Ligne directrice sécurité de l'information et vie privée

Cloud computing

(BLD CLOUD)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie de sécurité de l'information et protection de la vie privée au sein de la sécurité sociale. Ce document est destiné aux responsables et aux sous-traitants de l'information, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de sécurité sociale (IPSS).

Ce document fixe les directives de sécurité de l'information et de protection de la vie privée lorsqu'une organisation souhaite avoir recours à des services de « Cloud Computing ». A cet égard, l'accent est mis sur la validation que le fournisseur de services cloud (« cloud service provider » - CSP) offre des garanties suffisantes sur le plan de la protection de l'information, du respect de la vie privée et de la conservation durable des informations et sur le plan des dispositions techniques et juridiques à prendre en compte lors de la réalisation des prestations. Ceci permet à l'organisation de se former une idée de la qualité attendue du service avant de prendre une décision.

Dans le cadre des présentes directives, la notion de Cloud Computing comprend tous les services cloud tels que définis de manière universelle par le NIST[1]. Le Cloud Computing est un modèle permettant d'établir, à la demande, un accès par le réseau à un réservoir partagé de ressources informatiques configurables (par exemple réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement mobilisées et mises à disposition de manière flexible, moyennant un effort ou une interaction minimale avec le fournisseur de services cloud.

Ce document est pertinent dans la mesure où le recours à des services cloud a des conséquences pour l'endroit où les mesures de sécurité de l'information et de protection de la vie privée sont exécutées. Lorsqu'une organisation utilise des services cloud, elle reste responsable de la sécurité de l'information et de la protection de la vie privée.

2. Utilisation de cloud computing en toute sécurité

Toute organisation souscrit les directives suivantes de sécurité de l'information et protection de la vie privée pour l'ensemble des informations et systèmes d'information relevant de la responsabilité de l'organisation.

2.1. Directives générales de sécurité de l'information et protection de la vie privée

1. Avant de faire appel à des services cloud, l'organisation responsable du traitement doit clairement identifier les informations, les traitements ou les services qui seront hébergés dans le cloud. Lors de ce choix, il y a lieu de tenir compte des exigences en matière de sécurité de l'information et protection de la vie privée.
2. Lorsque la classification des données l'exige, l'organisation doit déterminer les conditions minimales ou restrictions à leur transfert.
3. La sécurité de l'information ne porte pas uniquement sur les données à caractère personnel mais sur toutes les données[2]. Dans ce cadre, les données doivent être inventoriées et classifiées en fonction de leur degré de criticité suivant le modèle de classification de données en vigueur au sein de l'organisme[3].
4. Il est nécessaire d'identifier le type de cloud approprié au traitement envisagé en fonction de l'offre actuelle de services cloud.
5. Il est essentiel de définir ses propres exigences minimales en matière de sécurité de l'information et de protection de la vie privée. L'objectif du cloud est de décharger l'organisation de certaines tâches opérationnelles. C'est pourquoi l'organisation doit s'assurer que le niveau d'exigence du fournisseur de services cloud est au moins égal

[1] National Institute of Standards & Technology : http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[2] Conformément à la définition figurant dans la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral

[3] L'organisation doit classer les données destinées au cloud conformément à la politique de classification des données.

à celui de l'organisation. En ce qui concerne les données et le traitement, l'organisation doit s'assurer de la réversibilité[4] et d'un niveau de disponibilité suffisant.

6. Suivant le scope du projet cloud, la criticité des actifs (en termes de disponibilité, d'intégrité et de confidentialité) et au regard du modèle attendu de « Cloud Computing », l'organisation doit conduire une analyse de risques formelle afin d'être en mesure de définir les mesures de sécurité de l'information et de protection de la vie privée appropriées à exiger du fournisseur de services cloud.

