Volet Infrastructures

# Guide de l'infonuagique

**Volume 3 - Considérations de contrôle et de sécurité**

## Architecture d'entreprise gouvernementale 3.1

Québec

Volet Infrastructures

# Guide de l'infonuagique

**Volume 3 - Considérations de contrôle et de sécurité**

# Architecture d'entreprise gouvernementale 3.1

**« Pour une utilisation responsable de l'infonuagique au gouvernement du Québec »**

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite en collaboration avec la Direction des communications
du Secrétariat du Conseil du trésor.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
5e étage, secteur 500
875, Grande Allée Est
Québec (Québec)  G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – mars 2015
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-72559-6 (en ligne)

# Table des matières


LISTE DES SIGLES ET ACRONYMES ____ II

HISTORIQUE DES VERSIONS ____ IV

AVIS ____ V

AVANT-PROPOS ____ V

1. INTRODUCTION ____ 1

1.1 Objectifs et portée du guide ____ 1

1.2 Présentation du contenu des documents sur l'infonuagique ____ 2

2. CONSIDÉRATIONS SUR LE CONTRÔLE ET LA SÉCURITÉ ____ 3

3. PRINCIPAUX RISQUES ASSOCIÉS À L'INFONUAGIQUE ____ 3

3.1 Risques liés à la gestion ____ 4

3.2 Risques financiers ____ 5

3.3 Risques d'interopérabilité ____ 6

3.4 Risques de sécurité ____ 7

4. EXIGENCES DE CONTRÔLE ET DE SÉCURITÉ ____ 11

5. PRATIQUES DE CONTRÔLE ET DE SÉCURITÉ À ADAPTER ____ 19

5.1 Pratiques administratives ____ 19

5.2 Pratiques en ressources informationnelles ____ 20

5.3 Pratiques en sécurité de l'information ____ 20

6. POSSIBILITÉS OFFERTES PAR L'INFONUAGIQUE EN MATIÈRE DE SÉCURITÉ ____ 25

7. DÉFI DE L'INFONUAGIQUE : LA CONFIANCE ____ 26

ANNEXE I – CADRE DE GESTION DES RISQUES ADAPTÉ À L'INFONUAGIQUE ____ 27

ANNEXE II – CRITÈRES D'ANALYSE POUR LA SÉLECTION D'UN SERVICE INFONUAGIQUE 29

ANNEXE III – LISTE DE VÉRIFICATION RELATIVE À LA PRÉSENCE DE CLAUSES PORTANT SUR LA SÉCURITÉ ____ 30

RÉFÉRENCES ____ 37

# Liste des sigles et acronymes

| | |
|---|---|
| API | *Application Programming Interface* |
| AIPRP | Accès à l'information et protection des renseignements personnels |
| CARRA | Commission administrative des régimes de retraites et d'assurances |
| COBIT | *Control Objectives for Information and related Technology* |
| CPU | *Central Processing Unit* |
| CSA | *Cloud Security Alliance* |
| CSPQ | Centre de services partagés du Québec |
| CSST | Commission de la santé et de la sécurité du travail |
| DIC | Disponibilité, intégrité, confidentialité |
| GIA | Gestion de l'identité et des accès |
| HSM | *Hardware Security Module* |
| HTTP | *HyperText Transport Protocol* |
| IAAS | *Infrastructure as a Service* |
| ISACA | *Information Systems Audit and Control Association* |
| ISO | *International Organization for Standardization* |
| ITIL | *Information Technology Infrastructure Library* |
| MAMROT | Ministère des Affaires municipales, des Régions et de l'Occupation du territoire |
| MAPAQ | Ministère de l'Agriculture, des Pêcheries et de l'Alimentation du Québec |
| MCE | Ministère du Conseil exécutif |
| MESS | Ministère de l'Emploi et de la Solidarité sociale |
| MJQ | Ministère de la Justice du Québec |
| MTQ | Ministère des Transports du Québec |
| OP | Organisme public |
| OWASP | *Open Web Application Security Project* |
| PAAS | *Platform as a Service* |

| | |
|---|---|
| PA-DSS | *Payment Application Data Security Standard* |
| PCI-DSS | *Payment Card Industry Data Security Standard* |
| PRP | Protection des renseignements personnels |
| RAMQ | Régie de l’assurance maladie du Québec |
| REST | *Representational State Transfer* |
| ROSI | Responsable organisationnel de la sécurité de l’information |
| RPV | Réseau privé virtuel |
| RRQ | Régie des rentes du Québec |
| SAAS | *Software as a Service* |
| SCT | Secrétariat du Conseil du trésor |
| SOAP | *Simple Object Access Protocol* |

# Historique des versions

| Version de l'AEG | Statut | Modifications |
|---|---|---|
| 3.0 | Novembre 2014 | Publication de la première édition |
| 3.1 | Mars 2015 | Aucune modification |

La version en vigueur est disponible à cette adresse :

http://www.tresor.gouv.qc.ca/ressources-informationnelles/architecture-dentreprise-gouvernementale/

# Avis

Le présent document intitulé Guide de l'infonuagique - Volume 3 ne constitue pas un manuel de gestion de sécurité de l'information ni un avis juridique, et il ne peut prétendre se substituer aux textes et aux lois en vigueur. Nous invitons les organismes publics à adresser leurs commentaires et leurs suggestions afin d'améliorer ce guide au Sous-secrétariat du dirigeant principal de l'information, responsable de son élaboration.

Le terme « organisme public » (OP) est utilisé selon la désignation qui en est faite dans la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement. Cependant, l'utilisation de ce guide peut être élargie à d'autres organisations telles que les entreprises du gouvernement et les municipalités.

Ce document sera révisé périodiquement.

# Avant-propos

Au cours des dernières décennies, l'apport des technologies de l'information (TI) pour les organismes publics (OP) a été indéniable. Levier de transformation organisationnelle par excellence, elles ont permis des améliorations notables au regard de la prestation de services aux citoyens.

Notion relativement récente, l'infonuagique (*cloud computing*) présenterait aussi des possibilités avantageuses pour les OP dans la gestion de leurs ressources informationnelles (RI) : possibilités de mise en commun, de partage, de réutilisation, entraînant agilité, économies d'échelle, etc.

Aux avantages qu'offre cette nouvelle façon d'acquérir des ressources en TI, s'opposent, comme c'est le cas lors de l'avènement de nouvelles technologies, certaines préoccupations. En effet, cette notion est encore méconnue et parfois même, sujette à appréhension, en raison notamment de la perception des risques qu'elle suscite. La protection des renseignements personnels et la sécurité des données figurent parmi les préoccupations liées à cette solution. Bien que réels, ces risques peuvent néanmoins être circonscrits et maîtrisés de différentes façons et permettre ainsi que la confiance du public envers les organismes qui y ont recours soit maintenue.

Ce document constitue un outil de référence pour l'OP qui envisage d'avoir recours à l'infonuagique. Dans l'élaboration de ses besoins, l'organisme devra déterminer quel service infonuagique et quel mode de déploiement conviennent le mieux. Selon les réponses obtenues, il pourra, si nécessaire, aborder de multiples approches pour faire face aux risques que peut présenter cette technologie, comme appliquer différents niveaux de sécurité en fonction de la sensibilité des données hébergées, ou préférer l'utilisation d'un « nuage privé », géré à l'interne ou par un prestataire, pour n'en nommer que quelques-unes.

Les utilisateurs de ce guide doivent garder à l'esprit qu'il n'existe pas de recette unique pour assurer la sécurité de l'information. Les modèles de services (infrastructure, plateformes de développement, logiciels, etc.), les modes de déploiement (privé, public, communautaire, hybride) et l'ampleur des projets peuvent être si variables que les mesures de mitigation des risques sont propres à chaque projet, en fonction du contexte de chaque organisation. Ce guide permettra néanmoins d'informer les parties prenantes sur les enjeux communs, notamment en ce qui a trait au contrôle, à la protection des renseignements personnels ou confidentiels, à la sécurité de l'information et au processus de négociation et de gestion des contrats de services infonuagiques.

Afin d'assurer une utilisation responsable de l'infonuagique, l'adoption graduelle devrait être préconisée pour la mise en place de ce nouveau mode de prestation en TI. Ceci permettra aux organismes, projet après projet, d'en évaluer les bénéfices, de s'approprier les nouveaux paramètres applicables aux

différentes solutions en constante évolution et, finalement, de développer l'expertise nécessaire à la réussite de leurs projets futurs.

Le présent guide de référence de l'infonuagique a été réalisé avec la collaboration de rédacteurs représentant plusieurs OP dont voici la liste :

| | | | |
|---|---|---|---|
| Claude Côté | MCE | Stéphane Fleurant | CSPQ |
| Ghyslain Garceau | MTQ | Stéphane Turcotte | RAMQ |
| Jean Rhéaume | SCT | Sylvain Levasseur | CSST |
| Nanette Maestre | RRQ | | |

Ce document a fait l'objet d'un cycle de validation par les intervenants suivants :

| | | | |
|---|---|---|---|
| Christian Boisvert | MJQ | Marc Bellavance | MAPAQ |
| Daniel Bouchard | MTQ | Patrick Boisvert | CARRA |
| Éric Gagnon | MAPAQ | Pierrette Brie | MESS |
| Fernande Rousseau | MCE | Stéphane Asselin | CSPQ |
| Ghislain Dubé | MJQ | Yvan Boulet | MAPAQ |
| Hugues Beaudoin | RAMQ | Yvon Gagné | MAPAQ |
| Jean-François Ducré-Robitaille | MAMROT | | |

# 1. Introduction

L'infonuagique (*cloud computing*) constitue une tendance mondiale en matière d'acquisition de services technologiques dont l'un des objectifs est de diminuer les coûts d'exploitation des infrastructures technologiques et des applications. Il s'agit d'un nouveau mode d'acquisition qui permet aux individus et aux organisations d'accéder, par les technologies d'Internet, à un bassin de ressources informatiques configurables, externalisées et qui sont proposées sous forme de services. Ce nouveau mode de livraison de services permet aux consommateurs de s'approvisionner en services de technologies de l'information (TI) auprès d'un prestataire infonuagique de façon automatisée et sur demande. La consommation des services est mesurée et facturée selon l'utilisation. L'infonuagique procure plusieurs avantages et bénéfices aux utilisateurs. En effet, les ressources infonuagiques offrent une agilité et une flexibilité à l'utilisation, puisqu'elles s'acquièrent rapidement, s'adaptent facilement à la demande et permettent un délestage tout aussi rapide. De plus, l'infonuagique présente des possibilités de faire des économies substantielles, puisqu'elle favorise une meilleure utilisation des infrastructures technologiques, réduisant les coûts en capitalisation, en exploitation et en entretien à l'échelle gouvernementale.

Plusieurs gouvernements, dont ceux des États-Unis, du Royaume-Uni et de l'Australie, considèrent que l'infonuagique est un levier de transformation et d'économie important. D'ailleurs, ces pays ont mis sur pied des stratégies d'adoption et leurs initiatives infonuagiques gouvernementales sont nombreuses. Toutefois, malgré les possibilités intéressantes qu'offre l'infonuagique, il existe des préoccupations et des risques inhérents à son utilisation, tant sur le plan juridique qu'en ce qui a trait à la protection des renseignements personnels (PRP), à la sécurité des données et au contrôle de gestion.

Afin de bien tirer profit des bénéfices et de saisir pleinement les possibilités rattachées à l'infonuagique, le dirigeant principal de l'information (DPI) a mandaté un groupe de travail interministériel dont l'objectif consistait à réaliser ce guide de référence fournissant l'information nécessaire pour une utilisation responsable de l'infonuagique et un ensemble de bonnes pratiques en la matière.

## 1.1 Objectifs et portée du guide

Compte tenu de l'intérêt croissant pour l'infonuagique au sein des organisations, ce guide vise à fournir des informations pertinentes aux OP qui désirent recourir à de tels services et leur permettre d'encadrer cette pratique de façon appropriée et sécuritaire. Ce guide vise, entre autres, les objectifs suivants :

- ✓ La prise en compte des enjeux et des risques en matière de contrôle et de sécurité qui sont associés au projet dès les premières étapes d'analyse préliminaire ou d'étude d'opportunité et tout au long de sa réalisation;
- ✓ Le respect des exigences en matière de contrôle, de sécurité et de protection des renseignements personnels ou autrement confidentiels.

Ce guide peut être utilisé par les différents intervenants d'un projet lorsque l'OP envisage de recourir à des services infonuagiques. Il est destiné à les accompagner dans leur démarche d'analyse, d'évaluation et d'encadrement légal et administratif. Son utilisation facilitera la prise de décision quant à l'opportunité de recourir à des services infonuagiques et aux mesures à mettre en place pour en assurer une utilisation responsable et sécuritaire.

Enfin, ce guide met l'accent sur les éléments particuliers à considérer dans le cas de recours à des services infonuagiques. Il ne traite pas de façon exhaustive de toutes les considérations en matière de contrôle ou de sécurité ni des normes et des bonnes pratiques qui s'appliquent à tout projet en ressources informationnelles réalisé par un OP. Il y aura donc lieu de s'assurer que ces divers éléments sont pris aussi en compte dans le projet ciblé.

## 1.2 Présentation du contenu des documents sur l'infonuagique

Le Guide de référence de l'infonuagique est composé de quatre volumes :

Le présent fascicule, intitulé Volume 3 – Considérations de contrôle et de sécurité, approfondit différents enjeux relatifs au contrôle et à la sécurité. Ce guide a notamment pour objectif d'aider les différents OP dans leurs définitions des exigences et des clauses de contrôle et de sécurité à inclure dans leurs processus d'abonnement à un service infonuagique. Les objectifs sont de déterminer et de maintenir le niveau de contrôle et de sécurité adéquat, permettant aux OP de continuer à se conformer à leurs cadres normatif et législatif, et de voir au respect de leurs besoins et objectifs d'affaires en matière de contrôle et de sécurité de l'information.

