



MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Azure Services dans le secteur public suisse

Version 1.4

Documents connexes

Nom du document

Microsoft Public Sector Cloud Design

Document : Cloud governance & Security dans le secteur public suisse V1.4

Identification : Governance and Security Guideline Swiss Public Sector_V1.4

Azure Blueprints for Public Sector (ISO 27001)

[Microsoft Docs](#)

© (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	Introduction à Microsoft Public Sector Cloud Design – MPSD.....	5
1.1	Le contrôle des données au cœur des préoccupations.....	5
2	Les défis juridiques du Cloud Design	6
2.1	Informations principales.....	6
2.1.1	Cloud computing comme externalisation de fait.....	6
2.1.2	À l'étranger.....	6
2.2	Dispositions légales	7
2.2.1	Généralités.....	7
2.2.2	Les directives les plus courantes	7
2.2.2.1	Accord contractuel.....	7
2.2.2.2	Traitement conforme aux instructions et aux intérêts de l'organisme public.....	8
2.2.2.3	Implication d'autres responsables de traitement de données.....	8
2.2.2.4	Sécurité des données.....	8
2.2.2.5	Traitement transfrontalier.....	9
2.2.2.6	Accès des autorités aux données	10
2.2.2.7	Données sensibles.....	11
2.3	Ordonnance concernant la protection des informations (OPrl).....	12
3	Objectifs de contrôle et risques	13
3.1	Objectifs du contrôle.....	13
3.2	Analyse des risques.....	14
4	Mesures et description des composants.....	17
4.1	M1 – Azure Blueprint – ISO 27001	17
4.2	M2 – Azure Purview	18
4.3	M3 – Azure Resources Tags.....	19
4.4	M4 – Azure Key Vault	19
4.5	M5 – Azure IAM (Role Based Access Control RBAC).....	20
4.6	M6 – Azure Policies	21
4.7	M7 – Azure Monitor.....	21
4.8	M8 – Microsoft Compliance Manager pour GDPR / RGPD	22
4.9	M9 – Azure Data Subject Requests pour GDPR / RGPD	23
4.10	M10 – Formation pour Microsoft Public Sector Cloud Design	23
4.11	M11 – Lockbox clients pour Azure	24
4.12	M12 – Azure Stack Hub	25
4.13	M13 – Azure Stack HCI	25
4.14	M14 – Azure Arc.....	26
4.15	M15 – Conventions	27
4.16	M16 – Shared Responsibility Model.....	29
	Appendix : Bases contractuelles et liens d'importance.....	30

Tableaux

Tableau 1 – Matrice des échelons de classification et des mesures selon OPrI	12
Tableau 2 – Objectifs de contrôle de la sécurité de l'information	14
Tableau 3 – Analyse des risques fondée sur la législation et les fondamentaux de la sécurité de l'information	16
Tableau 4 – Liste des mesures.....	17
Tableau 5 – Compilation de sources importantes d'information.....	30

Figures

Figure 1 – Blueprint ISO 27001.....	18
Figure 2 – Azure Purview	19
Figure 3 – Azure Key Vault.....	20
Figure 4 – Azure IAM (RBAC).....	20
Figure 5 – Azure Policies	21
Figure 6 – Azure Monitor.....	22
Figure 7 – Microsoft Compliance Manager pour RGPD	22
Figure 8 – Azure Data Subject Requests pour RGPD	23
Figure 9 – Formation en Microsoft Public Sector Cloud Design.....	24
Figure 10 – Lockbox clients.....	24
Figure 11 – Azure Stack Hub	25
Figure 12 – Azure HCI	26
Figure 13 – Azure Arc	27
Figure 14 – Microsoft Assurance Framework.....	27
Figure 15 – Interaction entre le Cloud Governance du client et Microsoft Assurance Framework	28
Figure 16 – Shared Responsibility Model	29

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 INTRODUCTION À MICROSOFT PUBLIC SECTOR CLOUD DESIGN – MPSD

L'utilisation de solutions en nuage est désormais largement répandue et, au vu du nombre croissant d'offres abordables, devient aussi de plus en plus plébiscitée par les autorités publiques. Les avantages manifestes s'accompagnent de défis que les autorités doivent prendre en compte : les données se trouvent chez le fournisseur du nuage mais restent sous le contrôle des autorités. Le traitement des données est, dit-on, « externalisé » chez le fournisseur du nuage. Pour assurer le contrôle sur le traitement des données externalisé, les autorités doivent considérer les conditions proposées par le fournisseur du cloud, notamment en termes de sécurité des informations.

La question est donc de savoir quelle aide Microsoft, à titre de fournisseur de services en nuage, peut offrir à ses clients du secteur public qui choisissent de recourir à ses services en ligne. Les autorités clientes doivent connaître les risques qui en résultent et les moyens contractuels, organisationnels et techniques que Microsoft déploie pour assurer la sécurité de ses services en ligne.

1.1 LE CONTRÔLE DES DONNÉES AU CŒUR DES PRÉOCCUPATIONS

Dans les solutions en nuage, les données sont traitées non pas sur ses propres ordinateurs ou serveurs locaux mais sur des infrastructures techniques de fournisseurs tiers spécialisés, tels que Microsoft. Sur le plan juridique, un tel traitement des données par des tiers est en principe admissible à condition que les exigences de conformité spécifiques à chaque cas soient respectées mais aussi et surtout que le responsable des données « conserve le contrôle ».

Un contrôle dans ce contexte implique d'une part la garantie par des mesures techniques, organisationnelles et contractuelles que seules les personnes autorisées ont accès aux données et que les obligations prévues par la loi sur la protection des données (mesures de sécurité, obligations de déclaration, respect des principes de traitement, etc.) sont respectées. Il doit être assuré d'autre part que les tiers autorisés à accéder aux données n'en font pas un usage non autorisé et les suppriment réellement et définitivement à la demande du responsable des données. Dans le cas de solutions cloud, cette exigence de contrôle implique également la possibilité de re-transférer, dans des délais et efforts raisonnables, les données externalisées vers sa propre ou une autre infrastructure.

Les exigences concrètes à saisir varient en fonction des circonstances et de la nature des données. Ces exigences sont notamment plus élevées quand les données sont transmises non chiffrées au fournisseur tiers (la transmission des données aux services Azure étant généralement toujours chiffrée) ou quand leur exploitation par un tiers non autorisé risque d'avoir un fort impact sur les personnes concernées (documents officiels secrets par exemple).

L'exigence de « contrôle » n'est pas explicitement formulée dans une loi ou une disposition légale générale. Toutefois, tous les actes de droit fédéral et de législation cantonale relatifs au droit de l'information visent implicitement à instituer les exigences de contrôle sur l'information. Si l'on ramène à l'essentiel les différentes normes légales applicables, c'est une obligation de contrôle qui en ressort d'une certaine manière en « distillat ».

De même, les instruments utilisés pour exercer et garantir le contrôle des données dans les infrastructures informatiques sur site et les solutions cloud sont fondamentalement semblables puisque toujours constituées de mesures techniques, organisationnelles et contractuelles.

2 LES DÉFIS JURIDIQUES DU CLOUD DESIGN

2.1 INFORMATIONS PRINCIPALES

Malgré le principe de «Cloud first» déjà présent dans la «Stratégie suisse d'informatique en nuage» adoptée il y a maintenant près de dix ans, les autorités font encore aujourd'hui preuve d'une certaine réticence qui peut probablement être attribuée à la méfiance inspirée par les solutions en nuage. Huit ans après l'adoption du principe «Cloud First», il est toutefois encore (ou déjà) question dans la Stratégie nuage 2020 d'un **changement de paradigme en faveur du «Cloud First»** (Cloud-Strategie 2020)¹.

La méfiance est à observer à tous les niveaux fédéraux des autorités, c'est à dire chez les autorités fédérales, cantonales et municipales. Alors que les autorités fédérales sont avant tout soumises à la loi sur la protection des données et autres actes fédéraux, les autorités cantonales et communales doivent non seulement se conformer à la loi sur la protection des données mais aussi le cas échéant à d'autres actes de leur canton. Ce qui s'applique cependant aux membres des autorités de tous les niveaux, c'est leur secret de fonction et leur responsabilité pénale en cas de violation de ce secret.

2.1.1 Cloud computing comme externalisation de fait

Dans le cadre des solutions en nuage, les données sont traitées non pas sur les propres ordinateurs ou serveurs locaux mais sur les infrastructures informatiques de fournisseurs tiers, et leur gestion est assurée par un personnel externe. Il s'agit donc bien d'une situation dite d'**externalisation** au sens de la législation sur la protection des données.

Il tient lieu toutefois de distinguer les solutions cloud des solutions classiques d'**externalisation**, qui constituent également une externalisation de fait selon les dispositions sur la protection de données applicables. En général, une externalisation « classique » désigne le cas où un prestataire de services gère des opérations à la place du client conformément aux instructions spécifiques de ce dernier et obtient à ce titre accès aux données qu'il peut donc consulter. Dans un modèle de nuage, par contre, le client reçoit une **prestation standardisée**. Le **caractère individuel** ou l'**absence de caractère individuel** de la relation de service (au niveau technique et organisationnel) est donc un critère majeur qui différencie l'informatique en nuage et l'**externalisation classique**. La transition entre ces deux formes est néanmoins fluide.

2.1.2 À l'étranger

Si, dans le cadre des solutions cloud, des données personnelles sont traitées dans des pays dont le niveau de protection des données est inférieur à celui de la Suisse, de l'UE ou de l'EEE (il est alors question d'une « absence d'équivalence » dans les pays étrangers dits « non sûrs »), la recevabilité de ce traitement des données dépendra du respect non seulement de l'exigence générale de contrôle mais aussi de conditions supplémentaires (p. ex. existence de mesures de protection contractuelles, voir aussi 4.15).

¹ <https://www.newsd.admin.ch/newsd/message/attachments/64752.pdf>

2.2 DISPOSITIONS LÉGALES

2.2.1 Généralités

La Confédération n'ayant pas de compétence générale pour légiférer dans le domaine de la protection des données, les cantons sont, en vertu de leur droit à s'organiser, autorisés à réglementer eux-mêmes la protection des données personnelles qui sont traitées par les autorités cantonales, les communes et les administrations. Tous les cantons ont adopté des décrets généraux sur la protection des données. En définissant les conditions et les principes généraux du traitement des données appliqués par les autorités cantonales et communales ainsi que les droits des personnes concernées, ces décrets concrétisent le droit fondamental à la protection de la personnalité et les principes de l'Etat de droit relatifs au traitement des données personnelles au niveau cantonal. La participation d'organismes publics cantonaux à la concurrence économique privée ne relève pas de l'exercice de fonctions souveraines ou de tâches publiques de droit cantonal (notamment pour les banques cantonales).