2.2. Garanties contractuelles minimales pour le fournisseur de services cloud

Toute organisation qui envisage de traiter des données professionnelles, confidentielles ou sensibles dans un « cloud » doit au minimum veiller aux garanties contractuelles suivantes :

1. Clause relative à la possibilité pour un fournisseur de services « cloud » de sous-traiter une partie de ses activités à d'autres parties (fournisseurs de services cloud).
   a) Le fournisseur de services cloud reste le seul responsable vis-à-vis de l'organisation en ce qui concerne l'exécution de ses obligations, également en cas de sous-traitance de certaines de ses activités.
   b) En cas de sous-traitance de certaines tâches particulières, le contrat stipule que le fournisseur de services cloud est tenu d'en informer préalablement l'organisation. Par ailleurs, le fournisseur de services cloud doit s'engager formellement à reprendre dans le contrat qu'il conclut avec le sous-traitant toutes les obligations qui lui sont imposées.
   c) Le fournisseur de services cloud doit s'assurer du respect de ces engagements par le sous-traitant. Il effectuera à cet effet les contrôles nécessaires. Les conditions d'exécution de ces contrôles sont fixées dans le contrat.

2. Clause relative à l'intégrité, à la continuité et à la qualité de la prestation de services par le fournisseur de services cloud
   a) Le fournisseur de services cloud est tenu de prendre les mesures nécessaires afin de garantir l'intégrité des informations traitées pendant la durée du contrat (par exemple en prévoyant des systèmes de sauvegarde et des tests).
   b) Un accord sur le niveau de service (SLA: Service Level Agreement) devra être formalisé dans un accord en annexe du contrat entre l'organisation et le fournisseur de services cloud. Ce contrat spécifie notamment, y compris pour la période de garantie, la disponibilité du service et le délai maximum de redémarrage en cas d'interruption suite à un incident et tous les autres critères relatifs à la reprise des activités (RTO et RPO)[5].
   c) Les mesures détaillées permettant de garantir la continuité de la prestation de services doivent être précisées dans le SLA à joindre en annexe au contrat.

3. Clause relative à la restitution des données par le fournisseur de services cloud
   a) Le fournisseur de services cloud s'engage à ne pas conserver les données de l'organisation au-delà de la durée convenue avec l'organisation.
   b) En cas de rupture anticipée ou au terme de la prestation, le fournisseur de services cloud s'engage à restituer l'intégralité des données de l'organisation, selon les modalités convenues et dans le délai convenu, dans un format structuré et courant de sorte que l'organisation puisse assurer la continuité de sa prestation de services. Une fois la restitution effectuée et avec l'accord de l'organisation, le fournisseur de services cloud s'engage à détruire de manière sécurisée et professionnelle toutes les copies de données en sa possession (y compris les back-ups et archives) dans un délai raisonnable et à apporter à l'organisation la preuve de la destruction.

[4] Définition : la réversibilité est la possibilité de revenir à une situation ou à une organisation antérieure viable. Ceci permet d'éviter une situation de blocage sans possibilité de retour ou de dépendance à l'égard d'un prestataire unique.

[5] RTO (Recovery Time Objective) : Durée maximale d'interruption admissible – RPO (Recovery Point Objective) : Perte de données maximale admissible.

4. Clause relative à la portabilité des données et à l'interopérabilité des systèmes
   a) Au terme de la prestation, le fournisseur de services cloud s'engage à fournir, selon les modalités prévues dans le contrat, l'aide nécessaire à la migration des traitements opérés dans son « cloud » vers une autre solution.

5. Clause relative à l'audit
   a) Le fournisseur de services cloud s'engage à permettre la réalisation d'audits à l'initiative de l'organisation, à collaborer étroitement et à traiter les déficiences observées dans les meilleurs délais. Ces audits peuvent être réalisés par une organisation d'audit agréée.
   b) Le fournisseur de services cloud peut également faire réaliser des audits et une certification par des organisations d'audit agréées et mettre ces rapports d'audit et de certification intégralement et gratuitement à la disposition de l'organisation (p.ex. ISAE 3402, ISO27001, CSA). L'organisation peut ainsi vérifier si le scope et les résultats répondent à ses exigences.
   c) En cas de sous-traitance complète ou partielle, le fournisseur de services cloud impose à ses sous-traitants des clauses qui garantissent le droit de l'organisation d'effectuer ces audits moyennant le respect des règles précitées.

   Les audits permettent de vérifier le respect du contrat et des règles de sécurité de l'information et de protection de la vie privée et de vérifier la conformité avec les bonnes pratiques recommandées par des organismes internationaux (p.ex. NIST, ENISA, ISO, CSA, ISACA, etc.). L'audit doit aussi permettre à l'organisation de s'assurer que les mesures de sécurité de l'information et de protection de la vie privée ne puissent pas être contournées sans que l'organisation n'en soit avisée.