Quant aux autres volumes (1, 2 et 4) du guide de référence, ils approfondissent différents sujets relatifs à l'infonuagique. Ils présentent, notamment, les notions fondamentales de l'infonuagique, une démarche d'adoption avec ses grandes étapes pour recourir à un service infonuagique ainsi que les principaux facteurs de succès à considérer pour tirer pleinement profit des bénéfices liés à l'infonuagique (volume 1), les considérations liées à l'aspect juridique et à la protection des renseignements personnels (volume 2) et celles en matière de gestion contractuelle (volume 4). Ils ont été développés dans le but d'outiller et d'orienter les décideurs, les gestionnaires de projets et les conseillers en architecture, les spécialistes juridiques ainsi que ceux du contrôle, de la sécurité et de la gestion contractuelle des organismes publics dans l'analyse et l'évaluation des possibilités et des risques, ou dans la rédaction d'un appel d'offres ou l'adoption de nouvelles pratiques adaptées à l'infonuagique.

Parallèlement aux travaux d'élaboration du guide de référence de l'infonuagique, le gouvernement du Québec a mandaté le Centre de recherche en droit public de l'Université de Montréal pour réaliser deux études.

La première, intitulée Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec, se veut une analyse des risques et des contraintes juridiques associés à l'infonuagique. Outre les éléments juridiques qui y sont soulevés, notamment ceux relatifs à la sécurité de l'information dans le contexte d'un service infonuagique, il est important de considérer l'ensemble des principes et des obligations de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. À cet égard, il y aura lieu de se référer au responsable de l'accès à l'information et protection des renseignements personnels (AIPRP) de chaque organisme.

La seconde, sous le titre Étude sur les risques et contraintes juridiques associés au chiffrement des données (cryptographie), se concentre principalement sur l'utilisation du chiffrement dans le cadre de la transmission ou de l'hébergement de données dans un contexte de services infonuagiques. Elle pousse l'examen plus loin en abordant plus largement le chiffrement des données transmises ou hébergées dans d'autres contextes bien définis (échange de courriels, etc.). Cette étude sera disponible à la fin 2014.

# 2. Considérations sur le contrôle et la sécurité

La maturité grandissante des offres du marché est susceptible de conduire de nombreux OP vers l'infonuagique. Puisque les organisations se tournent vers l'infonuagique pour fournir des services informatiques habituellement gérés à l'interne, elles doivent réaliser certaines modifications pour contrôler la bonne réalisation de leurs objectifs de performance, l'alignement stratégique de leur activité et de leur niveau technologique, ainsi que la gestion des risques.

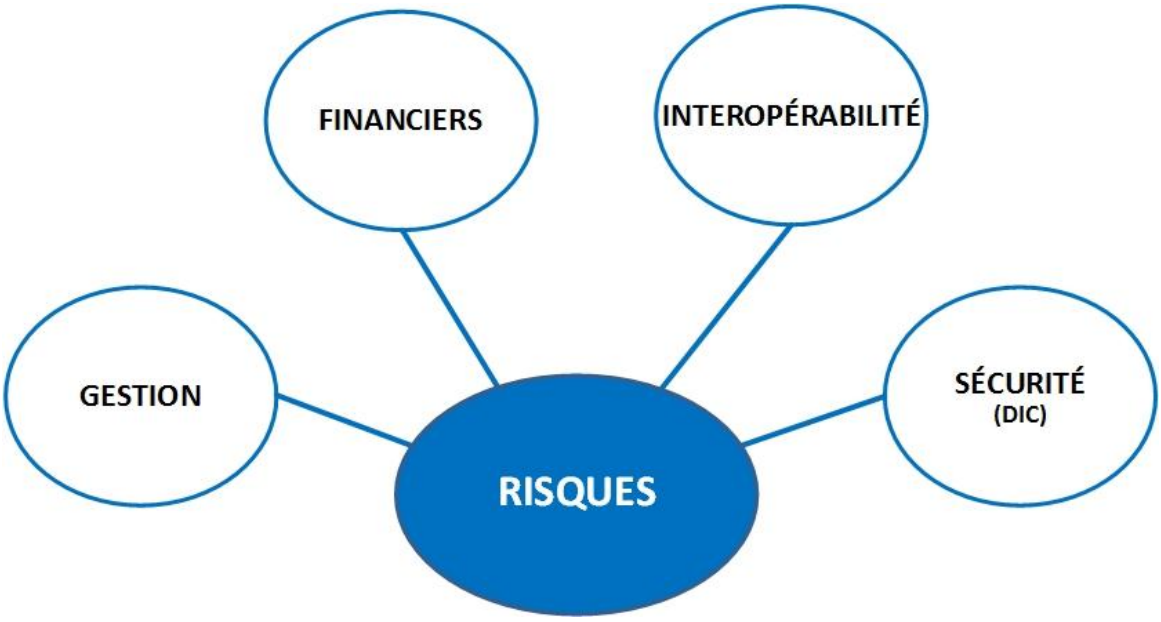
L'infonuagique offre des avantages aux OP, mais ceux-ci sont toutefois accompagnés de préoccupations au chapitre du contrôle, de la sécurité et de la protection des renseignements personnels ou autrement confidentiels. Dans n'importe quel environnement, et plus encore dans une relation avec une tierce partie, il est difficile de s'assurer que les technologies de l'information sont alignées sur l'activité, que les systèmes sont sécurisés et que les risques sont gérés. Les activités de gouvernance classiques, telles que la définition des objectifs, le développement de politiques et de normes, la détermination des rôles et responsabilités et la gestion des risques, doivent inclure des considérations spéciales lorsque l'organisation se tourne vers l'infonuagique et ses prestataires.

Comme la plupart des systèmes de l'organisme ont été conçus pour fonctionner dans un environnement contrôlé et sécurisé, les organisations ont besoin de comprendre pleinement les risques liés à l'informatique en nuage et, sur cette base, elles se doivent, dans leur planification stratégique, d'adopter une approche et des principes fondés sur le contrôle des risques. Dans cette optique, ce guide traite des principaux risques associés à l'infonuagique, énonce des exigences en matière de contrôle et de sécurité envers les prestataires et des ajustements à apporter à l'environnement de contrôle des organisations. Il aborde aussi les avantages liés à la sécurité qu'offre l'infonuagique et conclut sur l'enjeu principal de l'infonuagique, la confiance.

# 3. Principaux risques associés à l'infonuagique

Il faut notamment retenir le fait que les données seront transmises sur Internet et emmagasinées dans des lieux éloignés pouvant parfois être localisés dans plusieurs pays, de sorte qu'il peut devenir difficile d'assurer adéquatement le contrôle et la sécurité de l'information en raison des différentes lois, ou de l'absence de loi, qui régissent ces pays. De plus, l'utilisation d'Internet, d'un espace virtuel et délocalisé, accroît l'exposition des services externalisés aux menaces usuelles associées à l'exploitation d'un environnement technologique, auxquelles il faut ajouter les vulnérabilités propres aux caractéristiques des environnements infonuagiques. Les risques sont nombreux et de différents types (liés à la gestion, aux finances, à l'interopérabilité, à la conformité au cadre législatif et réglementaire, à la sécurité, au maintien de la résilience de l'organisation, etc.). Les OP doivent être sensibles aux risques générés par l'utilisation de l'infonuagique et ils devront adapter leur cadre d'analyse de risques afin de traiter des écarts entre le traditionnel et l'infonuagique. Pour plus d'information sur ce dernier point se référer à l'annexe I – Cadre de gestion des risques adapté à l'infonuagique et à l'annexe II - Critères d'analyse pour la sélection d'un service infonuagique. À des fins de présentation, les risques ont été regroupés en quatre grandes catégories.

**Figure 1 – Catégories de risques associés à l'infonuagique**




## 3.1 Risques liés à la gestion

### Intégration aux opérations courantes

Selon le modèle infonuagique, les opérations seront désormais systématiquement effectuées par le prestataire de services. Ainsi, les tâches de planification, de pilotage et d'évolution des services relèveront du prestataire, de même que la gradation des versions, qui pourra parfois être réalisée sans même en informer les organismes clients. Ces nouvelles façons de faire pourraient entraîner des difficultés pour l'organisation et les systèmes d'information patrimoniaux associés et les forcer à s'adapter à des évolutions du service infonuagique parfois très fréquentes.

De plus, les possibilités de personnalisation des applications et des services peuvent être moins nombreuses, ce qui ajoutera à la complexité au moment de l'intégration des services infonuagiques aux environnements patrimoniaux existants. Finalement, le modèle de licence de logiciels existants peut ne pas faciliter un déploiement en nuage.

### Adaptation à l'évolution des besoins

Ces nouvelles façons de faire posent aussi la question de la capacité du prestataire à répondre à l'évolution des besoins de l'OP. Ces risques peuvent être attribuables à la faible marge de négociation au moment de la contractualisation de l'offre de service. Ainsi, les organismes peuvent avoir des difficultés à obtenir des aménagements spécifiques corrigeant les problèmes ou risques qu'ils ont relevés car les prestataires se cantonnent à leur offre générique et qu'ils s'engagent rarement sur des résultats, mais préfèrent recourir à une obligation de moyens.

Dans le cas où le prestataire de services n'offre pas les niveaux de service convenus, l'OP aura beaucoup de difficulté à assurer la conformité des services offerts si de mauvaises conditions de surveillance de la performance ou de la conformité au contrat font que les niveaux de service garantis ne sont pas atteints. Ce risque est d'autant plus grand dans le cas des environnements infonuagiques où plusieurs prestataires de services sont parties prenantes à l'offre.

### Disponibilité des compétences

La migration vers un environnement infonuagique peut entraîner des lacunes dans la gestion des compétences de l'OP. Le passage à l'infonuagique se traduit par une diminution de la demande pour des équipements ou certains types de logiciels, et conséquemment pour certaines compétences techniques. Par ailleurs, elle requiert de nouvelles compétences spécialisées en analyse d'affaires, en architecture, en gestion de projet et en gestion de contrat complexe avec des prestataires d'importance.

## 3.2 Risques financiers

### Contrôle des coûts

Les difficultés à contrôler les coûts pourraient mettre en péril la rentabilité d'une solution. Des difficultés de maintien de la situation financière du contrat auront des répercussions sur l'atteinte des objectifs et des bénéfices escomptés. Les causes peuvent être multiples :

- ✓ Le dépassement de coût attribuable à une mauvaise estimation des coûts, tant à l'entrée qu'à la sortie du contrat. En particulier, il faut souligner les difficultés importantes si, lors de la préparation de l'appel d'offres, des clauses n'ont pas été prévues à cette fin.
- ✓ La difficulté de contrôler la croissance des coûts, en particulier ceux liés à l'exploitation, à cause d'une mauvaise compréhension du modèle économique de tarification utilisée par le prestataire de services infonuagiques, notamment, les points concernant la fixation des prix liés à l'augmentation de l'utilisation de niveau de service.
- ✓ Le contrôle des coûts d'utilisation des licences, ces coûts étant généralement basés sur le nombre d'installations ou le nombre de clients. Avec l'avènement des infrastructures virtuelles, les logiciels ne sont utilisés que quelques fois, et le prestataire peut avoir à acquérir beaucoup plus de licences que nécessaire à un moment donné. L'absence d'un régime de gestion des licences adapté à l'infonuagique, qui permettrait le paiement uniquement pour les licences utilisées, peut entraîner des coûts d'utilisation de logiciels inutiles.
- ✓ La découverte de coûts cachés, associés aux demandes de modification de services de la part de l'OP est une autre possibilité.

Finalement, lors de l'examen pour l'adoption d'une solution infonuagique, l'OP doit veiller à ce que le contrat avec le prestataire de services ne le « verrouille » pas à celui-ci au-delà de la durée du contrat, ce qui constitue un risque financier important pour l'OP.

### Mode de financement

En raison du mode de paiement à l'usage, une partie du budget de dépenses en capital pour les technologies de l'information et des communications (TIC) sera convertie en dépenses de fonctionnement. Les OP devront adapter leurs pratiques de gestion budgétaire afin de prendre en compte, entre autres, le contrôle et le respect des exigences réglementaires en ce qui a trait aux engagements sur plusieurs années des dépenses de fonctionnement. Les contrats de service sont limités à cinq ans au maximum, à moins d'obtenir les dérogations requises.

## 3.3 Risques d'interopérabilité

### La non-réversibilité ou le verrouillage (*vendor locking*)

Pour de nombreuses raisons, tant techniques que d'affaires, comme l'augmentation inacceptable des coûts au moment du renouvellement d'un contrat ou une diminution inadmissible de la qualité de service, un client de services infonuagiques peut vouloir changer de prestataire de services infonuagiques. La non-réversibilité ou l'enfermement est une situation dans laquelle un client serait dans l'impossibilité de reprendre ou déplacer des processus externalisés vers un prestataire infonuagique concurrent. La crainte du verrouillage (*vendor locking*) est souvent citée comme un obstacle majeur à l'adoption de l'infonuagique. Les principales causes sont :

- ✓ Une portabilité des données limitée ou impossible. Actuellement, il existe très peu d'outils ou de procédures standardisées offrant des garanties de portabilité entre les différents services infonuagiques;
- ✓ L'utilisation par le prestataire de technologies propriétaires qui sont incompatibles avec celles de ses concurrents. Cela pourrait être le cas si un prestataire de services infonuagiques s'appuie sur des hyperviseurs ou sur un format d'image de machine virtuelle non standard, et ne fournit pas d'outils pour convertir les machines virtuelles dans un format normalisé;
- ✓ Une connaissance insuffisante des technologies du prestataire. Cela a entraîné la création d'îlots de technologies de l'infonuagique, ayant pour conséquence de réduire l'interopérabilité entre les différents types de nuages d'implémentations associées;
- ✓ Une dépendance du client envers le prestataire. Cela peut empêcher la réversibilité de la prestation, car le contrôle exercé par le client sur la performance de la prestation est plus distant et restreint que dans les autres cas de gestion des ressources informationnelles;
- ✓ La difficulté à évaluer la capacité du prestataire à la reprise des activités ou la décision d'un prestataire de se retirer d'affaires ou de services particuliers de données ou d'applications;
- ✓ Des contraintes contractuelles.

