utilisées jusque-là dans cette optique.

Un facteur clé de succès est ainsi la mise en place en interne d'un processus de gouvernance mature capable de gérer des exceptions en termes de risques. À défaut, l'absence d'une due diligence rigoureuse peut conduire à mal évaluer, en l'occurrence surévaluer, les risques du cloud computing et à stopper net le projet. Le fournisseur de services cloud peut reprendre les points évoqués par l'équipe gestion des risques du client et contribuer, grâce à des mesures et contrôles divers, à une clarification des risques considérés comme élevées.

Résilience du service et gestion de la continuité d'activité

L'externalisation de données et de processus va de pair avec une plus grande complexité du système d'information concerné puisqu'il s'agit de réunir et de coordonner différents acteurs responsables de différentes composantes.

Les clients doivent être en mesure de prouver que leurs services et processus restent fonctionnels en cas de temps d'arrêt ou de catastrophe, conformément aux exigences de leur politique. Les processus de reprise d'activité et de continuité d'activité du client doivent prendre en compte à la fois le service informatique interne et le fournisseur des services cloud.

Par conséquent, l'équipe en charge de la gestion de la continuité d'activité (Business Continuity Management, BCM) du client doit non seulement tenir compte du fournisseur de services cloud dans la conception et la mise à l'épreuve de ses mesures mais aussi prouver que les éventuelles stratégies de sortie fonctionnent. Pour soutenir ces évaluations et solutions BCM et fournir au client en permanence les preuves attestant des capacités BCM, le portail Microsoft « Service Trust Portal » permet à tout moment et en toute transparence de trouver l'information sur les tests BCM réalisés par Microsoft et sur leurs résultats afin de les intégrer dans les rapports de conformité de l'entreprise.

Chaînes d'approvisionnement élargies (externalisation de la chaîne)

La plupart des fournisseurs de services cloud font appel à des tiers pour la fourniture d'une partie de leurs prestations. Microsoft s'engage à cet égard explicitement à exposer en toute transparence les modalités du recours à des tiers pour le fonctionnement et l'administration de services cloud. Du point de vue du client, l'externalisation vers un fournisseur majeur de ce type de services tel que Microsoft peut s'effectuer indirectement. Ainsi, la place de marché Azure, ou « Azure Marketplace », propose des centaines de services tiers qui fonctionnent avec « Azure ». Pour le client, le défi consiste alors à assurer de façon continue la sécurité et la visibilité du service de bout en bout dans le cadre d'une chaîne de services potentiellement longue, ce afin de garantir encore et toujours la conformité des services avec les exigences internes en matière de conformité. Ce type de chaînes de services comprenant plusieurs sous-traitants n'est pas nouveau dans le domaine de l'externalisation. Dans le domaine du cloud, il est plutôt fréquent.



3 L'ASSURANCE RISQUE (RISK ASSURANCE)

De nombreuses entreprises et organisations voient dans l'adoption de solutions cloud une opportunité de baisser sensiblement les coûts, d'améliorer de façon dynamique la performance et d'augmenter la scalabilité. Ceci notamment parce qu'une partie importante des ressources jusque-là gérées en interne sera désormais externalisée.

Il n'est pas rare pour un client d'emprunter une approche connue et classique de l'externalisation pour ses projets cloud. Or, même s'il y a des similitudes, il convient de prendre en compte un certain nombre d'aspects fondamentaux pour les projets d'externalisation basés sur le cloud.

Le cloud computing misant sur une grande échelle (l'hyperscale), beaucoup d'aspects sont réglés de manière standardisée. D'où l'importance pour le client d'étudier en amont les clauses des contrats pour clarifier les éventuelles questions ou doutes dans le cadre d'un dialogue libre et ouvert.

La pratique montre que l'évaluation d'une plateforme cloud est aussi l'occasion de réexaminer les aspects liés à la sécurité des données. La traditionnelle défense du périmètre est dépassée, et les entreprises doivent relever le défi de protéger contre des groupes criminels ou même le cyberespionnage entre États une surface d'attaque clairement hétérogène.

Il est donc primordial pour les entreprises d'identifier les opportunités et risques du cloud dans une approche globale et de les évaluer de façon exhaustive. Cela exige une démarche formalisée visant à mieux comprendre les risques d'un environnement d'exploitation basé sur le cloud et à y répondre. L'expérience montre que l'inaction est nettement plus risquée et entraîne souvent des coûts élevés.

Même si les responsabilités sont partagées, le client garde le contrôle

Les solutions cloud peuvent être réalisées sous forme d'infrastructure IaaS (Infrastructure as a Service), de plateforme PaaS (Platform as a Service) ou de logiciel SaaS (Software as a Service). La répartition des responsabilités entre le fournisseur de services cloud et le client varie en fonction du modèle de services cloud choisi. Le nombre de responsabilités que l'on peut déléguer au fournisseur de services cloud dépend de la part que représentent les services dans la solution choisie. Il faut toutefois savoir que la responsabilité sera toujours partagée entre les deux parties (répartition de la responsabilité) et que même pour les solutions SaaS (Microsoft 365 ou Dynamics 365, par exemple), le client garde en partie le contrôle.

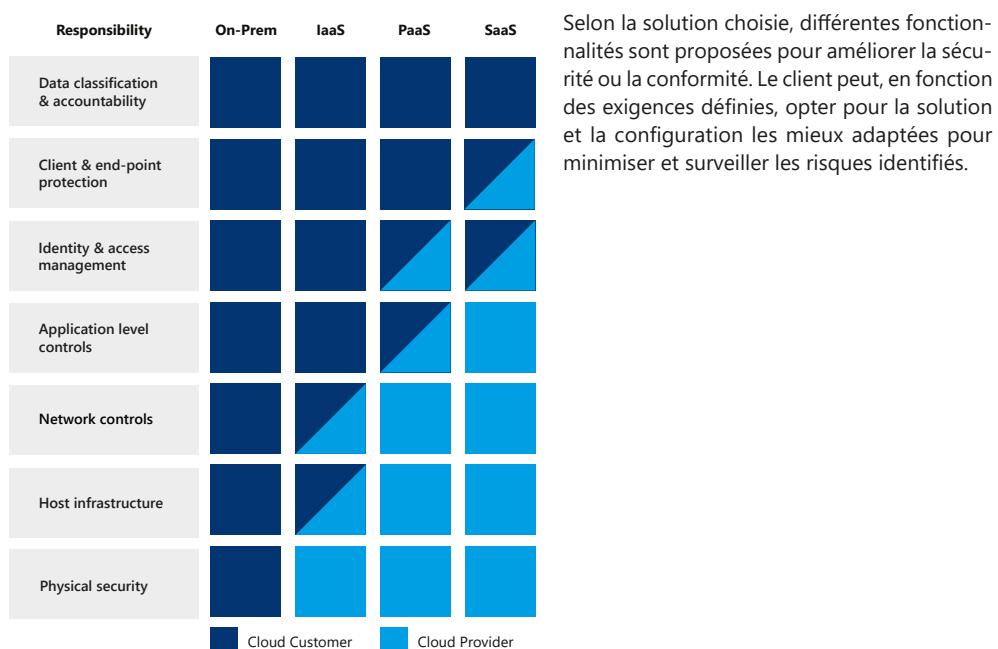


Figure 4 – Répartition de la responsabilité

Les facteurs clé de succès d'un projet cloud

Certains facteurs sont primordiaux pour la réussite d'un projet cloud :

- **des processus décisionnels** clairement définis, y compris une désignation claire des personnes en charge au niveau le plus haut de l'entreprise ;
- **un sponsor dédié** au niveau le plus haut de l'entreprise, capable de prendre des décisions définitives en raison des risques existants et de faire avancer les processus ;
- **une équipe interdisciplinaire** qui s'occupe de manière globale de toutes les questions liées au passage au cloud. Cette équipe doit être composée de représentants des domaines suivants : direction de l'entreprise, utilisateurs, propriétaires de systèmes et de données, service informatique, sécurité informatique, service juridique, gestion des risques et de la conformité, protection des données et approvisionnement. Elle doit évaluer collectivement les risques associés au projet concret et proposer des solutions à valider ensuite par la direction.

Ces éléments sont déterminants pour le bon déroulement d'un projet cloud. S'ils ne sont pas réunis, des malentendus, un manque de coordination et des retards coûteux peuvent survenir au cours du processus. Très important : les objectifs définis doivent être clairement visibles.

Les parties prenantes internes

Tout projet cloud implique des acteurs divers. C'est pourquoi il est important d'identifier précocement les fonctions de chacun et de formuler avec précision les tâches qui leur incombent. Certains rôles sont décrits ci-après, même s'ils peuvent varier en fonction de l'organisation et du projet :

Gestion des fournisseurs

- définir les rôles et les responsabilités en lien avec les différentes tâches à accomplir en interaction avec le fournisseur de services cloud ;
- surveiller les prestations du fournisseur de services cloud (contrôle du SLA) ;
- assurer la gestion opérationnelle du contrat.

Service juridique et conformité

- assurer la conception du contrat ;
- assurer la gestion de la protection des données ;
- intégrer le contrat dans la gestion des risques et dans le cadre de contrôle interne ainsi que dans la surveillance de la conformité et dans le reporting de conformité.

Service informatique interne

- préparer les applications au fonctionnement dans le cloud (mise en conteneur, adaptation au système d'exploitation...) ;
- intégrer le cloud dans la gestion des services informatiques propres à l'entreprise (assistance, gestion des incidents, des problèmes, des changements et des versions) et adapter les processus traditionnels aux processus DevOps désormais requis pour le cloud ;
- assurer la gestion technique du cycle de vie des fonctions réalisées dans le cloud ;
- gérer l'interface avec les équipements informatiques de l'entreprise utilisant les systèmes cloud ;
- assurer la connexion au cloud au moyen d'un réseau approprié et si possible redondant ;
- développer les mesures de continuité d'activité et de reprise d'activité en collaboration avec le ou la responsable de la sécurité des systèmes d'information (chief information security officer, CISO) et les tester régulièrement.

