Federal Information Security Policy Guideline

Guide pour un usage sécurisé du cloud

21/11/2019

FISPDOC07 V1.2

Remarque importante : ce document est un guide qui résulte d'une collaboration entre des experts en sécurité de l'information des différents services fédéraux (SPF, OIP, IPSS). Les mesures proposées sont considérées comme des avis raisonnablement applicables de manière commune à tous les services fédéraux. Elles se basent sur des normes internationales, des bonnes pratiques dans le domaine de la sécurité de l'information ainsi que sur les expériences des participants au groupe de travail FISP.

Si des mesures plus strictes sont nécessaires à un service fédéral pour des raisons réglementaires ou pour d'autres raisons formelles et contraignantes, il va de soi que ces mesures prévalent sur celles décrites dans le présent guide.

FISP

Groupe de travail

.be

TABLE DES MATIÈRES

I. Contenu du document 3
Orientation du document 3
Objectif de sécurité du document 3
Champ d'application 3
Clause de non-responsabilité 3
Responsabilités 3
Propriétaire 3
II. Introduction 4
III. Cloud Business Plan 5
IV. Définition du cloud 7
V. Attention au Shadow Cloud ! 10
VI. Responsabilité de l'organisme en matière de sécurité dans les environnements de cloud computing 11
VII. Paysage sécuritaire du cloud 13
VIII. Sécurité minimale et considérations en matière de vie privée 15
Actions recommandées afin de répondre à ces considérations 15
Détails sur la responsabilité d'un objectif de sécurité 16
Valeur, caractère critique et sensibilité des informations 16
Souveraineté des données 17
Respect de la vie privée 18
Gouvernance 19
Conditions d'utilisation : 19
Conformité : 20
Confidentialité 22
Authentification et contrôle d'accès 22
Architecture multi-entité 25
Environnements d'exploitation standard 26
Gestion des correctifs et des vulnérabilités 26
Cryptage 28
Menace interne chez le fournisseur de service cloud 30
Rémanence des données 30
Sécurité physique 31
Intégrité 32
Disponibilité 34
Accord de niveau de service 34
Attaques par déni de service 34
Disponibilité et performance réseau 35
Continuité de l'activité et reprise après catastrophe 35
Intervention et gestion en cas d'incidents 37
IX. Gestion du document 39
Historique 39
Approbations 39
Sources 39
X. Lien avec d'autres politiques 40
Dépendance de documents internes 40
Positionnement de la politique par rapport à la norme ISO 27001 40
Positionnement de la politique par rapport à la norme ISO 27002 40

Contenu du document

Orientation du document

Ce document fait partie intégrante de la méthodologie relative à la sécurité de l'information au sein de l'administration fédérale (projet FISP).

Objectif de sécurité du document

Ce document décrit les exigences en matière de sécurité du cloud

Champ d'application

Ce document permet aux organismes gouvernementaux d'identifier, d'analyser et d'évaluer de manière systématique les risques liés à la sécurité de l'information en matière de services cloud et met à leur disposition des mécanismes de contrôle afin d'assurer une gestion efficace de ces risques.

Clause de non-responsabilité

Les informations contenues dans ce document ne peuvent pas être utilisées individuellement comme documentation de référence. Ce document ne peut pas servir de substitut à la législation, mais vise à guider le lecteur dans la prise de mesures de sécurité appropriées.

Responsabilités

Ce document est destiné au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de l'administration fédérale ainsi qu'aux autres intervenants dans des domaines connexes.

Propriétaire

Le groupe de travail FISP est propriétaire du présent document.

Introduction

Le cloud computing offre de nombreux avantages potentiels au public et organismes gouvernementaux, notamment de l'adaptabilité, de la modularité, des performances élevées, de la rentabilité, de la souplesse et de la flexibilité.

La gestion de la sécurité et de la résilience dans les environnements informatiques traditionnels représente généralement un défi majeur pour les organismes gouvernementaux. Le cloud computing présente toutefois quelques défis supplémentaires. Par exemple :

- L'absence de définitions claires relatives au cloud, à ses services connexes et à ses différentes architectures
- L'absence de certification et de normes en matière de sécurité du cloud et un manque de compatibilité avec les normes de sécurité adoptées actuellement
- L'absence d'un langage et d'une méthodologie d'approvisionnement clairs dans le choix du service cloud le plus approprié
- L'absence de compréhension claire des implications liées au cloud computing en ce qui concerne le transfert transfrontalier des données
- Veiller au respect des lois et réglementations nationales

Ce guide a pour but de fournir aux organismes gouvernementaux une vue d'ensemble en matière de cloud computing et des défis qu'il pose sur le plan de la sécurité. En raison de l'architecture unique et de la nature transfrontalière des services cloud, les exigences de vie privée et de sécurité pour les informations personnelles et de sécurité concernant les données, transactions et communications gouvernementales doivent faire l'objet d'une approche différente. Le document aborde les menaces, risques technologiques et moyens de protection pour les environnements cloud et entend fournir aux responsables des services informatiques toutes les informations nécessaires afin de leur permettre de prendre des décisions en toute connaissance de cause.[1]

Ce document permet aux organismes gouvernementaux d'identifier, d'analyser et d'évaluer de manière systématique les risques liés à la sécurité de l'information en matière de services cloud et met à leur disposition des mécanismes de contrôle afin d'assurer une gestion efficace de ces risques. Même s'il présente les principales préoccupations liées au cloud computing, les risques identifiés dans ce document ne doivent pas être considérés comme exhaustifs et les organismes sont encouragés à identifier et à évaluer tout autre risque qui pourrait être propre à leur contexte d'activité ou aux services cloud qu'ils prévoient d'employer.

[1] Politique du cloud au Qatar

Cloud Business Plan

En raison du caractère spécifique de chaque organisme, il n'existe pas de modèle opérationnel unique pour l'utilisation des services cloud. Les organismes publics sont encouragés à se considérer comme décrits dans ce guide afin de les aider à identifier leur modèle opérationnel en matière de services cloud. Des considérations au cas par cas concernant le cloud seront nécessaires pour chaque département des administrations publiques et ce, par sa haute direction en collaboration avec le CISO et le DPO. Afin de sensibiliser aux exigences de sécurité lors de l'utilisation des services cloud, leurs décisions devraient également reposer sur une analyse comparative de risques des infrastructures gérées sur site et systèmes cloud. Seule l'adoption d'un niveau d'exigence identique par les deux parties garantira la crédibilité des décisions car elles seront fondées sur les mêmes éléments de base.

La définition et l'application d'un **Cloud Business Plan** sont recommandées. Les organismes doivent disposer d'un plan sur la manière dont ils prévoient d'utiliser les services cloud. Ce chapitre met également en évidence certains des changements à apporter au modèle opérationnel des TIC que les organismes devront prendre en considération. Cette recommandation vise à encourager les organismes à privilégier une approche stratégique pour l'adoption des services cloud.

Les plans cloud devraient tout d'abord décrire la manière dont les organismes gouvernementaux prévoient d'utiliser les services cloud afin de soutenir les améliorations opérationnelles majeures dans le but d'améliorer l'expérience de l'utilisateur, d'accroître leur niveau d'efficacité et d'efficience, de rationaliser leurs opérations ou de créer de nouveaux modèles de distribution. [2] Le premier conseil à donner aux organismes gouvernementaux lorsqu'ils élaborent leurs plans cloud est de tenir compte de ce qui suit :

- **Stratégie opérationnelle** : les services cloud publics devraient correspondre aux stratégies actuelles de l'organisme. La manière dont ces services seront employés afin de soutenir les principales améliorations opérationnelles doit être clairement définie. Une approche sectorielle doit être envisagée.
- **L'appétence au risque** : le niveau d'appétence au risque de l'organisme doit être clairement établi en matière d'utilisation de services cloud publics dans le contexte de la vie privée, des compétences juridiques, de la sécurité et des considérations légales.
- **Gouvernance et identité** : la manière dont la politique en matière de gouvernance des données, y compris en ce qui concerne l'identité et la gestion de l'accès, sera appliquée à travers plusieurs services cloud publics doit être clairement définie.
- **Considérations en matière de structure organisationnelle et technologique** : il convient d'établir clairement la manière dont l'opportunité offerte par les services cloud influencera la structure organisationnelle de votre organisme et sa stratégie technologique ainsi que les changements technologiques et de processus à mettre en œuvre afin d'utiliser les services cloud en toute sécurité.
- **Modèle opérationnel TIC** : le modèle opérationnel TIC cible pour votre fonction TIC et le plan de transition vers ce modèle devraient être définis.

[2] Cliquez sur ce lien pour obtenir un exemple de développement et de mise en œuvre d'un Plan cloud opérationnel : https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/guidance-and-resources/using-cloud-services/develop-and-implement-a-cloud-plan/implementing-the-cloud-plan/index.html (en raison du transfert du contenu « ict.govt.nz » vers « digital.govt.nz », le lien risque de ne plus fonctionner prochainement)

- **Maturité organisationnelle** : les fonctions de soutien au sein de votre organisme ayant besoin d'élever leur niveau de maturité afin de soutenir l'utilisation des services cloud publics devraient être définies (par ex. les fonctions commerciales, juridiques, architecturales, sécuritaires).
- **Les processus opérationnels** : il convient de définir la manière dont l'organisme gouvernemental adopte une approche systématique en matière d'utilisation de services cloud publics, y compris la gestion des risques liés aux services employés sans l'implication d'une équipe TIC (shadow cloud).
- **Feuille de route** : les services cloud publics ultra prioritaires pour l'organisme gouvernemental et le calendrier pour leur mise en œuvre devraient être définis.

Définition du cloud

Pour la définition du cloud computing, le gouvernement belge a décidé de suivre celle du National Institute of Science and Technology (NIST) :

> « Un modèle permettant un accès réseau omniprésent, pratique et à la demande à un bassin partagé de ressources informatiques configurables (par ex. réseaux, serveurs, stockage, applications et services) qui peut rapidement être activé et désactivé en réduisant au minimum les efforts de gestion ou les contacts avec le fournisseur
> de service. »

Le cloud computing est composé de cinq caractéristiques essentielles, de trois modèles de service et de quatre modèles de mise en œuvre Ce chapitre dresse un bref aperçu des principales caractéristiques du cloud computing et des modèles de service cloud et de mise en œuvre. Il est recommandé que les organismes se familiarisent avec les définitions du NIST afin de s'assurer de leur capacité à identifier et comprendre les risques liés à divers modèles de service cloud et de mise en œuvre.

L'infrastructure cloud doit être comprise comme un ensemble de matériel et de logiciels qui rendent possibles les cinq caractéristiques essentielles du cloud computing. L'infrastructure cloud peut être considérée comme contenant une couche physique et une couche d'abstraction. La couche physique se compose des ressources matérielles nécessaires pour soutenir les services cloud fournis tandis que la couche d'abstraction comprend le logiciel utilisé dans la couche physique.

4.1. Les caractéristiques du cloud computing selon la définition du NIST :

Le libre-service sur demande	L'utilisateur peut disposer de plusieurs fonctions informatiques selon ses besoins (par ex. un serveur virtuel ou un compte e-mail). La configuration de ces fonctions peut se faire intégralement en ligne sans le moindre contact avec le personnel du fournisseur d'accès.
L'accès global au réseau	Les services sont disponibles sur le réseau et l'accès est pris en charge par diverses plateformes (par ex. smartphones, tablettes, ordinateurs portables et stations de travail).
Le bassin de ressources	Les ressources informatiques du fournisseur de service cloud sont rassemblées afin de servir simultanément plusieurs consommateurs et ce, n'importe où dans le monde. Parmi les exemples de ressources, citons le stockage, le traitement, la mémoire et la bande passante du réseau.
L'adaptabilité	Les ressources cloud peuvent être facilement accessibles et libérées. Aux yeux de l'utilisateur, les ressources mises à disposition peuvent sembler illimitées et peuvent être utilisées à tout moment et en quantité illimitée.
L'utilisation mesurée du service	Les systèmes cloud contrôlent et optimisent automatiquement l'utilisation des ressources. Les utilisateurs paient uniquement les ressources du service qu'ils utilisent. L'utilisation des ressources peut être surveillée, contrôlée et synthétisée dans des rapports, un gage de transparence aussi bien pour le fournisseur que pour l'utilisateur.