Des dispositions légales spécifiques au traitement des données par la sous-traitance figurent dans la loi fédérale LPD et la plupart des lois cantonales sur la protection des données. Ce traitement se produit quand l'organisme public responsable confie à un tiers l'exécution d'un traitement de données.

Certains cantons disposent d'une réglementation spécifique aux conditions d'externalisation en cas d'opérations de traitement des données confiées à des tiers (accord dans un contrat écrit, réglementation spécifique à la sous-traitance, etc.). La plupart des cantons n'établissent toutefois pas ici de règles particulières allant au-delà des prescriptions de la LPD.

On peut dire d'une manière générale que la sous-traitance est en principe autorisée s'il n'existe aucune obligation de confidentialité légale ou contractuelle contraire et si le respect des règles de protection des données est garanti. La législation fédérale et cantonale relative à la protection des données repose ici sur un principe de base comparable.

L'organisme public qui passe le marché reste fondamentalement responsable du respect de la protection des données et doit prendre les mesures permettant d'assurer un niveau de protection des données suffisant.

2.2.2 Les directives les plus courantes

2.2.2.1 Accord contractuel

Un contrat d'externalisation est à conclure avec les tiers qui prennent en charge le traitement externalisé des données pour le compte d'une autorité publique (Microsoft p. ex.). Ce contrat réglera les garanties de respect de la protection et de la sécurité des données ainsi que le recours aux services cloud dans le domaine du droit public.

Il existe en fonction des cantons des dispositions légales stipulant le contenu du contrat à signer avec le sous-traitant. Certains cantons disposent également de « Conditions générales » qui devront obligatoirement accompagner les contrats d'externalisation de services informatiques ou de traitement de données personnelles.² Il est fondamentalement possible de déroger à ces exigences dans l'intérêt de trouver une solution adéquate, notamment dans la mesure où aucune raison impérieuse découlant de la situation juridique ne justifie une application inchangée de ces CG ou si après examen, les exigences d'une réglementation contractuelle suffisante en matière de protection et de sécurité des données sont déjà suffisamment prises en compte dans les contrats du prestataire.

Conformément à la nature d'un « cloud » et à ses offres standardisées pour tous les clients, Microsoft recourt à des contrats standards qui régissent l'utilisation de l'infrastructure cloud. La prise en compte des contraintes individuelles à plus grande échelle est difficile sur cette infrastructure informatique hautement standardisée et doit être clarifiée au cas par cas, Microsoft proposant ici toujours son aide.

² Notamment canton de Berne (Conditions générales du canton de Berne relatives à la sûreté de l'information et à la protection des données dans la fourniture de services informatiques) ; canton de Zurich (Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen)

2.2.2.2 Traitement conforme aux instructions et aux intérêts de l'organisme public

Le sous-traitant traite uniquement les données conformément aux instructions et aux intérêts de l'organisme public. L'article 10a alinéa 1 lettre a de la LPD ainsi que différentes législations cantonales contiennent à cet égard des dispositions stipulant que les données peuvent uniquement être traitées de la manière dont l'organisme public serait lui-même en droit de le faire.

La déclaration de confidentialité de Microsoft (Data Protection Addendum, DPA)³ prévoit ces dispositions. À titre de sous-traitant, Microsoft traitera les données du client (et en particulier les données personnelles) uniquement conformément aux instructions consignées du client et à la déclaration de Confidentialité afin de (a) fournir au client les services en ligne et (b) afin d'assurer ses opérations commerciales licites impliquées par le déploiement de ces services en ligne. Les conventions signées avec le client ainsi que la documentation sur le produit et l'utilisation et la configuration des fonctionnalités des services en ligne constituent ensemble les instructions complètes et définitives que le client donne à Microsoft pour traiter ses données.

En particulier, les données des clients ne seront pas utilisées à des fins de publicité, d'études de marché ou de profilage.

2.2.2.3 Implication d'autres responsables de traitement de données

Dans le paragraphe portant sur les consignes et contrôles en cas de sous-sous-traitance, la DPA explique comment Microsoft procède avec les sous-sous-traitants et informe les clients notamment des modifications survenues les concernant. Ce paragraphe décrit les exigences que Microsoft impose aux sous-sous-traitants et précise qu'il incombe à Microsoft de s'assurer que les sous-sous-traitants respectent toutes les exigences définies dans la DPA.

Le Services Trust Center⁴ en gère la liste, indiquant également les services qu'ils fournissent, le lieu de leur siège, ainsi que l'étendue et les conditions de leur accès aux données des clients : <http://aka.ms/mscloudsubprocessors>.

Dans les services en lignes essentiels, ni Microsoft ni les sous-sous-traitants n'ont un accès administratif permanent aux données et solutions des clients. Microsoft Cloud travaille avec « Zero standing ADMIN » également appelé « Least Privilege » où l'accès administratif est contrôlé par une procédure d'authentification (dite « Lockbox ») : si par exemple, un client fait appel au service assistance de Microsoft, la personne chargée de son cas se verra alors accorder des priviléges (lui permettant éventuellement un accès limité dans le temps aux données du client). L'attribution de l'accès administratif doit passer par plusieurs circuits, des time-boxes et une complète procédure d'audit - et si le client le souhaite, elle peut également impliquer son approbation définitive par la mise en place d'un processus étendu de « Lockbox », appelé « Customer Lockbox » (voir le chapitre 4.11).

2.2.2.4 Sécurité des données

Dans un contexte d'externalisation de services informatiques ou de sous-traitance, les législations fédérales et cantonales relatives à la sécurité de l'information et à la protection des données exigent généralement que le preneur d'ordre garantisse une sécurité des données suffisante. La plupart des actes cantonaux ne définissent pas de mesures de protection concrètes mais fixent des principes sur les objectifs de protection à garantir (**confidentialité, disponibilité et intégrité**). Il s'agit notamment de se protéger contre les risques suivants :

- destruction non autorisée ou accidentelle ;
- perte accidentelle ;
- défaillance technique ;
- falsification, vol ou usage illicite ;
- Modification, copie, accès ou autre traitement non autorisé.

Les données personnelles doivent être protégées contre ces risques par des **mesures techniques et organisationnelles appropriées**.

³ Services en ligne de Microsoft – Complément à la Déclaration de confidentialité : <https://aka.ms/dpa>

⁴ <https://servicetrust.microsoft.com>

Microsoft, qui, dans ses services en ligne, utilise à différents niveaux de nombreux chiffrements, a publié à ce sujet une documentation complète ainsi que des livres blancs. D'une part, différents chiffrements sont appliqués aux données stockées (« data at rest ») sur les environnements d'exploitation (« Volume Level ») comme sur les fichiers individuels de données, ce qui permet d'exclure tout accès physique aux données. La protection par chiffrement peut être encore complétée par des clés gérées par le client, les dites BYOK (« Bring Your Own Key »). Microsoft applique également des techniques de chiffrement à la transmission des données (« data in-transit »). De plus, les services en ligne offrent au client du cloud divers autres moyens d'appliquer et de gérer lui-même certaines techniques de chiffrement.

Via le Microsoft Trust Center⁵ et la certification de service du Security & Compliance Center⁶, les clients du cloud peuvent consulter directement et à tout moment des rapports de certification et d'audit ainsi que d'autres informations complètes sur les lieux de conservation des données, les possibilités d'accès aux données du client du cloud, les mesures de sécurité et de protection des données. Le client du cloud peut ainsi à tout moment se faire lui-même une idée de la manière dont Microsoft respecte ses obligations de sécurité.

2.2.2.5 Traitement transfrontalier

Les lois sur la protection des données de la Confédération et des cantons imposent des exigences particulières quand les données personnelles qui sont traitées dans des environnements cloud sont transférées à l'étranger ou accessibles depuis l'étranger.

En général, l'externalisation vers un pays qui applique le même niveau de protection des données que la Suisse ne requiert aucune mesure supplémentaire. Tel est le cas en particulier pour tous les pays de l'UE/EEE.

Pour les services en ligne SaaS destinés aux clients suisses, Microsoft recourt par défaut aux centres de données de la région Suisse et parfois de la région Europe (centres de données en Irlande, Autriche, Finlande et aux Pays-Bas). C'est dans ces centres de données que sont stockées les données des clients. Les lieux respectifs de conservation des données peuvent être consultés pour chaque service en ligne via la certification de service concernée du centre de sécurité et de conformité⁷.

Le déploiement effectif des services en ligne ou leur configuration individuelle par le client peut, dans certains cas, nécessiter que certaines données du client soient rendues accessibles à des collaborateurs ou sous-traitants de Microsoft qui se trouvent hors de la région du stockage primaire. Il peut de même arriver que les collaborateurs de Microsoft les plus compétents pour résoudre des problèmes de service spécifiques se trouvent sur des lieux situés hors de cette région du stockage primaire des données, et que ceux-ci aient besoin d'accéder en ligne aux systèmes ou aux données afin de résoudre le problème.

Conformément à sa déclaration de confidentialité applicable aux services en ligne, Microsoft est donc fondamentalement en droit de transférer, conserver et traiter les données de ses clients du cloud vers d'autres pays où Microsoft, ses sociétés affiliées ou ses sous-traitants disposent d'installations (aussi aux États-Unis). Pour toutes les données personnelles venant de Suisse, Microsoft s'engage ici à respecter à tout moment les exigences des lois suisses sur la protection des données en termes de collecte, d'utilisation, de transfert, de conservation et d'autres traitements.

⁵ <https://www.microsoft.com/fr-ch/trust-center>

⁶ <https://docs.microsoft.com/fr-ch/microsoft-365/compliance/service-assurance?view=o365-worldwide>

⁷ <https://docs.microsoft.com/fr-ch/microsoft-365/compliance/service-assurance?view=o365-worldwide>



En cas de données clients, données de services professionnels et données personnelles venant de l'UE/EEE et de la Suisse qui seraient à transférer vers des pays tiers non sûrs, Microsoft a conclu des dites clauses contractuelles standard (Processor-to-Processor) entre Microsoft Ireland Operations Ltd. et Microsoft Corp. USA. Pour les exportations de données depuis la Suisse, ces clauses contractuelles standard ont été adaptées aux conditions suisses conformément aux recommandations du PFPDT.

Le 6 mai 2021, Microsoft a annoncé avec son plan « EU Data Boundary » que pour ses principaux services en ligne Azure, Microsoft 365, Dynamics 365 et Power Platform, les données essentielles des clients seront traitées et stockées en Europe et l'assistance fournie depuis l'espace européen.⁸ Ce plan devrait être disponible fin 2022.