CISO

- concevoir un concept de sécurité informatique de bout en bout intégrant le fournisseur des services cloud ;
- définir les dispositifs de sécurité du cloud ;
- définir et développer une gestion opérationnelle de la sécurité informatique intégrant l'ensemble des composantes (cloud et localement) ;
- intégrer les services cloud dans la gestion existante des identités et des accès ;
- analyser et clarifier les failles de sécurité pouvant survenir lors du fonctionnement simultané de solutions durant la transition ou pendant l'utilisation opérationnelle d'un cloud hybride ;
- spécifier la conception de la continuité d'activité et de la reprise d'activité ;
- contrôler les tests de continuité d'activité et de reprise d'activité ;
- assurer un contrôle et un suivi réguliers de la sécurité informatique.

Les responsables des applications d'entreprise

- spécifier les exigences fonctionnelles ;
- participer à la collecte d'idées et à la révision des processus, ou à la mise en place de nouveaux services rendus possibles grâce au cloud computing ;
- spécifier les niveaux de service (« service levels ») requis ;
- fournir un retour d'information sur la satisfaction et le respect du SLA (en signalant les pannes, par exemple).

Direction financière (CFO)

- réaliser des analyses de rentabilité en matière de cloud ;
- définir le budget et les responsables du budget destiné aux services cloud ;
- contrôler la gestion des coûts du cloud, en collaboration avec la direction générale et les achats ;
- contrôler les analyses de rentabilité.

Conseil d'administration / CEO

- assurer l'intégration stratégique de l'informatique en nuage en tant qu'élément susceptible de contribuer à la mise en œuvre ou au développement de la stratégie de l'entreprise ;
- initier et imposer des processus d'activité améliorés ou nouveaux à réaliser au moyen de la technologie cloud ;
- définir les exigences des critères d'évaluation et les projets basés sur le cloud à réaliser ;
- prévoir les ressources et les budgets consacrés à l'innovation ;
- si nécessaire : prendre des décisions basées sur les risques du cloud ou de la transition ;
- mettre en place des contrôles des programmes cloud en cours.

Microsoft Assurance Framework

Pour pouvoir prendre en compte les risques d'un projet cloud et mettre en place un système de contrôle efficace, il est nécessaire de bien comprendre les conditions contractuelles applicables, les mesures techniques et organisationnelles, les certifications et les rapports d'audit sur les services cloud Microsoft. Le « Microsoft Assurance Framework » fournit un aperçu structuré. Il peut aussi donner des repères pour la réalisation d'une évaluation des risques et les aspects à prendre en compte.

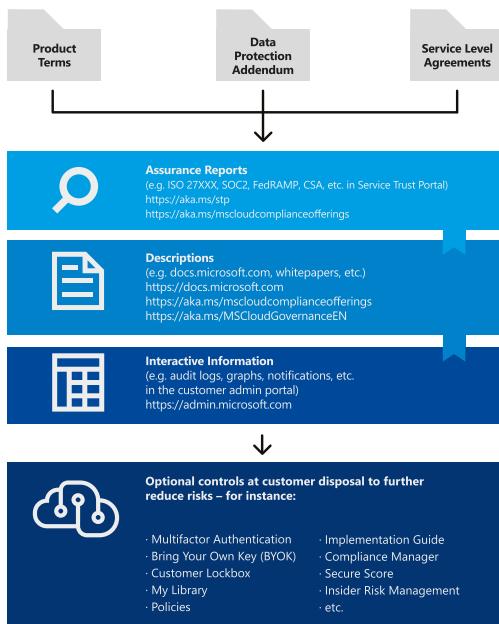


Figure 5 – Microsoft Assurance Framework

1. Tout en haut du Microsoft Assurance Framework se trouvent les accords contractuels, à savoir les conditions d'utilisation des produits (« Product Terms »), l'addendum sur la protection des données (« Data Protection Addendum ») et les accords sur les niveaux de services (« Service Level Agreements ») pour le cloud. Ces documents couvrent des aspects importants tels que le lieu du traitement des données, l'emplacement de stockage, les dispositions relatives à l'accès aux données, la collaboration avec des sous-traitants ou encore la suppression des données. Ils représentent en même temps les instructions données par le client à Microsoft.

2. Le niveau « Assurance Reports » permet de vérifier la manière dont Microsoft traduit les garanties contractuelles en contrôles organisationnels et techniques. Établis par des tiers indépendants, ces rapports confirment en même temps l'efficacité des contrôles pertinents. Le portail <https://servicetrust.microsoft.com/> permet d'accéder aux versions non rédigées des rapports d'audit des auditeurs indépendants, aux certificats de conformité standard et aux évaluations de l'optimisation de la sécurité (Security Optimization Assessment, SOA).

3. Le troisième élément est constitué de divers documents et guides, dont des descriptions exhaustives de certaines fonctions, caractéristiques, processus, ou autre. L'éventail va du livre blanc général à la documentation technique détaillée.

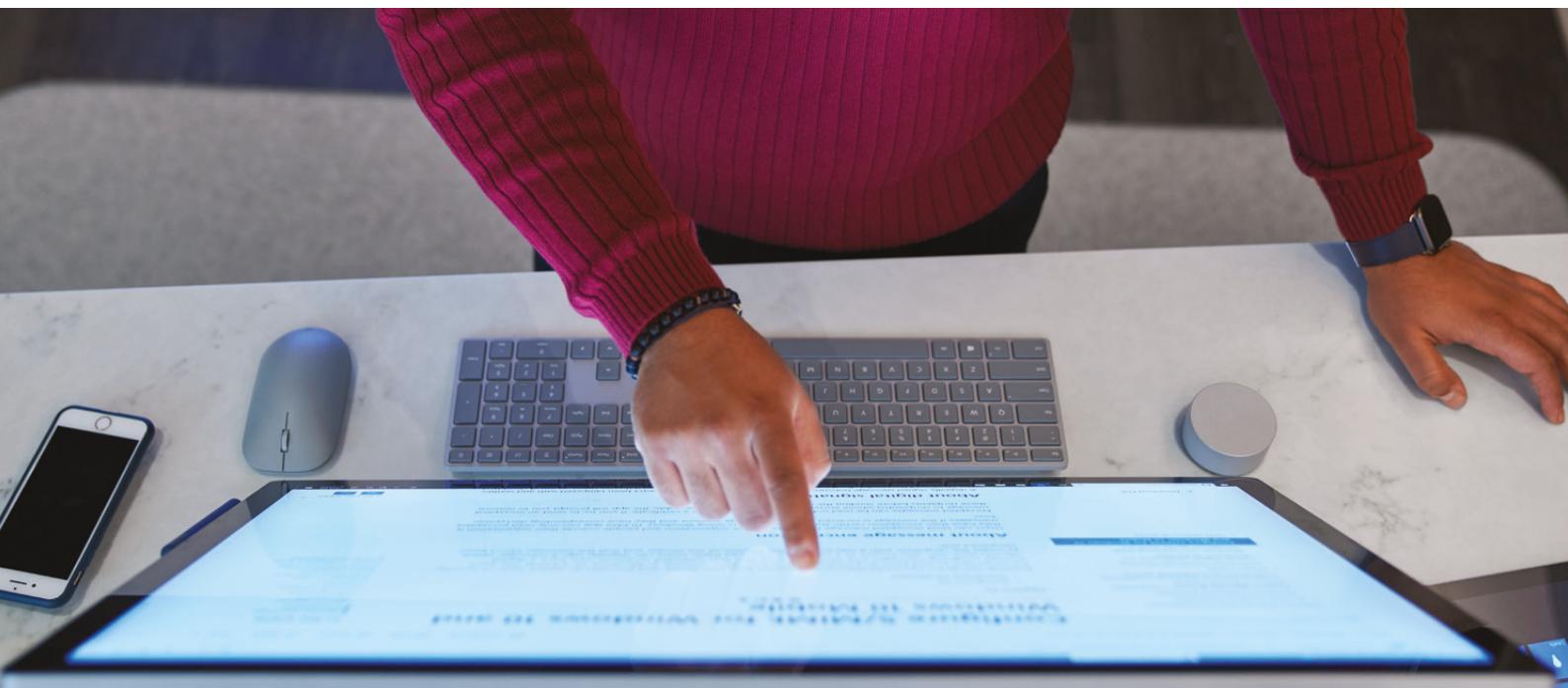
4. Le niveau « Informations interactives » met à disposition du client les documentations et informations régulières sur les services cloud de Microsoft. On y accède via le portail personnalisé de gestion des services cloud.

Chacun des quatre niveaux de l'Assurance Framework propose un grand nombre de fonctions, services et processus supplémentaires que le client peut implémenter à sa guise. Ces contrôles supplémentaires permettent d'atténuer encore plus les risques identifiés. L'encadré tout en bas du graphique présenté plus haut montre certains des contrôles les plus utilisés.

Le Microsoft Assurance Framework joue un rôle déterminant pour l'établissement du processus de gouvernance.

Types de données

Les contrats cloud de Microsoft comprennent un certain nombre de définitions relatives aux types de données qu'il faut comprendre pour stocker des données dans le cloud. Les définitions relatives aux catégories de données figurent au chapitre « Définitions » de l'addendum sur la protection des données.



4 LE PROCESSUS D'ÉVALUATION DES RISQUES

Le risque est souvent perçu comme quelque chose à éliminer puisqu'il se réfère par définition à la probabilité d'un résultat négatif. Or, la prise de risques « contrôlables » est d'une importance fondamentale pour la croissance de toute organisation. Une organisation qui suit une approche pondérée basée sur le risque peut atteindre un équilibre entre les opportunités de telle ou telle activité et les risques qu'elle présente, grâce à une juste mesure dans la gestion des risques. L'approche dite « basée sur le risque » est également l'un des principes fondamentaux des règlementations en la matière, comme par exemple du règlement général de l'Union européenne sur la protection des données. En juin 2021, la Commission européenne a d'ailleurs elle aussi choisi une approche basée sur le risque dans ses nouvelles clauses contractuelles types pour le transfert de données vers un pays tiers (les SCC, ou Standard Contractual Clauses). Une évaluation rigoureuse des risques et une documentation claire et précise de la part du client sont donc des facteurs clés.