6. Clause relative aux obligations du fournisseur de services cloud en matière de confidentialité des données
   a) Le fournisseur de services cloud doit s'engager, en ce qui le concerne et en ce qui concerne ses sous-traitants et éventuels repreneurs, à ne pas utiliser ou divulguer les données pour son propre compte ou celui d'un tiers.
   b) Le fournisseur de services cloud doit s'engager à protéger et à tenir à la disposition de l'organisation toutes les traces d'accès (permettant de déterminer qui a fait quoi et quand) aux données, aux applications et aux outils système, et ce pendant une durée déterminée contractuellement.
   c) Il doit immédiatement informer l'organisation de toute anomalie qu'il détectera dans ces traces d'accès telle que des tentatives d'accès de personnes non-autorisées. Ceci doit permettre à l'organisation d'informer la Commission de la protection de la vie privée dans les 72 heures[6] de toute violation de données.
   d) Le fournisseur de services cloud doit immédiatement informer l'organisation de toute enquête ou demande d'enquête provenant d'une autorité administrative ou judiciaire belge ou étrangère.

7. Clause relative à la souveraineté
   a) Le fournisseur de services cloud doit fournir à l'organisation l'assurance que ni lui, ni ses éventuels sous-traitants ne sont soumis à des actes d'instruction d'autorités étrangères à la Belgique ou à l'Union européenne.

8. Clause relative aux obligations du fournisseur de services cloud en matière de sécurité de l'information
   a) Le fournisseur de services cloud est tenu de respecter les bonnes pratiques en matière de sécurité de l'information, telles que celles mentionnées dans les normes de sécurité minimales du secteur de la sécurité sociale ou dans d'autres standards comme les normes de la série ISO 27000 cloud security[7], Cloud Security Alliance STAR[8].
   b) Le fournisseur de services cloud doit fournir à l'organisation la politique de sécurité de l'information en ce qui concerne les services qu'il fournit et il doit l'informer des évolutions de cette politique.
   c) Le fournisseur de services cloud doit communiquer annuellement à l'organisation l'identité et les coordonnées de son responsable de la sécurité de l'information et de son délégué à la protection des données.

[6] https://www.privacycommission.be/fr/declaration

[7] http://www.iso.org/iso/catalogue_detail?csnumber=43757 Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[8] https://cloudsecurityalliance.org/star/

d) Le fournisseur de services cloud doit fournir annuellement à l'organisation une évaluation formelle de la situation des exigences en matière de sécurité de l'information et de protection de la vie privée (via le SLA conclu entre les parties).

2.3. Directives de sécurité de l'information du fournisseur de services cloud

Toute organisation qui envisage de traiter des données professionnelles, confidentielles ou sensibles dans un « cloud » doit au minimum veiller aux garanties contractuelles suivantes :

Les bonnes pratiques mentionnées ci-après constituent une liste minimale, non-exhaustive des mesures de sécurité de l'information que le fournisseur de services cloud est tenu de respecter. L'évaluation des risques exécutée par l'organisation peut donner lieu à des mesures de sécurité de l'information complémentaires. En fonction du modèle de cloud, il y a lieu de définir de manière précise la responsabilité pour la gestion des mesures de sécurité de l'information.

1. Protection des données confidentielles :

Le fournisseur de services cloud garantit que :

- la localisation des données confidentielles est connue et répond aux exigences de l'organisation (centre de calcul, serveurs, etc…) ;
- les systèmes de sauvegarde et de restauration et le plan de continuité y afférent sont mis en œuvre et testés périodiquement ;
- il dispose d'un code de bonne conduite applicable à son personnel et à ses sous-traitants et appliqué par eux. Il n'exerce pas d'activités susceptibles d'entraîner un risque de conflit d'intérêts ;
- il sensibilise régulièrement son personnel à l'importance de la sécurité de l'information et de la protection de la vie privée ;
- il dispose d'outils permettant de détecter les violations de droits spécifiques ou des activités malveillantes ;
- il dispose d'une procédure pour les incidents incluant la détection, l'alerte, le traitement jusqu'à la résolution, l'identification des causes et la communication à l'organisation.