Microsoft ne communiquera pas non plus les données des clients aux autorités chargées de la poursuite pénale, à moins que la loi ne l'exige. Si des autorités chargées de la poursuite pénale contactent Microsoft pour demander des données du client, Microsoft tentera de renvoyer celles-ci vers le client afin qu'elles les lui demandent directement. En cas d'obligation de divulguer ou de donner accès à des données aux autorités chargées de la poursuite pénale, Microsoft en informera immédiatement le client et lui fournira une copie de cette requête, à moins que la loi ne l'interdise. Microsoft adopte une approche fondamentale et rigoureuse pour répondre aux demandes officielles d'accès aux données des clients qui sont en ses mains.⁹

Microsoft publie tous les six mois un « Law Enforcement Request Reports » en vue de garantir la transparence sur le nombre et la nature de ces incidents.¹⁰ Ces rapports sont publics et peuvent servir pour les évaluations des risques. Microsoft interagit quotidiennement avec les clients et les gouvernements du monde entier pour participer activement à établir le cadre réglementaire international régissant ces problèmes. En guise de fil conducteur, Microsoft a publié six principes qui reposent également sur les efforts continus déployés pour protéger les données de ses clients et améliorer la protection de leurs données.¹¹ Selon Microsoft, ces principes représentent les droits universels et les exigences de base minimales qui, à notre époque moderne, devraient régir l'accès des autorités chargées de la poursuite pénale aux données. Si l'application de ces principes peut varier d'un pays à l'autre, il convient toutefois de conserver les principes fondamentaux que sont le contrôle, l'équilibre des pouvoirs, l'obligation de rendre des comptes et la transparence.

2.2.2.6 Accès des autorités aux données

Selon les convictions de Microsoft, les clients ont le droit d'être protégés par leur propre législation. Microsoft adopte une approche rigoureuse et de principe pour répondre aux demandes d'accès des autorités aux données des clients qui sont en ses mains.¹² Voici les principales directives que Microsoft respecte dans tous ses services :

- Microsoft n'accorde à aucun gouvernement un accès libre et direct aux données de ses clients, et ne donne à aucun gouvernement les clés de chiffrement ou la capacité de casser le chiffrement.
- Un gouvernement qui souhaite obtenir les données d'un client doit suivre les procédures légales applicables. Il doit nous présenter un mandat de perquisition, une ordonnance judiciaire pour les données des contenus ou une ordonnance procédurale pour l'obtention d'informations relatives aux abonnements ou autres données non relatives au contenu.
- Toutes les demandes doivent porter sur des comptes et identifiants spécifiques.
- L'équipe de conformité juridique de Microsoft examine toutes les demandes pour s'assurer de leur validité, rejette celles qui ne sont pas valables et ne fournit que les données spécifiées.
- Suite à l'arrêt Schrems II, Microsoft s'est engagée à contester juridiquement les demandes officielles émanant de tiers¹³.

Une partie des travaux de Microsoft sur les demandes gouvernementales comporte la publication tous les six mois de « Law Enforcement Request Reports »¹⁴ qui entend garantir la transparence sur le nombre et la nature de ces incidents.

⁸ <https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/>

⁹ La procédure est ici décrite en détails : <https://aka.ms/mslerh>

¹⁰ À consulter ici : <https://aka.ms/mslerr>

¹¹ « Six Principles for International Agreements Governing Law Enforcement Access to Data » : <https://aka.ms/MS6dataaccessPrinciples>

¹² La procédure est ici décrite en détails : <https://aka.ms/mslerh>

¹³ Voir également : <https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/>

¹⁴ <https://aka.ms/mslerr>

Pour évaluer le risque d'accès des autorités aux données, il convient d'examiner le nombre réel des incidents indiqué dans les rapports « Microsoft Law Enforcement Request Reports » qui sont disponibles via le lien ci-dessus. Plus de 90 % des demandes émanant d'autorités portent sur des données de clients privés comme Hotmail ou Skype.

D'après ces chiffres, ...

- ... il est peu probable qu'une entreprise cliente spécifique soit visée par une telle demande,
- ... il est encore moins probable qu'une telle demande ne soit PAS rejetée ou redirigée et
- ... il est encore beaucoup moins probable qu'une telle demande portant sur des données stockées en dehors du pays d'origine de la demande ne soit PAS rejetée ou redirigée.

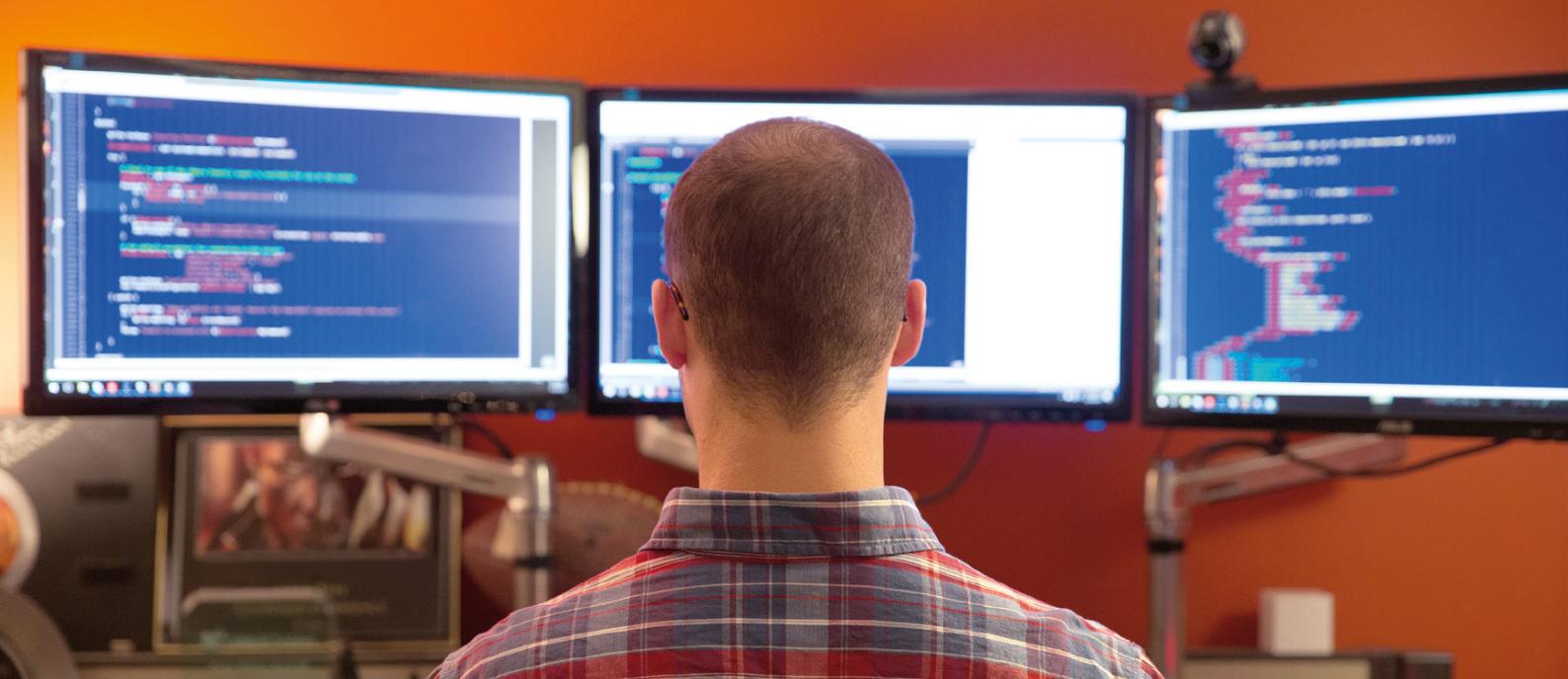
En se basant sur ces rapports et en considérant le processus fondamental de Microsoft ainsi que son historique en protection des droits à la vie privée de ses clients, ces derniers devraient être en mesure d'évaluer les risques et de voir que la probabilité (et donc le risque total) de demandes émanant d'autorités chargées de la poursuite pénale de pays tiers est absolument minime ou quasi inexistante.

Il est également à noter que la différence de chiffres entre les demandes portant sur les comptes de particuliers et celles portant sur les comptes d'entreprises reflète également les recommandations officielles¹⁵ du département « Computer Crime and Intellectual Property » du ministère américain de la justice. Selon ces recommandation, il est conseillé aux procureurs qui souhaitent accéder aux données d'une entreprise de s'adresser directement à elle et non pas d'essayer de passer par les fournisseurs de services cloud, dans la mesure où cela est faisable et ne compromet pas l'enquête par ailleurs.

2.2.2.7 Données sensibles

En cas d'informations très spécifiques qui, pour des raisons d'intérêt public, ne doivent pas tomber entre les mains de tiers car elles touchent par exemple la sécurité d'infrastructures critiques de la communauté, il pourrait être appliquée une restriction explicite ou implicite à l'utilisation d'un service cloud. Cette communauté serait à cet égard tenue de recourir à des classifications des informations permettant de délimiter les données qui ne sont pas à inclure dans un projet cloud. Il tient lieu de planifier ces aspects spécifiquement au cas par cas et de prendre des mesures appropriées à cet effet. Le chapitre suivant en étudie en détail les principes de base.

¹⁵ <https://aka.ms/USDoJSeekingEnterpriseData>



2.3 ORDONNANCE CONCERNANT LA PROTECTION DES INFORMATIONS (OPRI)

L'Ordonnance concernant la protection des informations de la Confédération (OPrl, 2015)¹⁶ règle la protection des informations de la Confédération et de l'armée, dans la mesure où elle est nécessaire dans l'intérêt du pays. Elle fixe notamment la classification et le traitement de ces informations. Pour l'essentiel, cette ordonnance définit des échelons de classification à attribuer aux informations en fonction du degré de protection requis et propose ensuite des mesures qui en découlent ou pourraient en découler. Elle définit les 3 échelons de classification suivants : SECRET, CONFIDENTIEL, INTERNE.

Le tableau ci-dessous résume toutes les mesures de traitement électronique des informations qui sont applicables par échelon.

Échelon / Prescription de traitement	INTERNE (RESTRICTED ¹⁷)	CONFIDENTIEL	SECRET
Mention de classification (label)	Mention INTERNE	Mention CONFIDENTIEL	Mention SECRET
Sauvegarde et conservation	Protection impérative	Sous forme chiffrée sur systèmes de poste de travail ou supports de données amovibles	Uniquement avec les moyens autorisés ou sous forme chiffrée sur systèmes de poste de travail ou supports de données amovibles
Transfert de données	Mode de transmission protégé (réseau de la Confédération p. ex.)	Chiffrement ou mode de transmission protégé	Chiffrement ou mode de transmission protégé
Traitement avec des moyens informatiques	Autorisé	Uniquement avec les moyens autorisés par l'organe de coordination (exception : armée) et en se servant des logiciels de sécurité conformes aux normes de la Confédération	Uniquement avec les moyens autorisés par l'organe de coordination et en se servant des logiciels de sécurité conformes aux normes de la Confédération
Prise en charge depuis un emplacement durable	Autorisé	Autorisé de manière limitée	Autorisé de manière limitée
Consignes pour le retrait et obligation de restitution	Aucun	Impératif	Impératif
Destruction ou effacement	Autorisé de manière limitée	Autorisé de manière limitée	Uniquement par l'auteur

Tableau 1 – Matrice des échelons de classification et des mesures selon OPrl

Cette ordonnance s'applique par ailleurs aux organisations et aux personnes de droit public et de droit privé ainsi qu'aux tribunaux fédéraux et cantonaux qui traitent des informations classifiées, pour autant que cela soit prévu par le droit fédéral ou qu'il en ait été convenu ainsi.