Dans ces cas, la portabilité des services, l'interopérabilité et la réversibilité doivent être considérées pour minimiser les dommages aux activités du client. Le client de services infonuagiques doit être en mesure de migrer en tout ou partie son service vers un autre prestataire, d'utiliser et intégrer des services de différents prestataires, ou de quitter définitivement l'infrastructure du prestataire.

### Intégration technologique

La migration vers l'infonuagique peut impliquer le transfert de grandes quantités de données, entraîner des changements de configuration à l'infrastructure du client (ex. : adressage réseau), ou nécessiter des changements importants dans la conception de l'infrastructure de celui-ci (réseau, politiques de sécurité réseau, etc.). Les principaux éléments techniques qui peuvent limiter un déploiement dans l'infonuagique sont les difficultés d'intégration aux systèmes d'information de l'organisation et le risque de multiplication des services infonuagiques interfacées. Une mauvaise intégration causée par des interfaces incompatibles ou l'application de politiques incohérentes peut entraîner des répercussions fonctionnelles et technologiques sur les systèmes d'information et en diminuer à moyen terme la flexibilité et la capacité d'évolution.

## 3.4 Risques de sécurité

Les risques de sécurité associés à l'infonuagique découlent principalement des menaces suivantes :

### Perte de contrôle ou perte de gouvernance

La décision prise par un client de migrer la totalité ou une partie d'une activité vers l'infonuagique implique de céder le contrôle partiel au prestataire de services. Une fois les données confiées à un prestataire de solutions infonuagiques, il devient difficile pour le client de vérifier si celles-ci sont manipulées dans les règles de l'art, que ce soit dans leur acquisition, leur traitement, leur transfert ou leur conservation. Cette perte de contrôle varie selon le modèle de service infonuagique acquis. Plus le service est évolué, plus le contrôle de l'organisme sur le service diminue.

Ainsi, pour l'IaaS (*Infrastructure as a Service*), seule est déléguée au prestataire la gestion des équipements et du réseau. C'est le type de service utilisé pour répondre aux besoins croissants en équipements et performances, qui nécessiterait autrement de forts investissements. L'énoncé du besoin devrait insister sur la capacité à rendre le service plutôt que sur la portabilité des informations. L'IaaS, à moins d'être très précis sur le type d'infrastructure recherché, est le service infonuagique qui offre le degré de dépendance à un prestataire le moins élevé et permet une migration d'un prestataire à l'autre sans problème particulier. À titre d'exemple, le stockage d'informations est habituellement insensible à l'infrastructure qui le supporte, cependant la capacité et la disponibilité deviennent des enjeux beaucoup plus grands.

Pour ce qui est d'une solution PaaS (*Platform as a Service*), il existe un très fort lien entre le service qui est rendu et la plateforme technologique de développement ou d'exploitation qui le rend disponible. À cause de ce lien, il faut comprendre que l'un est très dépendant de l'autre. Cependant, si le client prévoit des mécanismes d'exportation et de conversion, les effets en seront grandement limités. Il faut prendre conscience que ces procédures d'extraction, d'exportation et de conversion doivent être préférablement sous la responsabilité du client.

En ce qui a trait au SaaS (*Software as a Service*), le contrôle de l'application est délégué en plus. Ainsi, mieux les services utilisés sont définis, plus le risque de dépendance envers le prestataire sera élevé. Il est préférable de se limiter aux besoins précis et ponctuels. Il faut éviter de faire reposer les affaires ou une partie de celles-ci sur la capacité d'un prestataire à assurer le service de façon permanente.

En confiant leurs données à des systèmes gérés par des prestataires de services infonuagiques, les clients pourraient perdre le contrôle exclusif de leurs données et être privés de la capacité de déployer les mesures organisationnelles et techniques nécessaires pour garantir la disponibilité, l'intégrité et la confidentialité de celles-ci, ainsi que la possibilité d'intervention.

### Manque de visibilité (transparence)

Il est parfois difficile pour l'acquéreur d'un service infonuagique d'être en mesure de connaître l'emplacement de conservation des données ou le niveau de sécurité offert par le prestataire, en raison de la nature de boîte noire de l'infonuagique. Il peut être difficile pour le client d'avoir une vue globale de la sécurité, à cause du manque de visibilité des mesures de sécurité en place et de la dépendance du client à l'égard du prestataire en ce qui concerne l'exactitude des composantes de sécurité et leurs interactions, le maintien du cloisonnement logique des données dans un environnement multilocataires, l'investigation électronique (*e-discovery*), le droit d'audit et la continuité des affaires.

L'absence de partage d'information entre le client et le prestataire peut être occasionnée par l'impossibilité de connaître le niveau de sécurité de l'environnement du prestataire de manière formelle, ou par le fait que les clients de services infonuagiques n'ont pas les capacités pour évaluer le niveau de sécurité de l'environnement du prestataire. Un tel manque de partage au chapitre de la sécurité à l'égard du prestataire de services infonuagiques est une menace potentielle sérieuse pour les clients dans leur utilisation de ces services. Il est ainsi difficile pour le client d'avoir les éléments nécessaires pour

conserver un niveau approprié de contrôle sur le prestataire afin d'être en mesure d'évaluer les solutions de rechange et de fixer les priorités et les ajustements en matière de sécurité et de protection des données.

Ces problèmes ne peuvent être qu'amplifiés lorsque le prestataire de services infonuagiques a recours à des sous-traitants pour effectuer certaines tâches spécialisées. Ce genre de situation amène des risques supplémentaires de sécurité advenant le cas où le sous-traitant n'appliquerait pas les mêmes mesures de protection que le prestataire principal.

## Pratiques de sécurité du prestataire

La protection des données doit assurer la préservation de la confidentialité ainsi que l'intégrité et la disponibilité des données. Les clients de services infonuagiques sont préoccupés par la façon dont les prestataires gèrent leurs données afin d'assurer leur non-divulgation ou leur modification non autorisée. La sécurité de l'infonuagique est un facteur de différenciation important entre prestataires de services infonuagiques et un élément contribuant aux décisions de migration des systèmes d'information vers les environnements infonuagiques.

De plus, lors de l'acquisition de services infonuagiques, le client aura des préoccupations au sujet des manques à la gestion par les prestataires de services. Souvent, le manque de contrôle sur les opérations, l'insuffisance des procédures en authentification ou la faiblesse des mécanismes de surveillance sont à l'origine des brèches de sécurité. Les faiblesses associées aux processus de conservation des données, telles que l'absence de contrôle physique pour le stockage de données ou la fiabilité du processus de la sauvegarde des données, doivent être considérées comme importantes. Il en est de même en ce qui a trait à la fiabilité des procédés de continuité des services et de reprise après incident ou sinistre.

## Partage ambigu des rôles et des responsabilités

Les clients de services infonuagiques consomment des ressources externes selon un modèle de services. Une partie du système informatique des clients s'appuie donc sur des services externes. Différents intervenants sont concernés, tels que le prestataire de services, le consommateur de services, l'administrateur informatique client, le détenteur des données client, les responsables de la sécurité ou de l'accès à l'information et à la protection des renseignements personnels (PRP), etc. Toute ambiguïté dans la définition des rôles et des responsabilités liés à la propriété des données, le contrôle d'accès, l'entretien des infrastructures, etc., peut entraîner des incohérences en matière de sécurité, de PRP et des disputes contractuelles. En outre, toute incohérence contractuelle sur des services fournis pourrait induire des anomalies ou des incidents. L'absence d'une définition claire des responsabilités entre les partenaires aura d'autant plus d'effet lorsque le prestataire de services infonuagiques aura recours à des sous-traitants en ce domaine.

## Localisation des données

Le risque d'atteinte à la confidentialité des données est celui qui est le plus mis en avant. Le manque de visibilité sur la localisation des données et donc sur la législation et la réglementation applicables, ainsi que le nombre de parties prenantes dans une solution de l'infonuagique accentuent ce risque. La protection des données sensibles et personnelles, de même que le respect du droit à la vie privée, sont particulièrement difficiles au sein d'infrastructures partagées et potentiellement accessibles aux gouvernements locaux.

D'autres risques sont reliés à la méconnaissance de la localisation des données ou au droit d'accès aux données par certains États. Ainsi, le cas du *USA PATRIOT Act* des Etats-Unis est souvent cité en exemple. Il permet aux services de sécurité américains d'accéder à des données à caractère personnel, sur leur territoire ou à l'étranger, si elles sont détenues par des sociétés américaines. Certains y voient même un risque en matière de juridiction si les données et les traitements des organismes n'étaient plus situés au Québec ou au Canada. D'autres préoccupations importantes concernent les cas où un prestataire de services infonuagiques international peut entrer en conflit avec les lois et les règlements

pour ses centres locaux de traitement, ou un client peut avoir des difficultés à faire appliquer des clauses contractuelles, ce qui sont des menaces juridiques qui doivent être prises en compte.

## Atteinte à l'intégrité des systèmes patrimoniaux ou de l'information

Le recours à un prestataire de services infonuagiques crée un risque d'atteinte à l'intégrité globale du système d'information du client en raison de la perte d'expertise technique, voire de dépendance au prestataire quant aux moyens de protection des données mis en place par ce dernier. De plus, les faiblesses de l'infonuagique dans le domaine du contrôle et de la preuve, en ce qui a trait à la mise en place de moyens assurant la conservation de la valeur probante des informations ou documents électroniques d'intérêt, sont également à souligner.

## Accès aux informations par des employés du prestataire

La décision prise par un client de services infonuagiques de migrer des actifs informationnels vers l'infonuagique implique qu'il en cède le contrôle partiel au prestataire. Cela devient une menace sérieuse à la confidentialité de ses données, notamment en raison des accès accordés à des employés du prestataire. Le manque de transparence en ce qui concerne les pratiques de sécurité des prestataires est une autre menace qui peut conduire à une mauvaise configuration ou permettre les attaques de l'intérieur. Il en est de même de la difficulté à s'assurer que les employés du prestataire ne peuvent pas lire des données confidentielles au moment de la réalisation des activités de gestion de l'infrastructure ou lors de l'examen des journaux d'événements des systèmes. De plus, la difficulté de s'assurer que le prestataire a détruit les données en cas d'arrêt de la prestation se pose également en ce qui concerne l'assurance de leur destruction effective, y compris sur les copies de sécurité dans des sites qui peuvent être dispersés.

## Accès non autorisé aux services infonuagiques

Comme la plupart des accès aux services par les clients se font par une connexion à distance, des interfaces de programmation (API) non protégées (les API de gestion de l'infrastructure et des services PaaS) sont des vecteurs d'attaque facilement utilisables par des individus malveillants. La compromission des informations d'identification et des mots de passe ajoute à l'impact des méthodes d'attaques connues comme l'hameçonnage, la fraude et l'exploitation de vulnérabilités logicielles. Le compte ou l'instance de service infonuagique compromis peut servir de tremplin à l'attaquant et lui permettre d'exploiter la crédibilité de l'image du client pour lancer de nouvelles attaques. Ainsi, un individu malveillant qui obtient l'accès aux informations d'identification d'un compte d'accès à l'infonuagique peut espionner les activités et les opérations du client, manipuler des données, les falsifier ou rediriger les usagers vers des sites illégitimes.

## Perte ou divulgation d'informations

Les facteurs reconnus comme importants pour influer sur cette catégorie de menaces sont les processus d'authentification, d'autorisation et d'audit insuffisants. L'utilisation inconsistante des clés d'authentification ou de chiffrement, les défaillances de gestion opérationnelle, la destruction incorrecte des données; la fiabilité des centres de traitement, la qualité du processus de reprise des activités après incident ou sinistre et la compétence juridictionnelle sont d'autres facteurs souvent cités. Plus particulièrement, la perte d'une clé de chiffrement ou d'un code d'accès avec privilège important apportera de graves problèmes aux clients de services infonuagiques. En conséquence, toute faiblesse des processus de chiffrement ou d'authentification (clés de chiffrement, codes d'authentification et droits d'accès) peut entraîner des risques importants sur le plan de la confidentialité des données sensibles et se traduire par la perte ou la divulgation de telles données.

## Évolution des services infonuagiques acquis

L'un des avantages de l'infonuagique est de reporter certains choix systémiques de la phase de conception à la phase implantation ou d'exploitation. Cela signifie que certains composants logiciels dépendants d'un service acquis peuvent être mis à jour et implantés lorsque le service est en exploitation. Un service qui est considéré comme sûr pendant la phase d'analyse d'opportunité peut se fragiliser au cours de son exploitation en raison des composants logiciels nouvellement mis en place. Les méthodologies conventionnelles d'évaluation des risques ne sont pas adaptées à ces nouvelles façons de faire et donc, les clients peuvent être dans l'incapacité d'évaluer et de maintenir les risques à un niveau acceptable.

## Cloisonnement insuffisant des environnements partagés (perméabilité)

L'organisation des ressources d'infonuagique en mode virtualisé permet à différents consommateurs de services infonuagiques de partager la même infrastructure. Les principales préoccupations sont liées à l'architecture de cloisonnement, à l'isolement des ressources et à la ségrégation des données. Tout accès non autorisé à des données sensibles d'un client de service infonuagique peut en compromettre l'intégrité ou la confidentialité. Les prestations sous la forme de l'infonuagique publique ou hybride mettent en commun les services offerts à l'ensemble de leur clientèle, créant un risque de perméabilité des données entre les différents clients.

Ce risque aura tendance à s'accroître selon le type de service infonuagique retenu, à savoir que l'isolation des données sera probablement meilleure dans une infonuagique privée que dans une infonuagique publique. Le partage des ressources dans le cas de l'infonuagique publique amène de grandes économies, mais les activités des autres clients ne doivent pas nuire aux activités du nouveau client. Il faut donc en tenir compte dans le choix d'un prestataire. Mais il en va de même pour tout modèle de l'infonuagique privée externe dans lequel il existerait une mise en commun des services fournis à un organisme avec ceux proposés à d'autres clients, ce qui comprend l'infonuagique dite communautaire, les clients partageant des ressources entre un nombre limité de partenaires.