2. Sécurité des centres de calcul

Le fournisseur de services cloud garantit que :

- il dispose de systèmes sécurisés de contrôle d'accès physique, de détection d'intrusion, d'incendie, d'inondation et de vidéosurveillance ;
- les accès aux centres de calcul sont autorisés aux seules personnes habilitées, ils sont tracés et revus régulièrement ;
- les clauses de confidentialité prévues dans le contrat sont également applicables à tous les sous-traitants (en particulier en ce qui concerne la maintenance de systèmes contenant des données confidentielles) ;
- tout support de stockage contenant des données confidentielles et destiné à être réaffecté, supprimé ou recyclé fait l'objet d'une procédure préalable efficace.

3. La sécurité d'accès logique

Le fournisseur de services cloud garantit que :

- il applique les modalités d'accès aux données selon les instructions communiquées par l'organisation (création, consultation, modification et suppression) ;
- les accès des utilisateurs et administrateurs aux systèmes contenant des données confidentielles s'appuient sur des mécanismes garantissant la confidentialité et la traçabilité (p.ex. audit des accès aux données, problématique des comptes génériques) ;
- il applique une politique d'authentification conforme à celle de l'organisation.

4. Sécurité des systèmes

Le fournisseur de services cloud garantit que :

- les données sauvegardées, quel que soit le support, sont chiffrées de manière adéquate (algorithme, longueur de clef,…) en fonction du modèle « cloud » choisi et en concordance avec ce que l'organisation juge utile ;
- il gère les vulnérabilités des systèmes et organise au moins annuellement des tests de sécurité en veillant à corriger immédiatement les vulnérabilités critiques identifiées ;
- les serveurs sur lesquels les données confidentielles sont gérées sont configurés avec un niveau de sécurité très strict ;
- les patchs de sécurité sont gérés de façon centralisée, testés préalablement et installés dans des délais raisonnables et en fonction de leur criticité ;
- les logiciels de sécurité (tels anti-virus, anti-spam, anti-malware, anti-ransomware) sont installés sur les serveurs et les postes de travail et sont régulièrement actualisés et supervisés ;
- l'usage de clés USB et autres supports de stockage mobiles est géré et contrôlé ;
- les procédures et pratiques de gestion en matière de gestion des risques, gestion des incidents et gestion du changement sont appliquées et correctement documentées ;

5. Sécurité du réseau

Le fournisseur de services cloud garantit que :

- les accès au réseau sont limités, sécurisés et filtrés ;
- la gestion des systèmes est opérée depuis un réseau d'administration sécurisé, dédié et isolé moyennant une authentification forte ;
- les modifications au niveau des équipements réseau sont préalablement approuvés, suivis, et documentés ;
- dans le cas d'un service « Cloud computing » partagé :
  - l'accès au réseau est autorisé uniquement à des terminaux de confiance ;
  - le réseau sur lequel sont connectés les systèmes hébergeant les données confidentielles est isolé du réseau des autres organisations.

2.4. Directives de protection de la vie privée du fournisseur de services cloud

Avant d'avoir recours au « cloud computing », toute organisation doit évaluer au préalable les risques en matière de sécurité de l'information et de protection de la vie privée dans la solution cloud. En fonction de la sensibilité des informations telle que définie par l'organisation et l'évaluation des risques, l'organisation pourra avoir recours ou non aux services d'un fournisseur de services cloud.

Les règles suivantes sont d'application en cas d'utilisation de services cloud pour le traitement de données à caractère personnel :

- en fonction de ses activités, toute organisation doit non seulement respecter la législation belge et européenne, mais également la législation spécifique propre à son secteur ;
- L'organisation reste responsable de la protection des données à caractère personnel (règlement européen relatif à la protection de la vie privée[9]) lors du traitement de ce type d'informations au sein d'un service cloud en ce qui concerne les informations dont elle est le propriétaire ;
- Il y a lieu de réaliser toujours une évaluation des risques[10] , qui doit être validée, communiquée et entretenue afin de déterminer le niveau exact de sécurité de l'information et de protection de la vie privée. Les exigences définies doivent être garanties par le fournisseur de services cloud ;