¹⁶ <https://www.fedlex.admin.ch/eli/cc/2007/414/fr>

¹⁷ Les informations classifiées «RESTRICTED» ou de degré équivalent et qui proviennent de l'étranger sont traitées comme des informations classées «INTERNE»

3 OBJECTIFS DE CONTRÔLE ET RISQUES

Comme dans les autres domaines, l'utilisation du cloud n'est pas soumise à des lois ou règles qui l'interdisent ou l'autorisent en soi. Les responsables de la protection des données des organismes publics doivent donc procéder à une analyse des risques tenant compte de la législation applicable, du type de données, de leur forme de traitement et des mesures de protection et de contrôle possibles, afin de décider si le passage au cloud est envisageable ou non.

Avant de choisir les mesures appropriées, il est capital de connaître la classification des données et informations et de consulter la documentation à ce sujet (voir chapitre 2.3). Cette classification sert également de base à la configuration et au contrôle des technologies et moyens appliqués pour la mise en œuvre des mesures. Toute organisation devrait prévoir des mesures de protection adaptées à chaque catégorie de données en s'appuyant sur les dispositions de l'Ordonnance concernant la protection des informations (voir chapitre 2.3). Ces mesures de protection, qui sont notamment d'ordre contractuel, organisationnel et technique, pourraient être appliquées par une entreprise comme suit :

- **Données secrètes**

Dans un premier temps, les données secrètes ne sont pas sauvegardées dans le cloud mais sur site. Pour ici profiter autant que possible des fonctions de sécurité d'Azure, les données sont stockées sur un Azure Stack HCI qui est géré via Azure Arc.

- **Données confidentielles**

Le stockage des données confidentielles dans le cloud est permis sous forme chiffrée. Azure Information Protection (AIP) est ici la solution à choisir soit avec sa propre clé (BYOK) soit avec deux clés – une dans Azure et une autre sur site chez le client (Double Key Encryption).

Les chapitres suivants ne traiteront pas des mesures à appliquer à chaque niveau de classification mais proposent plutôt les objectifs de contrôle et risques envisageables qui sont à prendre en compte et à traiter dans la prise de décision en faveur d'un Public Cloud. Les mesures à engager dépendront ensuite de la nature, de la structure et des informations des données.

3.1 OBJECTIFS DU CONTRÔLE

Le modèle largement connu « Information Security Triad » (triade sécurité de l'information) peut servir de base pour classifier les risques et mesures. Il se concentre sur les trois principaux domaines de la sécurité de l'information Confidentiality (confidentialité), Integrity (intégrité) et Availability (disponibilité). Il s'agit ici pour l'essentiel d'atteindre les objectifs généraux de contrôle suivants en répondant aux questions associées.

ID	Domaine	Objectif et description	Bases
OC1	C	Droits d'accès Les données qui relèvent de la responsabilité du sous-traitant sont-elles suffisamment protégées contre tout accès physique non autorisé (protection de la confidentialité p. ex.)	Meilleures pratiques en sécurité de l'information (p. ex. norme minimale TIC de l'OFAE) art. 7 et art. 10a al. 2 LPD, art. 8 et art. 9 al. 1 let. a OLPD art. 8 al. 1-2 et art. 9 al. 2 LPD rév.
OC2	C	Contrôle d'accès Les droits d'accès électroniques sont-ils suffisamment réglementés ?	Meilleures pratiques en sécurité de l'information (p. ex. norme minimale TIC de l'OFAE) art. 7 et art. 10a al. 2 LPD, art. 8 et art. 9 al. 1 let. g OLPD art. 8 al. 1-2 et art. 9 al. 2 LPD rév.

OC3 C	Contrôles de l'utilisation Le contrôle des personnes ayant un accès permanent ou temporaire aux données est-il suffisant pour minimiser le risque d'utilisation non autorisée des données et permettre de retracer les infractions ?	Meilleures pratiques en sécurité de l'information (p. ex. norme minimale TIC de l'OFAE) art. 7 et art. 10a al. 2 LPD, art. 8 et art. 9 al. 1 let. d et h OLPD art. 8 al. 1–2 et art. 9 al. 2 LPD rév.
OC4 C	Contrôle de l'effacement Est-il assuré que le sous-sous-traitant supprime les données à la fin du contrat d'externalisation ?	Art. 10a al. 1 let. a LPD art. 9 al. 1 let. a LPD rév.
OC5 I	Contrôle de l'intégrité Quelles sont les dispositions prises pour empêcher le sous-traitant ou un autre tiers de manipuler les données ?	Meilleures pratiques en sécurité de l'information art. 7 et art. 10a al. 2 LPD art. 8 al. 1–2 et art. 9 al. 2 LPD rév.
OC6 A	Contrôle de la disponibilité Comment est assurée la disponibilité des données ?	Meilleures pratiques en sécurité de l'information (p. ex. norme minimale TIC de l'OFAE) art. 7 et art. 10a al. 2 LPD art. 8 al. 1–2 et art. 9 al. 2 LPD rév.
OC7 A	Restauration des données Comment est assuré que les données pourront être restaurées en cas de perte ou d'erreur ?	Meilleures pratiques en sécurité de l'information art. 10a al. 1 let. a LPD art. 9 al. 1 let. a LPD rév.

Tableau 2 – Objectifs de contrôle de la sécurité de l'information

3.2 ANALYSE DES RISQUES

La liste des risques présentée ci-dessous peut être évaluée par les décideurs des organismes publics et servir de base à la prise de décision. Les risques y sont assortis des mesures contractuelles, organisationnelles et techniques qu'ils impliquent et qui sont explicitées dans le chapitre suivant. Cette liste peut être étendue en cas de réglementation supplémentaire (cantonale ou communale p. ex.). Les risques découlent des objectifs de contrôle exposés au chapitre 3.1 et sont également classés selon la méthode générale C-I-A. Certains risques ne renvoient qu'à la base légale ou réglementaire (**REG**) car ils ne peuvent être affectés qu'indirectement à l'un des trois domaines de la sécurité de l'information. Les risques visent volontairement la relation entre le client et le sous-traitant. En plus des mesures contractuelles et organisationnelles touchant la relation avec son sous-traitant, le client a toutefois la possibilité, dans la plupart des domaines, de prévoir lui-même d'autres mesures techniques de protection et de sécurité qui répondent au risque spécifique. Il peut ici s'agir des mesures minimisant les risques encourus avec le sous-traitant ou avec des tiers potentiels non autorisés. Il faudra à chaque risque répondre à cette question supplémentaire : « Comment et avec quelles mesures supplémentaires à celles du sous-traitant est-ce que je peux et devrais mieux contrer ce risque en tant que client ? ».

Le tableau des risques présenté ci-dessous propose également les mesures correspondantes. Il s'agit des mesures prises par le sous-traitant (conventions, documentation) ainsi que des mesures que le client peut prendre.

ID	Domaine (C-I-A), REGlementation	Risque	ID des mesures	Impact du risque après la mesure Probabilité de survenance du risque	Évaluation du risque	Risque résiduel atténué ?
R1	REG	Sous-sous-traitant Est-il garanti que le sous-traitant informe le client du recours à des sous-sous-traitants et lui accorde un droit d'opposition en cas de remplacement ou avant de faire appel à de nouveaux (art. 9 al. 3 LPD rév.) ? Les sous-sous-traitants sont-ils soumis à la même base légale et réglementaire que le sous-traitant ?	M15			
R2	REG	Sécurité insuffisante des données Est-il garanti que le sous-traitant protège suffisamment la confidentialité, l'intégrité et la disponibilité des données personnelles du client (art. 10a, al. 2, LPD art. 9, al. 2, LPD rév.) ? La réalisation d'un audit sur le respect des procédures et directives de sécurité applicables est-elle assurée et clairement documentée ?	M8 M10 M15 M16			
R3	REG	Violation de la sécurité des données non signalée Est-il garanti que le sous-traitant signale au client les violations de la sécurité des données (art. 10a al. 2 LPD art. 9 al. 2 et art. 24 al. 3 LPD rév.) ? Le sous-traitant surveille-t-il les services pour y exclure toute violation de la sécurité et procède-t-il à des optimisations de manière proactive ?	M7 M15			
R4	REG	Finalités propres du sous-traitant Est-il garanti que le sous-traitant n'utilise les données personnelles traitées que pour le compte et aux fins du client et non pas à ses propres fins (art. 10a al. 1 let. a LPD art. 9 al. 1 let. a LPD rév.) ? Comment est réglementée la propriété des données ? Comment sont répartis les rôles et les responsabilités entre le client et le sous-traitant ?	M15 M16			
R5	REG	Communication transfrontalière Des garanties adéquates (de type clauses contractuelles euro-péennes p. ex.) sont-elles mises en place pour assurer une protection appropriée aux données personnelles transmises dans des pays qui n'offrent pas un niveau de protection des données suffisant (art. 6 et art. 10a al. 1 let. a LPD art. 16 et art. 9 al. 1 lit. a LPD rév.) ?	M15			
R6	C REG	Divulgation de faits secrets Les informations soumises au secret professionnel ou de fonction sont-elles suffisamment protégées contre l'accès du sous-traitant ou de tiers aux textes en clair (art. 320 CP, art. 321 CP) ? Le traitement des données par le sous-traitant est-il soumis à une obligation de confidentialité adéquate ?	M2 M3 M4 M11 M12 M13 M15 M16			
R7	REG	Accès des autorités aux données Le sous-traitant accorde-t-il un droit de regard suffisant sur ses processus et directives régissant l'accès de l'État aux données pour permettre au client de prendre ici une décision en connaissance de cause (meilleure pratique) ?	M15 M16			