## Sécurité des architectures distribuées

Les infrastructures infonuagiques de traitement sont souvent basées sur une architecture décentralisée qui se caractérise par l'intégration de modules distribués. Les composantes de sécurité étant aussi distribuées, il est difficile de maintenir la cohérence des mécanismes de protection des données pour ce type d'environnement. Par exemple, le refus d'accès par un module de sécurité de gestion des identités et des accès (GIA) peut être accordé par un autre. Cette menace peut être mise à profit par un individu malveillant, ce qui peut compromettre à la fois la confidentialité et l'intégrité des données.

## Interface de programmation insuffisamment sécurisée

Dans l'approche orientée services, les interfaces de programmation (API) sont les blocs de construction d'une infrastructure infonuagique. L'API est la couche logicielle (intergiciel) située entre l'infrastructure et l'utilisateur de services. Une attention particulière doit être apportée aux procédés de contrôle des interfaces au moment de la saisie des données d'identification et d'authentification. Ces API mal protégées sont des vecteurs de choix pour des attaques. Bien que non spécifique de l'environnement infonuagique, leur protection est une préoccupation majeure pour la sécurité des services de l'infonuagique.

## Isolement de l'hyperviseur

La technologie de la virtualisation est considérée comme le fondement des infrastructures infonuagiques. La technologie de l'hyperviseur permet de gérer des machines virtuelles cohébergées sur un même

serveur physique, en favorisant le partage des ressources de l'unité centrale de traitement (*central processing unit*) et de la mémoire. L'échec des mécanismes pour isoler des attaques l'hyperviseur a pour principales conséquences de permettre l'accès non autorisé à la mémoire d'autres machines virtuelles et de fragiliser l'ensemble de l'infrastructure par la dissémination de codes malveillants.

## Indisponibilité des services

L'indisponibilité des données et des traitements est un autre risque souvent mentionné, bien que les enjeux de disponibilité ne soient pas propres uniquement aux environnements infonuagiques. Le concept « as a service » (IAAS, PAAS et SAAS) caractéristique de l'infonuagique qui alloue les ressources et les déploie en tant que services, présente les vulnérabilités suivantes :

- ✓ L'ensemble de l'infrastructure de l'infonuagique, avec ses flux de travail, s'appuie donc sur un large éventail de services allant du matériel aux applications. Cependant, l'interruption de la prestation de composantes, à cause d'une panne ou d'un retard, peut avoir de graves répercussions sur la disponibilité;
- ✓ Le principe de conception orientée services et la dépendance dynamique entre les différentes composantes des environnements infonuagiques, offrent beaucoup plus de possibilités pour une attaque. Une attaque typique de déni de service réussi sur un service peut avoir un effet négatif sur l'ensemble de l'environnement du prestataire;
- ✓ La nature dynamique de la conservation des données dans le nuage fait en sorte que l'information peut ne pas être immédiatement située dans le cas d'un incident;
- ✓ La perte d'accès à Internet, pour les services dépendant de ce type d'accès, peut interrompre les services infonuagiques, et une attention particulière doit être apportée à cet aspect;
- ✓ La continuité des services externalisés du client peut être menacée par l'insuffisance des pratiques de reprise des opérations après incident, ou encore, parce que les plans de continuité des services et de reprise n'ont pas été suffisamment documentés ou testés;
- ✓ La relation asymétrique qui lie le prestataire à son client, caractérisée notamment par la difficulté d'inclure des engagements contraignants, des clauses de pénalité, sur un niveau minimal de disponibilité peut renforcer ce risque. Bien que le prestataire s'engage sur un taux de disponibilité, le fait que son non-respect ne soit sanctionné que par des pénalités financières, peut être une limite importante de l'effet dissuasif;
- ✓ Finalement, la faillite d'un prestataire peut avoir des répercussions catastrophiques pour les affaires de ses clients si ces derniers n'ont pas de solutions compatibles à court terme.

# 4. Exigences de contrôle et de sécurité

Lorsqu'elle concerne des activités essentielles, la mise en œuvre des prestations de l'infonuagique doit s'accompagner de mesures de maîtrise du risque adaptées. De nombreux éléments sont à prendre en compte lors du recours à un service infonuagique. Chez les prestataires de services, les OP doivent déceler des mesures qui démontrent l'existence de contrôles et de règles de sécurité strictes et efficaces, qui garantissent aux clients une réelle protection de leurs informations contre les accès, les modifications et les destructions non autorisés.

Pour chaque offre de service, les besoins de contrôle et de sécurité doivent être évalués et déterminés en fonction d'enjeux liés à la gestion, aux finances, à la transparence, à la localisation des informations, à l'accès aux informations par les employés du prestataire, à la séparation des tâches chez le prestataire, au partage des responsabilités entre le prestataire et le client, et au cloisonnement des informations. Le recours à des normes et à des cadres de référence permet aux OP d'évaluer la pertinence et la qualité du contrôle interne et des mesures de sécurité de leur prestataire afin d'empêcher, de détecter et de traiter

les manquements. Chaque OP devra s’assurer de répondre aux risques qu’il aura identifiés par des exigences de contrôle interne ou de sécurité adaptées au contexte d’acquisition et d’utilisation des services infonuagiques.

## Appréciation des pratiques de sécurité du prestataire

Afin de s’assurer que le prestataire d’infonuagique est en mesure de fournir des services appropriés en fonction des exigences de sécurité du client, l’approche d’évaluation de la sécurité du prestataire doit être précisée lors de l’appel d’offres : autoévaluation par questionnaire de sécurité, audit par le client ou tiers de confiance, ou obtention des résultats de certification par un tiers. En outre, les critères de sécurité utilisés pour l’évaluation et la sélection du prestataire doivent être mis en œuvre de manière à fournir aux différentes parties une compréhension mutuelle du niveau de sécurité de l’environnement. Le prestataire de services infonuagiques doit également être en mesure, afin de se conformer aux besoins de sécurité du client, de répondre à différentes exigences de sécurité de celui-ci et être capable de proposer différentes solutions à ce sujet.

La complétude des mécanismes de protection associés au matériel et aux logiciels de protection doit être établie ainsi que la cohérence des structures et des occurrences des données de contrôle et de sécurité conservées. Le prestataire doit être en mesure de démontrer la robustesse et la permanence des mécanismes de protection mis en place pour contrer la modification ou la destruction non autorisée de l’information. Des méthodes et des procédures de contrôle doivent aussi être en place afin d'assurer, entre autres, la fiabilité et l'exactitude des configurations de l'hyperviseur, des machines virtuelles, des systèmes d'exploitation et des logiciels systèmes. Lorsque l'utilisation de services infonuagiques nécessite l'établissement de relations de confiance avec le prestataire, des techniques normalisées doivent être employées. Les mécanismes normés incluent l'échange de certificats et des clés cryptographiques, la gestion de l'identité ainsi que la présence d'une politique de sécurité qui peuvent être utilisés pour établir les relations et les règles d'affectation ultérieures.

## Séparation des tâches incompatibles

De saines méthodes et procédures de contrôle interne sur les activités doivent avoir été mises en place par le prestataire, comme le partage de la garde des actifs, la séparation des activités d’autorisation des transactions des activités de garde des actifs associés, ou la séparation des responsabilités opérationnelles des responsabilités de tenue des dossiers. Aucun individu ni aucune entité organisationnelle ne devraient avoir le contrôle de deux ou plusieurs phases d'une transaction ou d'une opération sans qu’une surveillance opérationnelle soit exercée par un tiers. Les clients doivent être en mesure de revoir l’attribution des responsabilités pour assurer l’application appropriée du principe de séparation des tâches incompatibles.

## Gestion des menaces

Le prestataire a mis en place un processus de veille et de surveillance des menaces et des vulnérabilités et il possède des procédures adéquates de traitement de celles-ci. Le prestataire utilise des solutions reconnues, entre autres, contre les logiciels malveillants (virus, vers, pourriels) et elles sont régulièrement mises à jour.

## Pratiques de développement ou d'acquisition du prestataire

Le cadre normatif de développement ou d'acquisition du prestataire assure la prise en compte des exigences de contrôle et de sécurité lors du développement ou de l'acquisition de logiciels, et il utilise des normes pour le développement sécuritaire : OWASP[1], PA-DSS[2], ISO[3] 27034 : 2011.

## Localisation des actifs externalisés

Les exigences portent sur l'identification des lieux de conservation des actifs informationnels sensibles, le contrôle physique pour le stockage des données et la fiabilité du processus des copies de sauvegarde des données.

## Continuité des services

Au chapitre de l'identification des processus de continuité des services et de reprise des opérations en cas d'incident ou de catastrophe, il est important que le client connaisse la politique de sécurité du prestataire et qu'il soit en mesure d'évaluer l'agilité de celui-ci pour traiter de la protection de ses infrastructures et de sa capacité à mettre en œuvre des règles de sécurité pour ses clients.

## Gestion des licences et droits de propriété intellectuelle

Les licences et les droits de propriété intellectuelle seront gérés par le prestataire de services, en conformité avec les lois de la juridiction régissant son centre de traitement. La preuve de la conformité aux lois et réglementations de la juridiction est mise à disposition et tous les cas de modification ou de renouvellement doivent être documentés et autorisés. La disposition des licences doit être gérée conformément aux accords de licence de services mutuellement convenus.

## Gestion des identités

Le nombre et la diversité des acteurs, tant internes qu'externes, concernés par l'utilisation des services infonuagiques, ainsi que la quantité de ressources accessibles, demandent une gestion robuste des identités et des accès. La mauvaise administration des identités et des habilitations peut induire de nouvelles vulnérabilités dans une telle infrastructure dynamique et ouverte. L'identité doit être gérée de manière appropriée, non seulement pour leur protection, mais aussi pour la gestion des comptes des administrateurs, des clients et des ressources. Ceci est nécessaire pour protéger contre l'hameçonnage, la fraude et l'exploitation des vulnérabilités des logiciels, mais aussi pour assurer l'utilisation correcte du compte ou du service dans l'environnement infonuagique.

## Modèle de sécurité pour l'identification (fédération)

Un client peut vouloir recourir à plusieurs prestataires infonuagiques qui ont des modèles de sécurité différents, notamment pour la gestion de l'identification et des accès (personnes ou dispositifs). Certains prestataires peuvent utiliser des certificats, d'autres des interfaces adaptées aux services Web (SOAP ou REST), ou utiliser simplement l'authentification HTTP de base ou sécurisée. Afin de permettre à un client

1. OWASP, *Open Web Application Security Project*, https://www.owasp.org/index.php/Main_Page
2. PA-DSS, *Payment Application Data Security Standard*, http://fr.pcisecuritystandards.org/minisite/en/
3. ISO, *International Organization for Standardization*, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378

d'utiliser l'ensemble des services infonuagiques, le prestataire de services doit être en mesure de gérer différents types de connexions de sécurité.

## Contrôle d'accès à l'information

Tous les accès aux informations, aux systèmes et aux infrastructures doivent être contrôlés sur la base de rôles attribués selon le principe du privilège minimal (*least privilege*).

## Habilitation

Pour se protéger contre les initiés malveillants**,** certains rôles clés dans la gestion de l'infrastructure d'infonuagique nécessitent des privilèges spécifiques et possèdent par conséquent des accès à haut risque. Il faut s'assurer que l'utilisation de ces accès est bien encadrée et surveillée. Pour cette catégorie de personnel, il est recommandé de vérifier les antécédents (habilitation).

## Engagement à la confidentialité

Dans le contrat avec le prestataire de services infonuagiques, il faut s'assurer qu'une clause exige une conformité reliée à la signature d'un engagement à la confidentialité pour tous les employés du prestataire ayant accès aux données de l'organisme ainsi qu'à sa gestion de bout en bout. Le prestataire doit avoir établi des procédures d'embauche ainsi que des mécanismes de vérification d'antécédents.

## Chiffrement

Parmi les mesures techniques de sécurité, le chiffrement systématique des données est celle qui revient le plus souvent, notamment pour protéger les données dont la localisation n'est pas connue. Ces exigences visent à protéger également contre la perte ou la fuite de données en raison de l'insuffisance des mécanismes d'authentification, d'autorisation ou des mesures de sécurité, ou encore, des défaillances opérationnelles. Il faut préciser toutefois que si le chiffrement des données lors du transport est courant, il est plus complexe à mettre en œuvre pour le stockage ou l'utilisation des données. Les exigences portent sur les caractéristiques du processus de gestion du chiffrement, en particulier les clés de chiffrement, les codes et les justificatifs d'authentification ainsi que les privilèges d'accès. Plusieurs organismes de normalisation en sécurité préconisent que le chiffrement soit mis en œuvre par le déploiement d'une infrastructure à clés publiques qui ne serait pas gérée dans l'infonuagique.

## Gestion des clés de chiffrement

La solution de chiffrement doit être maîtrisée par le client, ce qui implique que la gestion des clés doit être faite par l'organisme. Des procédures de protection des clés, de récupération ou de changement des clés advenant la compromission de ces dernières doivent être prévues. La délocalisation des clés, pour offrir plus de protection, est recommandée ainsi que l'utilisation d'équipement dédié au chiffrement, du type *Hardware Security Module* (HSM)**,** technologie qui génère, stocke et protège les clés de chiffrement.

## Anonymisation

Généralement, on considère que le chiffrement n'est utile que pour les données sensibles et que l'anonymisation peut être utilisée dans les environnements hors production. En l'absence d'anonymisation, les données confidentielles confiées au prestataire doivent être chiffrées lors du transport ainsi que pendant le stockage. L'utilisation d'un réseau privé virtuel (RPV) est un autre de ces moyens de chiffrement des communications qui traite ce problème.

## Isolement dans les environnements multilocataires

L'infonuagique permet des économies potentielles par le partage entre plusieurs clients, sur une très grande échelle, de ressources nombreuses et variées. Plus il y a de clients chez un prestataire de services infonuagiques, plus grands sont les risques d'atteinte à la confidentialité des informations ou à la réputation du client. Il faut donc sélectionner le prestataire en fonction de sa capacité à assurer que les activités d'un de ses clients ne peuvent pas nuire aux activités des autres clients.