[9] https://www.privacycommission.be/fr/la-loi-vie-privee-et-ses-arretes-d-execution et http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[10] Des modèles d'évaluation des risques sont disponibles auprès de ENISA https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment , ISACA http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Controls-and-Assurance-in-the-Cloud-Using-COBIT-5.aspx , NIST https://www.nist.gov/news-events/news/2012/01/nist-issues-cloud-computing-guidelines-managing-security-and-privacy et Smals https://www.smalsresearch.be/tools/cloud-security-model-fr/

- Sauf dérogation autorisée, en cas d'externalisation de données à caractère personnel ou de données sensibles, le choix du fournisseur de services cloud par l'organisation se limite à des services cloud de type « communautaire » ou « privé » ;
- Sauf dérogation autorisée, toute externalisation de données à caractère personnel ou de données sensibles requiert un chiffrement des données durant le transfert (« en transit ») et pour le stockage (« in rest »). La gestion des moyens de chiffrement doit toujours rester sous le contrôle de l'organisation et ne peut pas être sous-traitée.

La gestion de données spéciales[11] et médicales est à éviter dans le cloud dans la mesure où le fournisseur de services cloud peut avoir accès à ces informations, étant donné que le traitement de ce type de données et l'accès à ces données doivent rester strictement limités. L'organisation doit opérer un choix bien réfléchi en ce qui concerne le traitement de données spéciales et médicales dans le cloud et elle doit à cet égard toujours demander au préalable un avis juridique et technique.

Une organisation doit toujours faire un choix bien réfléchi en ce qui concerne le traitement de données à caractère personnel, professionnelles, confidentielles ou sensibles dans le cloud. L'organisation reste le responsable final de l'information et du respect de la sécurité de l'information et de la protection de la vie privée.

[11] Par données à caractère personnel spéciales il y a lieu d'entendre notamment les données relatives aux convictions religieuses et philosophiques, à la race, aux convictions politiques, à la santé et à l'orientation sexuelle.

Annexe A : Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description de la modification	Date approbation	Date entrée en vigueur
2014		V2014	Première version	19/03/2014	01/04/2014
2017		V2017	Intégration UE GDPR	07/03/2017	07/03/2017

Erreurs et omissions

Si à la lecture du présent document, vous constatez des erreurs ou des problèmes, vous êtes invité, en tant que lecteur, à transmettre une brève description de l'erreur ou du problème et de sa localisation dans le document ainsi que vos données de contact au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'organisation.

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents de politique, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions sécurité de l'information et protection de la vie privée".

Annexe B : Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document :

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 p.
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 p.
- EU, WG29, "Avis 05/2012 relatif au cloud computing", 1 juillet 2012, 31 p.
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 p.
- ISACA, "Security considerations for cloud computing", septembre 2012, 80 p.
- CNIL[12], « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud Computing », juin 2012, 21 p.
- Smals Research, « Modèle d'évaluation de sécurité cloud », décembre 2014

Ci-dessous figurent les références aux sites web qui ont servi de source d'inspiration pour le présent document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- https://www.privacycommission.be/fr/cloud-computing
- http://www.isaca.org/cloud
- http://www.ccb.belgium.be/nl/work
- https://www.cybersimpel.be/nl
- https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
- https://www.sans.org/reading-room/whitepapers/cloud
- https://www.smalsresearch.be/tools/cloud-security-model-fr/

[12] Commission Nationale de l'Informatique et des libertés, http://www.cnil.fr

Annexe C : Cloud computing

Introduction

En cas de cloud computing, le matériel, les logiciels et l'information sont mis à la disposition via l'Internet. Souvent le collaborateur ne sait plus sur quel ordinateur se situent (physiquement) les services auxquels il fait appel. Dans le cadre du cloud computing, il est souvent fait appel à du matériel permettant une mise à l'échelle flexible en fonction des besoins de l'organisation et des collaborateurs. Par ailleurs, l'organisation n'est souvent plus le propriétaire du matériel et/ou des logiciels. Il s'agit d'infrastructure et de services « virtuels ». Le cloud computing permet également de virtualiser des serveurs, des ordinateurs et également des applications, avec tous les avantages et les inconvénients que cela peut entraîner.