R8	CIA	Manque de gouvernance	M1
	REG	Le sous-traitant a-t-il donné au client un aperçu suffisant sur son propre système de contrôle interne (SCI) (meilleure pratique) ?	M10
		La réalisation d'un audit sur le respect des procédures et directives de sécurité applicables est-elle assurée et clairement documentée ?	M15 M16
R9	I	Rapports insuffisants	M7
	REG	Le sous-traitant fournit-il des rapports suffisants sur les activités et services externalisés (meilleure pratique) ? La réalisation d'un audit sur le respect des procédures et directives de sécurité applicables est-elle assurée et clairement documentée ?	M15 M16
R10	C	Accès non autorisé au lieu de stockage des données (OC1)	M4
		Une certaine transparence est-elle assurée sur les mesures techniques et organisationnelles prises par le sous-traitant pour protéger les données des clients contre les accès non autorisés et les accès physiques, ainsi que sur le chiffrement lors du transfert, la protection contre les logiciels malveillants, la confidentialité, l'authentification et les directives opérationnelles applicables à son personnel ?	M5 M6 M15 M16
R11	C	Accès non autorisé aux contenus des données (OC2)	M5
		Le sous-traitant est-il en mesure de faire état de stratégies sur les accès aux composants et données et est-il manifeste que des procédures et stratégies de sécurité suffisantes sont appliquées ? Existe-t-il des procédures prévoyant d'assurer l'accessibilité aux données après la survenue de pannes ?	M6 M15 M16
R12	C, I	Utilisation non autorisée de données (OC3)	M7 M15
		Est-il garanti et prouvé que le sous-traitant soit n'a aucun accès aux données du client, soit peut uniquement les consulter dans le cadre de la sous-traitance qui lui est confiée ? Existe-t-il une journalisation des accès aux données qui se seraient produits ? Existe-t-il de la part du sous-traitant des obligations de confidentialité applicables dans le cadre des fonctions requises ?	
R13	C	Effacement non conforme de données (OC4)	M9 M15
		Le sous-traitant dispose-t-il de directives claires stipulant comment traiter la résiliation d'un abonnement ou l'effacement des données par le client ? Les composants matériels sont-ils éliminés selon les normes applicables dans le secteur ? Les données sont-elles portables ? Est-il garanti qu'il existe un droit contractuel de regard sur ce sujet ?	
R14	I	Atteinte à l'intégrité des données (OC5)	M15 M16
		Le sous-traitant veille-t-il à ce que son personnel soit formé aux procédures et directives de sécurité requises (gestion des sessions d'administration ou mots de passe p. ex.) et les applique activement ?	
R15	A	Disponibilité réduite et restauration des données (OC6 & OC7)	M9 M15 M16
		Le sous-traitant met-il à disposition, pour chaque service, une documentation sur le SLA et sur les garanties qui en découlent ? Le sous-traitant a-t-il mis en place une gestion de la poursuite de ses activités ? Sait-on clairement ce qui se passera si le sous-traitant décide de mettre fin à certains services ? Des procédures de restauration et leur vérification sont-elles mises en place sur la base de la plateforme ? Les responsabilités du client sont-elles dans ce contexte clairement définies ?	

Tableau 3 – Analyse des risques fondée sur la législation et les fondamentaux de la sécurité de l'information

4 MESURES ET DESCRIPTION DES COMPOSANTS

Ce chapitre propose et explicite les mesures envisageables pour contrer les risques énumérés ci-dessus. Ces mesures ne sont pas classées par ordre de priorité.

ID des mesures	Domaine	Mesure	Type de mesure
M1	C, I, A	ISO 27001	Organisationnel, contractuel
M2	C, I, A	Azure Purview	Technique, organisationnel
M3	C, I, A	Azure Resource Tags	Technique, organisationnel
M4	C, I	Azure Key Vault	Technique
M5	C	Azure IAM (RBAC)	Technique, organisationnel
M6	C, I, A	Azure Policies	Technique, organisationnel
M7	A	Azure Monitor	Technique
M8	C	Compliance Manager pour RGPD	Technique, organisationnel, contractuel
M9	C	Azure Data Subject Requests pour RGPD	Technique, organisationnel
M10	C, I, A	Formation en MPSCD	Organisationnel
M11	C	Lockbox clients pour Azure	Technique, organisationnel
M12	C, I, A	Azure Stack Hub	Technique, organisationnel
M13	C, I, A	Azure Stack HCI	Technique, organisationnel
M14	C, I, A	Azure Arc	Technique, organisationnel
M15	C	Conventions	Contractuel
M16	C, I, A	Shared Responsibility Modell	Organisationnel, contractuel

Tableau 4 – Liste des mesures

4.1 M1 – AZURE BLUEPRINT – ISO 27001

Azure Blueprints sont des modèles (templates) regroupant les ressources, stratégies et autorisations qui sont applicables et réutilisables comme un ensemble pour déployer un ou plusieurs environnements de base standardisés dans Azure.

Le modèle de base utilisé pour le Swiss Public Sector Cloud Design est un blueprint déjà existant qui s'appuie sur la norme de sécurité ISO 27001 et auquel sont ajoutées des extensions spécifiques permettant de répondre aux besoins identifiés.

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- Stratégie : limitation des ressources cloud de sauvegarde et traitement des données à la région Azure suisse ou européenne
- Stratégie : application de protocoles de transmission sécurisés ou chiffrés (TLS/SSL) imposée à la communication des ressources cloud
- Stratégie : application du regroupement des journaux des activités (logging) imposée à l'ensemble des ressources et services

- Autorisations : création et attribution des droits d'accès aux ressources et aux services assurant un contrôle d'accès aux composants et fonctions de l'environnement Azure qui est différencié et basé sur les rôles
- Ressource : création d'un Key Vault pour le stockage sécurisé des clés de chiffrement
- Ressource : création d'un Log Analytics Workspace pour la conservation et l'évaluation éventuelle des journaux des activités

D'autres composants peuvent à tout moment être ajoutés au blueprint ou mis en œuvre en dehors de lui comme mesures individuelles.

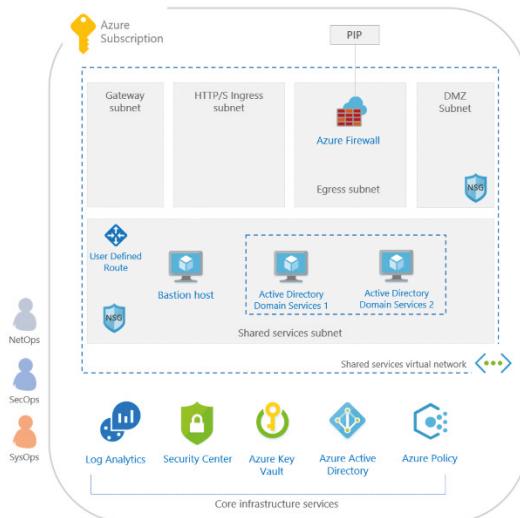
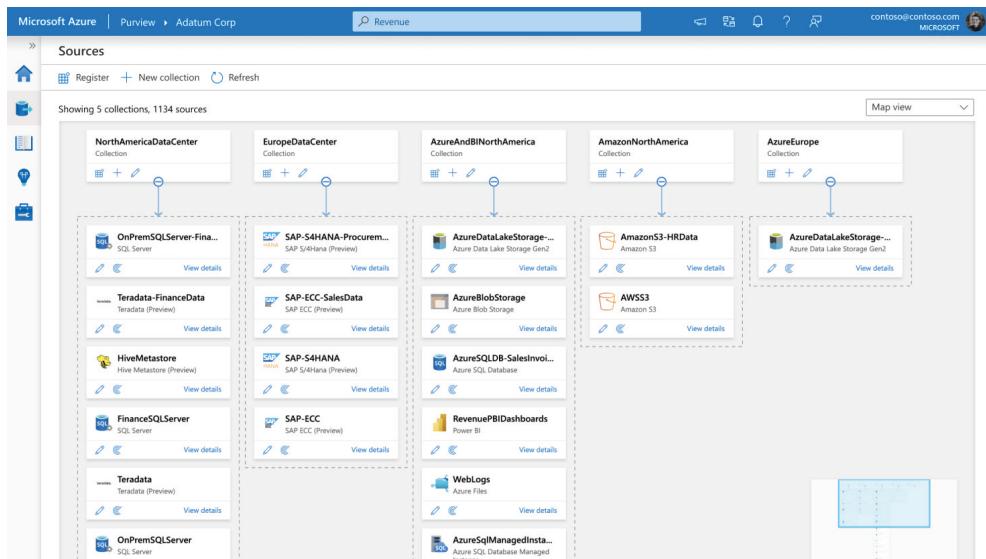


Figure 1 – Blueprint ISO 27001

4.2 M2 – AZURE PURVIEW

L'outil Azure Purview sert à la collecte universelle et centralisée de toutes les données stockées dans le cloud (pas uniquement Azure) et ainsi que des ressources sur site. Il permet ainsi d'obtenir une carte holistique de toutes les informations sous forme de métadonnées. La classification et l'origine des données y font l'objet d'une attention particulière pour permettre d'évaluer le patrimoine des informations, de prendre les mesures éventuellement nécessaires ou simplement de trouver des informations.

L'index des informations (catalogue des données) est automatiquement établi par des scans réguliers des ressources connues : les règles de classification standardisées et définies par l'utilisateur qui sont ici utilisées servent ensuite de filtres lors de la recherche de données. Les critères de classification mais aussi un glossaire facilitent également le repérage et la localisation des informations.



The screenshot shows the Microsoft Azure Purview interface. At the top, there's a navigation bar with 'Microsoft Azure', 'Purview', 'Adatum Corp', a search bar ('Revenue'), and a user profile ('contoso@contoso.com MICROSOFT'). Below the navigation is a left sidebar with icons for Home, Sources, Register, New collection, Refresh, and a magnifying glass. The main area is titled 'Sources' and shows 'Showing 5 collections, 1134 sources'. There are five main collections displayed in a grid: 'NorthAmericanDataCenter' (with sub-sources like 'OnPremSQLServer-Fin...', 'Teradata-FinanceData', 'HiveMetastore', 'FinanceSQLServer', 'Teradata', and 'OnPremSQLServer'), 'EuropeDataCenter' (with sub-sources like 'SAP-S4HANA-Procurement...', 'SAP-ECC-SalesData', 'SAP-S4HANA', 'SAP-ECC', 'RevenuePBI-Dashboards', 'WebLogs', and 'AzureSqlManagedInst...'), 'AzureAndBInNorthAmerica' (with sub-sources like 'AzureDataLakeStorage...', 'AzureBlobStorage', 'AmazonNorthAmerica' (with sub-sources like 'AmazonS3-HRData', 'AWS3'), and 'AzureDataLakeStorage...'), and 'AzureEurope' (with sub-sources like 'AzureDataLakeStorage...'). A 'Map view' button is located in the top right corner.

Figure 2 – Azure Purview

L’interface normalisée Apache Atlas permet d’importer dans le catalogue des données des métadonnées provenant d’autres sources.

Azure Purview est fortement recommandé pour la classification et l’indexation des données stockées dans Azure et comme outil de contrôle des responsables de la protection des données.

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- identification et gestion des données confidentielles.