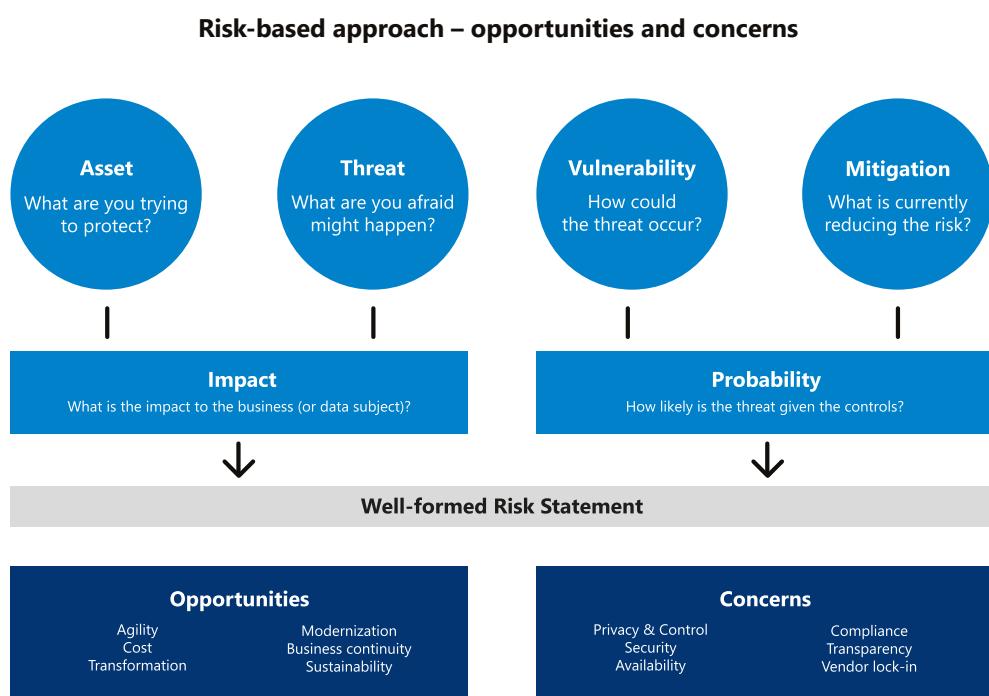


Figure 6 – Appréciation et évaluation des risques

Tout traitement de données comporte des risques, indépendamment de l'architecture, du modèle de déploiement, etc. L'objectif de l'évaluation de ces risques n'est donc pas de les éliminer, mais de les évaluer, minimiser et gérer dans le cadre d'un processus continu. Une gestion des risques rigoureuse sert les intérêts de l'entreprise ou de l'organisation au même titre que ceux du client final. Surtout dans le domaine du cloud, la plupart des organisations verront leur gestion des risques s'améliorer constamment grâce à l'évaluation permanente des risques. Ce d'autant plus si elles comparent les solutions locales actuelles aux possibilités de l'hypercloud. Il est donc primordial de ne pas seulement évaluer la possibilité d'utiliser des services cloud mais d'intégrer aussi la comparaison avec la situation actuelle dans la réflexion globale.

La norme ISO 31000 sur le management du risque

L'intégration de la gestion des risques au sein de l'organisation, y compris en ce qui concerne son fournisseur de services cloud, est un processus dynamique qui doit être constamment adapté aux objectifs et processus de l'entreprise. La norme ISO 31000 décrit six étapes pour le processus d'évaluation des risques, voir schéma ci-dessous.

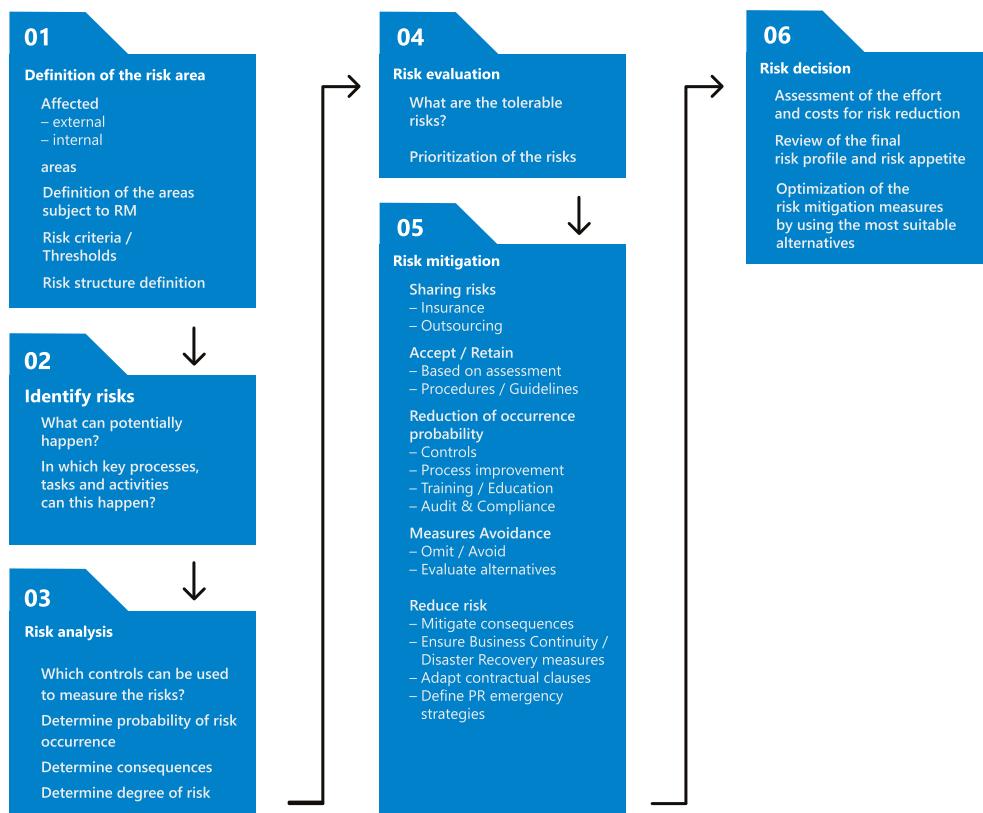


Figure 7 – Les six étapes du processus de gestion des risques selon la norme ISO 31000

Pour ce qui est de l'évaluation des risques, le présent chapitre s'appuie notamment sur la norme ISO 31000:2018, « Management du risque ». Cette norme préconise le développement d'une stratégie et d'une culture de gestion des risques permettant d'identifier rapidement et efficacement les risques. Il est possible d'atténuer ces derniers au moyen de mesures techniques, organisationnelles et/ou juridiques appropriées. Cette démarche permet d'améliorer la probabilité pour l'organisation d'atteindre ses objectifs et de protéger ses actifs.

Ci-après, seuls les éléments de la norme qui jouent un rôle essentiel pour le cloud computing seront pris en compte.

Le risque, c'est quoi ?

Le risque est défini comme « l'effet de l'incertitude sur l'atteinte des objectifs », l'effet constituant en l'occurrence un écart positif et/ou négatif. Le risque est considéré sous l'angle de sa cause, des événements potentiels, de leurs effets et de leur vraisemblance.

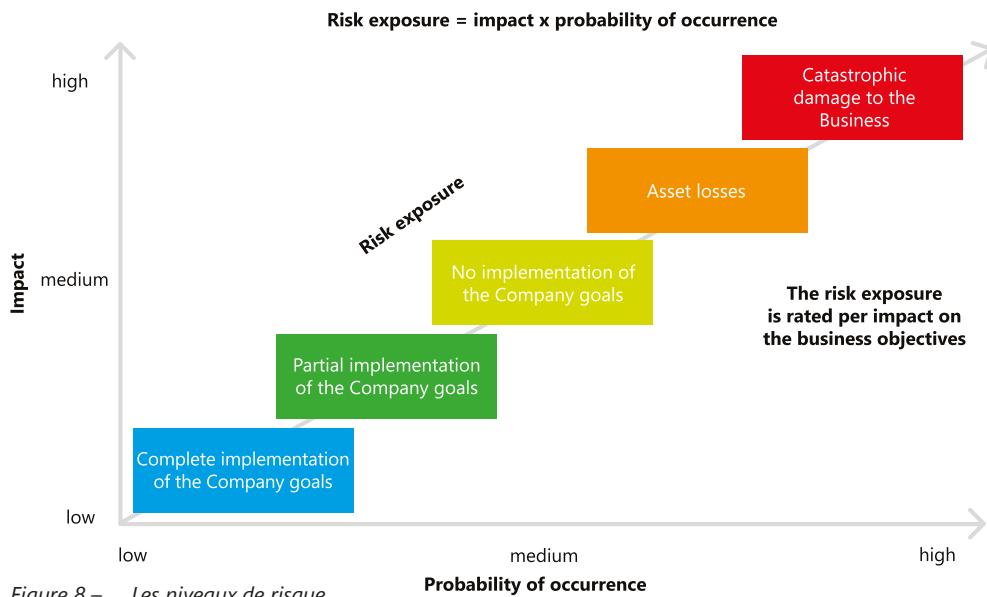


Figure 8 – Les niveaux de risque

Définir la zone de risque

Cette première phase vise à délimiter la zone dans laquelle l'évaluation des risques sera réalisée. Il s'agit aussi de déterminer les systèmes informatiques et les fonctionnalités concernés par le projet. En termes de contexte externe, les dispositions réglementaires pertinentes seront recherchées. Le contexte interne détermine quant à lui les règles propres à l'entreprise et la manière dont les différentes questions (portant par exemple sur l'innovation ou le lancement de nouvelles technologies) seront abordées au sein de l'organisation. Les parties prenantes du projet sont également à définir et à impliquer activement.

Identifier les risques

Pour accélérer le processus de catégorisation des risques, le présent document propose un modèle des risques auxquels l'entreprise pourrait être confrontée dans le cadre d'un projet cloud typique. Les risques mentionnés sont principalement basés sur la « Cloud Security Alliance » et sa « Cloud Controls Matrix 2 ». Certains risques sont spécifiques à un secteur. Ceux-là peuvent ne pas figurer dans ce modèle ; il conviendra alors de les ajouter à la liste des risques utilisée.