En cas de doute en ce qui concerne le recours au cloud computing et/ou le traitement de données (à caractère personnel) à l'étranger, il est judicieux de toujours consulter le service juridique. Avant d'utiliser des services cloud, il y a lieu de réaliser une évaluation des risques formelle et un business case avec tous les arguments.

Lorsque l'organisation fait appel à des services cloud, sa responsabilité n'est aucunement transférée au fournisseur de services cloud. L'organisation est et reste responsable de la manière dont le fournisseur de services cloud agit en termes de protection de l'information. Dans le cas de données à caractère personnel, ceci est réglé dans la réglementation européenne EU GDPR.

Quelle est la différence entre l'externalisation de l'IT et le cloud computing ?

Il n'y a aucune différence en ce qui concerne les exigences de sécurité. L'externalisation de l'IT est une méthode bien connue où une tierce partie prend en charge une ou plusieurs tâches de l'entreprise pour lesquelles l'entreprise manque de ressources (temps, expertise). Cette externalisation peut aller jusqu'au stockage des données et aux systèmes de traitement. Le cloud computing est en fait une évolution de l'externalisation IT. Dans ce cadre, le présent document peut également être pris en compte en cas d'externalisation IT.

Caractéristiques du cloud computing

Le cloud computing est parfois assimilé aux centres de shared service, mail il existe des différences fondamentales. Le cloud computing est uniquement applicable lorsque les caractéristiques suivantes sont présentes :

1. Libre-service (on-demand self-service) : l'utilisateur de services cloud peut, au besoin, modifier le temps serveur et le stockage sans intervention du fournisseur de services cloud.
2. Accès à large bande : un accès est possible via des liaisons à large bande avec divers types de plateformes clientes (fat client, thin client, appareils mobiles, ...).
3. Ressources partagées (resource pooling) : les ressources physiques et logiques du fournisseur de services cloud sont utilisées par tous les clients et affectées de manière dynamique au besoin. Les clients utilisent la même application mais les données sont enregistrées de manière séparée par client (multi tenancy model[13]). Le client ne sait pas où se situent les ressources. Exemples de ressources : puissance de calcul, enregistrement, mémoire et largeur de bande réseau.
4. Elasticité : les ressources peuvent être affectées à court terme (automatiquement) et libérées sur demande. Les ressources semblent illimitées à tout instant pour le client.
5. Service mesurable : les systèmes cloud contrôlent et optimisent les ressources au moyen de mesures applicables (enregistrement, mémoire, puissance de calcul, etc.). L'utilisation des ressources fait l'objet d'un monitoring transparent, de contrôles et de rapports au client et au fournisseur du service utilisé.

Modèles de cloud computing

Les offres actuelles de « Cloud Computing » peuvent être classées selon trois modèles de service et quatre modèles de déploiement de base.