Dans les situations où différents locataires ont recours simultanément aux services d'un même prestataire, cela expose de nombreuses interfaces potentiellement vulnérables et peut permettre à un locataire d'avoir accès à des machines virtuelles d'autres locataires, au trafic réseau, aux données actives ou résiduelles, etc. En outre, le locataire peut affecter le fonctionnement normal des autres locataires, en volant leurs données ou des identités. Pour éviter ces situations, les habilitations sont gérées par le donneur d'ordre et ce dernier exige le cloisonnement des données entre les différents clients. De plus, le prestataire doit être en mesure de chiffrer les données en transit et au repos, de sécuriser davantage les machines virtuelles (durcir), de façon à réduire l'exposition de la couche de virtualisation à des attaques et de mettre en place des environnements virtuels spéciaux, par l'utilisation du cloisonnement physique pour les clients de services infonuagiques aux exigences de sécurité particulières.

## Traçabilité des données et journalisation

Les principales préoccupations des clients relativement à une infrastructure partagée et virtualisée comprennent non seulement la perte de contrôle sur leurs données, mais aussi la localisation de celles-ci et le contrôle de l'ensemble de leur cycle de vie. À tout moment, un prestataire de services infonuagiques devrait être en mesure de savoir exactement où sont stockées et traitées les données des clients et des machines virtuelles, et où on peut y avoir accès. Sans mesure particulière de traçabilité et de surveillance, les données peuvent se déplacer librement entre les organisations, ou entre les pays. Ainsi, des gouvernements étrangers peuvent également avoir accès à des données hébergées à l'étranger. De plus, pendant et après utilisation, il ne devrait pas être possible pour des tiers (y compris les prestataires d'hébergement) d'accéder aux données. Le prestataire devrait posséder des mécanismes de connaissance et de contrôle des données. Leur traçabilité est nécessaire pour prouver aux clients que les données proviennent d'une source fiable. En tout temps le prestataire est tenu de journaliser toutes les actions effectuées sur les données par les clients ou par ses employés et il est tenu de transmettre les journaux à la demande du client. Toute anomalie détectée par le prestataire doit aussi être déclarée au client.

## Copies de sécurité

Concernant les mesures techniques permettant d'éviter la perte de données, la réponse majoritaire est la mise en place d'un plan de continuité des services avec une réplication des données sur des sites distincts. Faut-il rappeler l'importance d'un site de secours hors site? Il faut tester régulièrement les fonctions de sauvegarde et s'assurer que la copie est distante du site primaire. De plus, les organismes de normalisation recommandent de disposer d'un plan de secours testé par un organisme indépendant.

## Destruction des données

Pour une destruction effective des données, le client doit lui-même préciser par contrat le niveau requis de destruction et la procédure pour y arriver en fonction de la nature des informations.

## Restauration des données

Si la restauration des données est nécessaire (fin de contrat prévue ou non), le client doit déterminer comment (moyen, format, etc.) cette restauration doit se faire et le prestataire doit procéder à la

suppression uniquement lorsque les données restaurées, chez le client ou chez un autre prestataire, ont été vérifiées et reconnues conformes.

## Sécurité des environnements virtuels

Un centre de traitement est généralement construit à partir d’un ensemble de matériels et de logiciels hétérogènes, tels des serveurs, des baies de disques, des commutateurs, des hyperviseurs, des intergiciels et des logiciels systèmes. L'interopérabilité de ces solutions reste une préoccupation importante. Le prestataire de services infonuagiques doit analyser la sécurité de la coexistence et de la coopération de ces solutions hétérogènes. En outre, il doit veiller à la coordination et à la consolidation des différentes politiques et divers mécanismes de sécurité tributaires des technologies en place. Le prestataire doit garantir la cohérence des politiques, des règles de sécurité et de leur mise en œuvre.

## Normalisation de l’environnement virtuel

Les machines virtuelles, les API et les interfaces de service doivent, autant que possible, être déployées conformément aux normes de l'industrie et configurées afin d'être interopérables avec les environnements d’autres prestataires. Aucune adaptation ne doit empêcher ou limiter la migration d'une machine virtuelle dans l’environnement ou vers d’autres prestataires, ou altérer les configurations définies au moment de la création des machines virtuelles.

## Protection de l’hyperviseur

L'hyperviseur gère la cohabitation de plusieurs machines virtuelles sur un même serveur physique (hôte). Les machines virtuelles doivent être bien isolées afin d’assurer le partage sécuritaire de la mémoire, du CPU et du stockage. Cependant, l'isolement strict entre les machines virtuelles peut échouer si l'hyperviseur est compromis. Une nouvelle variété d'attaques, comme l'installation d’outils de dissimulation d’activités (*rootkits*), à l'intérieur de l'hyperviseur (*hyperjacking*), appelle à des degrés d'assurance plus élevés. La configuration de l'hyperviseur doit être faite de telle façon qu’elle assure une protection pour lui-même et pour les machines virtuelles qu’il contrôle, par exemple, en déplaçant de la machine virtuelle vers l’hyperviseur les mécanismes de protection comme les antivirus et les antipourriels.

## Application des règles de sécurité par les machines virtuelles

Les machines virtuelles doivent être en mesure d’appliquer les règles de sécurité conçues lors de leur configuration initiale. Celles qui sont configurées pour appliquer des règles de sécurité visant à restreindre le mouvement ou l’instanciation d’une machine virtuelle doivent être en mesure de mettre en pratique les règles de sécurité en tout temps. L'hyperviseur ou le matériel ne peuvent empêcher une machine virtuelle d’appliquer des règles de sécurité.

## Migration sécurisée des machines virtuelles

Lors de la migration des machines virtuelles entre des hôtes du prestataire de services ou entre des environnements d’autres prestataires, la sécurité de la machine doit être assurée à la fois au repos et en mouvement. Les meilleures pratiques recommandent de maintenir un fichier de journalisation et de produire des rapports de suivi afin de déterminer la situation ou l’état de la machine virtuelle. Ce contrôle peut être assuré par une console de gestion ou par programmation. En tout temps il faut être en mesure de déterminer où elle est conservée, si elle est au repos ou en mouvement, quels clients ont des permissions d’accès à la machine virtuelle et quels contrôles sont en place afin d’assurer la protection contre les accès ou les modifications non autorisés. La migration d’une machine virtuelle demande également la définition ou l’adaptation des règles de sécurité en fonction du nouvel hôte.

## Fiabilisation des machines virtuelles (*Trusted Compute Pool*)

Les technologies de la virtualisation permettent une flexibilité dans le déplacement des machines virtuelles chez le prestataire ou entre les nuages. Cette flexibilité met en difficulté les modèles d'attestation de l'intégrité des plateformes sur les aspects de sécurité. Les consommateurs de services infonuagiques doivent exiger des prestataires d'avoir des technologies qui permettent de valider ou d'attester la conformité technologique des machines selon des approches reconnues, généralement sur la base de la reconnaissance de signatures. L'utilisation des gestionnaires de machines virtuelles lors de migration en direct ou pour toute autre opération de mouvement de ces machines, doit assurer que la cible (hôte) est fiable avant d'effectuer une instanciation ou un mouvement d'une machine virtuelle vers une autre de plateforme.

## Isolement du stockage

L'infonuagique offre des capacités de stockage flexibles qui permettent l'extensibilité. Différents types de solutions de stockage peuvent être déployés dans un centre de traitement. De plus, la configuration des paramètres de stockage d'une machine virtuelle peut être affectée de manière dynamique en fonction du paramétrage des conditions d'exécution. L'interopérabilité et la protection des différentes technologies de stockage deviennent des questions importantes. Un prestataire de services infonuagiques doit garantir l'isolement de ses systèmes de stockage sans aucune contrainte sur la solution acquise par le client.

## Isolement du réseau

Les technologies des réseaux virtuels sont utilisées dans les infrastructures d'infonuagique. Par rapport aux réseaux traditionnels, un réseau virtualisé de l'infonuagique semble plus vulnérable, car le cloisonnement par zones du réseau n'est plus physique, mais logique. Les zones de réseau, où la circulation pouvait être physiquement cloisonnée, sont remplacées par des domaines de sécurité logiques où le trafic entre les machines virtuelles est filtré par des pare-feu virtuels. En conséquence, l'isolement est moins précis, et les garanties de sécurité sont plus faibles. Il est important que des mesures robustes de sécurité du périmètre soient mises en place pour éviter que le comportement inattendu d'un service affecte d'autres services et induisent des problèmes de sécurité. Il est important aussi de bien indiquer les équipements et les technologies de protection des périmètres (sondes de détection d'intrusion, pare-feu, etc.).

## Protection de l'élasticité du réseau

L'allocation flexible et l'attribution à demande des ressources réseau sécurisées sont des caractéristiques de l'environnement infonuagique. Les mécanismes de protection doivent s'adapter à cette élasticité. Afin de permettre à plusieurs locataires de partager dynamiquement la même infrastructure de réseau, la protection de l'élasticité du réseau doit être une priorité pour les prestataires. Ces derniers doivent être en mesure de garantir à la fois l'élasticité des connexions de bout en bout, la protection, la performance et la qualité de service.

## Reprise après incident

La disponibilité est un des trois objectifs de sécurité de l'information. Des données ou un système dans l'infonuagique doivent rester disponibles à tout moment. La reprise après incident ou sinistre représente la capacité de réagir aux incidents catastrophiques et de reprendre les opérations. Ce mécanisme peut garantir la continuité d'un service. Comme dans le cas de l'infonuagique, toutes les ressources sont livrées par le mode « *as a service*» (IAAS, PAAS et SAAS), et le fait que le client exerce peu de contrôle sur la disponibilité est considéré comme plus important dans le contexte de nuage que dans un contexte traditionnel.

## Sécurité physique

La sécurité des sites doit être garantie afin de prévenir les fuites, les vols d’informations ou l’intrusion de personnes non autorisées. Des mécanismes d’identification et de surveillance de l’accès aux locaux et aux équipements doivent être en place. Finalement, les centres de traitement sont dotés des protections environnementales requises contre les causes naturelles (eau, feu, électricité, tremblement de terre, etc.).

# 5. Pratiques de contrôle et de sécurité à adapter

Les OP devront sûrement avoir à adopter de nouvelles pratiques de contrôle et de sécurité afin d'assurer l'intégration harmonieuse des systèmes patrimoniaux aux services acquis dans l'infonuagique, la qualité de la prestation de services et la protection des données dans le respect du cadre contractuel défini avec le prestataire. Il est, par conséquent, essentiel d'aligner la structure, les processus et les procédures organisationnels ainsi que les rôles et responsabilités pour être certain de dégager la valeur ajoutée attendue des services de l'infonuagique et de pouvoir faire confiance aux services en nuage. Les OP doivent s'inspirer des pratiques décrites dans cette section pour adapter leur environnement de contrôle aux réalités de l'infonuagique.

## 5.1 Pratiques administratives

### Encadrement administratif

Afin de répondre à ces risques, le processus d'adoption de l'infonuagique doit suivre le même processus que celui de l'évolution normale des systèmes d'information de l'organisme. L'organisation et la gouvernance des systèmes d'information doivent être adaptées à l'utilisation de l'infonuagique. Il faut anticiper les changements à venir à travers l'intégration de l'infonuagique dans les stratégies d'évolution des systèmes d'information des organismes. Cette intégration devra, en particulier, couvrir la définition d'une politique d'organisme claire relative à la nature des données et des traitements qu'il est acceptable d'externaliser.

En matière d'organisation, l'infonuagique est un vecteur de transformation majeur des processus opérationnels, de l'allocation des rôles et responsabilités, et donc de l'organisation des fonctions en ressources informationnelles, mais aussi des relations entre les autres fonctions de l'organisation. Dans la très grande majorité des cas, le choix de recourir à l'infonuagique concernera la direction des systèmes de l'information et les intervenants en pilotage de projet et de système. L'adoption de l'infonuagique pour des projets touchant des données sensibles ou des systèmes de missions essentielles nécessiterait également une validation de la haute direction de l'organisme. Dans le cas des autres projets, cette décision serait du ressort de la Direction des systèmes d'information. Les services juridiques, le responsable organisationnel de la sécurité de l'information, le responsable de l'AIPRA, et les services informatiques conseillent les détenteurs de l'information et examinent les conditions d'intégration de la prestation au sein des systèmes d'information. Les services de vérification interne contribuent à la maîtrise de l'usage de l'infonuagique en évaluant le processus de sélection, l'environnement de contrôle du prestataire, la gouvernance de la prestation et l'exécution des contrats.

### Contrôle des coûts

Pour pallier ce type de risques, les clients doivent réaliser des études de marché adéquates, notamment en demandant des informations dans un avis d'appel d'intérêt. De plus, les clients devraient envisager d'inclure une équipe de surveillance des services afin d'assurer le suivi financier du contrat de service. Par exemple, le suivi pourrait prendre la forme de rapports quotidiens sur l'utilisation des services. De plus, les OP devront prévoir et obtenir les autorisations adéquates afin d'assurer un financement à long terme des solutions infonuagiques.

### Gestion des compétences

L'introduction de l'infonuagique va également avoir une incidence majeure sur les profils nécessaires au sein des fonctions en ressources informationnelles et pose donc un problème de gestion des compétences que doivent prendre en compte les OP.

## 5.2 Pratiques en ressources informationnelles

Avant de prendre la décision de passer à un environnement de l'infonuagique, les organismes doivent répondre à l'impact sur leurs processus d'affaires et voir à déceler et éliminer les obstacles techniques. Lors du passage à un environnement de l'infonuagique, les organisations devront mettre davantage l'accent sur la conception d'interfaces et des applications aptes à gérer les périodes de latence.

L'organisme doit aussi s'assurer de sa capacité à reprendre l'activité externalisée ou à la transmettre à un autre prestataire avec une rapidité suffisante. Cela nécessite l'acquisition ou le maintien de la connaissance fonctionnelle, applicative et technique. La dépendance au prestataire de la solution de l'infonuagique doit être évaluée régulièrement.