Type de risque Risques

| | |
|-----------------------|---|
| Risques de conformité | Structure de la gouvernance et de la gestion des risques non adaptée à une utilisation du cloud Incertitude quant à la conformité avec les exigences réglementaires existantes après la migration vers le cloud (circulaires FINMA, données personnelles particulièrement sensibles, données liées au contrôle à l'exportation, etc.) Points juridiques à éclaircir : contrats avec des fournisseurs de services cloud, profilage ou registres de données sensibles, résiliation de contrats existants avec des partenaires et fournisseurs Capacité de réaction aux incidents non réglée / insuffisante Transparence insuffisante par rapport aux données stockées dans différents territoires Absence de gestion de la conformité et des audits pour le cloud Risques en termes de protection des données liés aux exigences spécifiques d'un pays Nettoyage, maintenance, archivage et suppression de données sensibles Audits ou certifications non disponibles chez le fournisseur de services cloud ou ses sous-traitants Contrôles de conformité manquants ou inadaptés pour le cloud |
|-----------------------|---|

| | |
|---|---|
| Risques stratégiques | Gestion de l'information / sécurité des données absentes ou insuffisantes Interopérabilité et portabilité Choix de fournisseurs inadéquats Manque de volonté de la part de l'organisation Absence de diversification des fournisseurs Lock-in Classification des données absente ou insuffisante Migration de données locales vers le cloud (public, privé ou hybride) |
| Risques liés à la migration | Manque de formation et de compétences du personnel Manque de sécurité pour le transfert des données vers le cloud Assurance d'avoir la totalité des données à l'arrivée Défaillances suite à l'échec de la mise en place des services cloud Interférences lors du fonctionnement simultané de systèmes locaux et dans le cloud durant la transition Manque de solutions de secours en cas d'échec de la transition Manque de sécurité informatique durant la phase de projet Manque de suivi des certifications obtenus jusque-là, p. ex. ISO 27001, ISO 9001 Manque de collaboration avec l'auditeur pour la transition Absence de rapports d'audit ou rapports d'audit négatifs après le transfert opérationnel |
| Risques opérationnels | Absence d'adaptation du fonctionnement du centre de données et absence d'intégration des services cloud dans les opérations. En particulier, absence d'adaptation de la gestion des services informatiques et donc aussi d'organisation de la co-existence des processus ITIL classiques du centre de données de l'entreprise et des processus DevOps pour le cloud Maintenance des données et interférences en cas d'utilisation simultanée de systèmes locaux et dans le cloud, et mauvaise intégration aux solutions déjà utilisées par l'entreprise Manque de formation du personnel dans le domaine du fonctionnement du cloud Défaillance de capacités de logging et tracing Absence de concept de sécurité de bout en bout, et défaillance du dispositif de protection informatique Défaillance de la sauvegarde Mauvaise gestion de l'information donnant lieu à un manque de sécurité des données, y compris une perte de données, et par conséquent à une atteinte à la protection des données Processus opérationnels internes inadéquats Activités du personnel volontairement ou involontairement préjudiciables Absence de gestion des processus opérationnels Décisions impératives des autorités, y compris toute « fishing expedition », ou pêche aux renseignements, visant à obtenir dans le cadre d'une procédure d'e-Discovery l'accès à des informations sur l'entreprise ou sur ses clients stockées dans le cloud Accès non autorisé aux locaux Vol d'équipements informatiques Absence de sécurité des terminaux (ordinateur portable, ordinateur de bureau, smartphone, etc.) à partir desquels les services cloud sont utilisés Manque de ressources humaines Catastrophes naturelles Risques liés aux licences Cyberattaques avec perte de données en raison du manque d'adaptation des capacités en matière de cybersécurité, de continuité d'activité et de reprise d'activité Risque de réputation Résiliation ou défaillance de services |
| Risques liés au marché / risques financiers | Confiscation de données ou de systèmes par les autorités Manque de gestion de la capacité Manque d'agilité de l'environnement opérationnel et donc un « time to market » insuffisant Mauvaise réaction ou réaction tardive aux incidents |

Figure 9 – Liste des risques potentiels pour la migration vers le cloud et l'utilisation des services cloud

Procéder à une analyse des risques

Sur la base de la liste des risques potentiels, il convient de préciser ceux qui doivent être pris en considération pour l'initiative stratégique concrète. Il appartient ensuite à l'équipe interdisciplinaire d'évaluer les risques d'un projet de manière séquentielle mais aussi dans leurs interrelations.

Il est alors important de définir la façon dont le risque est mesuré. Les différents risques doivent être placés sur une échelle en fonction de leur criticité pour pouvoir les comparer. Plus tard, un contrôle permettra de voir si l'un ou l'autre des risques a changé de place sur l'échelle au fil du temps.

Effets d'un événement

| Catégorie | Conséquences de l'événement | Impact | | |
|----------------|---|--------|-----------------------|--|
| | | Durée | Portée opérationnelle | Perte de réputation Conséquences juridiques et en matière de conformité |
| Catastrophique | Destruction très importante ou totale d'actifs ou atteinte importante à la réputation, large visibilité externe et impact significatif sur les opérations et sur la confiance du public et notamment sur celle des clients et partenaires commerciaux. Frais très importants pour réparer le préjudice et ses conséquences; défaillances ou baisse très importante des commandes puis du chiffre d'affaires et des bénéfices. | | | |
| Grave | Préjudice important mais non total portant sur les actifs ou la réputation. Visibilité externe importante mais partielle, affectant les opérations et la confiance du public, des clients et des partenaires commerciaux. Frais considérables pour réparer le préjudice et ses conséquences; plusieurs défaillances ou baisse importante des commandes puis du chiffre d'affaires et des bénéfices. | | | |
| Important | Préjudice moyen ou perte moyenne, affectant par exemple les opérations internes, provoquant une hausse des dépenses d'exploitation ou une baisse de la performance de l'entreprise. Impact notable sur la productivité et sur les frais à engager pour réparer le préjudice et ses conséquences. L'impact sur le résultat d'exploitation est en partie visible mais relativement facile à absorber. | | | |
| Modéré | Dommages ou pertes relativement faibles, p. ex. un impact sur des processus internes. La hausse des coûts n'est pas mesurable. Aucun impact mesurable, légère augmentation des coûts de support ou de structure. | | | |
| Faible | Très peu ou pas de changement au niveau de l'activité opérationnelle. L'impact est absorbé par l'activité commerciale normale. Aucun impact mesurable sur les coûts de support, la productivité ou les engagements de l'entreprise. | | | |

Figure 10 – Effet du risque – grille d'évaluation

Probabilité d'occurrence d'un événement

| Catégorie | Réflexion | Probabilité d'occurrence | Fréquence |
|---------------|---|--------------------------|------------------------|
| Attendu | Il est pratiquement sûr que cet événement à risque ou cette situation se produira ou s'est déjà produit(e) au cours des 6 derniers mois | 90-100 % | Env. tous les 3 mois |
| Très probable | Il est très probable que cet événement à risque ou cette situation se produira | 70-90 % | Tous les ans |
| Probable | Il est plus probable que cet événement à risque ou cette situation se produise que le contraire | 50-70 % | Tous les 2 à 3 ans |
| Peu probable | Il est possible que cet événement à risque ou cette situation se produise | 10-50 % | Tous les 4 à 6 ans |
| Improbable | Il est extrêmement peu probable que cet événement à risque ou cette situation se produise | <10 % | Tous les 7 ans ou plus |

Figure 11 – Probabilité d'occurrence d'un risque : grille d'évaluation

Évaluation des risques

Il s'agit maintenant d'évaluer les risques identifiés selon ces deux aspects, puis d'entrer les résultats obtenus dans la matrice des risques. Il en résulte un aperçu simple de la criticité et, partant, de la priorisation des risques. Comme mentionné plus haut, une approche zéro risque n'est pas le but. Il y aura presque toujours un risque résiduel qu'il faudra sciemment accepter, gérer et surveiller pour les changements à venir.

La pratique montre bien souvent que l'évaluation initiale des risques liés au cloud évolue ensuite au fur et à mesure des concertations en interne, notamment si une comparaison est réalisée avec les solutions locales en place qui sont bien sûr également sujettes à risques, par exemple en termes de cybersécurité ou d'interruption de service.

Pour la définition et l'évaluation des risques, un regroupement pertinent de ces derniers s'impose. Il vaut mieux éviter de définir un trop grand nombre de risques individuels mineurs.

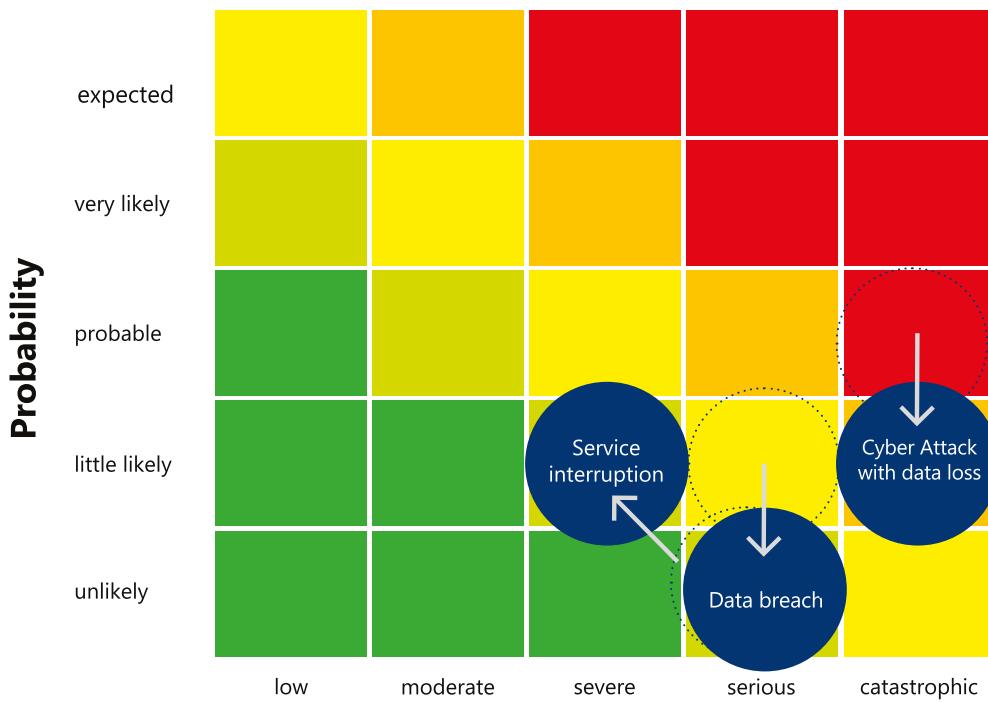


Figure 12 – Exemple de matrice d'évaluation des risques

Atténuation des risques : comment réduire les risques ?