[13] https://en.wikipedia.org/wiki/Multitenancy

- Les modèles de service de base
  - SaaS: « Software as a Service » ou la mise à disposition d'applications aux utilisateurs finaux via le cloud. Certaines organisations ont déjà recours à des applications via le modèle SaaS, et ce dans le cadre de cloud publics et de clouds privés. Ceci permet d'offrir des applications web développées avec des technologies modernes. L'utilisateur final n'a aucune idée de l'endroit où l'application se situe, de la plateforme sur laquelle elle fonctionne ni de l'endroit où se situent les informations.
  - PaaS: « Platform as a Service », lorsque l'organisation souhaite installer des logiciels dans le cloud, elle peut faire appel à PaaS. PaaS permet à une organisation de régler elle-même, dans certaines limites, le logiciel et la configuration. Le client final d'une solution PaaS est souvent la propre organisation ICT. Les propres applications sont souvent mises à la disposition de l'utilisateur final dans l'environnement PaaS.
  - IaaS: « Infrastructure as a Service », l'organisation peut se limiter à l'utilisation d'infrastructure (virtualisée). On y retrouve des serveurs, des composants réseau, de la capacité de stockage et d'autres types d'infrastructure. La section ICT d'une organisation peut choisir en toute liberté le matériel auquel a elle recours de manière virtuelle. Outre le matériel IaaS, la section ICT peut avoir recours à IaaS pour la mise à disposition de services plateforme et de logiciels propres. La gestion s'opère à distance à partir de n'importe quel ordinateur.
- Les modèles d'implémentation de base :
  - « Public » : L'infrastructure est accessible à un large public et appartient à un fournisseur de services «Cloud», dans ce cadre un service est partagé avec de nombreux clients ;
  - « Privé » : l'infrastructure cloud fonctionne pour une seule organisation, elle peut être gérée par l'organisation elle-même (cloud privé interne) ou par un tiers (cloud privé externe). Dans un cloud privé, l'organisation maintient entièrement le contrôle de l'information, de la sécurité et de la qualité du service. Souvent la responsabilité pour la maintenance et la gestion incombe à l'organisation, mais dans la pratique ce sera souvent un fournisseur qui s'en charge. Le cloud privé peut fonctionner dans un centre de calcul communal, mais également auprès d'un fournisseur. Dans ce cas, l'infrastructure virtualisée n'est pas partagée avec d'autres clients.
  - « Communautaire » : Il s'agit d'une infrastructure cloud utilisée par un groupe spécifique de clients qui ont des intérêts communs ou qui doivent répondre à des contraintes (légales, …) identiques. P.ex. en ce qui concerne les tâches, les missions, les exigences de sécurité, la politique et le respect des exigences. Le cloud communautaire peut être la propriété et être géré par un des participants, un tiers ou une combinaison des deux. P.ex. un cloud des autorités publiques ou un cloud d'une organisation. A l'instar du cloud privé, cette infrastructure peut être gérée par les organisations elles-mêmes ou par un tiers.
  - « Hybride » : cette infrastructure se compose d'au moins deux types de clouds (privé, communautaire ou public), qui coexistent mais qui sont liés par un standard ou une technologie propre, permettant la portabilité des données ou des applications. En d'autres termes, il est fait usage de services cloud en provenance d'un tiers tout en ayant également recours à un cloud propre.

Lorsqu'un cloud privé ne se situe pas dans le centre de calcul de l'organisation mais sur une infrastructure distincte auprès d'un fournisseur, il s'agit techniquement d'un service issu d'un cloud externe sur des environnements virtualisés spécifiques. Les exigences reprises dans le présent document sont alors d'application.

Préparation de la migration d'une infrastructure interne vers une infrastructure de cloud computing

- Préparer une analyse de rentabilité et évaluer les coûts et les bénéfices d'une migration vers un fournisseur de « Cloud Computing ».
- Identifier et classifier les ressources (informations, applications, processus) dans le champ d'application du « Cloud Computing ».
- Impliquer les personnes clés de l'organisation (juridique, sécurité, finances, etc.) dans le processus de décision de la migration vers un service de « Cloud Computing » avant de prendre une décision.
- Examiner en profondeur le design et les exigences de la solution proposée par le candidat pour le transfert vers le « Cloud Computing » et demander aussi au fournisseur de service « Cloud Computing » de prévoir une période de test afin d'identifier les problèmes potentiels.

Contrats et cloud

Dans les contrats avec le fournisseur de services cloud, il y a lieu de prêter attention aux aspects suivants :

- Mesures de sécurité spécifiques suite à l'évaluation des risques
- L'obligation de signaler immédiatement tout incident de sécurité et d'atteinte à la vie privée à l'organisation

- Durée du contrat
- Description du package de base et des services (optionnels) complémentaires et les tarifs applicables
- Escrow (ou escrow cloud)
- Licences de logiciels (qui en est le propriétaire et peuvent-ils être utilisés dans le cloud ?)
- Conversion de données
- Transfert de données à partir de l'environnement cloud et vers celui-ci
- Destruction des données au terme du contrat
- Continuité du système
- Transfert vers un autre fournisseur
- Sauvegarde et solution de repli
- Localisation des données et logiciels
- Règles additionnelles en ce qui concerne les données à caractère personnel (contrat sous-traitant)
- Obligation de secret
- Chiffrement des données
- Sous-traitance et transfert de droits et obligations (ou interdiction de sous-traitance)
- Droit de suspension
- Respect de la législation et de la réglementation
- Possibilité de consultation des données de logging
- Droit de (faire) exécuter des audits
- Droit applicable
- Règles d'exit : quid lorsque l'organisation souhaite quitter le fournisseur de services cloud ou souhaite migrer les données/services vers un autre fournisseur de services cloud ?
- Gestion des accords