4.3 M3 – AZURE RESOURCES TAGS

Les Resources Tags sont un autre moyen universel de classer les ressources et leurs données stockées. Ces balises représentent des méta-information librement définissables qui peuvent être appliquées à différents niveaux de l’infrastructure Azure contrôlée et elles-mêmes évaluées à différentes fins. Les Azure Resource Tags sont une Key Value Pair.

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- identification et gestion des données confidentielles.

4.4 M4 – AZURE KEY VAULT

La plateforme Azure est toujours chiffrée par Microsoft et c’est vous qui en gérez les clés. Azure Key Vault est un service PaaS permettant de générer les clés propres au client (a-/symétriques) qui sont dédiées au chiffrement de ses données. Les droits d’accès explicites aux clés qui sont accordées aux comptes de service des ressources, tels que les comptes de stockage ou Azure SQL DB, garantissent ici qu’aucune interaction humaine n’est requise avec les clés de chiffrement et les certificats et que le chiffrement et le déchiffrement se font de manière transparente.

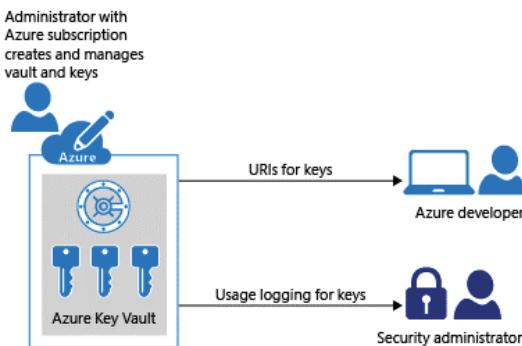


Figure 3 – Azure Key Vault

Les clés de chiffrement et certificats sont stockés dans des instances logicielles de Key Vault qui sont contrôlées par le client. Si le stockage des clés de chiffrement doit se faire dans des modules de sécurité matériels (HSM) dédiés ou même dans un propre HSM sur site, Key Vault Managed HSM pourra s'en charger.

Si l'une des exigences suivantes s'applique à votre organisation, il sera possible de protéger les contenus client en recourant à Key Vault avec ou sans Managed HSM :

- Vous devez impérativement être le seul à pouvoir déchiffrer les contenus protégés
 - Vous ne souhaitez pas que Microsoft puisse avoir accès à des données très sensibles
 - Vous êtes tenu par la loi à conserver les clés de chiffrement au sein d'une frontière géographique
- Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :
- chiffrement des données sensibles.

4.5 M5 – AZURE IAM (ROLE BASED ACCESS CONTROL RBAC)

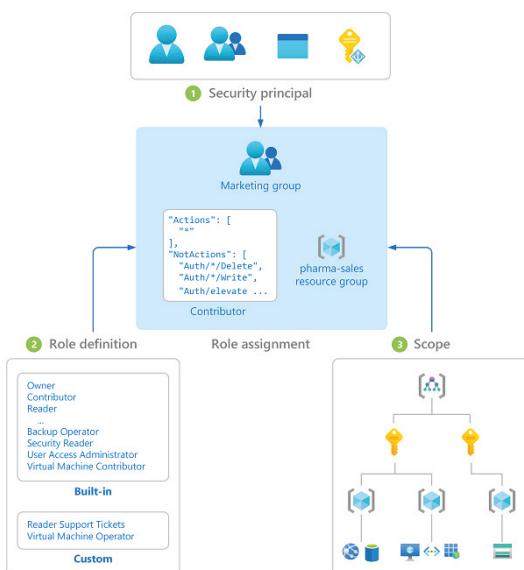


Figure 4 – Azure IAM (RBAC)

Le cloisonnement des tâches et le contrôle d'accès à la plateforme Azure et à ses ressources des services et applications sont assurés par le système d'autorisation intégré et basé sur les rôles, avec authentification préalable des identités par Azure AD. Azure propose ici de nombreux rôles prédéfinis qui déterminent les droits d'accès aux ressources et éléments de la plateforme et peuvent être attribués aux différents types d'identité.

Le système d'autorisation permet toutefois de créer des définitions de rôle propres à l'utilisateur et de les attribuer au cas où les rôles standards proposés ne suffiraient pas.

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- protection des accès aux ressources.

4.6 M6 – AZURE POLICIES

Azure Policies sont des stratégies qui règlementent l'infrastructure Azure afin de vérifier les exigences organisationnelles à grande échelle ou même de les imposer. Des dashboards permettent d'obtenir une vue d'ensemble consolidée de la conformité mais aussi de se focaliser sur la conformité par ressource ou stratégie.

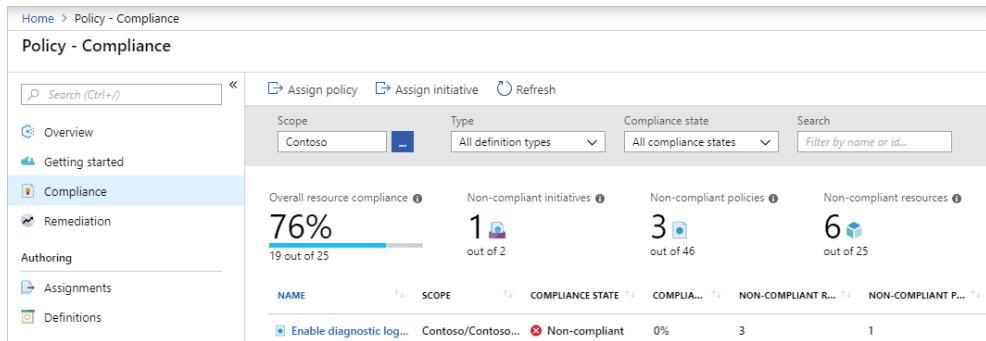


Figure 5 – Azure Policies

Ces stratégies sont d'excellents outils pour imposer ou contrôler notamment les exigences suivantes :

- limitation du déploiement des ressources aux régions Azure autorisées (CH, UE p. ex.) ;
- utilisation imposée d'une transmission de données chiffrée avec des certificats prédéfinis ;
- application imposée d'un chiffrement des données recourant à des algorithmes de chiffrement autorisés ;
- Regroupement imposé de tous les journaux des activités.

Il est ici proposé de nombreuses stratégies prédéfinies directement utilisables, qui peuvent être, si nécessaire, complétées par des règles spécifiques à l'utilisateur.

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- limitation des ressources cloud de sauvegarde et traitement des données à la région Azure suisse ou européenne ;
- application de protocoles de transmission sécurisés ou chiffrés (TLS/SSL) imposée à la communication des ressources cloud ;
- application du regroupement des journaux des activités (logging) imposée à l'ensemble des ressources et services.

4.7 M7 – AZURE MONITOR

Azure Monitor regroupe tous les moyens pour surveiller la disponibilité, la performance et les événements de la plateforme Azure et des services et ressources utilisés. Il permet de configurer des alertes en fonction de seuils et d'événements qui déclencheront des notifications supplémentaires (e-mail, SMS p. ex.) ou des automatismes en vue d'assurer la continuité des services.

À l'aide de Workbooks, il est également possible de créer des Monitoring Dashboards dotés d'indicateurs visuels sur la disponibilité et la performance ainsi que des journaux d'événements.

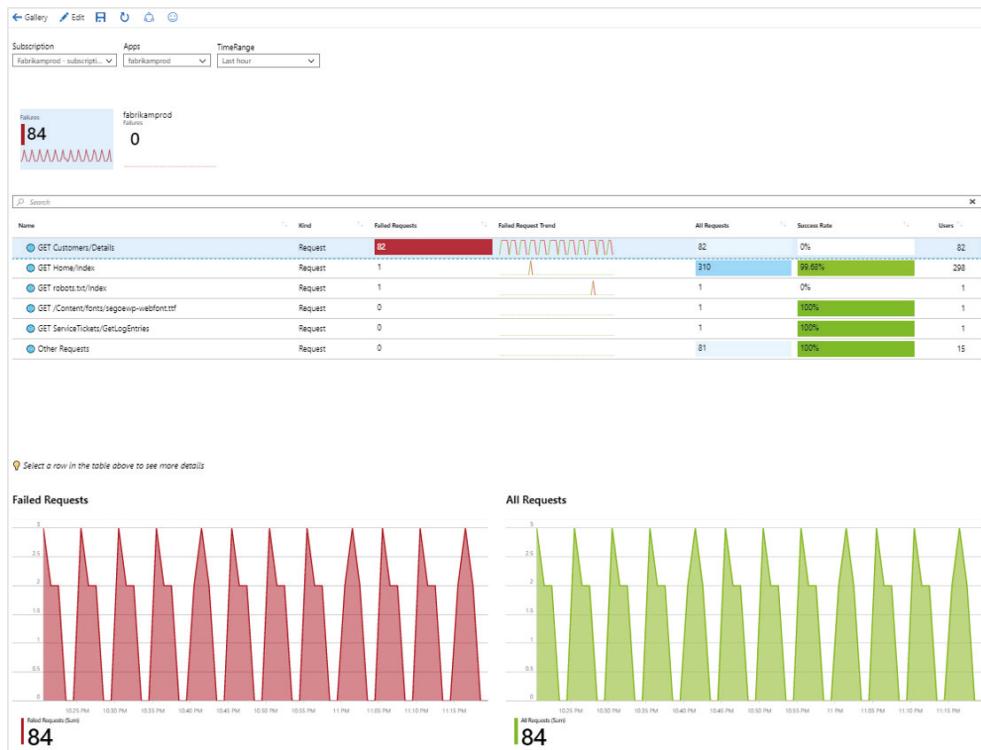


Figure 6 – Azure Monitor

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- vue d'ensemble sur la disponibilité des ressources ;
- alertes en cas d'éventuels dysfonctionnements et menaces.

4.8 M8 – MICROSOFT COMPLIANCE MANAGER POUR GDPR / RGPD

Compliance Manager est un outil permettant de surveiller et de vérifier la conformité de votre institution ainsi que sa mise en œuvre d'Azure avec le règlement général sur la protection des données de l'UE RGPD / GDPR.

GDPR Compliance Manager vous offre des fonctions supplémentaires :

Default Group
Azure - GDPR

Actions 

Created 10/26/2020 Modified 10/26/2020

Customer Managed Actions 0 of 82

Microsoft Managed Actions 45 of 48

Assessment Status



- combinaison des informations que Microsoft déploie pour les auditeurs et autorités de surveillance ;
- attribution des activités de conformité ainsi que leur suivi et enregistrement ;
- évaluation vous aidant à comprendre et à hiérarchiser les contrôles qui visent à minimiser les risques ;
- dépôt sécurisé pour la documentation et autres artefacts ;
- établissement de rapports détaillés qui peuvent être fournis aux auditeurs, aux autorités de surveillances ou autres parties prenantes.