Pour minimiser le risque global, il est possible de prendre des mesures permettant de réduire le facteur de l'impact ou celui de la probabilité, voire les deux. Ainsi, le risque identifié de voir des données à caractère personnel tomber entre les mains de tiers indésirables en raison de la perte physique de l'appareil numérique d'un membre du personnel peut être réduit pour passer de 3 à 5 à 2 à 3, tant pour la probabilité que pour l'impact, en mettant en œuvre des mesures supplémentaires telles qu'une protection forte des mots de passe, une authentification à facteurs multiples ou d'autres démarches similaires. Grâce au chiffrement complet du périphérique et à la possibilité de le supprimer à distance, ces deux facteurs peuvent même être abaissés à 1. De cette façon, le risque est au plus bas et donc à un niveau jugé acceptable dans la plupart des cas. La réponse à la question de savoir laquelle de ces mesures est adaptée à telle ou telle organisation et proportionnée au risque réel dépend de l'évaluation des risques liés aux données en question, des scénarios applicables, etc. Au final, c'est à la personne responsable des données qu'il incombe d'évaluer et de documenter l'adéquation et l'acceptation du risque résiduel.

Les principes de l'atténuation des risques

Développer les connaissances

Pour être efficace, l'évaluation des risques presuppose de très bonnes connaissances des risques anciens et nouveaux, doit être réalisée par une équipe interdisciplinaire et faire l'objet de vérifications constantes. Les membres de l'équipe doivent disposer des connaissances nécessaires et se comprendre mutuellement, ce qui peut poser des défis au regard de l'ampleur du sujet.

Il est recommandé de prévoir dans un premier temps une formation sur le principe de fonctionnement du cloud, sur ses différences par rapport à l'externalisation traditionnelle, sur les tenants et les aboutissants des données et de leur protection et sur les impératifs en matière de conformité et de maîtrise des risques.

Objectiver les risques

Les perspectives et opinions mises en avant au sein de l'équipe interdisciplinaire chargée d'évaluer les risques peuvent varier. C'est normal et même nécessaire car les priorités ne sont pas les mêmes d'un domaine à l'autre, et chaque partie prenante est tenue de représenter le sien (utilisation, protection des données, juriste d'entreprise, CISO...).

Chercher le compromis

La solution n'est donc pas toujours d'obtenir un consensus mais bien souvent de trouver un compromis entre les personnes impliquées. Cela doit être une évidence pour tout le monde dès le départ. Le processus d'évaluation des risques doit donc être orchestré avec soin et au besoin bénéficier d'un accompagnement externe compétent. À défaut, la discussion risque de s'enlisir et de n'aboutir à rien, tout en engendrant beaucoup de frais et de travail. En cas de désaccord au sein de l'équipe, des décisions basées sur le risque doivent être prises par la direction. Cette dernière doit en être consciente et s'impliquer activement dans la démarche. Une transformation cloud est essentiellement un projet qui s'inscrit dans la gestion du changement et devrait être orchestrée en tant que tel.

Vérifier les faits

L'appréciation factuelle des risques est primordiale pour la discussion car les approximations sont légion en ce qui concerne les risques du cloud. Il est vrai que la rapidité de l'évolution technologique n'aide pas à objectiver le débat, sachant en plus que certaines craintes évoquées dans le passé étaient tout à fait justifiées. Or, grâce aux avancées technologiques réalisées, ces craintes n'ont plus lieu d'être.

Une question importante à se poser pourrait être : « Ce risque existe-t-il vraiment et si oui, combien de fois s'est-il réalisé dans le passé ? » Dans le contexte du débat sur le « Cloud Act » adopté par les États-Unis, on pourrait par exemple poser la question suivante : au cours de ces dernières années, combien de fois le département de la justice des États-Unis a-t-il, dans le cadre d'une poursuite judiciaire, réquisitionné des données personnelles auprès du fournisseur de service cloud envisagé ou du client lui-même ? Ainsi objectivé, l'examen des cas concrets met en évidence le niveau de risque effectif dans un domaine donné.

Comparer aujourd’hui à demain

Comme déjà mentionné, l'informatique sans risque n'existe pas. La solution locale en place comporte déjà des risques identiques et souvent même plus importants que pour une solution cloud. Ainsi, il est quasiment impossible pour une entreprise de mettre en place par ses propres moyens un niveau de cybersécurité approchant celui du cloud.

L'évaluation du risque doit donc mettre en balance l'état actuel des choses et la solution cloud envisagée, avec pour objectif évidemment de voir au total les risques baisser avec l'utilisation du cloud.

Définir l'étendue du concept d'atténuation des risques

Souvent présentée comme exigence, l'élaboration d'un concept global à l'échelle de l'entreprise qui permettrait d'atténuer toute sorte de risques liés au passage au cloud ne fonctionne pas dans la pratique. Le sujet est si complexe et l'évolution des technologies et de la législation si dynamique qu'il n'est tout simplement pas possible de les inclure dans un concept passe-partout.

C'est pourquoi il vaut souvent mieux définir des règles générales sur la base de solutions individuelles qui fonctionnent bien. Les premières preuves de concept et les projets pilotes permettent ainsi d'avancer et d'acquérir de l'expérience qui sera utile pour les projets ultérieurs. Cette démarche ascendante est plus rapide, plus efficace et aussi plus adaptable.

Les différentes mesures d'atténuation des risques

Les mesures juridiques

Il s'agit de mesures contractuelles visant à pallier les risques du cloud. Parmi elles figure un contrat-cadre avec le fournisseur de services cloud, couvrant par exemple les lieux où sont stockés les données ou la possibilité du fournisseur d'y accéder. Les expertises juridiques internes peuvent aussi en faire partie. Elles permettent notamment à l'organisation de définir les règles pour les contrôles autorisés du personnel concernant une éventuelle transmission abusive de données.

Les mesures organisationnelles

Ces mesures comprennent notamment la définition des rôles et responsabilités pour gérer le cloud, contrôler les coûts et le respect du SLA, accorder les autorisations, configurer le cloud et, en cas de nécessité, activer et assurer la continuité d'activité. D'autres exemples sont les consignes relatives aux autorisations d'accès aux données dans le cloud ou les instructions précisant les données à stocker dans le cloud.

Les mesures techniques

Parmi ces mesures figurent notamment le chiffrement de données dans le cloud, l'authentification à deux facteurs des utilisateurs ou encore le blocage, à l'aide de « Data Leakage Prevention Tools » (outils destinés à prévenir la fuite de données), d'exportations de données violant les règles de conformité, que ce soit par négligence ou volontairement.

Mettre en place des contrôles

Mettre en œuvre des mesures n'est pas suffisant pour atténuer les risques. Il faut aussi que ces mesures soient efficaces dans la durée. Pour s'en assurer, il convient de mettre en place des contrôles et d'établir une gouvernance appropriée.

Les contrôles sont des activités permettant de réduire la probabilité ou l'impact d'un risque. Ils contribuent ainsi à l'atténuation des risques. Tout contrôle doit répondre à trois critères :

1. Il doit être efficace, en identifiant le risque le plus précisément possible et en le réduisant au maximum.
2. Il doit être réalisé à intervalles pertinents et documenté.
3. En cas de non-conformité, des actions correctives doivent être mises en place.

Un exemple de contrôle : vérifier si toutes les personnes autorisées à utiliser une application cloud travaillent effectivement toujours dans l'entreprise et si leur rôle actuel implique toujours cette autorisation d'accès. Pour garantir l'efficacité de ce contrôle, il convient d'exporter à partir du système RH la liste du personnel actuellement employé par l'entreprise pour la comparer à celle des personnes autorisées. On peut aussi vérifier, en collaboration avec les propriétaires des applications, les rôles assumés actuellement par les membres du personnel et leur concordance avec ceux spécifiés dans le système d'accès. Idéalement, ce contrôle sera effectué à une fréquence très élevée (voire au moyen d'une comparaison en temps réel du registre RH avec celui des autorisations d'accès) afin de garantir que d'anciens membres du personnel ne puissent pas accéder au système et télécharger secrètement des données.

Chaque contrôle est ensuite attribué à une personne qui en est responsable (« control owner ») et qui doit s'assurer qu'il est bien effectué et régulièrement vérifié. C'est à la fonction conformité, ou compliance, qu'il appartient de gérer les contrôles et de veiller à ce qu'ils soient réalisés. Si la compliance vérifie un contrôle et constate une irrégularité, il doit ressortir de la description du contrôle comment signaler ce problème et qui est en charge de rétablir l'état normal. Par ailleurs, des audits internes ou externes peuvent vérifier des contrôles.