4.2. Les modèles de service de cloud computing définis par le NIST

Logiciels en tant que service (SaaS).	Ce modèle offre à l'organisme public la possibilité d'utiliser les applications du fournisseur de services cloud fonctionnant sur la base d'une infrastructure cloud. Les applications logicielles sont accessibles en ligne à travers une interface web ou une application bureautique. Le consommateur n'a aucun contrôle sur la configuration matérielle sous-jacente. **Exemples de logiciels en tant que service :** les offres comprennent Office Productivity as a Service (OPaaS) de l'État, Microsoft Office 365, Google Apps, Salesforce.com et les applications Oracle Cloud. **Autre exemple** : Community Cloud (voir point **4.3.** ci-dessous **Modèles de mise en œuvre)** : G-Cloud « Composantes et applications » : https://www.gcloud.belgium.be/fr/services#service-2
Plate-forme en tant que service (PaaS).	Ce modèle offre à l'organisme public la possibilité de déployer ou d'installer sur l'infrastructure cloud une application développée ou acquise par l'organisme à condition que cette application soit créée à l'aide de langages de programmation, bibliothèques, services et outils pris en charge par le fournisseur de service cloud. L'utilisateur n'exerce aucun contrôle sur la configuration sous-jacente du logiciel, le stockage, le réseau, le système d'exploitation ou les niveaux de gestion. **Exemples de PaaS** : les offres comprennent le Desktop as a Service (DaaS) de l'État, Google App Engine, Microsoft Windows Azure, Force.com et Oracle Database Cloud. **Autre exemple** : Community Cloud (voir point **4.3.** ci-dessous **Modèles de mise en œuvre)** : G-Cloud « Plateformes » : https://www.gcloud.belgium.be/fr/services#service-3
Infrastructure en tant que Service (IaaS).	Ce modèle offre à l'organisme public la possibilité d'utiliser le traitement, le stockage, les réseaux et d'autres ressources informatiques permettant à l'utilisateur d'installer et exécuter n'importe quel logiciel pouvant comporter des systèmes d'exploitation et des applications. L'organisme public ne gère pas et ne contrôle pas l'infrastructure cloud sous-jacente mais il contrôle les systèmes d'exploitation, le stockage et les applications déployées. **Exemples de IaaS :** les offres comprennent les plateformes IaaS de l'État, Amazon Web Services (AWS), Elastic Cloud Compute (EC2), Google Compute Engine. **Autre exemple** : Community Cloud (voir point **4.3.** ci-dessous **Modèles de mise en œuvre)** : G-Cloud « Infrastructure dure » : https://www.gcloud.belgium.be/fr/services#service-5

4.3. Modèles de mise en œuvre définis par le NIST

Cloud privé	L'infrastructure cloud est activée uniquement afin d'être utilisée par une seule organisation/un seul organisme public composé(e) de plusieurs utilisateurs (par ex. divers départements). Elle peut être détenue, gérée et exploitée par l'organisme ou une tierce partie, ou par les deux, et être installée sur site ou en dehors. L'infrastructure peut aussi se trouver dans le pays ou à l'étranger.
Cloud communautaire	L'infrastructure cloud est mise en service afin d'être utilisée uniquement par une communauté/un groupe particulier d'utilisateurs appartenant à des organisations ayant en commun la nature de leurs activités et leurs obligations (par ex. même mission, exigences identiques en matière de sécurité informatique, considérations communes sur le plan juridique et de conformité propres au secteur). Elle peut être détenue, gérée et exploitée par un ou plusieurs organisme(s) membre(s) de la communauté, par une tierce partie, ou une combinaison de ceux-ci, et être installée sur site ou en dehors. L'infrastructure peut aussi se trouver dans le pays ou à l'étranger. (Par ex. Extranet)
Cloud public.	L'infrastructure cloud est mise en service en vue d'une utilisation ouverte par n'importe quelle organisation. Elle peut être détenue, gérée et exploitée par des organismes privés ou publics, ou les deux. Elle est installée dans les locaux du fournisseur de services cloud.
Cloud hybride.	L'infrastructure cloud est une combinaison d'au moins deux infrastructures cloud (privée, communautaire ou publique). Ces entités restent séparées mais elles sont liées par une technologie standardisée ou exclusive permettant la transférabilité de données et d'applications (par ex. équilibrage de charges entre clouds).

Attention au Shadow Cloud !

« Le shadow cloud » fait référence aux services cloud publics employés par les membres d'une organisation à l'insu ou sans l'autorisation du département informatique. L'utilisation d'appareils mobiles personnels à des fins professionnelles constitue un exemple de shadow IT (informatique de l'ombre). Les membres du personnel peuvent utiliser leurs propres appareils dans le cadre de leur fonction sans avoir prévenu le service informatique de leur organisation ou sans avoir obtenu son autorisation.

À l'instar du shadow IT non contrôlé, de telles pratiques sur le cloud peuvent présenter des risques pour les organismes. Mais si elles font l'objet d'une gestion efficace, elles offrent l'opportunité d'améliorer l'implication du personnel, d'accroître le niveau d'efficacité et de gérer les risques liés. Le contrôle du shadow cloud ne doit pas uniquement chercher à réduire les risques au maximum mais d'en exploiter les avantages. [3]

Compte tenu de l'importance croissante de la technologie et de la dépendance à l'égard de celle-ci, les organismes devraient évaluer l'étendue du shadow cloud dans leur organisation, communiquer les opportunités et les risques et identifier les mesures appropriées afin de traiter le problème. Les services cloud simples à utiliser tels que DropBox ont rendu les limites qui séparent les applications privées et commerciales plus floues. Tandis que les cas d'utilisation des applications du shadow cloud sont généralement valables, l'augmentation de leur usage s'accompagne de plusieurs implications, notamment :

- la perte ou la compromission de données provenant de services mal conçus, mal gérés ou malveillants exposant alors les données ou l'infrastructure de l'organisme à des risques imprévus ;
- la perte de données à cause de la diffusion des informations à travers plusieurs services et de leur accessibilité réduite au sein de l'organisme (cela peut également engendrer la perte de données à la suite de l'arrêt du service, du déplacement du personnel et de la perte de connaissances relatives à l'emplacement des données) ;
- l'augmentation des coûts en raison du recours à plusieurs services de cloud public pour la même fonction, une solution dont le support technique peut être onéreux sans permettre une tarification de volume (parmi les autres coûts éventuels, citons les opérations de restauration, de récupération et de réparation si un service cloud compromet les informations ou l'infrastructure de l'organisme).

Les organismes ont probablement eu peu de visibilité ou de contrôle sur les services utilisés, les données stockées dans ces applications et peu de garanties commerciales sur la disponibilité de leurs données. Une incertitude quant aux risques liés en a résulté. Il peut s'avérer utile de souligner qu'une distinction peut être établie dans le cadre de l'utilisation de services de shadow cloud par du personnel d'organismes gouvernementaux entre les besoins à des fins professionnels et privés.

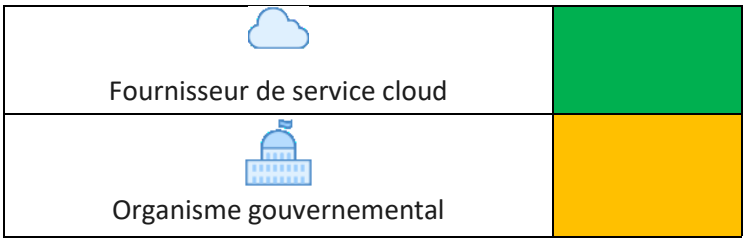
[3] Un exemple de gestion des risques liés au shadow cloud est disponible sur le lien suivant : https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/assets/Uploads/Shadow-Cloud-Guidance2.pdf (le contenu du domaine « ict.govt.nz » sera bientôt déplacé vers « digital.govt.nz », le lien pourrait prochainement expirer).

Responsabilité de l'organisme en matière de sécurité dans les environnements de cloud computing

Selon le modèle cloud choisi, un organisme gouvernemental souscrivant à un service IaaS peut conserver le contrôle total, et dès lors en supporter la responsabilité, de la sécurité et de la maintenance permanentes de l'ensemble des systèmes d'exploitation, applications, configurations virtuelles (y compris l'hyperviseur et les dispositifs de sécurité virtuels) et données.

Il est important de comprendre que même si les organismes peuvent externaliser la responsabilité à un fournisseur de service chargé de la mise en œuvre, de la gestion et du maintien des contrôles de sécurité, ils ne peuvent pas externaliser leur responsabilité de veiller à la protection adéquate de leurs données. Le fournisseur de cloud computing a une responsabilité opérationnelle adaptative selon le choix d'environnement de cloud computing. Toutefois, l'organisme gouvernemental reste légalement responsable de la protection des données. Il devrait convenir avec le fournisseur de service cloud d'une attribution adéquate des rôles et responsabilités en matière de sécurité des informations et confirmer qu'il est en mesure d'assumer les rôles et responsabilités attribués. Les rôles et responsabilités en matière de sécurité des informations de chaque partie devraient être définis dans un accord.[4]

Le diagramme suivant illustre la manière dont la responsabilité d'un organisme gouvernemental peut varier selon le modèle de cloud.



Responsabilité	Sur site	IAAS	PAAS	SAAS
Classification des données et responsabilité				
Protection de l'utilisateur et du terminal				
Gestion des identités et accès				
Contrôle au niveau des applications				
Contrôle des réseaux				
Infrastructure d'hébergement				
Sécurité physique				

[4] Iso 27027

Le tableau suivant donne un aperçu du seuil de responsabilité pour chaque modèle de service :

Logiciels en tant que service (SaaS).	L'organisme gouvernemental exerce un contrôle extrêmement limité sur la sécurité dans le cadre du modèle de service SaaS. En général, il restera responsable de la gestion de ses comptes utilisateurs afin de veiller à ce que ces derniers soient les seuls à obtenir les autorisations requises pour effectuer leurs tâches. Le fournisseur de service a quant à lui la responsabilité de s'assurer que les autres contrôles de sécurité sont appliqués et garantissent un niveau de protection adéquat.
Plate-forme en tant que service (PaaS).	Le modèle de service PaaS se base sur le modèle IaaS afin d'inclure le système d'exploitation hôte et les services d'application. Par conséquent, le fournisseur de service est également responsable de la mise en œuvre, de la gestion et du maintien des contrôles de sécurité destinés à la protection de ces composants. Les organismes gouvernementaux doivent s'assurer que les applications qu'ils déploient au sein de l'environnement PaaS sont sécurisées.
Infrastructure en tant que Service (IaaS).	Le fournisseur de service est responsable de la mise en œuvre, de la gestion et du maintien des contrôles de sécurité des informations, y compris jusqu'au niveau de l'hyperviseur de virtualisation (à savoir l'infrastructure sous-jacente). Les organismes gouvernementaux doivent s'assurer que des contrôles de sécurité adéquats sont mis en place afin de protéger et de maintenir l'ensemble des composants développés sur l'hyperviseur, y compris le système d'exploitation hôte, des services d'application et des applications qu'ils déploient au sein de l'environnement IaaS.

Paysage sécuritaire du cloud[5]

Les services cloud et les services non cloud traditionnels partagent des préoccupations sécuritaires similaires. Néanmoins, ces préoccupations sont même amplifiées en ce qui concerne le cloud computing en raison de l'existence d'une forme de contrôle externe sur les ressources de l'organisation et de la possibilité d'une gestion erronée de ces ressources. Lors d'une transition vers un environnement de cloud computing public, un transfert de responsabilité et de contrôle au fournisseur de service cloud s'opère également au niveau des informations et des composants du système qui étaient auparavant sous le contrôle de l'organisme gouvernemental. Néanmoins, ce dernier doit continuer à assumer la responsabilité de son utilisation des services cloud. Il est dans l'intérêt de l'organisme de garder une idée précise de la situation, d'envisager les alternatives, de fixer des priorités et d'apporter les modifications au niveau de la sécurité. Le cloud computing comporte un certain nombre de risques pour la sécurité qu'il convient de traiter adéquatement :[6]

● **Perte de propriété de la gouvernance**. Dans le cadre d'un déploiement cloud public, les utilisateurs cèdent le contrôle au fournisseur de service cloud sur un certain nombre de questions qui peuvent affecter la sécurité et la confidentialité. Les accords en matière de service cloud peuvent cependant ne pas offrir un engagement à résoudre ces questions de la part du fournisseur de service cloud, laissant alors des lacunes dans les systèmes de défense.

● **Ambiguïté en matière de responsabilité.** Les responsabilités concernant des aspects de sécurité et de respect de la vie privée peuvent être partagées entre le fournisseur de service cloud et l'utilisateur, ce qui engendre le risque d'une absence de contrôle de composants essentiels des systèmes de sécurité en cas de manque d'attribution et de délimitation claires des responsabilités. La répartition des responsabilités est susceptible de varier en fonction du modèle de service cloud employé (par ex. IaaS vs. SaaS).