Annexe D: Cloud computing : avantages, inconvénients et risques

Avantages du cloud computing

- Les services cloud sont accessibles via internet et permettent de travailler de manière flexible (indépendamment de l'endroit ou du moment).
- Les services cloud sont en mesure de répondre de manière flexible à des demandes changeantes. L'organisation peut s'agrandir ou rétrécir en fonction des besoins à très court terme.
- Mécanismes de calcul flexibles : payer par utilisateur, payer par machine virtuelle ou service.
- Une plus grande disponibilité semble logique, bien que ceci dépende du niveau de service du fournisseur de services cloud.
- Le fournisseur de services cloud dispose généralement de suffisamment de personnel spécialisé et l'organisation aura donc besoin de moins d'experts. L'utilisation du cloud computing permet non seulement de conserver des informations à distance, mais également de laisser la complexité des systèmes à distance.

Inconvénients et risques du cloud computing

La transition de l'IT interne vers le cloud computing requiert une approche claire et transparente au niveau de la gestion de la sécurité et des risques contractuels et juridiques. L'organisation qui souhaite faire appel à un fournisseur de services cloud est tenue de réaliser une évaluation des risques afin de vérifier si le fournisseur de services cloud en question applique dans la pratique les mesures de sécurité de l'information et de protection de la vie privée organisationnelles, techniques et procédurales adéquates. Dans le cadre de cette évaluation des risques, l'organisation doit en particulier évaluer les risques en termes de protection des données à caractère personnel (vie privée) à la lumière des nouvelles normes européennes en matière de protection de la vie privée (EU GDPR)[14]. Les risques majeurs identifiés à cet égard sont les suivants :

- une gouvernance limitée au niveau du traitement ;

[14] EU GDPR http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR

- les risques liés aux sous-traitants du fournisseur de services cloud, par exemple une erreur dans la chaîne de sous-traitance lorsque le fournisseur fait lui-même appel à un tiers pour la fourniture d'un service ;
- la dépendance technique vis-à-vis du fournisseur de services cloud, par exemple le risque de perte d'information lors de la migration vers un autre fournisseur de services cloud ou vers une solution interne ;
- une fuite de données, en d'autres termes le risque que l'information hébergée sur un système (virtuel) puisse être modifiée ou soit accessible à des tiers non autorisés suite à une défaillance ou une mauvaise gestion du fournisseur de services cloud ;
- l'exécution d'actions juridiques sur la base d'un droit étranger sans concertation avec les instances nationales;
- dans le cas de clouds externes, il n'est pas possible de vérifier dans quelle mesure le fournisseur de services cloud peut prendre connaissance des services et des informations
- le non-respect des règles édictées par l'organisation en ce qui concerne la conservation et la destruction des informations, notamment en cas de destruction inefficace ou non sécurisée des données ou d'une durée de conservation trop longue ;
- problèmes en matière de gestion de la sécurité et des droits d'accès inhérents à l'accès via internet ;
- l'indisponibilité du service fourni par le fournisseur de services cloud ;
- la cessation du service par le fournisseur de services cloud (p.ex. suite à une décision judiciaire ou à la reprise du fournisseur de services cloud par un tiers ou suite à une faillite) ;
- la non-conformité avec la réglementation, en particulier en ce qui concerne les transferts internationaux.

Une liste plus détaillée des risques et des modèles de risques en matière de cloud computing[15] pourra être prise en considération lors de l'exécution de l'évaluation des risques dès qu'une organisation envisage de passer au cloud computing.

Annexe E : Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Sécurité des ressources humaines	
Gestion des actifs	
Protection de l'accès	
Cryptographie	**Oui**
Sécurité physique et protection de l'environnement	
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	**Oui**
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	

***** FIN DU DOCUMENT *****

[15] Des modèles d'évaluation des risques sont disponibles auprès de ENISA https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment , ISACA http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Controls-and-Assurance-in-the-Cloud-Using-COBIT-5.aspx , NIST https://www.nist.gov/news-events/news/2012/01/nist-issues-cloud-computing-guidelines-managing-security-and-privacy et Smals https://www.smalsresearch.be/tools/cloud-security-model-fr/