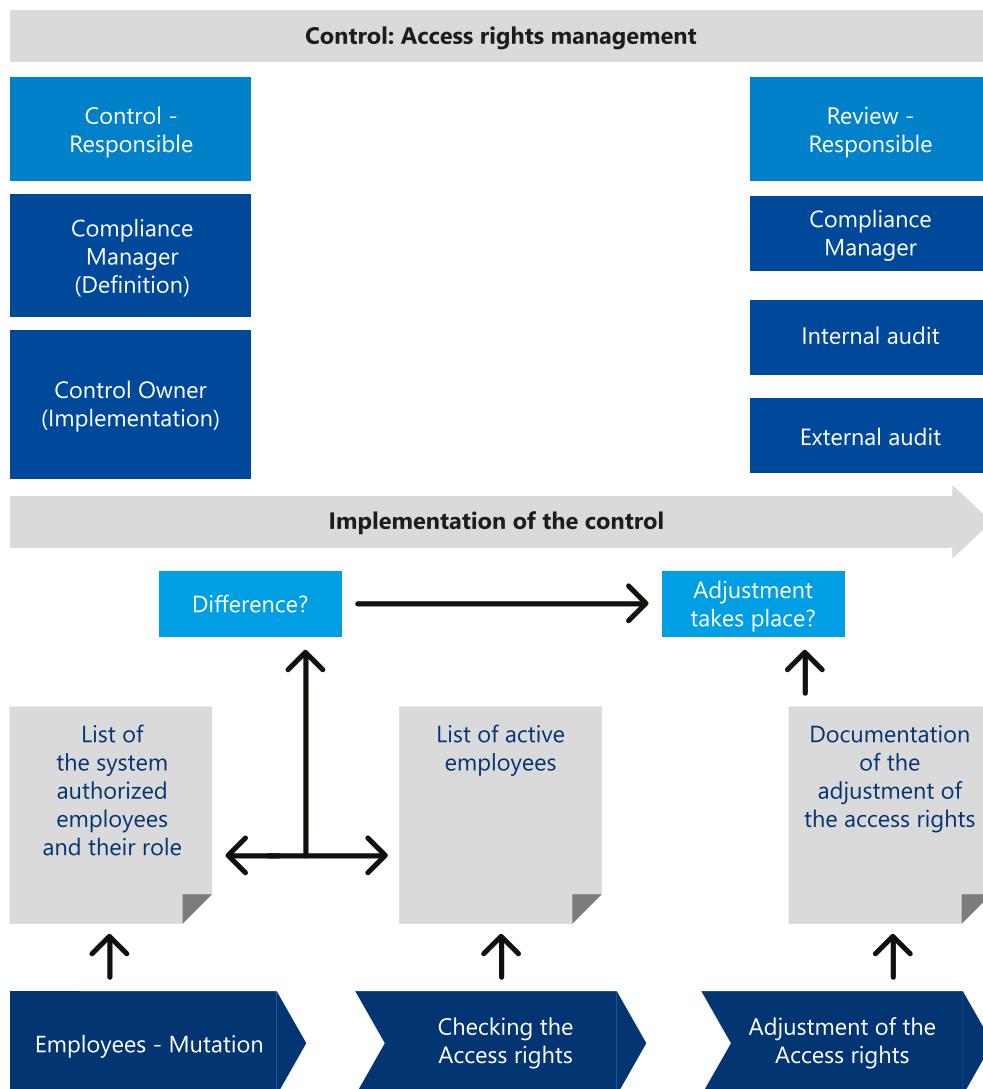


Figure 13 – Exemple de contrôle pour la gestion des autorisations d'accès

Une conformité de bout en bout grâce à l'intégration des contrôles réalisés par le fournisseur de services cloud

La compliance vise à assurer une articulation entre l'organisation concernée et le cloud qui soit conforme aux dispositions réglementaires. Il s'agit donc de synchroniser les contrôles internes et ceux mis en œuvre par le fournisseur de services cloud. La plupart des fournisseurs proposent une sélection de contrôles standards que l'entreprise peut intégrer dans son système de contrôles, ceci afin d'éviter que chaque client doive se concerter avec son fournisseur de services cloud pour définir et mettre en place différents contrôles.

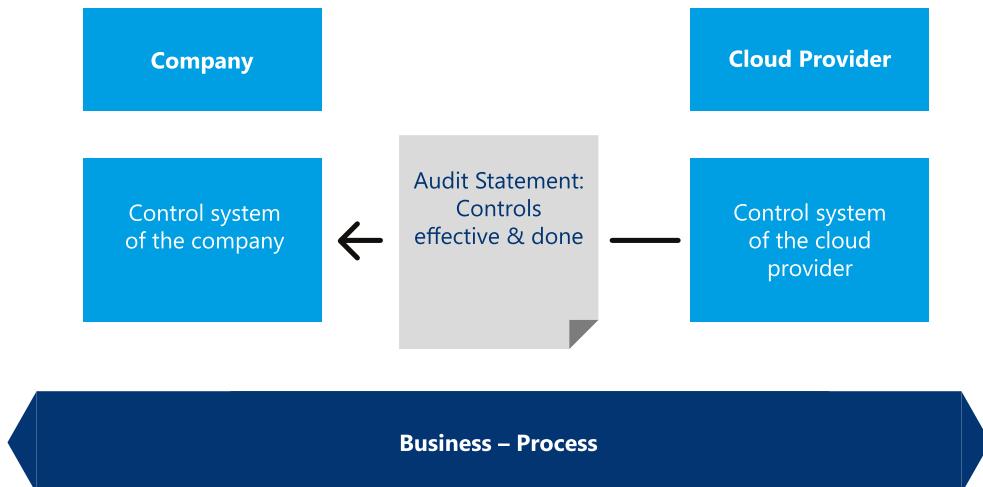


Figure 14 – Intégration des contrôles du fournisseur de services cloud

Le fournisseur de services cloud fait appel à des auditeurs externes pour pouvoir prouver au client qu'il établit, réalise et respecte effectivement tous les contrôles. Ces auditeurs confirment périodiquement sous forme de rapports d'audits la bonne exécution des contrôles ainsi que leur vérification en bonne et due forme. Ce concept permet aux clients de remplir leur obligation de diligence et d'assurer la conformité de bout en bout de leur processus.

Pour soutenir les entreprises et les organisations dans la définition des exigences applicables en matière de cloud, la « [Cloud Security Alliance](#) » a mis au point une série de contrôles qui sont librement mis à disposition du public. Microsoft a de son côté créé le « [Compliance Manager](#) », un outil qui définit trois types de contrôles et vérifie leur statut :

1. Contrôles gérés par et sous la responsabilité de Microsoft
2. Contrôles du client
3. Contrôles partagés, mis en œuvre et réalisés sous la responsabilité partagée du client et de Microsoft

Comment régler la répartition des responsabilités

La responsabilité pour la conformité ne peut être attribuée au seul fournisseur de services cloud, même si ce dernier fait tout pour adapter régulièrement ses offres aux exigences en la matière. Le fournisseur ne peut par exemple pas déterminer qui a accès ou non aux données du côté du client. Il ne peut pas non plus être tenu pour responsable de ce qui se passe dans le réseau qui mène vers lui et qui est géré par un autre fournisseur.

En fonction du modèle de services cloud (IaaS, PaaS, SaaS), le partage de la responsabilité entre le fournisseur de services cloud et le client varie cependant en ce qui concerne le respect de la conformité et les contrôles de sécurité qui en découlent pour un service en particulier, comme déjà vu plus haut.

Même pour des solutions SaaS comme Microsoft 365 ou Dynamics 365, le client garde une part de responsabilité. Pour s'assurer qu'une solution basée sur le cloud répond au niveau de conformité exigé, il est possible de sélectionner des fonctions de sécurité et de conformité dans une longue liste établie en fonction de la licence de services cloud choisie.

Il appartient aux responsables sécurité et conformité du client de définir le dispositif de sécurité et de choisir les bonnes options pour leur projet. Ils peuvent ainsi configurer leur solution cloud dans le contexte de leur propre situation de manière à avoir à tout moment le contrôle de bout en bout. Le fournisseur de services cloud doit quant à lui s'assurer que les fonctions qu'il propose sont à tout moment en mesure de répondre aux exigences de conformité du client.

Cloud Adoption Framework

Avec son [Cloud Adoption Framework \(CAF\)](#), Microsoft offre une base pour la transition vers le cloud. Une partie du CAF est dédiée au contrôle de la gouvernance pour les risques matériels. Les documents et modèles y relatifs sont disponibles [ici](#).

Gérer les risques

Le choix en matière de gestion des risques ne se base pas seulement sur l'évaluation globale de ces derniers mais aussi sur l'évaluation des coûts liés à leur réduction. La direction doit valider, expliquer par écrit et documenter durablement les décisions portant sur la manière de gérer les risques.

Il y a quatre options à cet égard :

Réduire ou éliminer les risques

Il est possible de réduire la probabilité et l'impact des risques par des stratégies appropriées. Ainsi, une structure redondante du fonctionnement peut minimiser le risque de défaillance.

Accepter les risques

L'entreprise peut déterminer si elle est capable et prête à tolérer le risque lié à la solution cloud. Cela dépend de son « appétit pour le risque », autrement dit de sa propension au risque.

Éviter les risques

L'entreprise peut estimer que tel ou tel risque est trop important et décider de ne pas migrer certains types de données vers le cloud, du moins pour le moment. Le risque est ainsi évité.

Transférer des risques

L'entreprise peut chercher des tiers qui seraient disposés à assumer tout ou partie des risques, par exemple des assureurs.



Prendre une décision par rapport aux risques

Au terme de ce processus, l'équipe aura déterminé des options visant à atténuer les risques. Ces options doivent être évaluées sur la base des résultats de l'évaluation des risques, des coûts attendus pour la mise en œuvre des mesures d'atténuation (contrôles...) et du bénéfice attendu.

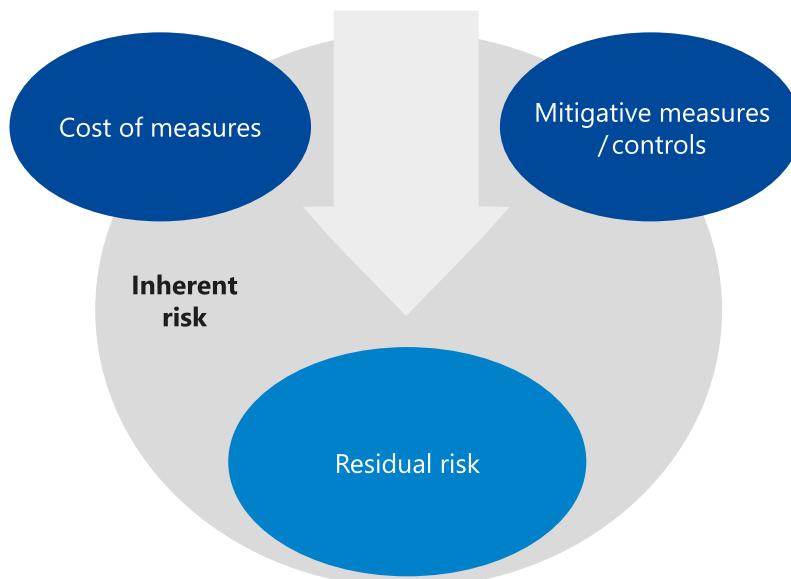


Figure 15 – Les éléments d'une option risque étudiée

Le concept de gestion des risques à établir découle du choix du mix idéal de mesures techniques, organisationnelles et juridiques capables d'atténuer le risque en fonction de l'appétit pour le risque propre à l'entreprise.

Il s'agit ici de rendre possible l'innovation et les transformations judicieuses plutôt que de les empêcher. Les parties prenantes doivent faire preuve d'une certaine flexibilité pour trouver le mix optimal parmi les trois types de mesures.