Figure 7 –
Microsoft Compliance Manager pour RGPD

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- assurance de la conformité à RGPD / GDPR.

4.9 M9 – AZURE DATA SUBJECT REQUESTS POUR GDPR / RGPD

Le Règlement général sur la protection des données de l'Union européenne (RGPD/GDPR) donne à toute personne concernée le droit d'influer sur les données personnelles qui sont collectées à son sujet par une organisation. Le RGPD accorde aux personnes concernées certains droits sur leurs données personnelles, en leur permettant notamment d'en exiger des copies ainsi que leurs corrections, une restriction de leur traitement, leur effacement ou leur fourniture sous format électronique en vue d'un transfert à un autre responsable du traitement ou autre sous-traitant. Une demande officielle émanant d'une personne concernée qui prie le responsable du traitement de prendre des mesures sur ses données personnelles est appelée Data Subject Request ou DSR en anglais.

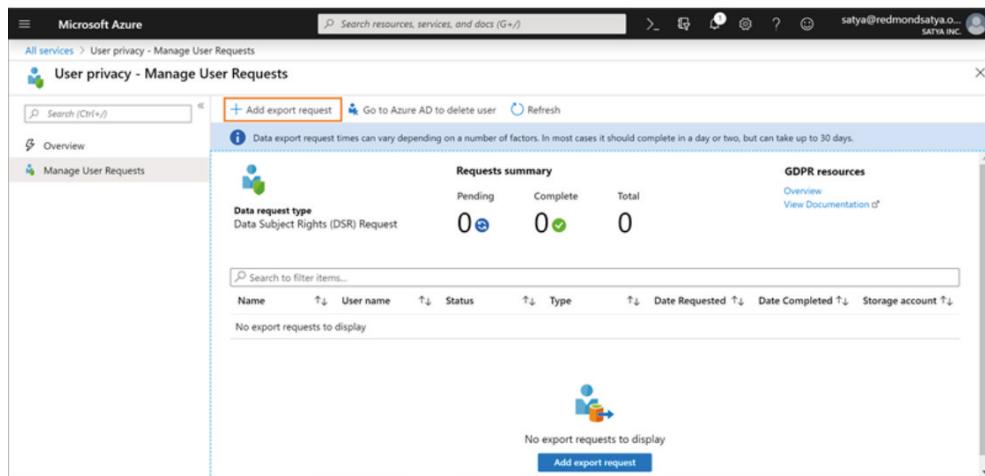


Figure 8 – Azure Data Subject Requests pour RGPD

L'outil Azure Data Subject Requests for GDPR permet de traiter les demandes des personnes concernées conformément au RGPD.

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- gestion (accès, restitution et effacement) de données pertinentes au sens du RGPD.

4.10 M10 – FORMATION POUR MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Pour assurer une utilisation efficace d'Azure comme plateforme cloud et de ses composants et concepts présentés ici, il est également nécessaire que le personnel chargé de s'en occuper suive une formation.

- Certains membres du réseau des partenaires de Microsoft proposent une introduction à Microsoft Cloud Design.

Bases	Technologie	Fonctionnement
<ul style="list-style-type: none"> – Introduction Cloud Design – Loi suisse sur la protection des données (LPD) – Ordonnance concernant la protection des informations (OPrl) – Sécurité de l'information (ISO 27001) – Classification des informations 	<ul style="list-style-type: none"> – Blueprints (modèles) – Purview (catalogue de données) – Policies (stratégies) – Key Vault (chiffrement) – Monitor (surveillance) – Lockbox clients 	<ul style="list-style-type: none"> – Blueprint Deployment – Analyse de la conformité – Création de stratégies – Configuration de l'environnement – Vérification continue – Surveillance

Figure 9 – Formation en Microsoft Public Sector Cloud Design

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- prévention des erreurs de manipulation ;
- assurance de la continuité opérationnelle ;
- meilleure compréhension des technologies, risques et possibilités pour les départements informatiques.

4.11 M11 – LOCKBOX CLIENTS POUR AZURE

La Lockbox clients (Customer) pour Microsoft Azure vous permet en tant que client d'examiner et d'approuver/rejeter une demande d'accès à vos données émanant de Microsoft. Elle sert pour les cas où un technicien de Microsoft a besoin d'accéder aux données du client lors d'une demande d'assistance.

Il est ainsi notamment possible d'évaluer si les informations à transmettre lors d'une demande d'assistance sont confidentielles ou non et si elles peuvent être consultées ou non.

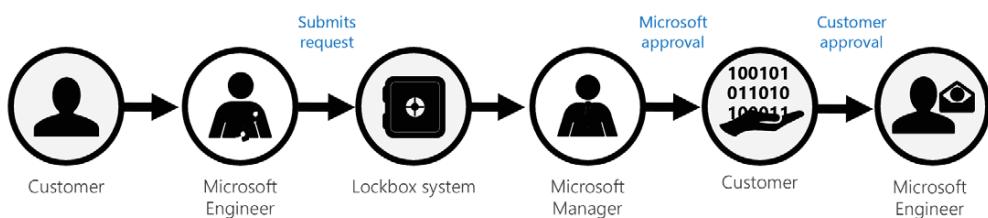


Figure 10 – Lockbox clients

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- préservation de la confidentialité des données personnelles.

4.12 M12 – AZURE STACK HUB

Azure Stack Hub est votre propre cloud Azure privé qui peut fonctionner entièrement ou partiellement déconnecté d'Internet. Azure Stack Hub est un élément du portefeuille Azure Stack qui constitue une extension d'Azure pour vous permettre d'exécuter des applications dans un environnement sur site et de déployer des services Azure dans votre centre de données. De nombreuses entreprises qui procèdent à une transformation numérique constatent qu'elles peuvent accélérer le processus en profitant des services de cloud public pour créer des architectures modernes et mettre à jour leurs applications. Certaines workflows doivent toutefois rester sur site - en raison notamment d'exigences techniques et juridiques différentes. Azure Stack Hub vous permet, par exemple, de stocker des données sensibles et classées secrètes.



Figure 11 – Azure Stack Hub

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- stockage des données dans ses propres centres de données.

4.13 M13 – AZURE STACK HCI

Azure Stack HCI remplit le même objectif qu'Azure Stack Hub : exploiter sur le site les données qui ne doivent pas migrer dans le cloud.

Azure Stack HCI est une plateforme de virtualisation hyperconvergée et standardisée qui a été développée et certifiée par des fabricants de matériel informatique et Microsoft. Elle permet d'y exploiter des serveurs virtuels et fournit les services d'infrastructure suivants :

- Système d'exploitation Azure Stack HCI
- Matériel vérifié par un partenaire OEM
- Services hybrides Azure
- Windows Admin Center
- Machines virtuelles sur hyper V
- Mémoire virtualisée directement sur Storage Spaces
- Réseau virtualisé basé sur SDN avec contrôleur de réseau (en option)

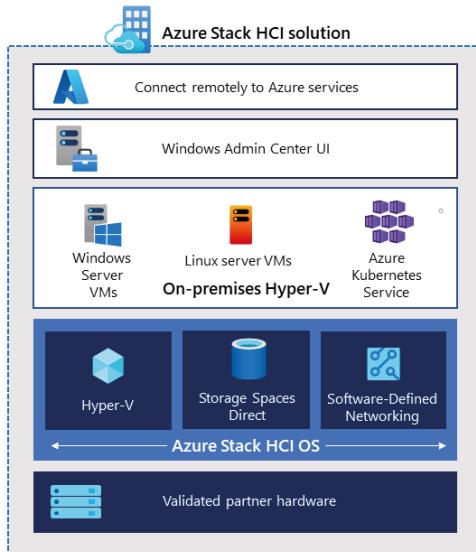


Figure 12 – Azure HCI

Il est par ailleurs possible de recourir à d'autres services hybrides d'Azure :

- Azure Site Recovery, pour assurer une haute disponibilité et le service de reprise après sinistre (Disaster-Recovery-as-a-Service, DRaaS)
- Azure Monitor, un pôle où vous pouvez surveiller l'activité de vos applications, réseaux et infrastructures - à l'aide d'analyses d'IA avancées
- Cloud Witness, pour utiliser Azure comme point d'arbitrage
- Azure Backup, pour protéger les données via un stockage sur d'autres emplacements et s'assurer contre les ransomware
- Azure-Update Management, pour évaluer et déployer les mises à jour sur les machines virtuelles Windows exécutées dans Azure et sur site
- Azure-Network Adapter, pour connecter des ressources locales à vos machines virtuelles hébergées dans Azure via un Point-to-Site-VPN
- Azure-File Sync, pour synchroniser votre serveur des données avec le cloud

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- stockage des données dans ses propres centres de données.

Azure Stack HCI permet de profiter des services d'Azure suivants :

- Surveillance : affichez tout en un l'ensemble de vos clusters Azure Stack HCI en les regroupant et référençant par groupes de ressources.
- Facturation : réglez Azure Stack HCI via votre abonnement Azure.

4.14 M14 – AZURE ARC

Azure Arc offre une plateforme cohérente pour divers public clouds et l'environnement sur site afin d'en simplifier la gouvernance et la gestion. Azure Arc permet de réaliser les opérations suivantes :

- Tout l'environnement peut être géré via une interface utilisateur centralisée grâce à la projection dans Azure Resource Manager des ressources existantes (ressources provenant d'Azure, de l'environnement sur site ou d'autres clouds)
- Gestion des ordinateurs virtuels, des clusters Kubernetes et des bases de données comme si exécutés dans Azure
- Mise en œuvre, dans tout votre environnement, d'une solution cohérente d'inventaire, de gestion, de gouvernance et de sécurité pour les serveurs
- Configuration d'extensions de machines virtuelles Azure pour utiliser les services de gestion d'Azure permettant de surveiller, protéger et mettre à jour vos serveurs
- Visualisation cohérente de vos ressources compatibles avec Azure Arc via l'utilisation d'Azure-Portal, Azure CLI, Azure PowerShell ou Azure-REST-API

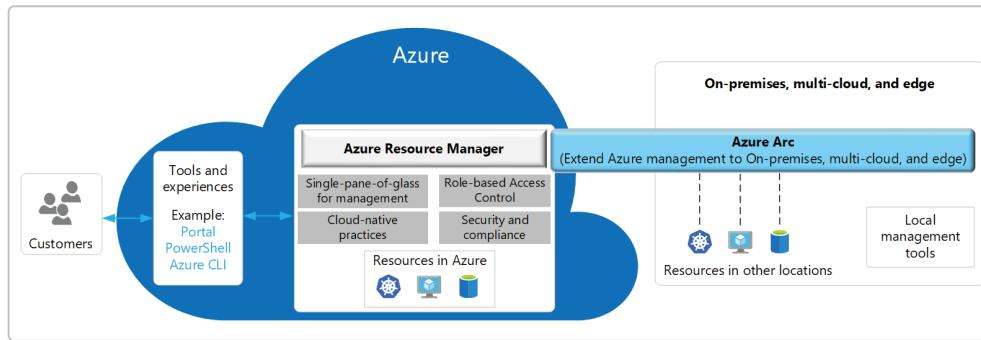


Figure 13 – Azure Arc

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- identification et gestion des données confidentielles ;
- minimisation des failles de sécurité via des mises à jour et des antivirus pour les workloads dans le Cloud et sur les sites ;
- gouvernance cohérente pour toutes les ressources utilisées ;
- conformité des ressources assurée par une gestion centralisée.