Afin de limiter les conséquences de la dépendance aux prestataires, les conditions de réversibilité doivent être prises en compte dès l'acquisition du service. La nécessité d'obtenir une garantie du prestataire sur la réversibilité de la prestation doit être incluse. Ce plan doit décrire le format des données restituées, définir les conditions de restitution de ces données, traiter la question de leur propriété et de leur destruction, et définir le délai de restitution.

De plus, afin de garantir la réversibilité, il faudrait disposer des moyens de récupération massive des données, tester régulièrement les outils et maintenir des compétences à l'interne. La réversibilité peut prendre la forme d'un transfert de données à un nouveau prestataire de l'infonuagique sans obligatoirement passer par un retour vers l'organisation; la portabilité vers un autre prestataire semble à première vue la plus simple à gérer.

Finalement, afin d'éviter l'enfermement, les OP doivent adapter une stratégie pour des normes et standards ouverts garantissant l'interopérabilité, la portabilité des données ainsi que favoriser l'utilisation de progiciels commerciaux sans adaptation. L'organisme pourrait demander au prestataire de fournir une certification pour les plateformes et versions prévues.

## 5.3 Pratiques en sécurité de l'information

### Gestion de la sécurité

Il est raisonnable de croire qu'à cette étape, l'OP véhicule déjà à l'interne les bonnes pratiques de gouvernance en ce domaine. La catégorisation de l'information, le registre des autorités ne sont que quelques prémisses dans l'éventualité d'un appel vers des services externes, tels que ceux fournis par les prestataires en infonuagique. En l'absence d'un niveau de maturité adéquat, les travaux requis par cette externalisation deviendront beaucoup plus importants à réaliser.

Les solutions d'infonuagique doivent respecter le cadre de gestion de la sécurité de l'OP (politiques, orientations et directives, etc.). Les solutions d'infonuagique doivent contribuer à maintenir les risques à un niveau acceptable pour l'organisme en adéquation avec les règles et les lois provinciales et fédérales.

L'utilisation des services infonuagiques amènera nécessairement une mise au point des processus de travail et de l'environnement technologique qu'il convient de prendre en charge par une gestion du changement bien orchestrée. Il est donc recommandé :

- ✓ De déterminer les modifications à apporter aux pratiques de gouvernance et de gestion de la sécurité de l'organisme afin que soit maintenue une sécurité adéquate des informations tant chez l'organisme que chez le prestataire.
- ✓ De qualifier et définir les changements technologiques et ceux liés aux processus d'affaires, à la localisation et au transport de l'information chez le prestataire.
- ✓ De définir les mécanismes de coordination et d'intégration de la sécurité entre le prestataire et l'OP afin d'assurer la cohérence entre la gouvernance des prestataires et celle de l'organisme, d'établir une coordination et une intégration des opérations et des activités de sécurité.

Une attention particulière doit être apportée à certaines pratiques, ainsi :

- ✓ L'ensemble des documents internes d'encadrement de la sécurité (politique de sécurité, etc.) doit être révisé pour s'adapter aux nouveaux environnements infonuagiques;
- ✓ Tout service d'infonuagique doit faire l'objet d'une catégorisation de sécurité DIC ou de la révision d'une catégorisation existante;
- ✓ Les solutions d'infonuagique ne doivent pas contraindre l'organisme à répondre aux exigences (ex. : licences) des logiciels utilisés par le prestataire de services. Le prestataire demeure responsable de s'assurer que les exigences reliées aux logiciels qu'il utilise sont respectées;
- ✓ Le nouveau mode d'acquisition des ressources en TI aura des répercussions importantes sur les façons de faire de l'organisme. On estime que l'infonuagique doit, en période d'introduction et d'apprentissage, être encadrée et intégrée par l'intermédiaire d'une entité (service, direction, etc.) nommée responsable de l'intégration de l'infonuagique chez l'organisme;
- ✓ On s'attend à ce qu'un service d'infonuagique, implanté et soutenu par son prestataire, occasionne des coûts de mise en place chez l'organisme, notamment pour la formation et, au besoin, l'intégration à l'infrastructure technologique en place;
- ✓ Le cadre de gestion des risques de l'organisme et la grille d'analyse utilisée pour la catégorisation des actifs informationnels doivent être adaptés en fonction des caractéristiques de l'infonuagique. Celle-ci doit s'appuyer sur les prescriptions de différents organismes de normalisation, entre autres, la CSA[4] , l'ISACA[5], l'ISO pour la formalisation de l'analyse de risques. Le lecteur intéressé peut se référer à l'annexe I du présent document pour une analyse des modifications à apporter à différentes pratiques en matière de sécurité. Il est nécessaire de s'appuyer sur l'ISO, le PCI DSS 3.0[6] pour la sécurité de l'information et le développement des applications et l'ITIL 3.0[7] pour la gestion opérationnelle de la sécurité et la gestion des incidents;
- ✓ L'organisme doit aussi se doter d'outils d'analyse pour la sélection du modèle de déploiement et du mode de prestation les plus adaptés aux besoins et aux risques. Le lecteur intéressé peut se référer à l'annexe II du présent document pour une analyse des caractéristiques requises concernant les outils d'analyse;
- ✓ Les préoccupations de sécurisation du cycle de vie des données[8], en raison du contexte de l'infonuagique, principalement en ce qui a trait à la conservation et à la circulation de l'information sur les réseaux et incluant le volet de la destruction des données à la fin d'une entente avec un prestataire, sont jugées critiques;
- ✓ Le cas échéant, si des services infonuagiques doivent être intégrés à des systèmes (ou composants) internes de l'organisme, une évaluation des répercussions doit être réalisée et des mesures doivent être prévues pour résoudre les difficultés d'intégration qui pourraient se présenter;
- ✓ L'organisme doit déléguer au prestataire une partie du contrôle dans le traitement des pannes et des incidents de sécurité, lesquels, autrement, seraient résolus par ses services internes. La gestion des incidents doit donc être adaptée en conséquence;
- ✓ De même, l'organisme doit être en mesure d'obtenir, comme il le ferait à l'interne, du ou des prestataires les preuves légales, sous forme électronique, nécessaires aux différents travaux d'audit ou d'investigation.

4. CSA, *Cloud Security Alliance*, https://cloudsecurityalliance.org/.
5. ISACA, Information Systems Audit and Control Association, https://www.isaca.org/Pages/default.aspx
6. PCI DSS 3.0, *Payment Card Industrie – Data Security Standard*, https://www.pcisecuritystandards.org/security_standards/
7. ITIL v3.0, *Information Technology Infrastructure Library*, http://itil.fr/.
8. http://commons.wikimedia.org/wiki/File:Cycle_de_vie_document-record_mac.png.

## Supervision et reddition de comptes (assurance)

Un OP peut avoir une capacité limitée à prescrire la sécurité pour la protection de l'environnement infonuagique des prestataires. Pourtant, les organismes resteront finalement responsables de l'information qui est stockée ou traitée dans le nuage. L'OP doit obtenir l'assurance que la sécurité du prestataire de services infonuagiques est en conformité avec sa propre politique de sécurité.

Avant d'en céder le contrôle, l'OP devra s'assurer que le prestataire a mis ce qu'il faut en place. Le prestataire doit présenter un répondant technologique et un répondant d'affaires afin de répondre de ses pratiques, services, fonctionnalités de sécurité, en ce qui a trait à la reddition de comptes, à la continuité des affaires et à la gestion du changement.

Selon le besoin, l'OP doit évaluer différentes pratiques de gouvernance, de gestion des identités et des accès, de gestion des problèmes et des incidents de sécurité chez le prestataire, des pratiques d'acquisition ou de développement des fonctionnalités et de leur maintenance, ainsi que des mesures de protection des infrastructures et des plateformes contre les menaces et les vulnérabilités.

Dans le but de limiter la perte de contrôle, il est fortement recommandé d'assurer l'assujettissement aux conditions du contrat par tous les sous-traitants du prestataire primaire. Une limitation du recours aux sous-traitants pourrait être aussi une option visant à limiter la perte de gouvernance. Bien entendu, la conduite d'audits permettra de vérifier les allégations du prestataire à l'égard de sa gestion de la sécurité.

L'OP doit s'assurer que les prestataires de services infonuagiques et leurs offres de services répondent aux exigences du cadre de sécurité de protection de l'information qu'il a élaborées. Il est de la responsabilité du détenteur, un gestionnaire, de s'assurer que le prestataire répond aux exigences légales de protection des renseignements personnels et de la politique en sécurité de l'information. Cette responsabilité ne peut être déléguée au prestataire.

L'appréciation des pratiques, des services et des fonctionnalités doit se faire en fonction de la criticité, de la permanence des services ou fonctionnalités utilisés, et des répercussions sur les activités liées à la mission de l'organisme.

Au chapitre de la gestion des identités et des accès, il est nécessaire d'harmoniser les services d'authentification unique (*single sign-on*) entre le prestataire et l'organisme. Dans la négative, le détenteur doit faire appliquer les règles requises par le prestataire. En principe, le pilote devrait être un employé de l'organisme. Si le pilote relève du prestataire, il n'exécute ses tâches que sous l'autorisation du détenteur désigné chez l'organisme.

En ce qui a trait à la gestion des incidents, le détenteur, en collaboration avec le responsable organisationnel de la sécurité de l'information (ROSI), doit s'assurer de l'existence et de l'application d'un processus de gestion des incidents, arrimer la déclaration des incidents au processus de l'organisme et auditer le processus régulièrement. Ainsi, avant d'arrêter son choix sur un prestataire en particulier, il est impératif de connaître comment le prestataire effectue la surveillance et la gestion des incidents de sécurité. De plus, il est important que l'OP puisse obtenir le droit d'enquêter et l'obligation du prestataire de collaborer en cas d'incident de sécurité (criminalistique).

D'autres exigences liées à la gestion et à la prévention sont à prévoir aux contrats et aux ententes. Pour les déterminer, il est requis d'inventorier et apprécier les pratiques, les services et les fonctionnalités de sécurité utilisés par le prestataire, en plus de préciser les mesures de sécurité pour assurer la confidentialité, l'intégrité et la disponibilité des informations externalisées.

En premier lieu, l'OP doit déterminer le niveau de sécurité requis afin de réduire le risque à un niveau acceptable. Afin de préciser les exigences de sécurité, le détenteur, en collaboration avec l'OP, doit établir une cote DIC (niveau de sécurité). Si la cote est déjà connue pour un actif existant et visé par le projet d'externalisation, elle doit faire l'objet d'une réévaluation. Elle doit tenir compte des spécificités de l'infonuagique et de l'entreposage externe des données de l'OP.

Au sujet des infrastructures, le détenteur, en collaboration avec le ROSI, doit s'assurer d'une gestion diligente en obtenant la liste des bonnes pratiques appliquées et des mesures de protection en place aux

sites de production, de relève et notamment dans tout environnement de pré-production ou de développement.

Dans le contexte de services externalisés de l'infonuagique, le respect des meilleures pratiques en sécurité[9] permet d'assurer à l'organisme une sécurité adéquate selon des normes établies. La nécessité d'auditer régulièrement le prestataire et le service est préconisée par les principaux organismes de normalisation en sécurité. L'obtention des résultats d'audit des prestataires, la réalisation d'audits par l'organisme, la réalisation de tests d'intrusion et de vulnérabilité, même si cela n'est pas toujours possible pour l'infonuagique publique, sont des pratiques importantes.

Plusieurs considèrent même que l'audit est un préalable à l'acquisition du service du prestataire. Soit le prestataire possède les certifications nécessaires en vue d'assurer la conformité et la sécurité de ses services, soit le client doit être en mesure de conduire des audits pour confirmer le respect des obligations du prestataire. Celui-ci doit s'engager à répondre aux demandes d'audit sans quoi ses services peuvent être refusés. Tout contrat de service infonuagique doit permettre à l'organisme d'obtenir un droit d'audit. Les caractéristiques des droits à acquérir par ce moyen afin d'assurer un niveau de sécurité suffisant doivent être établies.

L'OP n'exerçant pas un contrôle direct sur les activités du prestataire, il aura beaucoup de difficulté à assurer la conformité des services offerts, entre autres, sur les pratiques de gestion en RI et en sécurité. Lors du processus d'acquisition, dès l'étude d'opportunité, l'OP aura intérêt à préciser les exigences qui concernent les certifications de contrôle ou de sécurité que doit détenir le prestataire (ex. : PCI). Dans le cas où la certification serait impossible, il est préférable de privilégier les prestataires qui font preuve de transparence en permettant les audits ou qui font les efforts financiers requis afin d'améliorer ou certifier les mesures mises en place pour respecter les standards de l'industrie. Finalement, les OP attendent, aussi, de la part du prestataire, de la transparence sur les incidents à la sécurité et à la préservation de la confidentialité des renseignements personnels, ainsi que sur les résultats des exercices de plan de continuité des opérations et de plan de secours.

## Continuité des services

La continuité des services et la protection des actifs informationnels sont des éléments critiques importants pour l'OP. Les services infonuagiques doivent répondre aux exigences de disponibilité découlant de la cote DIC correspondante évaluée par l'OP, dont la criticité et d'autres préoccupations. Il est impératif que l'organisme demeure le seul et unique propriétaire de ses données et, selon le service infonuagique, de ses traitements. Dans une solution d'infonuagique, les actifs informationnels de l'OP doivent lui être rendus accessibles et récupérables afin d'être migrés soit à l'interne, soit vers un prestataire équivalent, principalement à la fin du contrat.

Lorsque nécessaire, toute solution d'infonuagique doit être interopérable avec les solutions technologiques et les services communs concernés de l'OP, et ce, dans le respect des exigences de sécurité.

La pérennité des solutions infonuagiques doit être garantie pour toute la durée des contrats. C'est pourquoi il faut, par exemple, dans les ententes contractuelles, se protéger le mieux possible contre la fermeture ou la vente d'entreprises, notamment contre les effets de lois étrangères telles que le *USA PATRIOT Act* des États-Unis.