Figure 15b – Mix optimal de mesures contractuelles, techniques et organisationnelles

Il y a toujours un risque résiduel, quel que soit la formule choisie. Et c'est à la direction générale de l'entreprise qu'il appartient d'accepter ou non ce risque. Les débats sur le dosage optimal du risque peuvent être longs et fastidieux, ce qui dépend surtout de la qualité du travail de l'équipe sur la présentation des risques, de la précision avec laquelle les mesures d'atténuation sont définies et de la disposition de la direction à trancher.

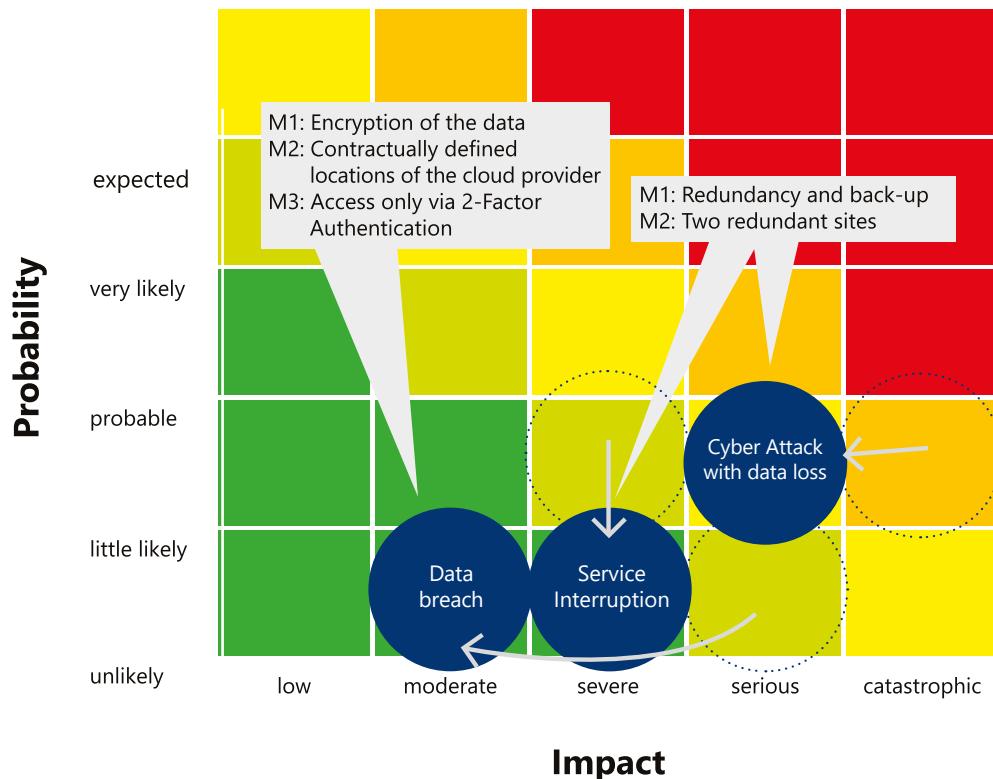


Figure 16 – Les risques évaluées, avant et après la mise en œuvre d'un ensemble de mesures d'atténuation

5 LA GOUVERNANCE DU CLOUD

La manière dont est réalisée une analyse de conformité et des risques varie d'une organisation à l'autre sur certains points. Elle repose néanmoins essentiellement sur la méthodologie suivante, comme déjà décrit dans les chapitres précédents :

Définition des exigences

1. Examiner les modalités de mise à disposition des services cloud (contractuelles, techniques, organisationnelles)
2. Identifier les risques
3. Évaluer les risques
4. Déterminer les mesures visant à minimiser les risques / les mécanismes de contrôle
5. Revalider la conformité

La répétition des différentes étapes du processus est nécessaire pour assurer la conformité continue de l'organisation et la capacité de cette dernière à offrir la meilleure protection possible des données et à veiller à la sécurité de ses opérations. Si l'un des facteurs change (une nouvelle menace potentielle, un changement du volume ou du niveau de sensibilité des données à caractère personnel collectées, stockées et/ou traitées...), le processus doit être recommandé. Il ne s'agit pas de le reprendre systématiquement à zéro mais plutôt de vérifier les éléments qui ont changé et de réévaluer les garanties, contrôles et processus (mesures techniques et organisationnelles) pour en tenir compte.

L'objectif de ce processus est de mettre en place une gouvernance optimale du cloud au sein de l'organisation.

La gouvernance du cloud définit comment surveiller et gérer de manière continue les risques et l'utilisation du cloud. Il ne s'agit pas seulement d'évaluer en permanence la nécessité d'effectuer à un moment précis tel ou tel contrôle ou telle ou telle activité en matière de sécurité, de protection des données ou de conformité mais aussi d'établir l'organisation, les processus nécessaires et les responsabilités et de s'assurer de leur ancrage opérationnel.

Cette gouvernance se fonde globalement sur deux axes :

- La gouvernance du cloud du point de vue réglementaire
- La gouvernance du cloud du point de vue opérationnel / gestion des services en ligne

Le contrôle du client sur ses données et sur son utilisation du cloud découle de l'articulation entre l'axe réglementaire et l'axe opérationnel de la gouvernance du cloud. Le client devra veiller à toujours garder le contrôle sur ces processus.

La gouvernance du cloud du point de vue réglementaire

Déployant ses services de cloud computing hyperscale sous forme standardisée en termes de technique, d'organisation et de contrat, Microsoft n'a cependant aucune connaissance du type de données que le client lui demande de traiter et ne procèdera pas non plus à une évaluation de l'environnement spécifique au client. Aussi est-il primordial pour l'établissement de la gouvernance et de la conformité du point de vue réglementaire que le client examine les conditions globales proposées par Microsoft, basée sur le Microsoft Assurance Framework, pour vérifier régulièrement et appréhender au mieux la compatibilité de ces conditions avec ses propres dispositions et l'impact qu'elles peuvent avoir sur ces dernières. Le Microsoft Assurance Framework a été présenté plus haut dans ce document.

Prendre en compte toutes les entités de l'entreprise

En général, le client doit non seulement vérifier les dispositions et conditions pertinentes au niveau du service informatique qui centralise la démarche mais aussi prendre en compte l'ensemble des entités de son organisation, y compris ses départements spécialisés ou ses divisions sectorielles. Si le service informatique peut jouer un rôle de pivot central et assurer la coordination du projet, les différentes entités sont généralement chargées d'élaborer les bases qui sont pertinentes pour elles et qui serviront plus tard à établir la gouvernance.

La gouvernance du cloud du point de vue opérationnel / gestion des services en ligne

La gouvernance du cloud du point de vue opérationnel est une mission liée à l'informatique. Il s'agit ici surtout d'assurer de manière continue la conformité des activités opérationnelles. Parmi les aspects à définir figurent notamment :

- la responsabilité ingénierie et opérationnelle ;
- la gestion de l'architecture ;
- la gestion du savoir ;
- la gestion des versions et du cycle de vie ;
- la gestion de la sécurité et de la conformité ;
- la gestion des coûts ;
- etc.

Microsoft met à disposition de ses clients divers portails de gestion des services cloud qui fournissent un soutien précieux pour l'accomplissement des tâches dans différentes disciplines (Compliance Center, Security Center, Monitoring, etc.)

Pour assurer et faciliter l'évaluation continue des risques par le client / la personne responsable des données, il est possible de choisir parmi plusieurs configurations basées sur des cadres de référence reconnus (ISO 27001...).

Comment élaborer une gouvernance du cloud

On peut supposer que chaque entreprise possède déjà ses propres processus de gouvernance, qu'il s'agit alors d'adapter à la nouvelle exigence. Le schéma ci-après offre un aperçu des démarches à effectuer par le client pour aligner les mécanismes en question sur ceux du fournisseur de services cloud.

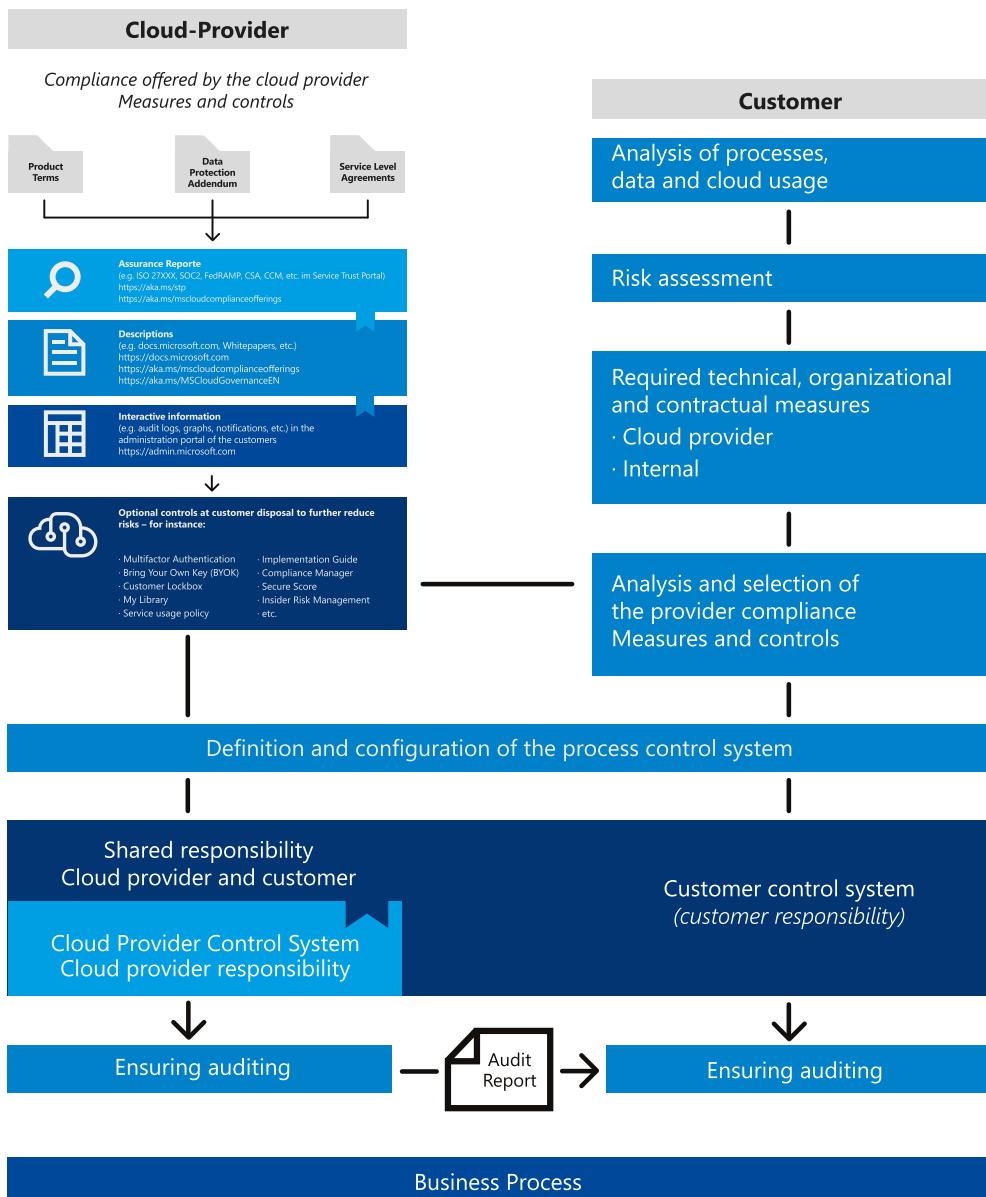


Figure 17 – Harmonisation des structures de gouvernance du client et du fournisseur de services cloud