4.15 M15 – CONVENTIONS

Pour mieux comprendre et appréhender les tenants et aboutissants et ainsi être en mesure de juger de ce contrôle, il est indispensable de connaître la structure globale des accords sur Microsoft Cloud, de la documentation, des guides et, enfin et surtout, des certifications et rapports d'audit. Le « Microsoft Assurance Framework » fournit ici la vue générale nécessaire et sert de guide pour le processus d'audit à suivre :

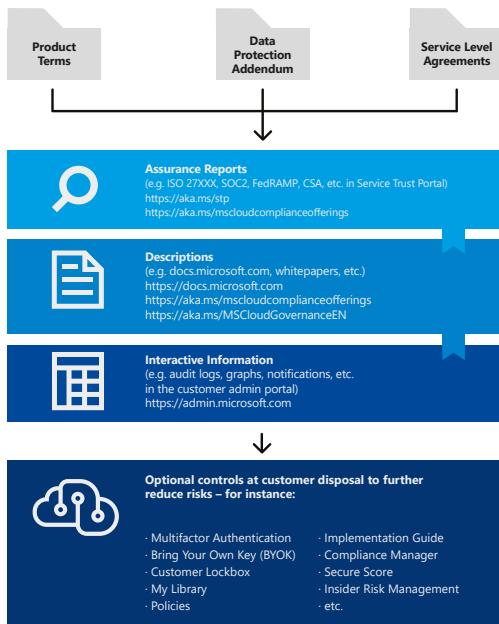


Figure 14 – Microsoft Assurance Framework

- Le premier niveau est constitué par les **conventions à signer avec Microsoft**, qui englobent notamment les **License Terms** stipulant l'accord sur le traitement des données (« **Data Protection Addendum** » pour Microsoft Cloud).
- Les obligations contractuelles de Microsoft qui sont définies dans les conventions figurent dans les documents du deuxième niveau, les « **Assurance Reports** ». Les clients peuvent accéder à tous les **rapports d'audit de tiers, certificats sur le respect des normes, SOA, etc.**
- Le troisième niveau comprend une documentation descriptive plus détaillée où Microsoft donne des **instructions et des descriptions** sur un certain nombre de fonctions, fonctionnalités, processus et autres. Une série de **white papers** sont également proposés sur des thèmes et secteurs spécifiques comme aussi ce document.

- Enfin, les clients ont accès à des documentations et informations actualisées qui portent sur l'utilisation de services cloud de Microsoft et qui sont disponibles via un **portail personnalisé de gestion des services cloud**.

Il existe pour tous ces quatre niveaux d'autres fonctions, services et processus qui peuvent être mis en œuvre selon le client. Leur déploiement se fonde sur l'évaluation globale des risques de la solution et des flux de données et s'inscrit dans un plan de mitigation répondant aux risques identifiés que le client souhaite atténuer. La figure ci-dessus présente dans l'encadré de droite quelques-unes des mesures les plus courantes qui seront explicitées plus loin dans ce document.

Microsoft Assurance Framework joue donc un rôle essentiel dans l'élaboration des contrôles à mettre en œuvre chez le client. Cette interaction est représentée dans le modèle de processus suivant :

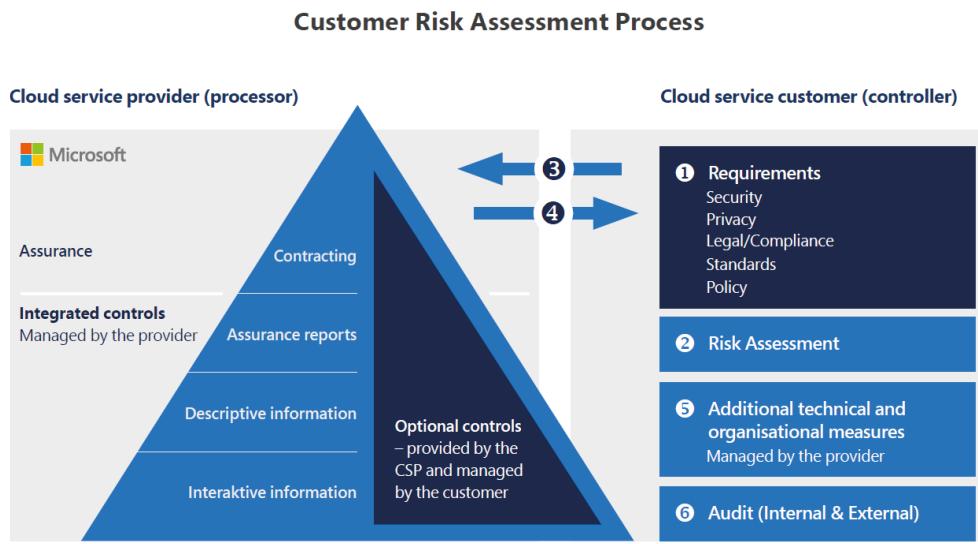


Figure 15 – Interaction entre le Cloud Governance du client et Microsoft Assurance Framework

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- assurance de la conformité ;
- limitation des risques par le biais de stratégies.



4.16 M16 – SHARED RESPONSIBILITY MODEL

La configuration ou l'organisation du contrôle, ou encore l'association et l'interaction des différents instruments de contrôle varient en fonction du degré d'intégration des solutions cloud impliquées. Il en est de même pour la répartition des responsabilités et des coûts engagés lors de la mise en place d'une protection adaptée à certains risques (notamment protection et sécurité des données).

Dans un environnement cloud, et contrairement à une infrastructure informatique sur site, le client et le fournisseur du cloud se partagent la responsabilité de la mise en œuvre et du suivi des contrôles de sécurité relatifs aux applications informatiques. Cette situation évoque un scénario classique d'externalisation. La responsabilité ultime des données traitées incombe néanmoins toujours au client.

Les solutions modernes de cloud sont fondamentalement basées sur un modèle de responsabilité partagée (« shared responsibility model »). Ce modèle répartit la responsabilité entre le client et le fournisseur du cloud en suivant la ligne de démarcation marquée par la virtualisation, de sorte que chaque partie est avant tout responsable de son côté de la ligne.

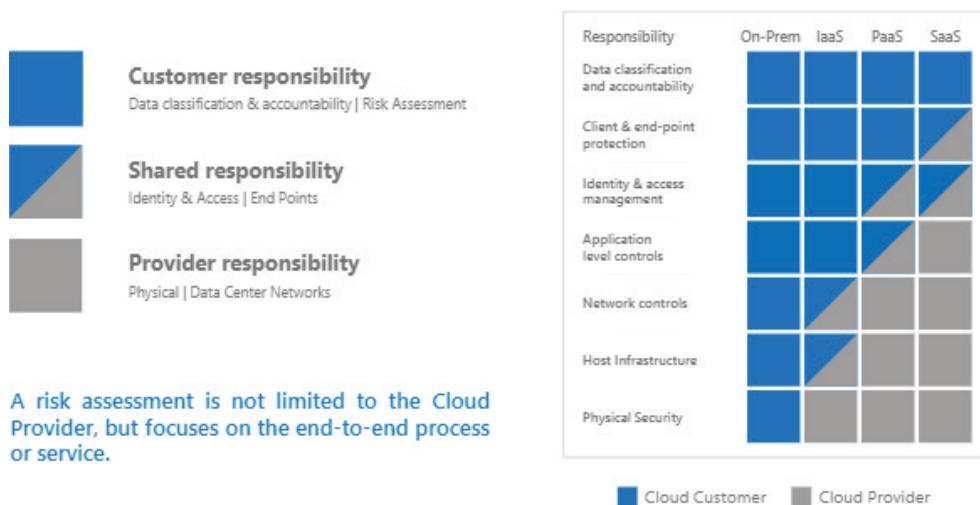


Figure 16 – Shared Responsibility Model

Avec les solutions cloud, la fonction de contrôle connaît une certaine évolution dans la mesure où ses aspects organisationnels / opérationnels gagnent en importance. Dans un environnement cloud, une autorité par exemple dispose de possibilités limitées pour mettre elle-même en place des mesures techniques contre l'accès non autorisé aux données (puisque c'est le fournisseur de cloud qui en fournit la technologie), et doit donc assumer sa responsabilité par d'autres mesures adéquates. Outre une évaluation minutieuse du fournisseur du cloud, elle pourrait, remplir son obligation de contrôle en contrôlant régulièrement l'efficacité de la protection des données fournie par le fournisseur (par exemple en surveillant en permanence les accès et tentatives d'accès dans les journaux d'événements).

Pour garantir la qualité de la partie du «Shared responsibility Model» incomptant au fournisseur du cloud, Microsoft a réalisé pour Azure de nombreux audits de sécurité, sectoriels et nationaux afin d'obtenir la certification par des tiers de la Security Compliance dans l'exploitation de la plateforme du cloud. Les normes de sécurité appliquées sont entre autres ISO et SOC, dont les rapports sont consultables dans Service Trust Portal¹⁸.

Cette solution permet de contrer les risques identifiés en réalisant les objectifs suivants :

- répartition des responsabilités entre le fournisseur et le client ;
- aide à l'évaluation des risques.

¹⁸ <https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide>

APPENDIX : BASES CONTRACTUELLES ET LIENS D'IMPORTANCE

Le tableau suivant énumère les principales sources d'information de ce document qui sont citées dans une optique de transparence.

Document ou sujet	Liens
Page d'accueil sur la Déclaration de confidentialité	https://privacy.microsoft.com/fr-ch/privacystatement
Addendum sur la protection des données pour les produits et services (Data Protection Addendum, DPA), septembre 2021	https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1&year=2021
Conditions universelles des licences dédiées aux services en ligne	https://www.microsoft.com/licensing/terms/product/ForOnlineServices
Microsoft Business and Services Agreement (MBSA)	https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4f5aA
Documentation technique des services Azure	https://docs.microsoft.com/fr-ch/
Microsoft Trust Center (documentations Compliance & Security)	https://www.microsoft.com/fr-ch/trust-center
Documentation SLA de tous les services Azure	https://azure.microsoft.com/fr-fr/support/legal/sla/summary/

Tableau 5 – Compilation de sources importantes d'information





Merci
Danke
Grazie
Engraziel