● **Authentification et autorisation**. L'accès à des ressources cloud sensibles depuis n'importe quel point dans le cyberespace accroît le besoin d'établir avec certitude l'identité d'un utilisateur, surtout si des membres du personnel, des sous-traitants, des partenaires et des clients font désormais partie des utilisateurs. Un niveau d'authentification et d'autorisation élevé devient crucial.

● **Défaut d'isolement.** L'implication de plusieurs utilisateurs et le partage des ressources sont des caractéristiques clés de la mise en œuvre du cloud public. Cette catégorie de risque englobe la défaillance des mécanismes de séparation du stockage, de mémoire, de routage et même de réputation entre les utilisateurs.

● **Conformité et risques juridiques.** L'investissement du client cloud pour obtenir les certifications nécessaires (par ex. dans le but de démontrer le respect des normes sectorielles ou des exigences réglementaires) peut être perdu si le fournisseur de service cloud n'est pas en mesure d'apporter la preuve de sa propre conformité aux exigences pertinentes. Le client doit vérifier que le fournisseur de service cloud dispose des certifications appropriées et pertinentes.

● **Traitement des incidents liés à la sécurité.** La détection, la notification et la gestion ultérieure des incidents de sécurité peuvent être déléguées au fournisseur de service cloud, mais ces incidents ont un impact sur le client.

---

[5] Les 10 étapes du CSCC pour une sécurité optimale en matière de cloud computing : https://www.omg.org/cloud/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

[6] Crédit : Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). Pour plus d'informations, rendez-vous à l'adresse http://www.enisa.europa.eu/

Les règles de notification doivent être négociées dans le contrat de service cloud afin que les clients ne soient pas pris au dépourvu ou informés avec un retard inacceptable.

● **Vulnérabilité de l'interface de gestion.** Les interfaces de gestion des ressources de cloud public (notamment l'autosubsistance) sont généralement accessibles via internet. Étant donné qu'elles permettent d'accéder à des ensembles plus vastes de ressources par rapport aux fournisseurs d'hébergement traditionnels, ces interfaces font peser un risque accru, surtout lorsqu'elles sont combinées à l'accès à distance et aux vulnérabilités du navigateur web.

● **Protection des applications.** Traditionnellement, les applications ont été protégées au moyen de solutions de sécurité complètes basées sur une séparation claire des ressources physiques et virtuelles et sur des zones fiables. Avec la délégation de la responsabilité de la sécurité de l'infrastructure au fournisseur de service cloud, les organismes doivent repenser la sécurité du périmètre au niveau du réseau, en appliquant davantage de contrôles au niveau des utilisateurs, des applications et des données. Un niveau identique de contrôle d'accès des utilisateurs et de protection à celui des centres de données traditionnels doit être appliqué aux tâches déployées dans les services cloud. Cette solution exige la création et la gestion de politiques orientées sur les tâches et la mise en œuvre d'une gestion centralisée des instances de tâches distribuées.

● **Protection des données.** Les principales préoccupations sont l'exposition ou la divulgation de données personnelles et/ou sensibles, la perte ou l'indisponibilité des données et la surconservation des données. L'organisme gouvernemental (en sa qualité de contrôleur de données) peut éprouver des difficultés à contrôler efficacement les pratiques de manipulation des données du fournisseur d'accès au cloud. Ce problème est exacerbé en cas de transferts multiples de données (par ex. entre plusieurs services cloud ou lorsque le fournisseur fait appel à des sous-traitants et à des fournisseurs tiers), ce qui engendre un manque de transparence de propriété et des objectifs ambigus en matière de traitement des données.

● **Réglementation en matière de données personnelles.** Il est courant dans la plupart des juridictions que les données personnelles doivent être traitées conformément aux exigences des lois et/ou règlements. Ce principe s'étend désormais généralement au-delà de la protection de ces données personnelles, mais il implique également des droits accordés à la personne concernée de consulter, corriger ou supprimer ses données et, dans certains cas, de demander le transfert de ses données. Tout recours à un service cloud qui conserve ou traite des données personnelles doit satisfaire ces exigences et, simultanément, protéger les données.

● **Comportement malveillant d'initiés**. Les dommages provoqués par les agissements malveillants de personnes employées au sein d'un organisme peuvent être conséquents au vu de leur niveau d'accès et d'autorisation. Cette situation est aggravée dans un environnement de cloud computing car de telles actions peuvent se produire au sein de l'organisme du client et/ou du fournisseur.

● **Faillite du fournisseur.** Cette faillite pourrait engendrer l'indisponibilité des données et applications essentielles dans le cadre des activités du client et ce, pour une longue période.

● **Indisponibilité du service.** Une telle situation peut être la conséquence de défaillances du matériel, du logiciel ou du réseau de communication.

● **Enfermement propriétaire.** La dépendance à l'égard des services exclusifs d'un fournisseur de service cloud particulier pourrait faire en sorte que le client soit lié à ce fournisseur. Le manque de transférabilité des applications et des données entre fournisseurs implique un risque d'indisponibilité des données et du service en cas de changement de fournisseurs. Bien qu'important, cet aspect sécuritaire est parfois négligé. Un manque

d'interopérabilité d'interfaces liées à des services cloud lie également le client à un fournisseur particulier et peut compliquer le changement de fournisseur.

● **Suppression de données non sécurisée ou incomplète**. La résiliation d'un contrat avec un fournisseur n'engendre pas toujours la suppression des données de l'utilisateur de la part du fournisseur et de ses systèmes tiers. Des copies de sauvegarde des données sont généralement effectuées et peuvent être mélangées sur le même support avec les données d'autres clients, ce qui complique l'effacement sélectif. L'avantage même de la multilocation (le partage des ressources matérielles) représente donc un risque plus élevé pour le client que le matériel dédié.

● **Visibilité et contrôle**. Certains utilisateurs au sein d'organisations instaurent un « shadow IT » en faisant l'acquisition de services cloud afin de développer des solutions IT sans l'approbation explicite de leur organisation. Les principaux défis pour l'équipe en charge de la sécurité consistent à connaître toutes les utilisations des services cloud au sein de l'organisation (par exemple, les ressources utilisées, dans quel but, dans quelle mesure et par quel membre), comprendre quels types de lois, réglementations et politiques peuvent s'appliquer à ces utilisations et évaluer régulièrement les aspects sécuritaires de ces utilisations.

Sécurité minimale et considérations en matière de vie privée

Actions recommandées afin de répondre à ces considérations

Les organismes gouvernementaux peuvent également déterminer les certifications utiles et pertinentes et s'ils décident ou non de faire davantage confiance à la capacité du fournisseur de service de protéger leurs informations. Un organisme gouvernemental doit impérativement comprendre si la certification à une norme ou un cadre reconnu à l'échelle internationale apporte l'assurance que le fournisseur de service satisfait à ses exigences de sécurité. La portée de la certification doit correspondre aux services offerts par le fournisseur de service cloud aux organismes gouvernementaux. Une liste non exhaustive d'actions conseillées pour chaque objectif de sécurité spécifique est fournie dans la suite de ce guide.

> Par exemple, les fournisseurs de service certifiés conformes aux exigences de la norme ISO/IEC 27001 sont en mesure de définir la portée de l'audit par le biais d'une Déclaration d'applicabilité. Les organismes gouvernementaux doivent donc vérifier précisément les contrôles couverts par l'audit en demandant au fournisseur de service une copie du dernier rapport d'audit externe (comprenant la portée ou la Déclaration d'applicabilité) ainsi que les résultats de l'ensemble des audits internes récents.
>
> Une autre source d'information potentielle en matière de contrôles de sécurité mis en place par un fournisseur de service est le programme Security, Trust & Assurance Register (CSA STAR) de Cloud Security Alliance. Le degré d'assurance fourni dépend du niveau atteint par le fournisseur de service dans l'Open Certification Framework (OCF) du CSA.

Enisa (l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information) propose un tableau de synthèse mettant en correspondance des objectifs de sécurité avec différents systèmes.[7]

[7] https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/

Détails sur la responsabilité d'un objectif de sécurité

Dans la mesure du possible, des informations plus précises sont transmises à propos de la responsabilité des objectifs de sécurité basés sur la norme ISO/IEC 27017.

Valeur, caractère critique et sensibilité des informations

Afin d'être en mesure d'évaluer les risques liés à l'utilisation d'un service cloud, les organismes doivent reconnaître la valeur, le caractère critique et la sensibilité des informations qu'ils ont l'intention de placer dans le service.

Considérations à prendre en compte pour cet objectif de sécurité :

- le propriétaire commercial de l'information devrait être identifié ;
- les processus commerciaux soutenus par l'information devraient être identifiés ;
- un classement de la sécurité de l'information devrait être établi ;
- des directives destinées à la protection des informations officielles devraient être définies ;
- les préoccupations particulières liées à la confidentialité de l'information qui sera stockée ou traitée par le service cloud devraient être identifiées ;
- il conviendrait d'établir clairement si les données comprennent des informations personnelles ;
- les utilisateurs de l'information devraient être identifiés ;
- les autorisations accordées aux utilisateurs leur permettant de demander des informations devraient être claires (lire, rédiger, modifier et/ou supprimer).
- la législation applicable à l'information devrait être claire ;
- les obligations contractuelles applicables à l'information devraient être claires ;
- l'impact commercial des informations dévoilées de manière non autorisée devrait être identifié ;
- l'impact commercial en cas de compromission de l'intégrité de l'information devrait être identifié ;
- l'organisme gouvernemental devrait mettre en place des plans de gestion et d'intervention en cas d'incident afin de réduire au maximum l'impact d'une divulgation non autorisée ;
- l'impact commercial lié aux informations non disponibles devrait être clairement identifié ;

Actions recommandées afin de répondre aux préoccupations :

- Le contrôle de sécurité de la Cloud Control Matrix[8]: DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07

Détails sur la responsabilité de cet objectif de sécurité :

Organisme gouvernemental	Fournisseur de service cloud
L'organisme gouvernemental devrait étiqueter l'information et les actifs connexes déployés dans l'environnent de cloud computing conformément à ses procédures en matière d'étiquetage. Le cas échéant, la fonctionnalité mise à disposition par le fournisseur de service cloud qui prend en charge l'étiquetage peut être adoptée.	Le fournisseur de service cloud doit documenter et divulguer toute fonctionnalité de service fournie permettant aux organismes gouvernementaux de classer et d'étiqueter leurs informations et actifs connexes.

[8] Fournie par le Cloud Working Group (Anciennement Cloud Security Alliance) du consortium Object Management Group (OMG) https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/

Souveraineté des données

L'utilisation de services cloud situés en dehors de la juridiction belge ou détenus par des entreprises étrangères comporte des risques en matière de souveraineté des données. Cela signifie que toute donnée stockée, traitée ou transmise par ledit service peut être soumise à la législation ou à la règlementation des pays par le biais desquels la donnée est stockée, traitée et transmise. De même, un fournisseur de service étranger qui propose un service en Belgique peut être soumis aux lois du pays dans lequel il a établi son siège social.

Les lois en vertu desquelles il pourrait être accédé à des informations détenues par le fournisseur de service diffèrent d'un pays à l'autre. Dans certains cas, lorsqu'un fournisseur de service est contraint de fournir des données appartenant à ses utilisateurs par un organisme étranger chargé de l'exécution de la loi, il peut être légalement tenu de ne pas avertir l'utilisateur de la demande. Il est dès lors essentiel qu'un organisme gouvernemental identifie les juridictions de droit au sein desquelles ses données seront stockées, traitées ou transmises. L'organisme doit en outre comprendre l'impact potentiel des lois de ces pays sur la confidentialité, l'intégrité, la disponibilité et le caractère privé des informations.

Dans le cas où le fournisseur de service impartit ou sous-traite tout aspect de la fourniture du service à un tiers, les organismes sont également tenus d'identifier si cela comporte des risques supplémentaires en matière de souveraineté des données.

Les informations confidentielles détenues dans des juridictions de droit autres que la Belgique peuvent être soumises aux lois sur le respect de la vie privée et la protection des données des pays dans lesquels le service cloud est fourni. En dépit du RGPD, les lois sur le respect de la vie privée et la protection des données peuvent différer d'un pays à l'autre au sein de l'Union européenne. Il est dès lors important que les organismes évaluent l'éventuelle incidence des lois de ces pays sur la confidentialité des informations relatives à leurs employés et/ou utilisateurs.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- le siège social du fournisseur de service devrait être connu ;
- les pays à partir desquels les services cloud sont fournis devraient être connus ;
- les juridictions de droit au sein desquelles les données de l'organisme gouvernemental seront stockées et traitées devraient être connues ;
- le fournisseur de service devrait permettre à ses utilisateurs de préciser les lieux dans lesquels leurs données peuvent ou non être stockées et traitées ;
- si le service dépend d'une quelconque manière de tiers (p. ex. des consultants externes, des sous-traitants ou un autre fournisseur de service) et que cela entraîne des risques juridictionnels supplémentaires, le fournisseur de service devrait communiquer les informations suivantes pour chaque tiers impliqué dans la fourniture du service :
    - le siège social du tiers ;
    - le(s) pays depuis le(s)quel(s) leurs services sont fournis ; et
    - l'accès qu'ils ont aux données d'utilisateurs stockées, traitées et transmises par le service cloud ;
- les lois du ou des pays dans le(s)quel(s) les données seront stockées et traitées devraient être examinées afin d'évaluer leur impact éventuel sur la sécurité et/ou la confidentialité des informations ;
- les lois devraient être effectivement applicables au fournisseur de service et/ou aux informations de ses utilisateurs ;
- la manière dont le fournisseur de service traite les demandes d'accès des organismes gouvernementaux aux informations des utilisateurs devrait être connue ;

Actions suggérées pour répondre à ces considérations :

- Les normes ISO/IEC 27001 et ISO/IEC 27018 peuvent aider les organismes gouvernementaux à bien respecter les considérations ci-dessus

Détail des responsabilités relatives à cet objectif de sécurité :

Organisme gouvernemental	Fournisseur de service cloud
L'organisme gouvernemental devrait identifier les autorités compétentes dans le cadre de l'exploitation combinée de l'organisme gouvernemental et du fournisseur de service cloud.	Le fournisseur de service cloud devrait informer l'organisme gouvernemental des lieux géographiques de son organisation et des pays dans lesquels le service cloud peut stocker les données de celui-ci.

Respect de la vie privée

Les organismes gouvernementaux qui envisagent d'enregistrer des informations à caractère personnel dans un service cloud devraient effectuer une analyse d'impact relative à la protection des données (AIPD) afin de s'assurer qu'ils identifient tout risque en matière de protection de la vie privée associé à l'utilisation du service et effectuer les contrôles nécessaires à une gestion efficace de ces risques.

Les services cloud peuvent permettre aux organismes d'exploiter plus facilement les opportunités de partage de l'information. Par exemple, le partage de données à caractère personnel avec un autre organisme gouvernemental peut s'effectuer simplement en créant des comptes utilisateur dotés des autorisations appropriées au sein d'une solution SaaS plutôt qu'en utilisant une interface système à système pour échanger des informations.

Bien que les services cloud disposent du potentiel pour limiter les obstacles techniques liés au partage de l'information, les organismes doivent veiller à gérer de manière appropriée l'accès aux informations à caractère personnel et à se conformer aux exigences du Règlement général sur la Protection des Données (RGPD) ainsi qu'à la loi belge relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel. Les organismes gouvernementaux devraient s'assurer que leur fournisseur de service cloud respecte ce règlement ainsi que cette loi, faute de quoi ils s'exposent à de lourdes amendes.

Étant donné que des violations de données peuvent se produire et que l'organisme gouvernemental est responsable de la protection de toute information à caractère personnel en sa possession, il est important que ce dernier mette tout en œuvre pour sécuriser lesdites données avant de les enregistrer dans des applications et des espaces de stockage cloud.

Quand bien même il apparaît qu'un service cloud a enfreint le RGPD, la responsabilité de l'organisme gouvernemental peut malgré tout être engagée en sa qualité de responsable du traitement. Ce dernier est dès lors tenu d'examiner attentivement les garanties octroyées par les fournisseurs de cloud en matière de conformité au RGPD.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- Il convient de savoir si les données qui seront stockées et traitées par le service cloud incluent des informations à caractère personnel telles que définies dans le RGPD ;
- une AIPD identifiant les risques d'atteinte à la vie privée associés à l'utilisation du service cloud ainsi que les contrôles requis pour gérer ces risques devraient avoir été réalisés ;

- le fournisseur de service devrait clairement définir son utilisation de données à caractère personnel dans sa politique de confidentialité ;
- la politique devrait être conforme aux obligations légales de l'organisme gouvernemental en vertu du RGPD ;
- l'endroit où l'organisme gouvernemental, son personnel et/ou ses utilisateurs doivent introduire une plainte en cas d'atteinte à la vie privée devrait être clairement défini ;
- l'organisme gouvernemental devrait prévoir une réalisation régulière d'audits afin de s'assurer que les systèmes et les services utilisés restent conformes au RGPD ;

Actions suggérées pour répondre à ces considérations :

- Les normes ISO/IEC 27001 et ISO/IEC 27018 peuvent aider les organismes gouvernementaux à bien respecter les considérations ci-dessus ainsi que le Règlement général sur la Protection des Données
- La norme ISO/IEC 27701, Techniques de sécurité - Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices, précise les exigences relatives à l'établissement, la mise en œuvre, la maintenance et l'amélioration continue d'un système de gestion de la sécurité de l'information en matière de protection de la vie privée. Il s'agit en quelque sorte d'un système de gestion de la protection des données à caractère personnel.

Détail des responsabilités relatives à cet objectif de sécurité :

- Pour obtenir plus d'informations sur les obligations relatives à la protection de la vie privée, nous recommandons de consulter le FISP - Vademecum sur la protection de la vie privée.

Gouvernance

Actions suggérées pour assurer la gouvernance cloud :

- Vous trouverez un guide pratique sur la gouvernance cloud ici : https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-governance.pdf
- Le contrôle de sécurité de la Matrice de Contrôle Cloud : GRM-01

Conditions d'utilisation :

Contrairement aux modèles d'impartition traditionnels, il se peut que les utilisateurs ne puissent pas pleinement négocier les conditions contractuelles avec le fournisseur de service, particulièrement dans le cas de services cloud publics. Les principaux outils de contrôle de la gouvernance dont disposent les organismes sont les conditions d'utilisation (ou le contrat), l'accord de niveau de service (ANS) connexe, les indicateurs clés de performance et les paramètres relatifs à la performance du service du fournisseur de service. Ceux-ci doivent être soigneusement examinés afin de garantir que le service est conforme aux obligations de l'organisme gouvernemental de protéger la confidentialité, l'intégrité et la disponibilité de ses informations officielles ainsi que la confidentialité de toutes les informations à caractère personnel identifiables qu'il compte soumettre.

Afin de pouvoir exercer tout niveau de contrôle sur les données contenues dans le service cloud, les organismes gouvernementaux doivent conserver la propriété de leurs données et savoir comment le fournisseur de service va utiliser les données lors de la fourniture du service. Il se peut que les fournisseurs de services utilisent les données des utilisateurs à leurs propres fins commerciales (p. ex. pour générer des revenus en proposant des publicités ciblées aux utilisateurs ou en récoltant et vendant des données statistiques à d'autres organisations). Bien que l'utilisation de données des utilisateurs se limite généralement à des contrats de consommation plutôt qu'à des contrats d'entreprise, il est important de déterminer si le fournisseur de service utilisera les données à des fins autres que pour la fourniture du service. Les conditions d'utilisation du fournisseur de service doivent dès lors être examinées afin de s'assurer qu'elles définissent clairement la propriété des données, la manière dont

elles seront utilisées dans le cadre de la fourniture du service et si le fournisseur de service les utilisera à des fins autres que pour la fourniture du service.

Il n'est pas rare qu'un fournisseur de service fasse appel à des composants provenant d'autres fournisseurs de services. Par exemple, un service SaaS peut être hébergé dans une infrastructure Iaas appartenant à un autre fournisseur. Il est essentiel d'identifier toutes les dépendances du fournisseur de service à des services de tiers afin de bien comprendre les risques que comporte l'adoption d'un service.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- il convient de savoir si le fournisseur de service négocie des contrats avec ses utilisateurs ou si ceux-ci sont tenus d'accepter les conditions d'utilisation standard ;
- Les conditions d'utilisation et l'ANS du fournisseur de service devraient clairement définir la manière dont le service protège la confidentialité, l'intégrité et la disponibilité d'informations officielles ainsi que la confidentialité de toutes les informations à caractère personnel identifiables ;
- les conditions d'utilisation du fournisseur de service devraient préciser que l'organisme gouvernemental restera propriétaire de ses données ;
- il convient de vérifier si le fournisseur de service utilise les données à des fins autres que pour la fourniture du service ;
- Il faut qu'il soit clairement indiqué si le service que propose le fournisseur dépend de tout autre service de tiers ;

Actions suggérées pour répondre à ces considérations :

- Guide pratique sur les contrats de service cloud V3.0 : https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-service-agreements.htm
- Contrats de service cloud public : À quoi s'attendre et que négocier V2.0 : https://www.omg.org/cloud/deliverables/public-cloud-service-agreements-what-to-expect-and-what-to-negotiate.htm

Conformité :

Le fournisseur de service cloud devrait se conformer à la loi belge établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique qui transpose la directive européenne NIS (2016/1148/EU) en droit belge. Le fournisseur de service cloud peut être considéré comme un fournisseur de service numérique tel que défini dans cette loi. Les fournisseurs de services de cloud computing ne doivent pas nécessairement établir leur siège principal en Belgique. De fait, ils peuvent proposer le service en Belgique et disposer d'un représentant établi en Belgique.

La loi NIS vise à garantir que les fournisseurs de tels services de cloud computing prennent des mesures de sécurité techniques et organisationnelles pour prévenir les incidents ou limiter leur impact, garantissant ainsi la sécurité et la continuité de la vie des citoyens et des entreprises belges. Les mesures de sécurité prévues par la loi NIS couvrent les points suivants :

- Prévenir les risques : mesures techniques et organisationnelles appropriées et en proportion avec le risque.
- Assurer la sécurité du réseau et des systèmes d'information : les mesures devraient garantir un niveau de sécurité du réseau et des systèmes d'information adapté aux risques.
- Gérer les incidents : les mesures devraient prévenir et minimiser l'impact des incidents sur les systèmes informatiques utilisés pour fournir les services.

- Les mesures de sécurité prises par les FSN devraient également prendre en compte certains facteurs spécifiques :
    - sécurité des systèmes et des infrastructures
    - gestion des incidents
    - gestion de la continuité de l'activité
    - surveillance, audit et test
    - respect des normes internationales

L'obligation des services de cloud computing qui découle de la loi NIS peut en principe constituer une garantie de sécurité pour les organismes gouvernementaux.

Actions suggérées pour répondre à ces considérations :

- La norme ISO/IEC 27001 peut aider les organismes gouvernementaux à bien respecter les considérations ci-dessus
- Recommandations de l'ENISA telles que les directives techniques à prendre par fournisseurs de services numériques pour garantir la mise en œuvre de mesures de sécurité minimales : https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

Détail des responsabilités relatives à cet objectif de sécurité :

Organisme gouvernemental	Fournisseur de service cloud
• L'organisme gouvernemental devrait prendre en compte le fait que les lois et les règlementations en vigueur dans les juridictions auxquelles le fournisseur de service cloud est soumis peuvent être applicables au même titre que celles qu'il est lui-même tenu de respecter. L'organisme gouvernemental devrait requérir la preuve que le fournisseur de service cloud respecte les règlementations et les normes nécessaires à son activité. Cette preuve peut se présenter sous la forme de certifications produites par des auditeurs tiers. • L'installation d'un logiciel sous licence commerciale dans un service cloud peut entraîner une violation des termes de licence du logiciel. Avant de permettre l'installation de tout logiciel sous licence dans un service cloud, l'organisme gouvernemental devrait disposer d'une procédure permettant d'identifier les conditions de licence spécifiques au cloud. Une attention particulière devrait être portée aux cas qui impliquent un service cloud élastique et évolutif et un logiciel pouvant être utilisé sur un plus grand nombre de systèmes ou de cœurs de processeur que ce que le permettent les conditions de licence. • L'organisme gouvernemental devrait demander des informations au fournisseur de service cloud sur la protection des enregistrements que celui-ci a collectés et	• Le fournisseur de service cloud devrait informer l'organisme gouvernemental de la juridiction de droit à laquelle le service cloud est soumis. Le fournisseur de service cloud devrait identifier ses propres exigences légales (notamment en matière de cryptage des données à caractère personnel identifiables). Ces informations devraient en outre être communiquées à l'agence gouvernementale sur demande. Le fournisseur de service cloud devrait fournir la preuve à l'organisme gouvernemental de sa conformité actuelle avec la législation et les exigences contractuelles en vigueur. • Le fournisseur de service cloud devrait mettre en place un processus de traitement des plaintes relatives aux droits de propriété intellectuelle. • Le fournisseur de service cloud devrait fournir des informations à l'organisme gouvernemental sur la manière dont il protège les enregistrements qu'il a recueillis et stockés dans le cadre de l'utilisation de services cloud par l'organisme gouvernemental. • Le fournisseur de service cloud devrait fournir à l'organisme gouvernemental des descriptions des contrôles cryptographiques qu'il a mis en place pour veiller au respect des accords, des lois et de la règlementation en vigueur. • Le fournisseur de service cloud devrait fournir la preuve documentée à l'organisme

stockés et qui s'inscrivent dans le cadre de son utilisation de services cloud. • L'organisme gouvernemental devrait vérifier que tous les contrôles cryptographiques liés à l'utilisation d'un service cloud sont conformes aux accords, à la législation et à la règlementation en vigueur. • L'organisme gouvernemental devrait requérir la preuve documentée que la mise en œuvre de contrôles et de directives de sécurité de l'information pour le service cloud est conforme aux dires du fournisseur de service cloud. Cette preuve peut inclure des certifications relatives aux normes en vigueur.	gouvernemental qu'il a mis en œuvre les contrôles de sécurité de l'information qu'il dit exercer. Si la réalisation d'audits individuels par les organismes gouvernementaux s'avère compliquée ou lorsque celle-ci augmente les risques liés à la sécurité de l'information, le fournisseur de service cloud devrait fournir la preuve indépendante que la sécurité de l'information est mise en œuvre et assurée conformément à ses politiques et procédures. Cette preuve devrait être accessible aux organismes gouvernementaux en prospection avant la signature d'un contrat. Un audit indépendant adapté, sélectionné par le fournisseur de service cloud, devrait normalement constituer une méthode acceptable pour répondre à la demande de l'organisme gouvernemental d'examiner les activités du fournisseur de service cloud, à condition qu'une transparence suffisante soit garantie. Si la réalisation d'un audit indépendant s'avère compliquée, le fournisseur de service cloud devrait procéder à une auto-évaluation et en divulguer le processus ainsi que les résultats à l'organisme gouvernemental.

Confidentialité

De nombreux facteurs peuvent entraîner un accès non autorisé à des informations stockées dans un service cloud ou une divulgation de celles-ci. Cela dit, il est important de noter que la grande majorité de ces facteurs ne se limitent pas au cloud computing.

Comme indiqué précédemment, la responsabilité de la mise en œuvre et de la gestion des contrôles destinés à protéger la confidentialité des informations stockées, traitées ou transmises par le service dépend du modèle de service cloud (IaaS, PaaS ou CAA). De même, le modèle de déploiement du cloud (c.-à-d.. public, privé, communautaire ou hybride) affectera la capacité d'un utilisateur à dicter ses exigences en matière de contrôle.

Authentification et contrôle d'accès

L'adoption de plusieurs services cloud peut représenter une charge inacceptable pour les utilisateurs si l'organisme gouvernemental ne dispose pas d'une stratégie de gestion des identités appropriée. Par exemple, chaque service cloud adopté peut contraindre les utilisateurs à créer un autre identifiant et mot de passe. La discussion sur les approches en matière de gestion des identités dépasse la portée du présent document. Cependant, les organismes gouvernementaux sont invités à élaborer une approche de la gestion des identités et des accès qui facilite l'adoption de services cloud, à la fois pour leurs employés et pour leurs utilisateurs. Celle-ci devrait tenir compte des implications et des risques en matière de sécurité.

L'accès global au réseau qui caractérise le cloud computing augmente la nécessité pour les organismes de recourir à des pratiques de gestion solides en ce qui concerne le cycle de vie des identités. En effet, les utilisateurs peuvent en général accéder aux informations contenues dans un service cloud depuis n'importe quel endroit, ce qui peut représenter un risque considérable dans la mesure où se peut que des employés ou des sous-traitants conservent

un accès au service lorsqu'il est mis fin à l'emploi. Par conséquent, les organismes devraient garder un processus de gestion du cycle de vie des identités qui garantit que :

- Les permissions sont approuvées au niveau approprié dans l'organisation.
- Le contrôle d'accès basé sur les rôles (RBAC) est suffisamment granulaire pour contrôler les autorisations.
- Les utilisateurs ne reçoivent que les autorisations nécessaires à l'exécution de leurs tâches.
- Les utilisateurs ne cumulent pas plusieurs autorisations lorsqu'ils changent de rôle au sein de l'organisation.
- Les comptes utilisateur sont supprimés au moment opportun lorsqu'il est mis fin à l'emploi.

En outre, les organismes gouvernementaux devraient régulièrement auditer les comptes utilisateur ainsi que les autorisations qui leur sont accordées dans les services cloud qu'ils ont adoptés afin de s'assurer que les comptes redondants sont supprimés et que les utilisateurs continuent de n'avoir accès qu'à ce dont ils ont besoin pour exécuter leurs tâches.

Un accès ubiquitaire implique également que les utilisateurs peuvent accéder aux informations contenues dans le service cloud depuis n'importe quel endroit et au moyen de nombreux appareils différents. Les organismes doivent examiner avec attention les implications qui en découlent en termes de sécurité de l'information et évaluer les contrôles qui sont requis pour protéger leurs informations de manière appropriée. Par exemple, un organisme gouvernemental qui adopte une solution de gestion de la relation client (CRM) fondée sur un modèle SaaS pourrait déterminer qu'il a besoin de limiter l'accès à certaines caractéristiques et fonctionnalités spécifiques (p. ex. le téléchargement d'enregistrements d'utilisateurs ou la sauvegarde de rapports) lorsque des utilisateurs accèdent au service en dehors des locaux de l'organisme ou utilisent un périphérique qui n'est pas détenu et géré par l'organisme.

Lors de l'adoption de services cloud, une autre préoccupation consiste à déterminer si les mots de passe permettent d'assurer avec suffisamment de certitude que la personne qui se connecte au service est le propriétaire du compte utilisateur. Les organismes doivent déterminer s'ils ont besoin d'un mécanisme d'authentification renforcé (p. ex. une authentification à facteurs multiples) qui soit suffisamment fiable pour garantir que la partie qui s'identifie est bien l'utilisateur autorisé.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- l'organisme gouvernemental devrait disposer d'une stratégie de gestion des identités favorable à l'adoption de services cloud ;
- le service cloud devrait être en adéquation avec la stratégie de gestion des identités de l'organisme ;
- un processus interne efficace devrait garantir une gestion des identités tout au long de leur cycle de vie ;
- un processus d'audit efficace devrait être régulièrement lancé afin de garantir une gestion efficace des comptes utilisateur ;
- les contrôles requis pour gérer les risques qu'entraîne un accès ubiquitaire au cloud devraient être identifiés ;
- le service cloud devrait répondre à ces exigences en matière de contrôle ;
- il convient de savoir si un niveau de certitude plus élevé est nécessaire pour garantir que la partie qui s'identifie est bien l'utilisateur du compte autorisé au moment de l'authentification pour accéder au service ;

Actions suggérées pour répondre à ces considérations :

- Le contrôle de sécurité de la Matrice de Contrôle Cloud : AIS-03, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13,..
- Pour obtenir plus d'informations sur IAM et PAM, nous recommandons de consulter le document : FISP-Manuel sur IAM & PAM

Détail des responsabilités relatives à cet objectif de sécurité :

Organisme gouvernemental	Fournisseur de service cloud
• La politique de contrôle d'accès de l'organisme gouvernemental pour l'utilisation des services réseau devrait préciser les exigences d'accès utilisateur à chaque service cloud distinct utilisé ; • L'organisme gouvernemental devrait utiliser des techniques d'authentification satisfaisantes (p. ex. une authentification à facteurs multiples) pour authentifier ses administrateurs du service cloud en fonction des capacités administratives d'un service cloud et des risques identifiés. • L'organisme gouvernemental devrait vérifier que la procédure de gestion du fournisseur de service cloud en matière d'octroi d'informations d'authentification secrètes, telles que des mots de passe, est conforme à ses exigences.	• Pour gérer l'accès des utilisateurs d'un organisme gouvernemental à des services cloud, le fournisseur de service cloud devrait proposer des fonctions d'enregistrement et de désenregistrement à ces utilisateurs et communiquer les spécifications relatives à l'utilisation de ces fonctions à l'organisme gouvernemental ; • Le fournisseur de service cloud devrait proposer des fonctions permettant de gérer les droits d'accès des utilisateurs du service cloud de l'organisme gouvernemental et communiquer les spécifications relatives à l'utilisation des fonctions ; • Le fournisseur de service cloud devrait mettre à disposition des techniques d'authentification satisfaisantes permettant d'authentifier les administrateurs du service cloud de l'organisme gouvernemental en fonction des capacités administratives d'un service cloud et des risques identifiés. Par exemple, le fournisseur de service cloud peut fournir la possibilité de recourir à une authentification à facteurs multiples ou permettre l'utilisation de mécanismes d'authentification à facteurs multiples de tiers. • Le fournisseur de service cloud devrait communiquer des informations sur les procédures qu'il prévoit dans le cadre de la gestion des informations secrètes d'authentification de l'organisme gouvernemental, en ce compris les procédures de communication de telles informations et d'authentification de l'utilisateur.

Architecture multi-entité

La mutualisation des ressources qui caractérise le cloud computing signifie que les services cloud utilisent en général une certaine forme d'architecture multi-entité. Les risques liés à cette dernière ont généralement trait à la virtualisation de l'infrastructure ou au regroupement de données. La préoccupation le plus souvent mise en avant dans le cadre d'un environnement virtualisé concerne le fait qu'une partie malveillante pourrait exploiter une vulnérabilité au sein de l'hyperviseur pour accéder aux informations d'un autre utilisateur (par exemple en menant une attaque « guest-to-host » ou « guest-to-guest »). La virtualisation a facilité la création d'un instantané (c.-à-d. une copie de la mémoire et du disque d'un serveur en cours d'exécution à un moment donné à des fins de sauvegarde et de redondance). Si les instantanés ne sont pas correctement protégés, une partie malveillante pourrait obtenir un accès non autorisé aux informations stockées sur les disques locaux de la machine virtuelle ainsi qu'à toutes les clés de cryptage et les données en mémoire.

Par conséquent, l'architecture, la mise en œuvre, la gestion permanente et la surveillance de l'environnement de virtualisation du fournisseur de service ainsi que les pratiques de gestion des correctifs et des vulnérabilités de ce dernier sont essentielles pour garantir la sécurité des informations stockées et traitées dans le service cloud.

Une autre préoccupation commune des environnements IaaS et PaaS réside dans le fait que l'utilisateur disposant des pratiques et des contrôles de sécurité les moins performants pourrait déterminer le niveau de sécurité de l'ensemble de l'environnement (problème du plus petit dénominateur commun). Les services SaaS et PaaS utilisent des contrôles logiques au sein de l'application ou plateforme et de l'infrastructure de support pour compartimenter l'accès aux données de chaque utilisateur. Cela dit, les données sont généralement mélangées dans l'application, la base de données et le support de sauvegarde. Un tel système repose entièrement sur la qualité de la conception, la mise en œuvre et l'application des contrôles d'accès au sein des plateformes et les applications.

Le libre-service à la demande propre au cloud computing soulève des préoccupations en matière de sécurité, car les processus d'enregistrement pour devenir utilisateur ne permettent pas toujours de confirmer avec certitude l'identité d'un utilisateur (c.-à-d. l'auto-inscription via Internet). Cette faiblesse peut permettre à une partie malveillante de s'enregistrer à un service et de l'utiliser ensuite à des fins malveillantes ou frauduleuses, telles que tenter de déjouer les contrôles d'accès dans le but d'obtenir un accès non autorisé aux données d'un autre utilisateur. Un organisme gouvernemental doit avoir l'assurance suffisante que d'autres utilisateurs du service cloud ne sont pas en mesure de déjouer les contrôles du fournisseur de service dans le but d'accéder à ses informations. Comme énoncé plus haut, la tâche peut s'avérer délicate dans la mesure où la nature de « service rendu » du cloud computing va généralement de pair avec un manque de transparence en ce qui concerne les contrôles et les pratiques de sécurité du fournisseur de service pour protéger les données des utilisateurs. Par conséquent, cela se traduit là encore par une forte dépendance aux rapports d'audit et aux tests de pénétration de tiers.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- le fournisseur de service devrait autoriser l'organisme à examiner un rapport d'audit de tiers récent comprenant une évaluation des contrôles et des pratiques de sécurité relatifs à la virtualisation et à la séparation des données de l'utilisateur ;
- le fournisseur de service devrait permettre aux utilisateurs d'effectuer des tests de sécurité (y compris des tests de pénétration) afin d'évaluer l'efficacité des contrôles d'accès mis en place pour garantir la séparation des données des utilisateurs ;

- les processus d'enregistrement des utilisateurs du fournisseur de service devraient permettre d'assurer un niveau de certitude approprié en fonction de la valeur, du niveau de risque et de la sensibilité des informations à enregistrer dans le service cloud ;

Actions suggérées pour répondre à ces considérations :

- L'application de sécurité de la Matrice de Contrôle Cloud : IVS-09, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, ...

Environnements d'exploitation standard

Si le fournisseur de service est pleinement responsable de la configuration et de la gestion appropriées de sa solution SaaS, la responsabilité est partagée entre l'organisme gouvernemental et le fournisseur de service en ce qui concerne les autres modèles de services cloud (c'est-à-dire IaaS et PaaS). Les organismes gouvernementaux qui n'ont pas défini et documenté des normes de conception et de renforcement des systèmes d'exploitation et des applications qu'ils prévoient de déployer dans des services cloud IaaS ou PaaS peuvent rencontrer des difficultés pour protéger efficacement leurs systèmes contre les accès non autorisés.

Si un organisme gouvernemental décide de déléguer la conception et le renforcement des systèmes d'exploitation et des applications au fournisseur de service, il doit déterminer s'il convient d'accepter les normes du fournisseur ou d'en définir d'autres. Quelle que soit l'approche pour laquelle opte l'organisme, il est recommandé de réaliser un test de pénétration afin de s'assurer que les services sont initialement déployés de manière sécurisée.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- des normes appropriées de conception et de renforcement devraient être définies et documentées pour les parties du service gérées par l'organisme gouvernemental ;
- l'organisme gouvernemental devrait déployer des systèmes d'exploitation et des applications conformes aux normes internes de conception ou de renforcement ou mettre en place des normes appropriées de conception et de renforcement qui répondent à ses exigences de sécurité ;
- l'image virtuelle devrait contenir un pare-feu hôte configuré pour autoriser uniquement le trafic trafic d'entrée et de sortie nécessaire à la fourniture du service ;
- le fournisseur de service devrait permettre l'installation d'agents permettant un service hôte de détection et de prévention des intrusions (IDS/IDP) dans les machines virtuelles ;
- le fournisseur de service devrait effectuer des tests réguliers de ses processus et contrôles de sécurité ;
- le service devrait pouvoir être soumis à un test de pénétration afin de garantir qu'il a été déployé de manière sécurisée ;

Actions suggérées pour répondre à ces considérations :

L'application de sécurité de la Matrice de Contrôle Cloud : IVS-02, IVS-07...

Gestion des correctifs et des vulnérabilités

L'amélioration de la gestion des correctifs et des vulnérabilités est régulièrement citée parmi les principaux avantages du passage au cloud. Les vulnérabilités représentent un risque considérable pour tout système d'information, en particulier ceux exposés à l'Internet. L'accès ubiquitaire fourni par les services cloud signifie qu'il est essentiel que les organismes s'assurent que ces services font l'objet de correctifs au moment opportun. Il est important d'identifier la partie qui est responsable de la correction de chaque composant d'un service cloud

(par exemple l'application, le système d'exploitation, le logiciel hyperviseur, l'interface de programmation d'applications [API], etc.). Comme indiqué ci-dessus, le modèle de service cloud (SaaS, PaaS ou IaaS) dicte généralement la partie qui est responsable de la gestion et de la maintenance des composants individuels. Si la responsabilité incombe au fournisseur de service, l'organisme gouvernemental doit veiller à ce que les conditions d'utilisation et l'ANS précisent le délai maximal autorisé entre la sortie d'un correctif par un fournisseur et son application à l'ensemble des systèmes concernés (c.-à-d. la fenêtre d'exposition maximale).

Si la responsabilité du déploiement de correctifs incombe à l'organisme gouvernemental, il convient de s'assurer que ce dernier dispose d'un processus de gestion des correctifs efficace et surveille les sources d'alertes de vulnérabilité appropriées afin de garantir que les correctifs sont identifiés et déployés au moment opportun.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- le fournisseur de service devrait être responsable de l'application de correctifs pour l'ensemble des composants du service cloud ou l'organisme doit identifier les composants qui sont à sa charge et à celle du fournisseur ;
- les conditions d'utilisation ou l'ANS du fournisseur de service devraient comporter des niveaux de service qui incluent une fenêtre d'exposition maximale prédéfinie en ce qui concerne la gestion des correctifs et des vulnérabilités.
- l'organisme devrait disposer d'un processus efficace de gestion des correctifs et des vulnérabilités ;
- l'organisme devrait s'assurer que tous les composants dont il est responsable ont été intégrés dans son processus de gestion des correctifs et des vulnérabilités ;
- l'organisme devrait s'abonner, pour les composants dont il est responsable, aux sources appropriées d'alertes de vulnérabilité et de correctifs ou les surveiller ;
- le fournisseur de service devrait permettre à ses utilisateurs d'effectuer des évaluations régulières de la vulnérabilité ;
- les conditions d'utilisation ou l'ANS devraient comprendre une clause de compensation en cas de violations dues à des vulnérabilités du service ou, au minimum, prévoir une compensation adéquate en cas de violation ;

Actions suggérées pour répondre à ces considérations :

- L'application de sécurité de la Matrice de Contrôle Cloud : TVM-01, TVM-02, TVM-03

Détail des responsabilités relatives à cet objectif de sécurité :

Organisme gouvernemental	Fournisseur de service cloud
• L'organisme gouvernemental devrait demander des informations au fournisseur de service cloud sur la gestion des vulnérabilités techniques susceptibles d'affecter les services cloud fournis. Les agences gouvernementales devraient identifier les vulnérabilités techniques dont elles sont responsables et définir clairement le processus de gestion de celles-ci.	• Le fournisseur de service cloud devrait mettre des informations à la disposition de l'organisme gouvernemental sur la gestion des vulnérabilités techniques susceptibles d'affecter les services cloud fournis.

Cryptage

Le cryptage est souvent présenté comme la solution pour écarter les risques liés à la confidentialité dans le cloud. Cette technique comporte toutefois un certain nombre de limitations majeures que les organismes gouvernementaux devraient comprendre et prendre en compte lorsqu'ils envisagent d'adopter des services cloud. Les organismes gouvernementaux doivent déterminer leurs exigences spécifiques en matière de protection des données à l'aide du cryptage et le cryptage devrait être conforme en fonction du niveau de la catégorie de date défini dans le document « FISP - Catégorisation des données ». Une attention particulière doit être accordée aux points suivants :

- Quelles sont les données qui doivent être cryptées ? Toutes les informations détenues par le service cloud, uniquement certains types de données ou certaines lignes, colonnes ou entités de la base de données ?
- Pourquoi les informations doivent-elles être cryptées ? Par exemple, un cryptage est-il nécessaire afin de respecter une politique ou une norme ?
- Comment les informations devraient-elles être cryptées ? Par exemple, quels protocoles et algorithmes devraient être utilisés ?
- Qui sera responsable du cryptage des données et de la gestion des clés de cryptage ? L'organisme ou le fournisseur de service ?
- À quels endroits les données devraient-elles être cryptées ou non ? Au sein de l'organisme, sur les appareils de l'utilisateur ou dans le service cloud ?
- Quand les données doivent-elles être cryptées ou non ? En transit, par l'application (cryptage des messages) et/ou en inactivité ?

Bien que le cryptage constitue un moyen efficace de protéger la confidentialité des données inactives, pour que les données puissent être traitées selon une règle opérationnelle au sein d'un système d'information, elles doivent généralement être non cryptées. Par conséquent, il peut s'avérer difficile ou impossible de crypter des données stockées dans un service cloud qui traite des informations (par opposition à un simple stockage). Dans le cas où un service cloud est en mesure de stocker des données dans un format crypté, il est important de savoir quelle partie (l'organisme ou le fournisseur de service) est responsable de la gestion des clés de cryptage. Il est important de noter que si le fournisseur de service a accès aux clés de cryptage ou les gère, celui-ci pourra décrypter les informations contenues dans le service cloud et y accéder.

L'interception de données en transit constitue un risque inhérent à chaque fois que des informations sensibles traversent un réseau, en particulier un réseau qui n'est ni détenu ni géré par l'organisme gouvernemental tel qu'Internet ou le réseau d'un fournisseur de service. Les organismes doivent veiller à ce que le service cloud crypte toutes les données sensibles en transit (y compris les données d'authentification) en utilisant uniquement des protocoles et des algorithmes de cryptage approuvés. Les organismes qui ont recours au cryptage devraient déterminer si le protocole et l'algorithme de cryptage ainsi que la longueur de la clé utilisés sont appropriés.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- les exigences relatives au cryptage des informations qui seront enregistrées dans le service cloud devraient avoir été déterminées ;
- la partie responsable de la gestion des clés cryptographiques devrait être spécifiée ;

Actions suggérées pour répondre à ces considérations :

- L'application de sécurité de la Matrice de Contrôle Cloud : EKM-01, EKM-02, EKM-03
- Le document « Guide pour la cryptographie» est également recommandé

Détail des responsabilités relatives à cet objectif de sécurité :

Organisme gouvernemental	Fournisseur de service cloud

• L'organisme gouvernemental devrait mettre en œuvre des contrôles cryptographiques dans le cadre de son utilisation des services cloud lorsque l'analyse de risque le justifie. Les contrôles devraient être suffisamment efficaces pour atténuer les risques identifiés, qu'ils soient réalisés par l'organisme gouvernemental ou le fournisseur de service cloud.
Si le fournisseur de service cloud fournit un service de cryptographie, l'organisme gouvernemental devrait examiner toute information fournie par le fournisseur de service cloud en vue de vérifier si les fonctionnalités cryptographiques :
  • sont conformes aux exigences de la politique de l'organisme gouvernemental ;
  • sont compatibles avec toute autre protection cryptographique utilisée par l'organisme gouvernemental ;
  • s'appliquent aux données inactives et en transit vers, depuis et dans le service cloud.
• L'organisme gouvernemental devrait identifier les clés cryptographiques de chaque service cloud et mettre en œuvre des procédures en matière de clés cryptographiques. Si le service cloud fournit une fonctionnalité de gestion de clés pour l'organisme gouvernemental, ce dernier devrait demander les informations suivantes sur les procédures utilisées pour gérer les clés associées au service cloud :
  • le type de clés ;
  • les spécifications du système de gestion des clés, y compris les procédures pour chaque étape du cycle de vie de la clé, à savoir la création, la modification ou la mise à jour, le stockage, la suppression, la récupération, la conservation et la destruction ;
  • les procédures de gestion des clés que l'organisme gouvernemental est recommandé d'utiliser.
L'organisme gouvernemental ne devrait pas autoriser le fournisseur de service cloud à stocker et à gérer les clés de cryptage dans le cadre d'opérations cryptographiques s'il utilise sa propre gestion de clés ou un service de gestion de clés séparé et distinct.
	• Le fournisseur de service cloud devrait fournir des informations à l'organisme gouvernemental sur les circonstances dans lesquelles il utilise la cryptographie pour protéger les informations qu'il traite. Le fournisseur de service cloud devrait également fournir des informations à l'organisme gouvernemental concernant toutes les fonctionnalités qu'il propose pour aider celui-ci à mettre en œuvre sa propre protection cryptographique.

Menace interne chez le fournisseur de service cloud

L'accès non autorisé à des informations sensibles par les employés du fournisseur de service est une préoccupation commune des organisations qui envisagent d'utiliser des services cloud. Les organismes gouvernementaux devraient vérifier si le fournisseur de service a mis en place des procédures appropriées pour garantir que son personnel est fiable, digne de confiance et ne pose aucun risque de sécurité pour ses utilisateurs. Le niveau d'assurance auquel peuvent prétendre les organismes peut varier considérablement en fonction de la localisation physique du fournisseur de service et de ses employés.

La journalisation et la surveillance des activités des employés constituent un contrôle important afin de gérer les risques liés au personnel malveillant. La journalisation devrait couvrir toutes les activités pertinentes effectuées par les employés du fournisseur de service qui disposent d'un accès logique ou physique à un équipement ou à un média contenant des données utilisateur. Le fournisseur de service devrait surveiller et examiner les fichiers journaux afin d'identifier les activités suspectes qui nécessitent une enquête. De plus, les fonctions devraient être séparées afin de garantir une protection des fichiers journaux contre les modifications et les suppressions non autorisées (p. ex. l'administrateur d'un composant du service ne devrait pas recevoir les droits pour modifier ou supprimer la gestion des informations et des événements de sécurité [SIEM]).

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- le fournisseur de service devrait procéder à un filtrage approprié avant d'embaucher tout membre du personnel ayant accès à des données des utilisateurs ;
- le fournisseur de service devrait effectuer des contrôles constants pendant toute la durée de l'emploi ;
- lorsque le fournisseur de service dépend d'un tiers pour délivrer une partie de son service, il devrait procéder à un filtrage approprié avant d'embaucher tout membre du personnel ayant accès à des données des utilisateurs ;
- le fournisseur de service devrait disposer d'un service SIEM qui effectue une journalisation et une surveillance de tous les accès logiques aux données des utilisateurs ;
- le fournisseur de service devrait imposer une séparation des fonctions afin de s'assurer que les fichiers journaux d'audit sont protégés contre les modifications et les suppressions non autorisées,
- les conditions d'utilisation ou l'ANS devraient contraindre le fournisseur de service à signaler les accès non autorisés de ses employés aux données des utilisateurs ;
- le fournisseur de service devrait être tenu de communiquer aux utilisateurs concernés des informations détaillées sur l'incident afin de permettre à ceux-ci d'évaluer et de gérer l'impact associé ;

Exemples d'actions en vue de répondre aux considérations :

- L'application de sécurité de la Matrice de Contrôle Cloud : HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11
- Le document « Guide pour le logging et le monitoring » est également recommandé

Rémanence des données

Il peut s'avérer difficile de supprimer définitivement des données d'un service cloud à entités multiples lorsque l'entreprise décide de réduire ou de mettre fin à son utilisation du service. Si les données ne sont pas supprimées de manière sécurisée, une compromission future du service peut encore entraîner la divulgation d'informations appartenant à des organismes gouvernementales. Des problèmes similaires se posent lorsque le fournisseur de service ne dispose pas de processus garantissant que le matériel TIC et les médias de stockage (p. ex. disques durs, bandes de sauvegarde, etc.) seront vidés de leur contenu en toute sécurité avant d'être réutilisés ou jetés. Il est

dès lors essentiel que les organisations s'assurent que le fournisseur de service a mis en place des processus de destruction et d'élimination des données performants et démontrables.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- le fournisseur de service devrait disposer d'un processus d'assainissement sécurisé des médias de stockage avant que ceux-ci ne soient mis à la disposition d'un autre utilisateur ;
- le fournisseur de service devrait disposer d'un processus auditable de suppression ou de destruction sécurisée du matériel TIC et des médias de stockage (p. ex. disques durs, bandes de sauvegarde, etc.) qui contient des données des utilisateurs ;

Actions suggérées pour répondre à ces considérations :

L'application de sécurité de la Matrice de Contrôle Cloud : DSI-07, DCS-05

Sécurité physique

Les contrôles de sécurité physiques sont cruciaux pour assurer que les informations sont physiquement protégées contre les accès non autorisés tant du personnel malveillant du fournisseur de service que des tiers. Une sécurité de l'information performante dépend de l'efficacité des contrôles physiques mis en œuvre pour protéger les bureaux, les centres de données et les actifs physiques du fournisseur de service. Cependant, comme mentionné ci-dessus, il se peut qu'il soit difficile ou impossible d'évaluer directement les contrôles physiques que le fournisseur de service a mis en place pour protéger les données de ses utilisateurs au sein d'un service cloud. Un organisme gouvernemental peut être limité à l'examen d'un rapport d'audit de tiers.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- les contrôles de sécurité physique du fournisseur de service devraient être directement examinés ou évalués par l'organisme gouvernemental si les conditions le permettent ou le fournisseur de service doit au moins permettre à l'organisme gouvernemental d'examiner un rapport d'audit de tiers récent qui contient une évaluation de ses contrôles de sécurité physique ;

Actions suggérées pour répondre à ces considérations :

- L'application de sécurité de la Matrice de Contrôle Cloud : DCS-02, DCS-07, DCS-08, DCS-09
- Le document « Guide pour le contrôle et la sécurité des accès physiques» est également recommandé

Détail des responsabilités relatives à cet objectif de sécurité :

Organisme gouvernemental	Fournisseur de service cloud
L'organisme gouvernemental devrait demander au fournisseur de service cloud de confirmer que celui-ci dispose des politiques et des procédures nécessaires à une élimination ou une réutilisation sécurisée des ressources.	Le fournisseur de service cloud devrait s'assurer que des dispositions sont prises pour garantir une élimination ou une réutilisation sécurisée des ressources au moment opportun.

Intégrité

Les canaux d'entrée et de sortie de la solution cloud doivent garantir l'identification de la source et de la destination des données, ainsi que la sécurité de tous les transferts entrants et sortants, de sorte que l'exactitude et la fiabilité des données traitées puissent être garanties de bout en bout. Les fournisseurs de services peuvent proposer des niveaux de protection sensiblement différents contre la perte ou la corruption de données. Certains fournisseurs incluent des services de sauvegarde de données dans leur offre de service de base, d'autres proposent ces services moyennant un coût supplémentaire et d'autres encore n'offrent tout simplement pas cette possibilité (p. ex. Google Apps for Business ne fournit pas de service de sauvegarde sans un abonnement à Google Apps Vault moyennant un coût supplémentaire). Par conséquent, il est important d'identifier le niveau de protection offert par le fournisseur de service et de déterminer s'il répond ou non aux exigences de l'organisme gouvernemental en termes de récupération des données après des incidents entraînant la perte ou la corruption de données.

Les organismes gouvernementaux devraient vérifier le niveau de granularité proposé dans le cadre de la restauration des données (p. ex. un fichier ou un e-mail individuel peut-il être restauré ou les utilisateurs sont-ils limités à la restauration d'une boîte de réception ou d'une base de données entière ?). De plus, ils devraient identifier et comprendre le processus de lancement d'une restauration. Il est important de réaliser que l'utilisation de services cloud n'exclut pas forcément la nécessité pour un organisme d'élaborer, de mettre en œuvre et de tester sa propre stratégie de sauvegarde des données afin de garantir que celui-ci puisse suffisamment se remettre d'un incident entraînant la perte ou la corruption de données. Les canaux d'entrée et de sortie de la solution cloud doivent garantir l'identification de la source et de la destination des données, ainsi que la sécurité de tous les transferts entrants et sortants, de sorte que l'exactitude et la fiabilité des données traitées puissent être garanties de bout en bout.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- le fournisseur de service devrait inclure des services de sauvegarde ou d'archivage contre la perte ou la corruption des données dans son offre de services standard ou doit au moins délivrer des services de sauvegarde ou d'archivage contre la perte ou la corruption des données sous la forme d'une offre de service supplémentaire ;
- il convient de savoir comment les services de sauvegarde et d'archivage des données sont fournis ;
- le service de sauvegarde ou d'archivage des données devrait répondre aux exigences opérationnelles en matière de protection contre la perte de données ;
- le niveau de granularité qu'offre le fournisseur de service pour la restauration des données devrait être clairement défini ;
- le processus de lancement d'une restauration du fournisseur de service devrait être clairement défini ;
- le fournisseur de service devrait effectuer des tests de restauration réguliers afin de s'assurer que les données peuvent être récupérées à partir d'un média de sauvegarde ;
- l'organisme gouvernemental devrait mettre en place une stratégie de sauvegarde des données afin de s'assurer qu'il peut effectuer une restauration après un incident entraînant la perte ou la corruption de données ;

Actions suggérées pour répondre à ces considérations :

- Le contrôle de sécurité de la Matrice de Contrôle Cloud : IVS-02, IVS-07

Détail des responsabilités relatives à cet objectif de sécurité :

Organisme gouvernemental	Fournisseur de service cloud
• Si le fournisseur de service cloud propose une fonctionnalité de sauvegarde dans son offre de service cloud, l'organisme gouvernemental devrait demander les spécifications de la fonctionnalité de sauvegarde au fournisseur de service cloud. Le service cloud devrait également vérifier qu'il répond aux exigences de l'organisme en matière de sauvegarde. L'organisme gouvernemental est responsable de la mise en œuvre de fonctionnalités de sauvegarde si le fournisseur de service cloud n'en propose pas.	• Le fournisseur de service cloud devrait mettre des informations à la disposition de l'organisme gouvernemental sur la gestion des vulnérabilités techniques susceptibles d'affecter les services cloud fournis. Le fournisseur de service cloud devrait transmettre les spécifications de ses fonctionnalités de sauvegarde à l'organisme gouvernemental. Les spécifications devraient contenir les informations suivantes, selon le cas : • portée et programmation des sauvegardes ; • méthodes de sauvegarde et formats de données, y compris en ce qui concerne le cryptage, le cas échéant ; • délais de conservation des données de sauvegarde ; • procédures de vérification de l'intégrité des données de sauvegarde ; • procédures et durée nécessaires à la restauration des données à partir d'une sauvegarde ; • procédures de test des fonctionnalités de sauvegarde ; • emplacement de stockage des sauvegardes. Le fournisseur de service cloud devrait fournir un accès sécurisé et séparé aux sauvegardes, telles que des instantanés virtuels, si un tel service est proposé aux organismes gouvernementaux.

La répartition des responsabilités en ce qui concerne la création de sauvegardes dans l'environnement de cloud computing est souvent peu précise. Dans le cas d'une infrastructure IaaS, la responsabilité de créer des sauvegardes incombe généralement à l'organisme gouvernemental. Toutefois, un organisme gouvernemental peut ne pas être conscient de la responsabilité qui lui incombe de sauvegarder toutes les données qu'il a générées dans le système de cloud computing, notamment des fichiers exécutables issus de l'utilisation des fonctionnalités de développement d'un service PaaS.

Il se peut que différents niveaux de sauvegarde et de restauration soient proposés sous la forme d'un service supplémentaire payant. Dans ce cas, le contenu et la programmation des sauvegardes sont laissés à la discrétion des organismes gouvernementaux.

Disponibilité

Accord de niveau de service

Il est important que les organismes comprennent exactement ce que signifie le pourcentage défini et évaluent si ces niveaux répondent ou non aux exigences en matière de disponibilité. L'ANS devrait inclure les détails de toute période d'interruption planifiée. Cela permettra de garantir que le fournisseur de service ne pourra pas planifier de longues interruptions (y compris des interruptions d'urgence) avec peu ou pas de notification sans enfreindre l'ANS.

Si des périodes d'interruption planifiées sont définies dans l'ANS, celles-ci devraient être examinées afin de garantir qu'elles n'auront pas d'effet négatif sur les activités opérationnelles.

Une autre considération importante réside dans la pertinence de la compensation fournie en cas de violation de l'ANS et la méthode de calcul des pénalités relatives à une période de service. En règle générale, l'ANS de services cloud fera état d'une compensation minimale sous la forme de crédits supplémentaires ou de factures à prix réduit. Les organismes gouvernementaux devraient examiner toute clause de compensation en tenant compte de l'impact d'une interruption de service sur les activités afin de déterminer si le niveau de réparation est suffisant.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- l'ANS devrait inclure un pourcentage de performance attendu et minimal en termes de disponibilité sur une période clairement définie ;
- les exigences opérationnelles en matière de disponibilité devraient être satisfaites ;
- l'ANS devrait inclure une clause de compensation en cas de violation des pourcentages de disponibilité garantis ;

Actions suggérées pour répondre à ces considérations :

- Un guide pratique sur les Contrats de service cloud V3.0 : https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-service-agreements.htm
- Contrats de service cloud public : À quoi s'attendre et que négocier V2.0 : https://www.omg.org/cloud/deliverables/public-cloud-service-agreements-what-to-expect-and-what-to-negotiate.htm

Attaques par déni de service

Les attaques par déni de service (DoS) constituent un risque inhérent à tous les services liés à l'Internet. L'utilisation de services cloud peut augmenter le risque qu'une telle attaque se produise dans la mesure où le regroupement de plusieurs organismes sur un même service peut constituer une cible plus attractive pour les attaquants. De même, un organisme gouvernemental peut subir des dommages consécutifs ou collatéraux lors d'une attaque contre un fournisseur de service ou une autre de ses entités.

Une attaque DoS peut être lancée contre le fournisseur de service ou l'organisme lui-même. L'utilisation de services cloud peut atténuer l'impact de certaines formes d'attaques DoS dans la mesure où les fournisseurs de services disposent d'une bande passante réseau et d'une capacité informatique de réserve. De plus, certains fournisseurs de services utilisent des protocoles et des technologies (p. ex. Anycast, Application Delivery Networks et Content Delivery Networks) ainsi que des centres de données géographiquement dispersés pour répartir le trafic réseau et le traitement informatique à travers le monde. La nature élastique des services cloud peut également avoir des conséquences financières.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- le fournisseur de service devrait utiliser des protocoles et des technologies capables d'assurer une protection contre les attaques DoS ;
- l'organisme gouvernemental devrait préciser ou configurer des limites d'utilisation des ressources afin d'assurer une protection contre les EDoS/mauvaises surprises à la réception de la facture ;

Actions suggérées pour répondre à ces considérations :

- Le contrôle de sécurité de la Matrice de Contrôle Cloud : IVS-13

Disponibilité et performance réseau

La disponibilité et la performance des services cloud dépendent fortement de l'infrastructure réseau sous-jacente. Les organismes gouvernementaux devraient évaluer la connectivité du réseau entre leurs utilisateurs et le service cloud afin de s'assurer que les exigences en matière de disponibilité et de performance sont satisfaites. Les organismes gouvernementaux devraient s'assurer que les services réseau qu'ils gèrent directement ou auxquels ils sont abonnés offrent un niveau de disponibilité et de bande passante suffisant ainsi qu'une latence et une perte de paquets suffisamment basses pour répondre aux besoins opérationnels.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- les services réseau gérés directement par l'organisme gouvernemental ou auxquels celui-ci est abonné devraient fournir un niveau de disponibilité suffisant ;
- les services réseau gérés directement par l'organisme gouvernemental ou auxquels celui-ci est abonné devraient fournir un niveau adéquat de redondance/tolérance aux pannes ;
- les services réseau gérés directement par l'organisme gouvernemental ou auxquels celui-ci est abonné devraient fournir un niveau adéquat de bande passante (sur l'ensemble du réseau)
- la latence entre le(s) réseau(x) de l'organisme gouvernemental et le service du fournisseur devrait être suffisamment acceptable pour permettre de fournir l'expérience utilisateur souhaitée ou la latence doit au moins se produire sur les services réseau directement gérés par l'organisme gouvernemental ou auxquels celui-ci est abonné ;
- la perte de paquets entre le(s) réseau(x) de l'organisme et le service du fournisseur devrait être suffisamment acceptable pour permettre de fournir l'expérience utilisateur souhaitée ou la perte de paquets doit au moins se produire sur les services réseau directement gérés par l'organisme gouvernemental ou auxquels celui-ci est abonné ;

Actions suggérées pour répondre à ces considérations :

- Le contrôle de sécurité de la Matrice de Contrôle Cloud : BRC-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, IVS-04

Continuité de l'activité et reprise après catastrophe

Le fournisseur de service doit disposer de plans appropriés et l'organisme gouvernemental doit comprendre le niveau de continuité et de reprise proposé pour le fournisseur. Il est également important de réaliser que l'utilisation de services cloud n'exclut pas la nécessité pour un organisme gouvernemental d'élaborer, de mettre en œuvre et de tester ses propres plans de continuité de l'activité et de reprise après catastrophe afin de s'assurer que celui-ci puisse continuer à fonctionner en cas d'interruption du service.

Les organismes gouvernementaux devraient veiller à ce que le fournisseur de service utilise des normes de formatage des données communes ou de facto et propose une méthode d'extraction des données dans un format qu'ils peuvent utiliser.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- le fournisseur de service devrait disposer de plans de continuité de l'activité et de reprise après catastrophe ;
- le fournisseur de service devrait permettre à l'organisme d'examiner ses plans de continuité de l'activité et de reprise après catastrophe ;
- les plans du fournisseur de service devraient couvrir la restauration des données de l'organisme ou uniquement la restauration du service ;
- les plans du fournisseur de service devraient couvrir la restauration des données de l'organisme et la restauration des données de l'utilisateur doit constituer une priorité ;
- il devrait être clairement défini si les utilisateurs sont classés par ordre de priorité en fonction de la taille et de la valeur du contrat ;
- le fournisseur de service devrait effectuer un test formel de ses plans de continuité de l'activité et de reprise après catastrophe ;
- la fréquence à laquelle de tels tests sont effectués devrait être clairement définie ;
- il devrait être clairement défini si le fournisseur de service proposera une copie des rapports connexes aux utilisateurs ;
- l'organisme gouvernemental devrait avoir mis en place son propre plan de continuité de l'activité et de reprise après catastrophe pour s'assurer qu'il peut se remettre d'une interruption de service dans le cas où le fournisseur de service devait interrompre ses activités ou mettre un terme au service ;
- l'organisme gouvernemental devrait disposer de sa propre stratégie de sauvegarde des données pour s'assurer qu'il peut se remettre d'une interruption de service dans le cas où le fournisseur de service devait interrompre ses activités ou mettre un terme au service ;
- les sauvegardes (qu'elles soient effectuées par le fournisseur de service ou l'organisme) devraient être cryptées au moyen d'un algorithme de cryptage approuvé et d'une longueur de clé appropriée ;

Actions suggérées pour répondre à ces considérations :

- Le contrôle de sécurité de la Matrice de Contrôle Cloud : BRC-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11

Intervention et gestion en cas d'incidents

Les agences gouvernementales doivent pouvoir assurer avec suffisamment de certitude qu'un fournisseur de service est en mesure d'intervenir de manière effective et efficace en cas d'incident de sécurité de l'information, car même les contrôles préventifs les plus méticuleusement planifiés, mis en œuvre et gérés peuvent ne pas suffire à éviter les risques. Par conséquent, les organismes gouvernementaux doivent examiner les conditions d'utilisation et l'ANS du fournisseur de service afin d'identifier le support que celui-ci fournit à ses utilisateurs en cas d'incident de sécurité de l'information.

Quel que soit le service ou le mode de déploiement, l'utilisation de services cloud n'exclut pas la nécessité pour un organisme gouvernemental de disposer de ses propres processus et plans d'intervention et de gestion en cas d'incidents.

Les considérations à prendre en compte afin de réaliser cet objectif de sécurité sont les suivantes :

- le fournisseur de service devrait disposer d'un processus et de plans d'intervention et de gestion formels en cas d'incidents qui définissent clairement la manière dont il détecte les incidents de sécurité de l'information et y répondent ;
- il devrait fournir à l'organisme une copie de leur processus et de leurs plans afin de permettre à celui-ci de déterminer s'ils sont suffisants ;
- le fournisseur de service devrait régulièrement tester et affiner son processus et ses plans d'intervention et de gestion en cas d'incidents ;
- le fournisseur de service devrait faire appel à la participation de ses utilisateurs lors du test de ses processus et plans d'intervention et de gestion en cas d'incidents ;
- le fournisseur de service devrait dispenser une formation appropriée à son personnel en matière de processus et des plans d'intervention et de gestion en cas d'incidents afin de garantir une réaction efficace et efficiente en cas d'incidents ;
- les conditions d'utilisation ou les ANS du fournisseur de service devraient clairement définir le soutien que celui-ci apportera à l'organisme en cas d'incident de sécurité de l'information. Par exemple, le fournisseur de service devrait :
    - Avertir l'organisme gouvernemental lorsqu'un incident susceptible de compromettre la sécurité de ses informations ou de ses systèmes interconnectés a été détecté ou signalé ;
    - Indiquer un point de contact et un canal permettant aux utilisateurs de signaler de potentiels incidents de sécurité de l'information ;
    - Définir les rôles et les responsabilités de chaque partie en cas d'incident de sécurité de l'information ;
    - Fournir aux utilisateurs un accès aux preuves (p. ex. fichiers journaux d'audit horodatés et/ou instantanés légaux de machines virtuelles, etc.) pour leur permettre de mener leur propre enquête sur l'incident ;
- une partie responsable de la restauration des données et des services après un incident de sécurité de l'information devrait être identifiée ;
- les rapports post-incident devraient être partagés avec les utilisateurs concernés afin de leur permettre de comprendre la cause de l'incident et de décider en toute connaissance de cause s'ils continuent à utiliser le service cloud ;

- le contrat devrait préciser les limites et des dispositions en termes d'assurance, de responsabilité et d'indemnisation en cas d'incidents de sécurité de l'information ; (Remarque : il est recommandé aux organismes d'examiner attentivement si les clauses relatives à la responsabilité et à l'indemnisation comportent des exclusions.)

Actions suggérées pour répondre à ces considérations :

- L'application de sécurité de la Matrice de Contrôle Cloud suivante : SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-02, BCR-O2

Détail des responsabilités relatives à cet objectif de sécurité :

Organisme gouvernemental	Fournisseur de service cloud

• L'organisme gouvernemental devrait vérifier la répartition des responsabilités en termes de gestion des incidents de sécurité de l'information et veiller à ce que celle-ci réponde à ses exigences.
• L'organisme gouvernemental devrait demander des informations au fournisseur de service cloud sur les mécanismes permettant :
  • à l'organisme gouvernemental de signaler au fournisseur de service cloud les événements liés à la sécurité de l'information qu'il a détectés ;
  • au fournisseur de service cloud de signaler à l'organisme gouvernemental les événements liés à la sécurité de l'information qu'il a détectés ;
  • à l'organisme gouvernemental de suivre l'état d'un événement lié à la sécurité de l'information signalé.
• L'agence gouvernementale et le fournisseur de service cloud devraient s'entendre sur les procédures à suivre pour répondre aux demandes de preuves numériques ou d'autres informations éventuelles issues de l'environnement de cloud computing.
	• « Dans les spécifications du service, le fournisseur de service cloud devrait définir la répartition des responsabilités et des procédures en matière de gestion des incidents de sécurité de l'information entre l'organisme gouvernemental et le fournisseur de service cloud.
	Le fournisseur de service cloud devrait fournir à l'organisme gouvernemental une documentation couvrant :
	  • la portée des incidents de sécurité de l'information que le fournisseur de service cloud va signaler à l'organisme gouvernemental ;
	  • le niveau de divulgation relatif à la détection des incidents de sécurité de l'information et les interventions y associées ;
	  • l'intervalle de temps cible dans lequel des notifications relatives aux incidents de sécurité de l'information seront émises ;
	  • la procédure de notification des incidents de sécurité de l'information ;
	  • les informations de contact relatives au traitement des problèmes liés à des incidents de sécurité de l'information ;
	  • toute solution pouvant être apportée lorsque certains incidents de sécurité de l'information se produisent.
	• Le fournisseur de service cloud devrait prévoir des mécanismes permettant :
	  • à l'organisme gouvernemental de signaler au fournisseur de service cloud un événement lié à la sécurité de l'information ;
	  • au fournisseur de service cloud de signaler à un organisme gouvernemental un événement lié à la sécurité de l'information ;
	  • à l'organisme gouvernemental de suivre l'état d'un événement lié à la sécurité de l'information signalé.
	• L'agence gouvernementale et le fournisseur de service cloud devraient s'entendre sur les procédures à suivre pour répondre aux demandes de preuves numériques ou d'autres informations éventuelles issues de l'environnement de cloud computing.

Gestion du document

Historique

Date	*Auteur*	*Version*	*Description des modifications*
17/09/2019	BOSA	V.0.1	Première ébauche
5/10/2019	BOSA	V.1	Mise à jour sur la base de commentaires du groupe de travail FISP
16/10/2019	BOSA	V.1.1	Mise à jour sur la base de commentaires de participants FISP
21/11/2019	FISP workgroup	V1.2	Distribution publique

Approbations

Date	*Approbateur(s)*	*Version*
10/10/2019	FISP Workgroup	V1.2

Sources

Ce document a été rédigé à l'aide des sources suivantes :

- https://www.digital.govt.nz/dmsdocument/1-cloud-computing-information-security-and-privacy-considerations
- https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/
- Guide GEA-NZ : Gestion des services de shadow cloud
- DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union
- Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique
  http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2019040715&table_name=loi
- RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
  https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=NL
- Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
  https://www.timelex.eu/sites/default/files/pdf/Nieuwe-belgische-privacywet-30-07-2018.pdf
- ISO/IEC 27017/27018

Lien avec d'autres politiques

Dépendance de documents internes

Réf.	*Titre*
FISPDOC01	Guide pour la catégorisation des informations

Positionnement de la politique par rapport à la norme ISO 27001

Section	*Objectifs et mesures de référence*	*En relation (X = Oui)*
4	Contexte de l'organisation	
5	Leadership	
6	Planification	
7	Support	
8	Fonctionnement	
9	Évaluation des performances	
10	Amélioration	

Positionnement de la politique par rapport à la norme ISO 27002

Section	*Objectifs et mesures de référence*	*En relation (X = Oui)*	*Objectifs/Mesures (Détail)*
A5	Politique de sécurité de l'information		
A6	Organisation de la sécurité de l'information		
A7	Sécurité des ressources humaines		
A8	Gestion des actifs		
A9	Contrôle d'accès		
A10	Cryptographie		
A11	Sécurité physique et environnementale		
A12	Sécurité liée à l'exploitation		
A13	Sécurité des communications		
A14	Acquisition, développement et maintenance des systèmes d'information		
A15	Relations avec les fournisseurs		
A16	Gestion des incidents liés à la sécurité de l'information		
A17	Sécurité de l'information dans la gestion de la continuité de l'activité		
A18	Conformité		