Compte tenu de l'évolution dynamique des services cloud à très grande échelle, une démarche itérative s'impose aussi pour l'élaboration initiale de structures de gouvernance. Ceci afin de garantir que les conditions globales définies sont adaptées et développées dans les plus brefs délais au regard des charges de travail/services concernés. Une approche « produit minimum viable » (ou MVP, de l'anglais minimum viable product) semble indiquée, notamment pour la réalisation des premiers projets. Une première version des structures de gouvernance doit être établie rapidement, sans toutefois viser l'exhaustivité. Dans le cadre d'une démarche agile, il convient d'élaborer et de définir progressivement l'ensemble des points essentiels de la gouvernance à mettre en place, pour éviter que les projets prévus ne prennent du retard. L'objectif est d'améliorer le degré de maturité de cette gouvernance au fur et à mesure de l'adoption de services cloud.

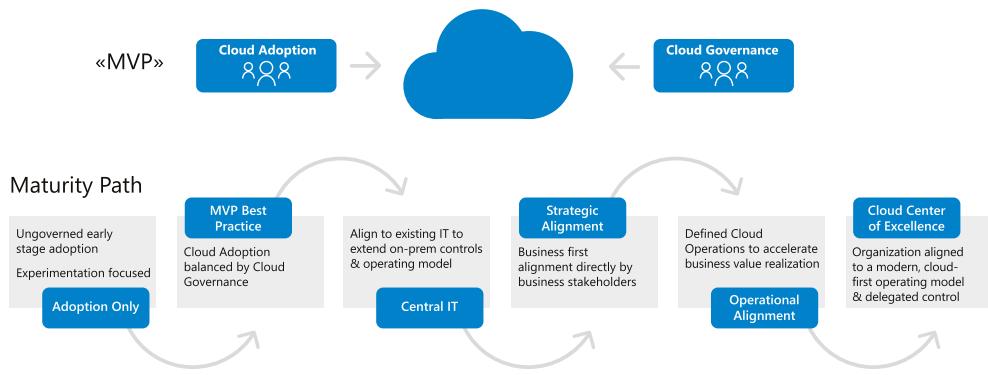


Figure 18 – L'approche MVP pour l'élaboration de la gouvernance du cloud

La gouvernance des données

Il est incontestablement pertinent de disposer de données. Or, pour que ces données puissent permettre de créer de la valeur et être pertinentes pour l'activité concernée, elles doivent à minima être :

- trouvables ;
- définies formellement / structurées ;
- fiables ;
- protégées.

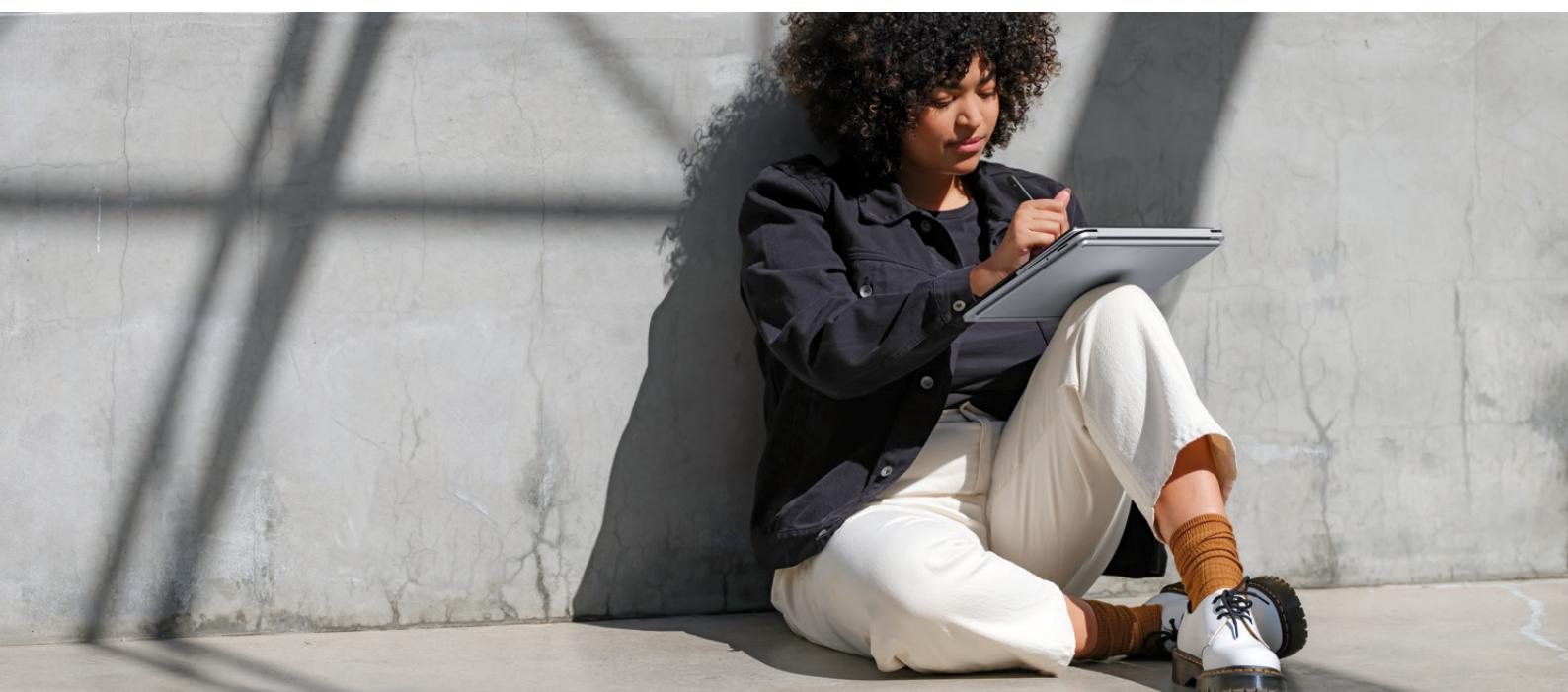
Pour pouvoir garantir ces caractéristiques, l'indispensable gouvernance des données doit prendre en compte les aspects suivants :

- désigner les responsables du projet ;
- analyser et documenter le processus opérationnel, son périmètre géographique et la localisation des parties prenantes internes et externes ;
- analyser et documenter les systèmes et applications supportant ce processus opérationnel ;
- analyser et documenter les données et types de données utilisés pour ce processus opérationnel ;
- documenter les lieux où les différents types de données sont physiquement stockés ;
- analyser, identifier et documenter les règles de conformité légales et internes en vigueur et applicables aux données selon les différents lieux/territoires ;
- analyser et documenter les risques associés à l'utilisation de ces données dans les différents lieux concernés ;
- définir des mesures techniques, organisationnelles et/ou contractuelles adéquates pour atténuer les risques en interne, à l'externe et à l'égard du fournisseur de services cloud, en fonction de la propension au risque existante au sein de l'organisation ;
- analyser si le fournisseur de services cloud est en mesure de proposer les mesures d'atténuation exigées ;
- décider de l'opportunité d'utiliser le cloud dans les circonstances données et des mesures d'atténuation à adopter à partir du cloud ;
- concevoir un système de contrôle adéquat pour les données, comprenant les mesures d'atténuation et contrôles mis à disposition par le fournisseur de services cloud ;
- assurer le fonctionnement opérationnel et l'auditabilité du système de contrôle.

Conclusions

La technologie cloud offre aujourd’hui incontestablement de nombreuses possibilités aux entreprises, organisations et administrations de toute taille. Ceci est notamment dû aux progrès conséquents réalisés en matière de sécurité des données. Le véritable potentiel de la technologie cloud est toutefois encore peu compris, et encore moins exploité. C'est pour cette raison aussi qu'il est aujourd’hui utile de s'intéresser sérieusement à une transition vers le cloud et de l'asseoir sur des bases durables. Une erreur fréquente consiste en effet à trop axer l'évaluation des risques sur des cas isolés, ce qui équivaut à renoncer à toute possibilité de reproductibilité. Or, cette reproductibilité est justement essentielle si l'on souhaite à moyen terme entrer dans un mode d'adoption industrialisée du cloud.

Dans la très grande majorité des cas il est utile d'attaquer la transition vers le cloud avec un partenaire qui a déjà accompagné avec succès d'autres organisations dans cette démarche. Fort de plus de 30 ans d'expérience en Suisse et d'un réseau de plus de 4'600 entreprises partenaires ancrées localement, Microsoft bénéficie d'une excellente assise et est en contact permanent avec les régulateurs et les autorités de surveillance. Enfin, Microsoft est en mesure de proposer ses propres services cloud à partir de centres de données situés en Suisse et de stocker les données dormantes de certains services sur sur le territoire suisse, ce qui représente un avantage non négligeable en termes de sécurité des données.





Merci
Danke
Grazie
Engraziel