À l'instar des autres types de services externalisés, tels que l'impartition, la viabilité des prestataires (qui inclut aussi leur solidité financière) est un facteur important dans la livraison de services de qualité. Aussi, les ententes doivent prévoir des dispositions particulières pour protéger l'OP en cas de rachat ou de fermeture du prestataire.

9 . Telles que les versions les plus récentes de CSA , COBIT, ISO 27002, PCI.

Finalement les principales activités à élaborer ou à réviser en fonction de l'infonuagique sont :

- ✓ Adapter le plan de continuité des services;
- ✓ Développer un plan de réversibilité;
- ✓ Définir les exigences sur la portabilité et l'interopérabilité des données;
- ✓ Prévoir des clauses de fin de relation d'affaires avec le prestataire;
- ✓ Recourir à des clauses parapluie qui engagent les sous-traitants envers le prestataire d'infonuagique.

## Gestion contractuelle

L'encadrement contractuel des prestations de l'infonuagique constitue une pratique importante contribuant au contrôle de la prestation, entre autres, sur les aspects de sécurité. À ce chapitre, différents organismes de normalisation recommandent de renforcer les obligations du prestataire. En plus, tout changement dans la nature de la prestation doit être maîtrisé, y compris dans les versions logicielles. L'organisme client d'une offre infonuagique doit mettre en place un pilotage contractuel continu, en s'appuyant sur des clauses de pénalité à utiliser en cas d'insuffisances dans le service rendu par le prestataire. L'encadrement contractuel doit également permettre d'obtenir la visibilité sur l'organisation du prestataire, notamment en matière de sous-traitance éventuelle.

En passant à un mode de facturation à l'usage, l'organisme doit ajuster sa façon de suivre et de contrôler les résultats de ses services d'affaires, y compris son suivi budgétaire. Le suivi et le contrôle des résultats sont jugés essentiels. Dans le contexte de l'infonuagique, ce suivi nécessite la revue diligente des résultats livrés par le prestataire de services. Il est nécessaire de mettre en place une entente de services avec les prestataires, notamment pour le maintien et le suivi des niveaux de service tant sur des aspects de contrôle et de sécurité.

Bien que le service d'infonuagique soit, à la base, soutenu par son propre prestataire, l'organisme doit lui aussi déployer des efforts pour faire le suivi de la qualité des services livrés par le prestataire, notamment pour s'assurer que les besoins et les préoccupations de l'organisme sont pris en compte. Plus précisément, voici l'approche préconisée pour mettre en place la supervision et la reddition de comptes sur la prestation de services comprenant des aspects de contrôle et de sécurité des informations pour les services et les applications externalisés :

- ✓ Les services infonuagiques doivent répondre au niveau de service prévu, notamment en matière de disponibilité, de capacité, de performance et de sécurité. Ils doivent donc être définis clairement dans les ententes contractuelles.
- ✓ Les niveaux de service doivent être mesurés quotidiennement (voire en temps réel) et les écarts par rapport aux objectifs attendus, comblés par les ajustements nécessaires. Des pénalités devraient être prévues le cas échéant.
- ✓ L'organisme requiert que des mesures documentées et vérifiables soient en place pour assurer le contrôle, la sécurité, la PRP et la reprise des services en cas de problème majeur au chapitre de la disponibilité (haute disponibilité et reprise en cas de sinistre).
- ✓ La gestion du contrat et des ententes de services nécessite la définition d'indicateurs de gestion. Pour s'assurer d'obtenir un service répondant à ses attentes, l'organisme a besoin d'outils (métriques, indicateurs de gestion et tableaux de bord, analyses de services) pour en suivre la progression.
- ✓ Le contrôle des sous-traitants requiert une attention particulière. Il est attendu que le prestataire, le signataire contractuel de services infonuagiques, est le seul responsable de la qualité des services rendus. Cependant, s'il peut faire appel à des sous-traitants, prestataires de services infonuagiques ou non, on estime que le risque pour l'organisme augmente dans ces situations. Ce risque devra être connu, mesuré et géré avant la signature des ententes contractuelles.

- ✓ La fixation des modalités de la déclaration de reddition de comptes par le prestataire est importante afin que l'organisme soit avisé formellement des changements technologiques planifiés pouvant avoir des répercussions sur la disponibilité des services, ainsi que tout incident pouvant compromettre la qualité de la prestation, le contrôle, la sécurité et la PRP. L'OP doit être informé également des sous-traitants pendant la durée de l'entente. Pour répondre aux exigences gouvernementales, la déclaration doit se faire au minimum tous les deux ans.
- ✓ Le suivi de fin de contrat demande la production d'un bilan. Au terme d'un contrat avec un prestataire de services infonuagiques, un bilan doit donc être réalisé. Ce bilan doit couvrir, au minimum, les résultats attendus et obtenus, les problèmes rencontrés et les solutions mises en place, les coûts et les bénéfices prévus et réalisés ainsi que les leçons apprises.

Pour un complément d'information se référer à l'annexe III – Liste de vérification relative à la présence de clauses portant sur la sécurité

# 6. Possibilités offertes par l'infonuagique en matière de sécurité

Le recours à l'infonuagique peut s'avérer utile dans l'acquisition des ressources de sécurité spécialisées ou d'importance pour l'OP. Le prestataire devient un spécialiste en matière de sécurité, car il doit acquérir cette expertise afin de répondre aux exigences de nombreux clients. Il doit mettre en place et documenter un nombre élevé de pratiques de sécurité. Le prestataire doit donc disposer à l'interne, entre autres, d'une politique sur l'accès à l'information, la protection de la vie privée et la sécurité, d'un plan de continuité, de ressources qualifiées, de guides et de rapports d'audit ou de certification pour démontrer la robustesse et la permanence des processus et des services d'accès à l'information, de protection des renseignements personnels et de sécurité en place.

Le recours à l'infonuagique favorise l'agilité par l'amélioration de la disponibilité des services, de la capacité de reprise après sinistre ou de la résilience aux demandes de services de sécurité imprévues**.** Le prestataire doit répondre à des attentes d'accessibilité aux services externalisés, selon les besoins de l'OP en disponibilité et à ses exigences, établies par la catégorisation de l'information (DIC) et l'analyse des risques. Le prestataire doit prévoir, entre autres, des prises de copies selon les exigences de l'OP, une synchronisation des activités de récupération et de reprise à la suite d'un sinistre ainsi que des services de migration pour faciliter l'entrée et la sortie des services infonuagiques.

L'infonuagique peut être le moyen pour améliorer la réponse de sécurité grâce à l'uniformité, la robustesse et l'évolutivité des plateformes de sécurité offertes par les prestataires. Le prestataire doit coordonner avec l'OP l'utilisation de l'infonuagique en ce qui concerne les interfaces. L'interopérabilité passe par des normes ouvertes, facilitant le choix des services. Le prestataire doit garantir un cloisonnement parfait pour protéger l'accès aux actifs de l'OP de tout autre client, ainsi que pour protéger les actifs critiques à l'intérieur même des unités de l'OP.

L'infonuagique peut être l'occasion de transférer davantage de services de sécurité vers le prestataire de services infonuagiques. Celle-ci devient intéressante si l'on considère les économies matérielles et logicielles, la redondance des moyens, le stockage à grande échelle, etc. L'infonuagique peut être aussi l'occasion d'utiliser des services infonuagiques comme solution de rechange afin d'améliorer la capacité de sécurité globale et réelle de l'OP. Les services infonuagiques peuvent offrir des niveaux de sécurité supérieurs à ceux en place dans les OP, en particulier, ceux de petite et moyenne taille.

# 7. Défi de l'infonuagique : la confiance

Afin de favoriser l'utilisation de l'infonuagique, il faut mettre en place un ensemble de conditions qui font que les OP qui ont recours à ce type de services aient l'assurance que les services acquis répondent à leurs besoins informatiques, y compris ceux liés au contrôle, à la sécurité, à la protection des renseignements personnels et à la disponibilité des services.

À court et à long terme, ces actions contribueront à accroître la confiance des OP et celle des citoyens à l'égard de l'utilisation des services infonuagiques en atténuant les conséquences des divers risques qui y sont associés. Pour établir cette relation de confiance, plusieurs conditions doivent être réunies.

Entre autres, l'environnement de contrôle et l'architecture de sécurité de la solution infonuagique du prestataire de services respectent les exigences de contrôle et la politique de sécurité de l'organisme, les exigences de protection des renseignements personnels, présente des garanties de contrôle et de sécurité au moins égales à celles de l'OP et respecte les exigences légales.

Tel un partenaire, le prestataire de services infonuagiques reste transparent et informe l'OP de tout incident ou faille de sécurité, tient à jour ses politiques internes de contrôle et de sécurité et avise l'OP que tout sous-traitant agit selon des exigences de contrôle et de sécurité au moins semblables à celles du prestataire. De plus, il accepte d'être vérifié (audité) pour que la capacité de reprise du prestataire réponde aux exigences de l'OP, établies par la catégorisation de l'information et l'analyse des risques.

Le prestataire doit être flexible dans ses solutions de contrôle et de sécurité, et il assure l'interopérabilité et l'évolution des solutions technologiques de sécurité en tenant compte de la capacité de l'OP. Car l'organisme conserve sa responsabilité quant au contrôle de ses données, tout au long de leur cycle de vie. Le prestataire garantit la réversibilité et la remise à l'OP des données hébergées, il l'assure que sa gestion des accès (authentification) fait en sorte qu'aucune personne non autorisée n'y aura accès.

Les éléments de gouvernance et de gestion de la sécurité confiés aux prestataires infonuagiques devront convenir à l'OP et lui permettre de poursuivre le respect de leur politique de sécurité visant à garantir le maintien de la qualité des pratiques et des mesures de sécurité adéquates. Les ententes de service et les clauses des contrats liant l'organisme au prestataire devront satisfaire aux exigences de reddition de comptes, de conformité, de surveillance, de contrôle, de sécurité et de protection des renseignements personnels et confidentiels de l'OP.

Au moment de s'approprier ces nouvelles façons de faire, une approche par étape doit être préconisée pour une transition progressive afin de mieux appréhender les risques. Une révision périodique des risques et des éléments de contrôle et de sécurité demeure cependant incontournable pour maintenir le contrôle et la sécurité globale de l'utilisation de l'infonuagique et surtout, l'organisme doit être en mesure de s'en assurer.

# Annexe I – Cadre de gestion des risques adapté à l'infonuagique

Un cadre de gestion des risques adapté à l'infonuagique utilise un processus de catégorisation des actifs informationnels (processus, données, applications) et, selon la portée de l'analyse, différents types de critères d'évaluation seront employés (contrôle, sécurité[10], financier, etc.). Le processus de catégorisation permet d'établir des exigences selon les caractéristiques des actifs et de leur valeur. Les exigences définies à cette étape doivent servir à établir des critères qui alimenteront le cahier des charges de l'appel d'offres. Les OP doivent considérer, afin d'alléger le processus d'analyse, prédéfinir des classes d'actifs informationnels dont la sensibilité ou la criticité limiteront leur transfert vers l'infonuagique à certains modes de déploiement, ou empêcheront leur transfert si le risque d'altération, de perte ou de divulgation est considéré comme trop élevé par ceux-ci.

Lors de la préparation de l'appel d'offres, le cadre de gestion des risques doit prévoir une étape d'analyse d'impact afin d'étudier les facteurs de risque propres à l'infonuagique qui peuvent réduire ou accroître les conséquences des menaces aux actifs externalisés. Cet exercice permet à l'OP de comprendre comment la migration de ses actifs informationnels vers l'infonuagique va influer sur le niveau de risque actuel. Une fois cette étape réalisée, de nouvelles exigences peuvent être formulées afin de réduire ou maintenir les risques potentiels à un niveau acceptable. Elles doivent s'ajouter à la liste des critères de l'appel d'offres.

En ce qui concerne plus précisément les domaines du contrôle, de la protection des renseignements personnels ou autrement confidentiels et de la sécurité, il faut prévoir des conditions, lorsque requis, demandant au prestataire de services de présenter avec son offre soit un rapport d'audit annuel ou un rapport de certification, ou encore, autoriser l'OP à organiser lui-même un audit ou tout autre procédé d'appréciation (questionnaire de contrôle interne, de contrôle financier, de sécurité). Le recours à ces moyens permet à l'OP d'apprécier la capacité du prestataire de maintenir un environnement contrôlé et sécurisé tout en assurant la protection des renseignements personnels ou autrement confidentiels. Les rapports présentés par le prestataire doivent être préparés par une firme indépendante et répondre aux prescriptions d'un organisme de normalisation reconnu en matière de contrôle, de protection des renseignements personnels ou de sécurité.

De plus, le cadre de gestion des risques doit prévoir, lors de l'analyse de conformité des soumissions des prestataires aux critères de l'appel d'offres, une actualisation de l'analyse de risques. À la réception des soumissions et après la vérification des exigences obligatoires, l'examen par l'OP des rapports d'audit ou de certification, ou de tout autre document d'appréciation pour le ou les prestataires conformes, peut relever des lacunes dont les effets doivent être évalués. Une fois l'analyse terminée, l'OP détermine quels sont les risques qui doivent être réduits. Il convient de les gérer et de déterminer quelles mesures de sécurité réduisent ces risques à un niveau acceptable. Il est important de bien établir les mesures de mitigation qui devront faire l'objet de clauses particulières à l'entente avec le prestataire. L'OP peut imposer des clauses contractuelles au prestataire de services infonuagiques pour diminuer certains risques.

Il est à souligner que tout au long de la réalisation de ces différents travaux le détenteur des actifs informationnels externalisés participe à ces processus ou en est informé. Durant ces travaux, il faut déterminer les conditions d'acceptation des risques et obtenir l'acceptation de la part du ou des détenteurs de l'information engagés dans le projet d'infonuagique, seul le détenteur de l'information pouvant décider si un risque résiduel est acceptable ou non.

10. Pour plus d'information sur la catégorisation en matière de sécurité, voir le Guide relatif à la catégorisation des documents technologiques en matière de sécurité. Ce guide peut être consulté sur le site du réseau d'expertise et de vigie en sécurité (REVSI). Pour l'obtenir, vous devez communiquer avec le responsable organisationnel en sécurité de l'information (ROSI) de votre organisation.

Finalement, il faut considérer que la gestion du contrôle, de l'accès, de la protection des renseignements personnels ou autrement confidentiels et de la sécurité sont des processus continus, c'est-à-dire qu'ils ne s'arrêtent pas à l'établissement d'un service dans l'infonuagique. Les OP doivent être en mesure d'évaluer les risques de façon continue pendant l'exploitation du service infonuagique. L'OP utilisateur de services infonuagiques doit vérifier régulièrement que le prestataire de services remplit ses obligations contractuelles et, s'il le faut, obtenir des preuves. De plus, il est souhaitable que l'OP obtienne de façon systématique des rapports sur les incidents survenus en matière de contrôle, d'atteinte à la vie privée, de sécurité ou d'interruption de service afin de valider, entre autres, l'évaluation des risques.

# Annexe II – Critères d'analyse pour la sélection d'un service infonuagique

Au moment d'adapter leur cadre de gestion des risques, il est souhaitable que les OP se dotent aussi d'outils d'analyse pour faciliter la sélection du modèle de prestation de services ou du mode de déploiement le plus adapté aux caractéristiques des technologies à acquérir (services), des informations qui seront externalisées et des risques qui peuvent les affecter. L'utilisation d'une grille d'analyse, sous forme d'arbre de décision, peut s'avérer un outil utile pour représenter des situations complexes de façon à faire apparaître les différents résultats possibles en fonction des décisions prises à chaque étape. Cet outil doit permettre l'analyse multifactorielle.

L'analyse pour la sélection d'un modèle de prestation de services a pour objectifs d'évaluer si l'acquisition d'un service de prestation infonuagique représente une solution technologique valide et de déterminer quel modèle de prestation (IaaS, PaaS, SaaS) convient le mieux au traitement considéré par l'OP. Une telle analyse permet non seulement de choisir l'offre la plus adaptée aux besoins d'affaires de l'OP, mais également de garantir une meilleure identification des contraintes technologiques. L'outil d'analyse vise donc, dans un premier temps, à évaluer des facteurs technologiques qui limiteraient ou empêcheraient la migration du service vers l'infonuagique. Les facteurs utilisés doivent permettre l'appréciation du degré de normalisation et d'indépendance des services à externaliser ainsi que du niveau de personnalisation des technologies utilisées pour le service à externaliser (applicatifs, logiciels systèmes, équipements). Il est avantageux de compléter l'analyse par l'utilisation de critères économiques afin d'évaluer la capacité d'atteindre les bénéfices attendus de l'acquisition d'un service de prestation infonuagique tenant compte des contraintes révélées par l'analyse des facteurs technologiques.

En ce qui a trait au choix du mode de déploiement, le facteur déterminant est le degré de confiance qui lie les participants; le prestataire de services et les clients ou les clients entre eux. Pour déterminer le mode de prestation de services le plus adapté, l'outil d'analyse doit se concentrer premièrement sur l'appréciation des facteurs de criticité et de sensibilité du service et des informations à externaliser, ainsi que des risques propres aux différents modes de prestation. En particulier, les risques associés à la localisation des données, à la propriété des données et à la conformité légale aux cadres législatifs et réglementaires. Dans un second temps, l'outil utilise d'autres critères qui cherchent à apprécier le niveau d'assurance (de contrôle) que peut obtenir l'OP par la négociation d'un contrat et des niveaux de service tenant compte de la criticité des services ou informations externalisés et des risques.

Avant d'identifier le modèle de prestation ou le mode de déploiement, il est indispensable que l'OP se dote d'une stratégie afin d'orienter les divers aspects de l'infonuagique qui tiennent compte de ses besoins d'affaires et favorisent l'atteinte de ces objectifs. De plus, l'OP doit avoir procédé à une analyse des possibilités existantes dans le marché et vérifier si elles s'alignent sur les besoins d'affaires définis, les coûts prévus et si elles répondent à l'ensemble des exigences fonctionnelles, techniques, de conformité, de contrôle, d'accès, de protection des renseignements personnels ou autrement confidentiels et de sécurité.

# Annexe III – Liste de vérification relative à la présence de clauses portant sur la sécurité

Les clauses contractuelles se veulent le reflet de l'état des risques résiduels auxquels l'organisme aura consenti. Puisque le résultat de l'analyse de risques dépend des exigences de sécurité élaborées à la suite de la catégorisation des informations, il est essentiel que ces exigences soient présentes dans les clauses. De même, il faut être en mesure d'inclure des clauses permettant d'évaluer les mesures (actuelles ou recommandées) ayant été établies lors de l'analyse de risques de la solution.

Au moment de l'élaboration des exigences du prestataire, il est également possible que l'organisme doive s'engager à respecter lui-même certaines exigences. Par exemple, le prestataire peut exiger de l'organisme qu'un service d'impression externe soit accessible selon les mêmes modalités que celles incluses dans l'entente.

Les critères suivants représentent une liste non exhaustive des clauses pouvant être incluses dans une entente avec le prestataire de services. Ces clauses peuvent varier en fonction du type de service, du mode d'infonuagique, des exigences de sécurité sans oublier les clauses légales que le prestataire devra respecter.

## Gouvernance

La gouvernance doit être prise en compte autant que les mesures de sécurité. Si elle est bien gérée, elle offre un encadrement permettant le maintien des exigences de l'entente et un arrimage adéquat entre le prestataire et l'organisme.

Liste de vérification :

Est-ce que le prestataire a mis en place des politiques et des procédures en vue de restreindre l'accès à l'information hébergée? ☐

Préciser : _____

Est-ce que le prestataire a mis en place un cadre de gestion de la sécurité de l'information? : ☐

Préciser : _____

Y a-t-il un processus d'autorisation pour les activités relatives à la sécurité? ☐

Préciser : _____

Y a-t-il une gestion des ententes de confidentialité du personnel et des sous-traitants? ☐

Préciser : _____

Est-ce que le prestataire s'engage à lier les sous-traitants à l'entente? ☐

Préciser : _____

Est-ce que des documents d'engagement ou d'accréditation sont à faire signer?

Engagement de confidentialité ☐

Engagement de sécurité (selon le niveau de confidentialité requis) ☐

Accréditation de sécurité (selon le niveau de confidentialité requis) ☐

_____

Est-ce que le prestataire a mis en place une gestion des incidents et des réponses? ☐

Préciser : _____

Est-ce que le prestataire s'engage à arrimer son comité de crise à celui de l'organisme? ☐

Préciser : _____

Est-ce que le prestataire a une description des rôles et des responsabilités du personnel? ☐

Préciser : _____

Est-ce qu'une évaluation continue est nécessaire afin d'évaluer la performance du prestataire? ☐

Quelles sont les informations requises? (rapports, journaux, validation, etc.)

Préciser : _____

Est-ce que l'organisme doit prévoir un processus ou un recours en responsabilité pour divulgation d'information confidentielle? ☐

Préciser : _____

Est-ce que les clauses de pénalités sont clairement indiquées? ☐

Préciser : _____

# Audit et supervision

L'audit et la supervision sont des moyens de contrôle permettant à l'organisme de vérifier l'application des clauses de l'entente de même que les mesures de sécurité telles que précisées lors de l'analyse de risques. L'absence ou l'application incorrecte de mesures de sécurité aura une influence sur les risques résiduels ayant été acceptés par l'organisme.

Liste de vérification :

Est-ce que l'entente doit inclure des activités d'audit chez le prestataire? ☐

Si oui, quelles normes de vérification doivent être appliquées?

Préciser :
_____

Est-ce que les coûts d'audit sont inscrits à l'entente? ☐

Si oui, qui les assumera?

Préciser : _____
_____

Est-ce qu'un audit doit être réalisé lors de l'activation du service? ☐

Préciser :
_____

Est-ce que l'entente prévoit un processus pour le suivi du rapport d'audit sur les constatations et les recommandations? ☐

Préciser :
_____

Est-ce que la portée et l'étendue des audits ont été définies? (examen, vérification, certification, etc.) ☐

Préciser :
_____

Est-ce que le mandat d'audit sera réalisé par des auditeurs?

Si oui, des auditeurs internes? ☐

Si oui, des auditeurs externes? ☐

Est-ce que le rapport d'audit sera distribué? Identifier es personnes ☐

_____

Existe-t-il des clauses de recours possible à la suite des constatations d'audit? Les indiquer ☐

_____

# Niveaux de service

Les niveaux de service de la sécurité correspondent, pour la plupart, aux exigences de sécurité élaborées à la suite de la catégorisation des informations.

Liste de vérification :

Disponibilité

Est-ce nécessaire d’avoir un service opérationnel en mode 24/7 ou de 8 h à 18 h? Quelle disponibilité de services est attendue? L’indiquer ☐

_____

Est-ce que la capacité de traitement requise est précisée? L’indiquer (niveau de performance attendu, temps de réponse du service)? ☐

_____

Est-ce que le prestataire sera tenu de fournir un registre des périodes de maintenance? Indiquer la fréquence. ☐

_____

Est-ce que la quantité de perte de données maximale admissible a été fixée? L’indiquer ☐

_____

Est-ce que le délai maximal entre la prise de copie et la perte de données a été établi (pour un recouvrement complet ou partiel)? L’indiquer ☐

_____

Est-ce que le temps maximal alloué pour la correction des problèmes a été fixé? L’indiquer ☐

_____

Est-ce que le temps maximal alloué pour assurer la continuité des services a été établi? L’indiquer ☐

_____

Intégrité ☐

Doit-on prévoir une procédure de notification en cas de bris de confidentialité? ☐

Existe-t-il une clause portant sur une procédure de correction des dommages advenant la perte de données accidentelle ou délibérée? L’indiquer ☐

_____

Est-ce que le prestataire doit mettre en place un processus de destruction sécuritaire des informations? ☐

Résolution de problèmes ☐

Est-ce que des exigences de temps maximal ont été fixées pour :

Rendre compte des événements de sécurité? L'indiquer _____ ☐

Résoudre des problèmes de sécurité? L'indiquer _____ ☐

Appliquer les correctifs de sécurité? L'indiquer _____ ☐

Est-ce que le délai de transmission des rapports périodiques sur les problèmes, les audits et les rapports de système a été fixé? L'indiquer_____ ☐

## Opérations sécurisées

Quelques opérations sécurisées doivent être spécifiées lors de l'élaboration de l'entente. Ces opérations peuvent être réalisées par le prestataire ou conjointement avec l'organisme.

Liste de vérification :

Doit-il y avoir un processus de gestion du changement (approbation des changements selon un calendrier de maintenance)? ☐

Préciser : :_____

Est-ce que les politiques, normes et méthodes de destruction sécuritaire des données sont établies? ☐

Préciser : :_____

- Si oui, est-ce que la couverture de l'ensemble des localisations a été décrite? ☐

Doit-on prévoir des services d'assistance (assistance requise)? ☐

- Si oui, établir les niveaux de disponibilité des services d'assistance.

Préciser :_____

## Terminaison de service

Devant la possibilité d'une cessation des activités d'une entreprise, il y aura lieu de prévoir des clauses permettant de protéger l'organisme ou, à tout le moins, minimiser les conséquences d'un arrêt éventuel. Les clauses, outre celles légales, doivent porter sur les informations hébergées chez le prestataire. À cet effet, l'organisme aura prévu, dans son plan de continuité des affaires, une activité en cas d'arrêt du service chez le prestataire.

Liste de vérification :

- ✓ Retrait des comptes utilisateurs et des droits d'accès (retrait effectué en temps opportun) ☐

Préciser : _____

- ✓ Traitement de la documentation (destruction ou retour sécuritaire des informations à l'organisme). ☐

Préciser : _____

- ✓ Obligations contractuelles (ex. : maintien de l'exigence de confidentialité). ☐

Préciser : _____

- ✓ Clauses en cas de fin de relation d'affaires avec le prestataire, planifiée ou rupture de contrat, pour services inadéquats, faillite du prestataire ou dispute du prestataire avec des tiers. ☐

Préciser : _____

- ✓ Provisions concernant le non-respect de l'entente de service prévoyant la fin de contrat et les pénalités. ☐

Préciser : _____

# Références


Australie, *Cloud Computing Security Considerations*, http://www.asd.gov.au/infosec/cloudsecurity.htm

*Cloud Security Alliance*, *Cloud Computing Top Threats in 2013*, https://cloudsecurityalliance.org

*Cloud Security Alliance*, *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*, https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

*Cloud Security Alliance*, *Cloud Controls Matrix v3.0*, https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/

*Cloud Standards Customer Council (2012, Security for Cloud Computing: 10 Steps to Ensure Success,* http://www.cloud-council.org/Security_for_Cloud_Computing-Final_080912.pdf

*Cloud Standards Customer Council (2012*). *Practical Guide to Cloud SLAs,* http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_to_Cloud_SLAs.pdf

ENISA*, Cloud Computing: Benefits, risks and recommendations for information security, 2012,* http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

ENISA*, Cloud Computing: Information Assurance Framework,* http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework

ENISA*, Good Practice Guide for securely deploying Governmental Clouds,* *http://www.globalregulatoryenforcementlawblog.com/2014/01/articles/data-security/enisa-publishes-report-good-practice-guide-on-government-cloud-deployment/*

ENISA*, Procure Secure: A guide to monitoring of security service levels in cloud contracts,* http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-*service-levels-in-cloud-contracts*

ISACA*, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives* *http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx*

ISACA*, Security Considerations for Cloud Computing,* http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Security-Considerations-for-Cloud-Computing.aspx

ISACA, *IT Control Objectives for Cloud Computing*, *http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Cloud-Computing-Controls-and-Assurance-in-the-Cloud.aspx*

NIST Special Publication 800-144, *Guidelines on Security and Privacy in Public Cloud Computing,* http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

NIST*, Inventory of Standards Relevant to Cloud Computing,*

http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique