Volet Infrastructures

Guide de l'infonuagique

Volume 4 - Considérations en gestion contractuelle

Architecture d'entreprise gouvernementale 3.1

Québec

Volet Infrastructures

Guide de l’infonuagique

Volume 4 - Considérations en gestion contractuelle

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 978-2-550-72560-2 (en ligne)

Table des matières

Liste des sigles et acronymes

AIPRP	Accès à l'information et protection des renseignements personnels
IaaS	*Infrastructure as a Service*
LCOP	Loi sur les contrats des organismes publics
PRP	Protection des renseignements personnels
PaaS	*Plateform as a Service*
SaaS	*Software as a Service*
SCT	Secrétariat du Conseil du trésor
SEOA	Système électronique d'appels d'offres du gouvernement du Québec
SLA	*Service Level Agreement*
SSMP	Sous-secrétariat aux marchés publics
OP	Organisme public
RI	Ressources informationnelles
TI	Technologies de l'information

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 Volume 4 - Considérations en gestion contractuelle du Guide de l'infonuagique, ne constitue pas un manuel de gestion de projet ni un avis juridique et ne peut prétendre se substituer aux textes et lois en vigueur. Nous invitons les organismes publics à adresser leurs commentaires et leurs suggestions afin d'améliorer ce document au Sous-secrétariat du Dirigeant principal de l'information et le Sous-secrétariat des marchés publics, responsables de son élaboration.

L'emploi du 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 document peut être élargie à d'autres organisations telles que les entreprises du gouvernement et les municipalités.

Ce document est produit à titre de document de référence et 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. Leviers 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 perspectives 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 le maintien de la confiance du public envers les organismes qui y ont recours.

Ce document constitue un outil de référence pour l'OP qui envisage d'avoir recours à l'infonuagique. Il met en lumière les différentes caractéristiques de ce nouveau mode de prestation de services, et propose une démarche et des étapes à suivre pour son utilisation. Dans l'élaboration de ses besoins, l'organisme devra déterminer quel service infonuagique et quel mode de déploiement conviennent le mieux, en fonction, notamment, de la nature (portée, répercussions sur l'organisation, etc.) du service qu'il souhaite acquérir et du type d'information à héberger dans le nuage. Au terme de l'analyse de ses besoins, il pourra, s'il y a lieu, envisager de multiples approches pour faire face aux risques que peut présenter cette technologie; il pourra, par exemple, 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 fournisseur, 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 acquérir un service infonuagique. 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 d'atténuation 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 à la protection des renseignements personnels ou

confidentiels, 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 futurs projets.

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

Cynthia Morin	CSPQ	Marie-Claude Landry	CSPQ
Dieu Hang	SCT	Martin Saint-Amand	RAMQ
François Bélanger	SCT		

Ce document a fait l'objet d'un cycle de validation par les personnes suivantes :

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		

Parallèlement aux travaux d'élaboration de ce guide, le gouvernement du Québec a mandaté le Centre de recherche en droit public de l'Université de Montréal pour la réalisation d'une **Erreur ! Référence de lien hypertexte non valide.**. Cette étude se veut une analyse des risques et contraintes juridiques associés à l'infonuagique. Outre les éléments juridiques soulevés dans cette étude, 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 consulter le responsable de l'accès à l'information et de la protection des renseignements personnels (AIPRP) de chaque organisme.

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'opération des infrastructures technologiques et des applications. Il s'agit d'un nouveau mode d'acquisition qui permet aux personnes et aux organisations d'accéder, par les technologies d'Internet, à un bassin de ressources informatiques pouvant être configurées et externalisées 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 fournisseur infonuagique de façon automatisée et sur demande. La consommation des services est mesurée et facturée selon l'utilisation. L'infonuagique présente plusieurs avantages et bénéfices pour les utilisateurs. En effet, les ressources infonuagiques offrent une agilité et une flexibilité d'utilisation, puisqu'elles s'acquièrent rapidement, s'adaptent facilement à la demande et permettent un délestage tout aussi rapide. De plus, l'infonuagique offre la possibilité de réaliser 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 celui des États-Unis, celui du Royaume-Uni et celui de l'Australie, considèrent que l'infonuagique est un levier de transformation et d'économie important. D'ailleurs, ces pays ont élaboré des stratégies d'adoption et leurs initiatives infonuagiques gouvernementales sont nombreuses. Toutefois, malgré les perspectives intéressantes qu'offre l'infonuagique, il existe des préoccupations et des risques inhérents à son utilisation, tant au niveau juridique qu'en ce qui a trait à la protection des renseignements personnels (PRP) et à la sécurité des données.

Afin de bien tirer profit des bénéfices et de saisir pleinement les avantages qu'offre l'infonuagique, le dirigeant principal de l'information a mandaté un groupe de travail interministériel dont l'objectif était de réaliser le présent 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 que les organisations portent à l'infonuagique, l'objectif du présent guide est de fournir toute l'information pertinente aux OP qui désirent recourir à de tels services, dans le but d'encadrer cette pratique de façon appropriée et sécuritaire. Le guide vise, entre autres, les objectifs suivants :

- ✓ offrir de l'information sur la signification et la portée des services infonuagiques;
- ✓ dresser la liste des questions à se poser et proposer des pratiques à envisager, entre autres :
  - la prise en compte des enjeux et des risques qui sont associés au projet, dès les étapes d'analyse préliminaire ou d'étude d'opportunité, et tout au long de sa réalisation;
  - le respect des exigences en matière de protection des renseignements personnels ou confidentiels, et de sécurité de l'information;
  - la réglementation contractuelle applicable et la gestion des services infonuagiques;
  - la gestion de projet.

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

Exemples de questions auxquelles le guide se propose d'apporter des éléments de réponse :

- ✓ Quels sont les avantages de l'infonuagique par rapport aux solutions traditionnelles?
- ✓ Quels sont les services, les traitements et les données susceptibles de migrer vers l'infonuagique?
- ✓ Quels sont les risques à maîtriser?
- ✓ Quelles sont les considérations juridiques à respecter?
- ✓ Quelles sont les exigences de PRP et de sécurité à prendre en compte?
- ✓ Comment définir les modalités contractuelles avec un fournisseur infonuagique et comment en sélectionner un?

En dernier lieu, 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 juridiques ou administratives ou de toutes les normes et 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 également pris en considération dans le cadre du projet ciblé.

1.2 Présentation du contenu

Le présent document, intitulé Volume 4 – Considérations en gestion contractuelle, est le dernier de quatre volumes. Il présente l'information contractuelle permettant de guider les OP dans l'élaboration de leurs documents d'appel d'offres et de leurs contrats relatifs à l'infonuagique. Toutefois, cette information ne peut se substituer à une analyse adéquate et rigoureuse des besoins et du contexte de l'OP. Il est donc conseillé que l'OP, en amont de son projet, établisse ses besoins et la meilleure stratégie à mettre en place pour répondre à ceux-ci, en consultant son service de gestion contractuelle, et, au besoin, son service des affaires juridiques.

Quant aux autres volumes (1, 2 et 3) du guide de référence, ils sont constitués de différentes sections détaillées qui approfondissent divers enjeux relatifs à l'infonuagique, notamment les notions fondamentales de l'infonuagique (volume 1), les considérations juridiques et de protection des renseignements personnels (volume 2) ainsi que le contrôle et la sécurité (volume 3). Ils ont été élaborés dans le but d'outiller et d'orienter les spécialistes juridiques et de sécurité ainsi que les analystes des organismes publics, lors de l'analyse et de l'évaluation des risques.

2. Considérations en gestion contractuelle

L'information relative à la gestion contractuelle que renferme la présente section ne se veut pas exhaustive; elle vise, entre autres, à susciter, chez les chargés de projet et les responsables en gestion contractuelle, les bons réflexes en fonction de la réglementation existante, laquelle évolue continuellement, tout comme les technologies.

Les clauses contractuelles données à titre d'exemple à l'annexe 1 sont tirées d'un appel d'offres pour l'acquisition de services infonuagiques, selon la formule « logiciel en tant que service » (*Software as a Service* ou *SaaS,* en anglais) tarifée en mode forfaitaire et comprenant une portion de services à exécution sur demande. Ces clauses peuvent être réutilisées, mais elles devront cependant être adaptées aux besoins propres à chaque projet.

Malgré les clauses contractuelles énumérées à l'annexe 1, les lecteurs sont invités à toujours consulter, dans le cadre de l'élaboration de leurs documents d'appel d'offres, les documents officiels les plus à jour en la matière.

Il est important de rappeler que les clauses de confidentialité et de protection des renseignements personnels et de la propriété intellectuelle sont nécessaires et qu'elles doivent être incorporées aux contrats, en raison de la nature même des services en mode infonuagique.

2.1 Avis d'appel d'intérêt et appel d'offres publics

2.1.1 L'avis d'appel d'intérêt

Afin de mieux connaître le marché en fonction de la définition de ses besoins, ou avant d'aller en appel d'offres public, un OP peut décider de publier un avis d'appel d'intérêt. Ce dernier vise à aller chercher, par exemple, des réponses ou des compléments d'information sur des questions précises ou à mesurer l'intérêt des prestataires de services quant à des besoins détaillés, avant de lancer un appel d'offres. Les réponses obtenues à l'avis d'appel d'intérêt peuvent permettre à l'OP d'apporter des précisions à la définition de ses besoins et d'améliorer la formulation de sa demande dans ses futurs documents d'appel d'offres, le cas échéant. En ce sens, il est important de retenir que l'on ne peut pas procéder à l'adjudication ou à la conclusion d'un contrat, ou même à la création d'une liste de prestataires de services qualifiés, à la suite d'un avis d'appel d'intérêt; par contre, les réponses obtenues aux questionnements exprimés dans l'avis d'appel d'intérêt ou la formulation de commentaires de la part des fournisseurs seront utiles.

Un avis d'appel d'intérêt, contrairement à un avis d'appel d'offres public, peut ne contenir que quelques pages. Bien qu'il ne soit pas mentionné dans le cadre législatif applicable, l'avis d'appel d'intérêt peut être utilisé; ce type d'avis existe d'ailleurs toujours sur le SEAO. Il peut également être utilisé pour explorer de nouveaux marchés. L'avis d'appel d'intérêt peut permettre de trouver des fournisseurs potentiels et de mieux définir certaines exigences qui feront partie des documents d'appel d'offres. Il peut également permettre à un OP d'améliorer sa connaissance des biens ou des services et l'aider à définir, de façon adéquate et rigoureuse, ses besoins. Le fait qu'un seul fournisseur se manifeste pendant la période de publication d'un avis d'appel d'intérêt ne suffit pas en soi à justifier que l'on puisse conclure un contrat de gré à gré avec lui ou qu'il y ait absence de concurrence. Toutefois, un tel résultat, combiné à de la documentation additionnelle, pourrait être utilisé dans le cadre de l'élaboration d'un dossier pouvant servir à justifier la conclusion d'un contrat de gré à gré, lorsque la loi le permet.

2.1.2 L'appel d'offres public

Un appel d'offres public doit être émis pour les contrats dont la dépense estimée est égale ou supérieure au seuil minimal prévu dans tout accord intergouvernemental applicable. La procédure d'appel d'offres public vise notamment à promouvoir les principes d'accessibilité des marchés publics pour les concurrents qualifiés et le traitement intègre et équitable des concurrents. En outre, l'adjudication et la conclusion de contrats dont le montant est inférieur au seuil d'appel d'offres public doivent également être effectuées dans le respect des principes de la Loi sur les contrats des organismes publics (LCOP). Ainsi, un OP ne peut pas, entre autres, scinder ou répartir ses besoins ou apporter une modification à un contrat dans le but d'éluder l'obligation de recourir à la procédure d'appel d'offres public ou de se soustraire à toute autre obligation découlant de la LCOP.

L'appel d'offres public est défini comme une procédure d'appel à la concurrence, qui consiste, pour l'élaboration d'un projet de TI, par exemple, à inviter plusieurs prestataires de services à présenter une soumission en vue de l'obtention d'un contrat. Globalement et de façon non exhaustive, les documents d'appel d'offres comprennent la description des besoins du donneur d'ouvrage, lesquels sont généralement traduits en biens livrables attendus, les modalités relatives à l'évaluation des offres, les exigences vis-à-vis des prestataires de services ainsi que d'autres instructions et formulaires. Ils renferment aussi le contrat à être signé, accompagné de ses annexes, de ses divers formulaires, des addendas, le cas échéant, et de tout autre renseignement requis en vertu de la réglementation applicable, selon que l'appel d'offres serve à l'acquisition de biens ou à l'obtention de services. Les donneurs d'ouvrage sont responsables du processus d'appel d'offres, dont les procédures peuvent varier selon la nature du mandat proposé et le montant (inférieur ou supérieur au seuil minimal prévu dans tout accord intergouvernemental applicable) du contrat à adjuger.

Afin de garantir le bon déroulement du processus lors de l'acquisition de biens ou de l'obtention de services, il est essentiel que le donneur d'ouvrage s'assure de la qualité de ses documents d'appel d'offres, et ce, avant leur publication. Au gouvernement du Québec, tout contrat comportant une dépense égale ou supérieure au seuil minimal prévu dans tout accord intergouvernemental applicable doit faire l'objet d'un appel d'offres public[1] diffusé dans le système électronique d'appel d'offres approuvé par le gouvernement, soit le SEAO.

2.2 Définir le type d'appel d'offres

Il n'est pas toujours facile de faire la distinction entre le domaine de l'approvisionnement et celui de l'obtention de services, lorsqu'il est question des technologies de l'information, particulièrement dans les cas où ce que l'on souhaite se procurer est immatériel et prend la forme d'une solution informatique, d'une application ou d'un logiciel. Dans le domaine des technologies de l'information, avant de statuer sur le type d'appel d'offres à effectuer ou sur la nature d'un contrat, il faut définir si nos besoins correspondent ou s'apparentent davantage à un contrat d'approvisionnement ou à un contrat de services.

Le contrat d'approvisionnement porte sur l'acquisition d'un bien meuble. Un bien, c'est le résultat d'un travail, une chose réelle (matérielle ou immatérielle) ou un produit dont on connaît à l'avance les caractéristiques et particularités. L'acquisition d'ordinateurs, d'imprimantes, de serveurs, mais également de systèmes d'exploitation ou de logiciels, y compris les licences d'utilisation correspondantes, sont des contrats d'approvisionnement. Rappelons que ces contrats peuvent inclure des frais d'installation, de

1. À moins qu'il s'agisse d'une acquisition de bien ou de l'obtention d'un service dont le contrat puisse se conclure de gré à gré en vertu d'une exception prévue à la Loi sur les contrats des organismes publics ou l'un de ses règlements.

fonctionnement ou d'entretien. Ils peuvent également comporter des droits d'utilisation. Dans cette situation, la principale obligation du fournisseur est la livraison du bien requis. En ce sens, la LCOP précise que le contrat d'approvisionnement porte sur l'achat ou la location de biens meubles et que ce contrat peut inclure des frais d'installation, de fonctionnement ou d'entretien des biens achetés ou loués. Ceci étant dit, au sens de la LCOP, les logiciels sont considérés comme étant des biens meubles.

En ce qui concerne le contrat de services, il porte plutôt sur l'acquisition du travail ou de l'activité d'une personne. Il peut s'agir de services professionnels qui portent sur des activités de conception, de création, de recherche, d'analyse, ou de rédaction, ou encore de services de nature technique, lesquels consistent davantage en l'exécution d'une tâche particulière. Le développement d'une infrastructure de réseau ou d'un système personnalisé de gestion est un bon exemple de contrat de services dans le domaine des technologies de l'information. Un autre exemple serait le paiement d'un « abonnement » pour une licence d'utilisation d'une solution informatique qui se trouve sur les serveurs d'une entreprise et auquel l'OP peut accéder à distance, si, par exemple, ce type d'abonnement requiert certains services de la part de l'entreprise (configuration, établissement des connexions des bases de données, mises à jour régulières, soutien aux utilisateurs, etc.). Dans ce genre de situation, l'OP n'acquiert, en fait, rien. Il loue un service d'hébergement et un droit d'utilisation d'un produit précisé, ainsi que les autres services connexes nécessaires à une utilisation optimale. À la fin du contrat, il ne subsiste donc rien, sauf, peut-être, si cela a été négocié en ce sens, une copie de la base de données qui a été construite au cours de la période contractuelle. Dans toutes ces situations, la principale obligation du prestataire de services est de mettre en œuvre les meilleurs moyens en vue de l'atteinte du résultat souhaité.

Dans certains cas, l'acquisition d'une nouvelle solution informatique ou d'une application développée par un tiers exigera parfois un travail considérable d'adaptation aux particularités des systèmes de l'acquéreur et à ses besoins. Dans de tels cas, il faut donc se questionner. Est-ce que l'OP procède à l'acquisition d'un produit fini (approvisionnement) ou confie-t-il plutôt un mandat de développement (services)?

De façon non exhaustive, la réflexion devant mener à cette détermination pourrait, notamment, inclure la considération des éléments suivants :

- ✓ le fait que l'on désire acquérir un produit fini ou un concept qui demeure à développer;
- ✓ la portée du droit de propriété de l'acquéreur (données seulement, leur support, l'infrastructure, etc.);
- ✓ le niveau, la complexité et l'importance des opérations effectuées par le contractant;
- ✓ le degré de liberté du contractant dans le choix des moyens qu'il prendra en vue de l'atteinte du résultat attendu.

Il est à noter que le seul fait qu'une application soit hébergée en infonuagique est insuffisant pour conclure, dans tous les cas, qu'un contrat est un contrat de services ou d'approvisionnement. En somme, pour statuer sur la nature du contrat, il importe d'analyser l'ensemble de la situation, les besoins du donneur d'ouvrage, la prestation attendue du contractant et la finalité du contrat.

2.3 Protection de l'information

2.3.1 Hébergement et communication des renseignements personnels et confidentiels

Avant de communiquer des renseignements personnels à l'extérieur du Québec ou d'accorder, à une personne ou à un organisme à l'extérieur du Québec, la permission de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, l'OP doit s'assurer que de tels renseignements bénéficieront d'une protection équivalente à celle prévue à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1).

Si l'OP estime que les renseignements visés au premier paragraphe ne bénéficieront pas d'une protection équivalant à celle prévue à la loi mentionnée précédemment, il doit refuser de les communiquer ou d'accorder, à une personne ou à un organisme à l'extérieur du Québec, la permission de les détenir, de les utiliser ou de les communiquer pour son compte. Cette exigence doit s'appliquer à tout lieu d'hébergement ou de communication, y compris, notamment, les sites de relève et de copies de sécurité.

À cet effet, dans ses documents d'appel contractuels, l'OP peut prévoir un mécanisme lui permettant d'autoriser, préalablement au dépôt des soumissions, les lieux d'hébergement et de communication proposés par un éventuel soumissionnaire. L'OP pourra également exiger que le prestataire de services (PS) obtienne son autorisation préalable s'il désire modifier, en cours de contrat, le lieu d'hébergement ou de communication, ou bien si des modifications sont apportées notamment aux lois, règlements, standards, directives et politiques en vigueur aux lieux d'hébergement ou de communication du PS.

De plus, lorsque le service désiré concerne l'utilisation d'infrastructures pour emmagasiner des données, il existe des standards, reconnus internationalement pour les sites d'hébergement, dont on peut exiger le respect dans l'appel d'offres (réf. : ANSI/TIA-942, *Telecommunications Industry Association*). Les centres de données y sont catégorisés par paliers (de 1 à 4, 1 étant le plus faible). Cette catégorisation prend en compte plusieurs facteurs tels la sécurité, le risque de panne et la redondance.

Un exemple de clause contractuelle adaptée à l'infonuagique est présenté au point A de l'annexe 1.

2.3.2 Sous-traitance[2]

Comme la sous-traitance pourrait, dans certains cas, constituer un risque pour la sécurité et la protection des données si le PS y a recours, il y aurait lieu de baliser, au besoin, la sous-traitance, soit en prévoyant de la soumettre à une autorisation préalable de l'OP, ou encore en l'interdisant, si cela ne limite pas indûment la concurrence.

Le lecteur pourra également consulter les points 2.3.1. et 2.3.3. de la présente section.

2. Documents types d'appels d'offres du Sous-secrétariat aux marchés publics (SSMP) du Secrétariat du Conseil du trésor (SCT), clause : Sous-contrat (RENA et Autorité des marchés financiers).
Coffre à outils pour protéger l'intégrité des contrats publics, SSMP du SCT.

2.3.3 Cession des droits et obligations du PS[3]

L'OP doit s'assurer que les droits et obligations du PS relativement à l'hébergement et à l'exploitation de la solution d'infonuagique ne puissent être cédés, vendus, transportés ou autrement aliénés, en tout ou en partie, sans le consentement écrit de l'OP.

Advenant une autorisation de la cession par l'OP, ce dernier doit fixer les conditions dans lesquelles cette cession devra se faire. Inversement, advenant une cession sans autorisation de l'OP, ce dernier doit indiquer les conséquences potentielles d'une telle décision pour les organisations impliquées dans la transaction.

Un exemple de clause contractuelle adaptée à l'infonuagique est présenté au point B de l'annexe 1.

2.3.4 Audits de conformité

Afin d'assurer que les installations et activités du PS demeurent conformes aux exigences de sécurité pendant toute la durée du contrat, l'OP peut prévoir la tenue d'audits de conformité.

Ces audits pourront prendre la forme, par exemple, d'une validation des exigences du contrat et des autres règles de sécurité reconnues par le PS, ou bien de tests d'intrusion sur les réseaux et applications du PS. L'OP doit définir les mesures à prendre en cas de manquement à l'une des exigences contractuelles. L'OP peut décider de confier la réalisation de ces audits à un partenaire de son choix.

L'OP devrait exiger d'être avisé de tout changement apporté aux mesures de sécurités des sites d'hébergement du PS.

L'OP doit s'assurer d'avoir défini clairement, dans ses documents contractuels, les exigences en matière de sécurité de l'information auxquelles le PS, et par extension ses sous-traitants, devront se soumettre en cours de contrat.

Référence :
Un exemple de clause contractuelle adaptée à l'infonuagique est présenté au point C de l'annexe 1.

2.3.5 Relève et continuité des affaires

L'OP peut exiger, en fonction de ses niveaux de services, que le PS s'engage à assurer une relève de la solution en cas de sinistre, soit la prise de copies de sécurité des données, et que ces mécanismes soient testés à intervalles réguliers. À cet effet, il est recommandé que l'OP définisse minimalement ses objectifs en matière de temps de reprise de la solution, de point de retour arrière et de temps de reprise des opérations après sinistre.

De plus, un partage clair des responsabilités devrait être défini entre l'OP et PS, relativement à ces activités.

Un exemple de clause contractuelle adaptée à l'infonuagique est présenté au point E de l'annexe 1.

3. Références : Documents types d'appel d'offres, SSMP du SCT, article : Cession de contrat.

2.3.6 Cessation ou suspension des activités du PS

Dans le cadre d'un projet d'infonuagique comportant l'hébergement des données chez un PS, il est recommandé d'envisager le risque que ce PS cesse ou suspende ses activités (p. ex. faillite, lock-out, fermeture) et que les données deviennent inaccessibles pour l'OP.

L'aspect juridique d'un tel risque pour l'OP doit être étudié avant la publication de l'appel d'offres. L'OP doit prévoir des clauses contractuelles lui permettant de disposer d'outils techniques et juridiques pour reprendre possession de ses données.

Pour atténuer ce risque, l'OP peut, par exemple :

- ✓ exiger d'avoir régulièrement une copie de sécurité de ses données à jour, intègre et exploitable;
- ✓ lorsqu'il y a développement d'un logiciel, prévoir la remise automatique des codes sources dès la fin des travaux, ou, lorsque ce n'est pas possible ou que la survie économique du PS est à craindre, prévoir un contrat d'entiercement, c'est-à-dire une remise des codes chez un fiduciaire;

- ✓ prévoir des clauses lui permettant d'exiger la suspension des travaux ou de résilier le contrat, et ce, afin de limiter sa propre responsabilité et de prévoir les retombées financières.

Référence :
Documents types d'appels d'offres du SSMP du SCT, article : Propriété matérielle et droits d'auteurs.

2.3.7 Respect des règles de sécurité

L'OP doit exiger que le PS respecte les politiques, directives et autres règles de sécurité de l'OP, ainsi que toute modification pouvant y être apportée en cours de contrat. C'est particulièrement vrai lorsque l'OP respecte l'article 17 de la LCOP, soit que la modification reste accessoire, et qu'une rémunération est associée à cette modification. L'OP doit donc incorporer à ses documents contractuels les règles de sécurités auxquelles il est soumis. L'OP devra veiller à informer le PS en cas de modification ou de nouvelles versions de ces politiques, directives et autres règles de sécurité.

Par ailleurs, l'assurance de l'engagement au respect des politiques, directives et autres règles de sécurité par les personnes qui participent à la réalisation du contrat peut être obtenue, entre autres, au moyen d'un formulaire d'engagement annexé au contrat.

L'OP devrait également exiger que le PS l'avise, en cours de contrat, de tout manquement à ces politiques, directives ou autres règles de sécurité ainsi que de toute violation ou tentative de violation de celles-ci. De plus, il devrait exiger que le PS l'informe de tout événement dont il a connaissance qui pourrait porter atteinte à la sécurité de l'information gouvernementale.

Un exemple de clause contractuelle adaptée à l'infonuagique est présenté au point H de l'annexe 1.

2.3.8 Mise au rebut ou réparation

L'envoi du matériel au rebut ou en réparation par le PS doit se faire selon la directive émise par le Conseil du trésor concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou sur un support informatique amovible (disquette, disque dur, cédérom).

L'OP devrait incorporer cette exigence à ses documents contractuels en plus d'y joindre, en annexe, une copie de la directive en question.

2.3.9 Engagement de confidentialité

L'OP doit s'assurer que tout le personnel du PS et de ses sous-traitants pouvant potentiellement avoir accès à de l'information confidentielle dans l'exercice de leurs fonctions signent des formulaires d'engagement à la confidentialité.

De plus, si la nature du contrat ou les fonctions à accomplir l'exigent, notamment lorsque les personnes qui participent à la réalisation du contrat ont accès à de l'information dont la valeur est élevée, l'OP peut exiger du personnel du PS une attestation de sécurité ou une vérification d'antécédents criminels délivrée par un corps policier.

Références :
Documents types d'appels d'offres du SSMP du SCT, articles : Confidentialité, Protection des renseignements personnels et confidentiels.

Des exemples de clauses contractuelles adaptées à l'infonuagique sont présentés aux points F et G de l'annexe 1.

2.3.10 Mesures de sécurité

L'OP peut exiger du PS qu'il mette en place des mesures de sécurité appropriées à la valeur des données qu'il héberge ou qu'il communique, et ce, pour tous les lieux d'hébergement ou de communication utilisés en cours de contrat.

Un exemple de clause contractuelle adaptée à l'infonuagique est présenté au point I de l'annexe 1.

2.3.11 Sécurité des accès

Le PS doit s'assurer de ne rendre l'information gouvernementale accessible qu'aux seules personnes qui doivent y avoir accès aux fins de l'exécution du contrat.

2.3.12 Désignation d'un interlocuteur en matière de sécurité

Désignation d'un interlocuteur en matière de sécurité

Afin de faciliter la gestion contractuelle, il est recommandé que l'OP exige que le PS désigne un interlocuteur en matière de sécurité de l'information, pour toute la durée contractuelle. De même, l'OP désignera à son tour un interlocuteur. Il importe de pouvoir identifier facilement cet interlocuteur, par exemple, en cas de bogue ou de bris de sécurité.

2.3.13 Journalisation des opérations

Dans le cas où des données de l'OP sont hébergées chez un PS, l'OP devrait exiger que le PS effectue la journalisation des enregistrements, dans un journal, un registre ou un autre document détaillant les

opérations informatiques effectuées dans un système. La journalisation permet de garder une trace de certains événements en vue de constituer une preuve ou lors d'audits ultérieurs.

Un exemple de clause adaptée à l'infonuagique est présenté au point J de l'annexe 1.

2.3.14 Propriété matérielle et intellectuelle

L'OP doit encadrer contractuellement la propriété matérielle et les droits d'auteurs du matériel, des travaux, des biens livrables et des données qui font l'objet du contrat.

Plus particulièrement au niveau de toutes les données transférées au PS, l'OP doit s'assurer d'en conserver la propriété matérielle exclusive et intellectuelle, y compris les copies de sécurité. Il doit s'assurer d'avoir facilement accès à ses données en tout temps, sans autres frais que ceux prévus au contrat.

Références :
Documents types d'appels d'offres du SSMP du SCT, article : Propriété matérielle et droits d'auteurs.

Un exemple de clause contractuelle adaptée à l'infonuagique est présenté au point L de l'annexe 1.

2.3.15 Fin du contrat

L'OP peut prévoir que les obligations du PS et de ses sous-traitants relativement à la protection des renseignements personnels et confidentiels perdurent au-delà de la fin du contrat.

Un exemple de clause contractuelle adaptée à l'infonuagique est présenté au point K de l'annexe 1.

2.4 Responsabilités

L'OP doit prévoir une clause d'assurance responsabilité civile dans son document d'appel d'offres. Le montant doit être déterminé selon la nature du contrat. On peut consulter la clause standard du gabarit d'appel d'offres au besoin.

Une clause de responsabilité pour dommage peut également être incluse, comprenant une limitation de montant, selon la nature du contrat et la valeur de celui-ci. À cet égard, on peut consulter les clauses standards du gabarit d'appel d'offres.

Le prestataire doit détenir le contrat d'assurance au moment de la signature du contrat. L'assurance exigée peut être une condition d'admissibilité ou de conformité.

2.5 Niveaux de services et performance

Les niveaux de services et de performance doivent être clairement définis dans les documents d'appel d'offres et contractuels. Ils doivent être en relation avec la nature du produit ou le service confié en infonuagique et respecter la mission de l'OP et les niveaux de services qu'il doit rendre à sa clientèle. Le niveau de services et de performance exigé du PS doit correspondre à l'utilisation faite par l'OP de la solution ou du service consommé. La question à se poser est la suivante : « Quelle serait la conséquence

d'une interruption de service à une période donnée pour l'OP? » À ce sujet, on peut consulter l'exemple de clause contractuelle adaptée à l'infonuagique présenté au point N de l'annexe 1.

Il est important de prévoir, dans l'appel d'offres, des mécanismes permettant de vérifier l'efficacité et la performance du service ou de la solution. Il est possible de vérifier la disponibilité de la solution selon des critères établis. À cet égard, on peut consulter l'exemple de clause contractuelle adaptée à l'infonuagique présenté au point N de l'annexe 1.

Le responsable de la mesure des niveaux de services et de performance doit être clairement identifié. L'OP devrait demander au PS de désigner un responsable (interlocuteur) pour le suivi des niveaux de services et de performance lors de l'exécution du contrat. Des pénalités doivent être associées si les exigences minimales relatives au niveau de services et de performance ne sont pas respectées.

De plus, les niveaux de services et de performance peuvent être impactés par le lien Internet que l'OP utilise. L'OP doit s'assurer que son entente de service avec son fournisseur Internet comporte le même genre de clauses contractuelles.

Note : Il est recommandé que la définition des niveaux de services respecte les principes de l'ITIL *(Information Technology Infrastructure Library).*

2.5.1 Support opérationnel et appels de service :

Il est important de déterminer à l'avance les modalités désirées pour obtenir des services de support opérationnel. Veut-on du support téléphonique au moyen d'une ligne sans frais? Veut-on avoir la possibilité d'avoir accès directement au spécialiste du PS lorsque la situation l'exige? Veut-on obtenir du support en dehors des heures normales d'ouverture des bureaux?

2.5.2 Procédure d'escalade

Lorsque la vulnérabilité face à la disponibilité du produit ou du service du PS est élevée, il est important que l'OP prévoie un mécanisme pour s'assurer de prioriser ses demandes en cas d'incident majeur, et ce, sous forme de procédure d'escalade. À ce sujet, on peut consulter l'exemple de clause contractuelle adaptée à l'infonuagique présenté au point N de l'annexe 1.

2.5.3 Audits et vérifications d'usage

Il est recommandé que l'OP se réserve la possibilité de faire des audits et des vérifications d'usage chez le PS, afin de vérifier, notamment, la qualité des services rendus et leur juste prix (dans le cas où des services à exécution sur demande étaient exigés dans l'appel d'offres). Pour ce faire, l'OP peut retenir les services d'une firme externe spécialisée en la matière qui aura préalablement accepté de signer une entente de confidentialité. L'OP devrait exiger du PS une pleine collaboration pendant ces audits ou ces vérifications et exiger un délai pour qu'il se conforme aux recommandations issues de ces activités.

Un exemple de clause contractuelle d'audit adaptée à l'infonuagique est présenté au point D de l'annexe 1.

2.6 Pénalités

Lorsque la situation l'exige, il peut être raisonnable de prévoir des pénalités si le PS ne respecte pas une exigence requise et essentielle pour l'OP. La notion de pénalité peut être dissuasive et peut représenter un incitatif supplémentaire pour que le PS respecte ce à quoi il s'est engagé lorsqu'il a répondu à l'appel d'offres.

Lors de la détermination de la pénalité, il faut s'assurer que celle-ci est le reflet du préjudice causé à l'OP en cas de non-respect de l'exigence. Elle doit donc être proportionnelle au dommage envisagé. Elle doit être assez élevée pour être punitive, mais pas trop, afin de ne pas générer une augmentation indue du montant de la soumission ou de ne pas réduire la concurrence en cours d'appel d'offres. La détermination de la pénalité et de la méthode utilisée pour sa déduction doit être indiquée dans l'appel d'offres. Un exemple de clause contractuelle adaptée à l'infonuagique est présenté au point O de l'annexe 1. Prenez note que cette clause n'a pas encore été entérinée par le Secrétariat du Conseil du trésor.

Il est conseillé que l'OP élabore et vérifie la détermination de la pénalité, en collaboration avec son service juridique.

Plusieurs types de pénalités peuvent s'appliquer :

- ✓ non-respect des niveaux de services;
- ✓ non disponibilité de la solution ou du service;
- ✓ perte ou vol de données;
- ✓ non-respect des plages de maintenance de la solution;
- ✓ modification du service sans avis à l'OP;
- ✓ omission du PS à fournir un certificat de destruction des données lors de la disposition et du remplacement de son équipement.

2.7 Résiliation de contrat

L'OP doit inclure une clause de résiliation de contrat. À cet égard, on peut consulter le gabarit standard présenté à l'annexe 1.

L'article 2125 du Code civil du Québec, qui s'applique aux contrats de services, accorde un droit unilatéral de résiliation qui n'a pas à être motivé. Cependant, cet article ne doit pas être utilisé de façon déraisonnable. La clause de résiliation sert en effet à déterminer les modalités d'application de la résiliation et ses conséquences pour les parties. Il faut prévoir les dédommagements et préciser les sommes auxquelles aura droit le prestataire de services et celles qu'il ne pourra pas réclamer.

Dans le cas d'une résiliation motivée, le PS devra indemniser l'OP pour les dommages causés à la suite de la non-exécution totale ou partielle du contrat.

2.8 Résolution des différends

Le Règlement sur les contrats prévoit que les parties doivent tenter de régler à l'amiable les difficultés pouvant survenir à l'égard du contrat. L'OP doit inclure une clause de résolution des différends. À cet égard, on peut consulter le gabarit standard présenté à l'annexe 1.

2.9 Autres dispositions contractuelles

a) L'OP devrait incorporer à ses documents contractuels une clause à l'effet que, sous aucune condition en cours de contrat, le PS ne pourra suspendre l'accès de l'OP à ses données, même pour des raisons de défaut de paiement ou de différends.
b) L'OP devrait exiger que le PS l'avertisse, au moins 48 heures à l'avance, des arrêts planifiés de la solution (p. ex. pour des raisons de maintenance).
c) L'OP devrait déterminer la durée du contrat en fonction de l'étude coûts-efficacité réalisée préalablement. Il devrait aussi tenir compte des incidences et des exigences liées à la transition vers un nouveau PS à la fin du contrat. Il devrait donc se garder une marge de manœuvre, en prévoyant au contrat la durée optimale, y compris la transition, ou des options d'années de renouvellement.
d) Il est important de bien définir, dans un lexique, les termes utilisés dans les documents d'avis d'appel d'intérêt et d'appel d'offres, surtout ceux qui pourraient avoir une incidence sur les prix des soumissions. Ceci facilitera la compréhension des PS quant à l'élaboration de leur soumission et la gestion contractuelle.
e) Si le marché de l'infonuagique est peu connu de l'OP ou s'il doute du sérieux des éventuels soumissionnaires, il peut exiger, dans les conditions de conformité de l'appel d'offres, une garantie de soumission. Celle-ci visera à dédommager l'OP dans le cas d'un désistement d'un PS avant la signature du contrat et aura un effet dissuasif sur ce dernier. L'OP peut aussi exiger que cette garantie de soumission soit échangée contre une garantie d'exécution avant la signature du contrat. Cette garantie d'exécution demeurera valide pour la durée du contrat et visera à dédommager l'OP contre un défaut d'exécution du contrat par le PS. Cette garantie ne peut cependant pas être utilisée en cas de service insatisfaisant. Ces garanties doivent être utilisées avec discernement puisqu'elles imposent une charge financière supplémentaire aux PS, ce qui pourrait avoir pour effet de réduire la concurrence ou d'augmenter le prix des soumissions.

Documents types d'appels d'offres du SSMP du SCT, articles : Garantie de soumission, Garantie d'exécution et Conditions de conformité.

2.9.1 Transition à la sortie

L'OP devrait incorporer à ses documents contractuels des dispositions relatives à la transition vers un nouveau PS au terme du contrat. Ces dispositions visent à permettre une transition organisée, efficace et sécuritaire des services et des données, et ce, tout en minimisant les répercussions au niveau de l'OP. Il est important, entre autres, que des délais suffisants pour la réalisation des activités y soient prévus et que le partage des rôles et responsabilités y soit clairement établi. Selon le projet, une transition du PS vers l'OP pourrait également être envisagée.

Un exemple de clause de transition à la sortie adaptée à l'infonuagique est présenté au point M de l'annexe 1.

Annexe 1 – Clauses contractuelles

Les clauses contractuelles données à titre d'exemple dans la présente annexe sont tirées, pour la majeure partie, d'un appel d'offres en infonuagique selon la formule « logiciel en tant que service » (*Software as a Service* ou *SaaS*). Ces clauses peuvent être réutilisées; elles doivent cependant être adaptées aux besoins propres de chaque projet.

a) Clause d'hébergement

Les renseignements personnels et confidentiels recueillis dans le cadre de « *titre de l'appel d'offres* » doivent être hébergés au Québec. En aucun temps ces renseignements ne pourront être transférés à l'extérieur du Québec à moins que l'organisme public, ci-après appelé OP, soit assuré qu'il bénéficie d'une protection équivalente à celle prévue à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1), ci-après appelée Loi sur l'accès. Cette exigence inclut tout lieu d'hébergement des renseignements personnels et confidentiels, dont, notamment, les sites de relève et de copies de sauvegarde permettant de répondre aux exigences du présent appel d'offres.

Le prestataire de services, ci-après appelé PS, doit avoir préalablement obtenu l'autorisation écrite de l'OP pour que ce dernier lui accorde la permission de détenir des renseignements personnels, de les utiliser ou de les communiquer à l'extérieur du Québec.

Pour que l'OP puisse fournir cette autorisation, le PS doit soumettre au client, aux fins d'examen, les lois, règlements, procédures, standards, directives, politiques ou documents de même nature, de la province ou du pays où le PS détiendra les renseignements personnels et confidentiels, les utilisera ou les communiquera. Le PS devra déposer les documents, aux fins d'examen, et faire une demande d'autorisation auprès du représentant désigné de l'OP, au plus tard dix (10) jours avant la date de clôture de l'appel d'offres.

Si l'OP estime, après analyse des documents déposés par le PS, que les renseignements personnels et confidentiels ne bénéficieront pas d'une protection équivalente à celle prévue à la Loi sur l'accès, l'autorisation de l'OP à l'effet que le PS puisse détenir, utiliser ou communiquer des renseignements personnels à l'extérieur du Québec ne pourra pas lui être accordée.

De plus, lorsqu'en cours d'exécution du contrat, des modifications sont apportées aux lois, règlements, procédures, standards, directives, politiques ou documents de même nature, de la province ou du pays où le PS détient les renseignements personnels, ce dernier doit en aviser l'OP et lui fournir une copie des documents modifiés. Si l'OP est d'avis que les modifications apportées sont de nature à compromettre et à ne plus assurer une protection équivalente à celle prévue à la Loi sur l'accès, l'OP se réserve le droit de résilier le contrat, selon les dispositions visées à l'article « Résiliation » du document d'appel d'offres.

Si, en cours d'exécution du contrat, le PS souhaite modifier le lieu d'hébergement, il devra obtenir l'autorisation de l'OP, comme le stipulent les paragraphes précédents.

b) Norme reconnue pour les sites d'hébergement

Lorsque le service contracté concerne l'utilisation d'infrastructures pour emmagasiner des données, il existe des normes reconnues, dont on peut exiger le respect dans l'appel d'offres. Ce sont des normes reconnues internationalement (par exemple, système de paliers de 1 à 4, 1 étant le niveau le plus faible). Cette catégorisation prend en compte plusieurs facteurs (sécurité, risque de panne, redondance, etc.).

Lorsque l'OP utilise une solution d'un PS, il peut demander à ce dernier de lui fournir l'information concernant l'hébergement de sa solution.

c) Cession de contrat

Les droits et obligations du PS relativement à l'hébergement et l'exploitation de la solution ne peuvent être cédés, vendus, transportés ou autrement aliénés, en tout ou en partie, sans le consentement écrit de l'OP.

Advenant le cas où l'OP accepte que les services d'hébergement et d'exploitation de la solution soient transférés à un autre prestataire, ce dernier sera tenu de fournir le service d'hébergement et d'exploitation de la solution décrit aux présentes. Tous les frais relatifs à un transfert autorisé devront être assumés par le prestataire d'origine ou par l'organisation à qui les droits et obligations auront été transférés.

Le non-respect de cette obligation pourrait entraîner, à la discrétion de l'OP, un recours en dédommagement pour les frais engagés pour le remplacement de la solution proposée par une solution équivalente (respectant les mêmes exigences), soit :

- ✓ contre le prestataire d'origine;
- ✓ contre l'organisation à qui auront été transférées les obligations relatives aux services d'hébergement et d'exploitation de la solution;
- ✓ la résiliation du contrat, laquelle prendra effet de plein droit à la date de ladite cession, à moins que celle-ci ne soit autorisée par l'OP.

d) Audits de conformité

L'OP peut procéder, sur préavis, à un audit de conformité du PS aux lois, politiques, directives et autres règles de sécurité reconnues par l'OP, notamment celles relatives à la protection des renseignements personnels et confidentiels, mentionnées à la section 8 – Considérations juridiques, ainsi que celles relatives à la sécurité de l'information, mentionnées à l'annexe 3 (exigences de sécurité de l'OP). L'OP se réserve également le droit de procéder à des tests d'intrusion réseaux et applicatifs des systèmes, dans ces mêmes conditions. L'OP pourra également déléguer ces audits à un partenaire de son choix. Ces audits pourront être faits de la façon prescrite à l'article X de l'annexe X du présent appel d'offres.

À la suite de ces audits de conformité, l'OP pourra prendre les mesures définies à l'annexe 3 (exigences de sécurité de l'OP) qu'il juge appropriées.

Par ailleurs, le PS doit aviser l'OP de tout changement apporté à ses sites d'hébergement ayant un effet sur les mesures de sécurité mises en place.

e) Audits et vérifications d'usage

L'OP peut faire effectuer des vérifications, à ses frais, par des firmes spécialisées, ce qui inclut des audits; ces vérifications porteront notamment sur la qualité d'un service offert ou de toute solution fournie ou développée par le PS de même que sur les éléments de sécurité présentés à l'annexe 3 (exigences de sécurité de l'OP). L'OP peut également, par le même moyen, faire effectuer des études technico-économiques quant aux services offerts ou à la justesse des coûts qui leur sont rattachés.

Ces demandes de vérification auprès de firmes spécialisées peuvent aussi prévoir des modalités de suivi, lequel serait effectué par ces firmes pour assurer que les recommandations de la firme sont bel et bien

exécutées par le PS. Ce dernier devra, à ses frais, se conformer aux recommandations des rapports d'audits et de vérifications, dans un délai maximal de trente (30) jours à compter de la réception de ces rapports.

Dans tous les cas de tenue d'audits et de vérifications d'usage, le PS doit collaborer pleinement et gratuitement avec la firme et lui transmettre tous les renseignements requis pour effectuer la vérification. Le PS devra donner accès aux locaux, plans et documents nécessaires à la réalisation des audits et vérifications d'usage. La firme retenue à cette fin signera un engagement de confidentialité visant à assurer le PS que les renseignements ne serviront qu'aux fins mentionnées dans la demande de vérification.

Tout audit ou vérification ainsi effectués ne dégagent pas pour autant le PS de sa responsabilité à l'égard de l'objet du contrat.

f) Relève et continuité des affaires

Le PS s'engage à assurer une relève de la solution et une continuité des affaires, comme le définissent les niveaux de services de l'annexe X et les exigences de sécurité de l'annexe X.

La responsabilité de la relève informatique est partagée entre l'OP et le PS.

L'OP est responsable :

- ✓ d'élaborer la stratégie de relève;
- ✓ en cas de désastre, de définir, en lien avec sa clientèle, le niveau de relève souhaité et les moyens appropriés pour assurer la continuité des opérations;
- ✓ en cas de désastre, du soutien à la clientèle et de la prise de décision;
- ✓ des niveaux de services en mode dégradé ainsi que du processus de retour à la normale.

Le PS est responsable :

- ✓ de proposer un plan de relève, avec un site de relève externe comprenant la relève des serveurs, des équipements et des liens de télécommunications ainsi que la prise de copies de sécurité;
- ✓ de mettre en œuvre la relève informatique en fonction des orientations de l'OP;
- ✓ de remettre en service sa solution, dans le respect du niveau de services défini à l'annexe X, lors de la perte de tous les services en cas de désastre;
- ✓ de brancher son site de relève ou tout autre réseau appelé à le remplacer;
- ✓ de tester son plan de relève, par simulation d'une situation réelle, au minimum une (1) fois par année;
- ✓ de collaborer avec l'OP pour définir les mesures de la performance (métriques) et les niveaux de services à maintenir pendant un désastre ainsi que la mise en œuvre du processus de retour à la normale;
- ✓ des mesures de relève qui devront être testées, documentées et approuvées par l'OP.

g) Engagement de confidentialité du PS

Le représentant du PS doit :

- ✓ s'engager à signer l'engagement de confidentialité applicable aux renseignements personnels auxquels le signataire a accès dans l'exercice de ses fonctions (annexe X);
- ✓ s'engager à faire signer, par les membres de son personnel et, le cas échéant, par les membres du personnel d'un sous-traitant, préalablement à l'accès à des renseignements personnels et

confidentiels, l'engagement de confidentialité applicable aux renseignements personnels auxquels le signataire a accès dans l'exercice de ses fonctions (annexe X) et à les transmettre aussitôt que possible au client;
- ✓ informer les membres de son personnel et, le cas échéant, les membres du personnel d'un sous-traitant, des obligations stipulées aux présentes dispositions et diffuser à cet égard toute l'information pertinente.

Lorsque la réalisation du présent contrat ou d'une partie de celui-ci est confiée à un sous-traitant (quel que soit le niveau de sous-contrat) et qu'elle comporte la communication de renseignements personnels et confidentiels ou la collecte de renseignements personnels et confidentiels par le sous-traitant :

- ✓ informer l'OP du nom du ou des sous-traitants, des services qu'ils réaliseront, de la liste des renseignements personnels et confidentiels qui leur seront communiqués et des lieux d'hébergement des renseignements personnels et confidentiels;
- ✓ conclure un contrat avec le ou les sous-traitants, stipulant les mêmes obligations que celles exigées du PS en matière de protection des renseignements personnels et confidentiels;
- ✓ exiger du ou des sous-traitants qu'ils s'engagent à ne conserver, à l'expiration du sous-contrat, aucun document contenant un renseignement personnel ou confidentiel, quel qu'en soit le support, et à remettre au PS, dans les soixante (60) jours suivants la fin de ce sous-contrat, un tel document;
- ✓ fournir, à la demande de l'OP, toute l'information pertinente au sujet de la protection des renseignements personnels et confidentiels et donner accès à toute personne désignée par l'OP à la documentation, aux systèmes, aux données et aux lieux physiques relatifs au contrat. afin de s'assurer du respect des présentes dispositions.

h) Confidentialité

Le PS s'engage à ce que ni lui ni aucun de ses employés ne divulguent, sans y être dûment autorisés par l'OP, les données, analyses ou résultats inclus dans les rapports réalisés en vertu du contrat ou, généralement, quoi que ce soit dont ils auraient eu connaissance au cours de l'exécution du contrat.

L'OP, en tant qu'OP assujetti à la Loi sur l'accès, traite les renseignements confidentiels du PS ou les renseignements traités de façon confidentielle par un PS conformément, mais non limitativement, aux articles 23, 24 et 25 de cette loi.

i) Respect des règles de sécurité

Le PS s'engage à respecter les documents du cadre légal et administratif auxquels l'OP est assujetti, notamment les politiques, directives et autres règles de sécurité applicables à l'information gouvernementale en vigueur pendant la durée du contrat, y compris la « politique de sécurité de l'information » de l'OP (fournir en annexe). Il s'engage également à respecter les exigences minimales obligatoires relatives à la protection des renseignements personnels et confidentiels, présentées à la section 8 – Considérations juridiques, ainsi que celles relatives à la sécurité, présentées à la section 9 – Considérations de sécurité.

À cet égard, le PS s'engage à ce que toute personne qui participe à la réalisation du contrat respecte ces politiques, directives et autres règles de sécurité.

Le PS s'engage à aviser sans délai l'OP de tout manquement à ces politiques, directives et autres règles de sécurité ou de toute violation ou tentative de violation de ces dernières par toute personne qui participe à la réalisation du contrat; il s'engage également à informer l'OP de tout événement pouvant porter atteinte à la sécurité de l'information gouvernementale.

j) Mesures de sécurité

Le PS s'engage à prendre les mesures requises afin d'assurer, en tout temps, la sécurité de l'information gouvernementale en fonction de la valeur de cette information, déterminée selon les instructions de l'OP. Le PS s'engage également à informer l'OP des mesures prises à cet égard.

Lorsque cette information doit être conservée, utilisée ou communiquée à l'extérieur de l'OP (ou à un endroit différent de celui convenu par les parties), le PS s'engage à obtenir de l'OP son autorisation préalable et à prendre, à la satisfaction de l'OP, toutes les mesures de sécurité requises

k) Journalisation des opérations

Comme le mentionne l'annexe X du présent document, le PS s'engage à conserver, aux fins de preuve et selon les exigences de l'OP, des journaux, registres et autres documents consignant les opérations, événements ou autres faits relatifs à l'information gouvernementale et permettant notamment de connaître la date des opérations, événements ou faits en cause ainsi que leurs auteurs.

Le PS s'engage à prendre des mesures afin d'assurer l'intégrité de ces journaux, registres et autres documents, tout au long de leur cycle de vie.

À la demande de l'OP, le PS s'engage à lui remettre ces journaux, registres et autres documents ou à lui donner accès à ceux-ci.

l) Fin du contrat

La fin du contrat ne dégage aucunement le PS et le sous-traitant de leurs obligations et engagement relativement à la protection des renseignements personnels et confidentiels. Les principales dispositions applicables se retrouvent, notamment, mais non limitativement, aux articles 1, 9, 18 à 41.3, 53 à 60.1, 62, 64 à 67.2, 83, 89, 158 à 164 de la Loi sur l'accès.

Cette loi peut être consultée à l'adresse suivante : www.publicationsduquebec.gouv.qc.ca.

m) Propriété matérielle et droits d'auteur

Définitions

Aux fins de cette section, on entend par :

- ✓ « travaux du PS » : tous les travaux à être réalisés par le PS en vertu du présent contrat, y compris les accessoires tels les rapports, études, manuels ou autre documentation, quel qu'en soit le support, qui accompagneront ces travaux; ces travaux du PS sont notamment décrits dans le document d'appel d'offres et, le cas échéant, dans la soumission du PS, lesquels font partie intégrante du présent contrat;
- ✓ « matériel antérieur du PS » : tous les travaux ou accessoires qui existaient avant le présent contrat qui seront incorporés, d'une façon ou d'une autre, aux « travaux du PS » et pour lesquels il est titulaire du droit d'auteur;
- ✓ « matériel préexistant » : tous les travaux ou accessoires qui existaient avant le présent contrat qui seront incorporés, d'une façon ou d'une autre, aux « travaux du PS » ou au « matériel antérieur du PS » et pour lesquels le PS a obtenu une licence, conformément à l'article 6.11.5;

- ✓ « Niveau de services » : Les niveaux de services sont définis comme les mesures de la qualité des services pour lesquels tout manquement aura des répercussions sur les affaires du client et de sa clientèle. Ils doivent être réalistes et mesurables. On doit s'assurer que les outils de mesure ou rapports nécessaires à la mesure de ces niveaux de services sont inclus à la solution et accessibles par l'OP en tout temps;
- ✓ « biens livrables » : biens constitués des travaux visés au paragraphe a) et, le cas échéant, du matériel visé aux paragraphes b) ou c).

Propriété matérielle

L'organisme public (OP)

L'OP conserve en entier tout droit de propriété qu'il détient sur toute chose, et, notamment, sur tout écrit, matériel informatique, modèle, concept, méthode et procédé, qu'il communique au PS ou qu'il met à sa disposition. Ce dernier ne doit pas, sans l'autorisation de l'OP, se servir de ces éléments à des fins autres que l'exécution des travaux faisant l'objet du présent appel d'offres.

En outre, le PS transfère au client ou à une tierce partie désignée par l'OP toutes les données, y compris les copies de sécurité, lesquelles sont la propriété entière et exclusive de l'OP. En aucun cas, le PS ne doit conserver une partie de ces données.

À cet égard, le PS doit fournir des instructions précises, tels un script d'utilisation et un modèle de données, permettant à toute personne normalement formée en administration de systèmes informatiques, mais sans connaissances de la solution du PS, d'accéder à la « totalité des données » et de les manipuler pour permettre leur réutilisation ou leur importation dans un nouveau système. La « totalité des données » inclut, mais sans s'y limiter, les données de mission, les données de configuration, les données du flux des travaux et toutes données transmises par l'OP.

Le prestataire de services (PS)

Les « biens livrables » demeurent la propriété entière et exclusive du PS, qui pourra en disposer à son gré, à l'exception des données et des accessoires, tels les scripts d'utilisation et un modèle de données, et de tout autre élément transféré au client ou à une tierce partie, lesquels sont la propriété entière et exclusive de l'OP, conformément à la clause 6.11.1. a), sous réserve des dispositions relatives au droit d'auteur énoncées ci-après.

Droits d'auteur

Licence de droits d'auteur à l'OP (travaux du PS et matériel antérieur du PS)

Le PS accorde à l'OP, qui accepte, une licence irrévocable, non exclusive et transférable aux ministères et OP, lui permettant de reproduire, d'adapter, d'installer et d'utiliser les « travaux du PS » et le « matériel antérieur du PS » à toutes fins liées à une mission gouvernementale. Cette licence est assortie des mises à jour et des mises à niveau qui permettent de maintenir, d'améliorer et de faire évoluer la solution, et ce, durant toute la durée du contrat.

Cette licence est accordée sans limite territoriale, et ce, pour toute la durée du contrat.

Licence pour le matériel préexistant

Le PS a obtenu ou obtiendra, pour l'OP, une licence d'installation et d'utilisation du « matériel préexistant » à toutes fins utiles à la bonne exploitation des « travaux du PS » et du « matériel antérieur du PS ». Le PS s'engage à défrayer le coût de ces licences jusqu'à la fin du contrat, y compris les renouvellements.

Considération

Toute considération pour la licence de droits d'auteur consentie en vertu de l'article 6.11.4 est incluse à même le prix soumis par le PS.

Garanties et représentations du PS

- ✓ Le PS garantit au client qu'il a respecté la Loi sur le droit d'auteur et qu'il détient tous les droits de propriété intellectuelle nécessaires ou qu'il a obtenu toutes les autorisations requises lui permettant de réaliser le présent contrat et, notamment, de consentir la licence de droits d'auteur prévue à l'article 6.11.4.
- ✓ Le PS acquitte entièrement les droits et redevances relatifs aux droits de propriété intellectuelle, y compris l'utilisation de procédés brevetés, de dessins ou modèles déposés qui pourraient être exigibles et qui sont requis pour permettre l'utilisation des biens, et, le cas échéant, la réparation, l'entretien, la mise à niveau ou la remise en état.
- ✓ Le PS se porte garant envers l'OP contre tout recours, réclamation, demande, poursuite et autres procédures pris par toute personne relativement à l'objet de ces garanties.
- ✓ Le PS s'engage à prendre fait et cause, à indemniser et à libérer l'OP pour tout recours, réclamation, demande, poursuite et autres procédures pris par toute personne relativement à l'objet de ces garanties. Dans ce cas, le PS paiera tous les frais judiciaires, les dommages et intérêts et les dépenses accordés en dernier ressort par un tribunal.
- ✓ Pour sa part, l'OP s'engage à :

    - aviser sans délai le PS d'une telle réclamation;
    - coopérer pleinement avec le PS et lui permettre de mener seul la défense ainsi que toutes les négociations entreprises en vue de régler le litige.

Si une telle réclamation est faite ou apparaît probable, l'OP convient de permettre au PS soit d'obtenir pour lui le droit de continuer à utiliser le service, soit de le modifier ou de le remplacer, de manière à ce que l'infraction cesse, tout en offrant une performance fonctionnellement équivalente.

Le PS n'aura aucune obligation à l'égard d'une réclamation fondée sur :

- ✓ la modification d'un bien et service par l'OP;
- ✓ l'utilisation par celui-ci d'un programme;
- ✓ la combinaison, l'exploitation ou l'utilisation par celui-ci d'un bien avec un autre produit (matériel, logiciel ou données) non fourni par le PS et dans un cadre autre que celui prescrit par le présent appel d'offres.

n) Transition à la sortie

À la demande de l'OP, le PS s'engage, conformément aux conditions prescrites ci-dessous, à préparer et à déposer un plan préliminaire de transition à la sortie.

Chaque plan préliminaire de transition à la sortie doit être déposé auprès de l'OP, six (6) mois avant la date de fin du contrat. Le plan devra être soumis à l'approbation de l'OP, aux fins de révision et de correction. Le plan final de transition à la sortie devra être remis à l'OP trois (3) mois avant la date de fin du contrat, afin de récupérer les données, le paramétrage et la configuration.

Ce plan final de transition à la sortie devra comprendre, sans s'y limiter :

- ✓ l'approche et la stratégie de transition à la sortie, tant du point de vue de la technologie que du cadre de gestion;
- ✓ la façon dont les transferts de connaissances et de documentation vers le futur PS seront effectués. Ceci inclut les documents et schémas d'architecture, les descriptions et la programmation des applications des clients, les fichiers de sauvegarde et les descriptions des flux d'acheminement des contacts;
- ✓ une période de chevauchement de deux (2) mois avec le futur PS;
- ✓ la liste des ressources et des fonctions qui seront assignées au maintien des services en place;
- ✓ tout autre élément qui minimise les répercussions de la transition à la sortie sur les activités de la clientèle.

Processus

Durant la période de transition à la sortie, le PS s'engage à offrir, sans aucuns frais additionnels, une coopération pleine et entière à l'OP, au futur PS et à ses sous-traitants. Le PS devra offrir une pleine et entière coopération et un transfert de connaissances à l'OP, en répondant à toutes ses questions concernant, notamment, la structure des données. Sur demande de l'OP ou du futur PS, le PS actuel devra assurer la continuité des services jusqu'à la fin de la période contractuelle.

Dans les quinze (15) premiers jours ouvrables de la phase de transition à la sortie, le PS doit remettre à l'OP toutes les dernières versions des configurations et toute la documentation technique afférente, en format papier et en format numérique. Le PS devra remettre à jour toute la documentation sur les applications en service, afin d'assurer un transfert efficace et efficient du soutien des applications d'un PS à un autre.

Entre autres, le PS devra assigner un chargé de projet et un nombre suffisant de ressources lors de cette phase.

Le PS s'engage à collaborer étroitement avec l'OP et le futur PS, et ce, afin de minimiser les coûts et les incidences sur les services offerts aux clients de l'OP. À cette fin, le PS s'engage à transmettre à l'OP toute l'information exigible pour assurer les services, tels les configurations et les documents existants, à l'exception de son information confidentielle.

Si le futur PS l'exige, toute demande raisonnable d'accompagnement et d'assistance qui excède les exigences mentionnées précédemment devra faire l'objet d'une proposition de services professionnels du PS actuel.

Cette proposition, basée sur les tarifs du bordereau de prix du contrat, sera soumise à l'OP aux fins d'approbation.

Chargé de projet du PS

Le PS devra maintenir, durant la période de transition à la sortie, un nombre suffisant de ressources humaines, y compris un chargé de projet assigné, qui deviendra le point de contact de l'OP et du nouveau PS, pour toute la période.

Le chargé de projet devra assumer, de façon continue, les responsabilités suivantes :

- ✓ coordonner les opérations réalisées par le PS pour la transition à la sortie;
- ✓ assurer la coordination des activités de transition;
- ✓ être le point de contact principal pour l'équipe de l'OP dans la réalisation des projets;
- ✓ maintenir un contact continuel et une communication efficace avec le coordonnateur de migration de l'OP et l'interlocuteur principal du futur PS;
- ✓ informer l'OP du suivi de l'avancement des travaux et régler les problèmes, de nature opérationnelle et de nature administrative, en lien avec les services, conjointement avec le futur PS;
- ✓ utiliser les pratiques de gestion de projets actuellement en vigueur chez l'OP;
- ✓ présenter les interventions prévues pour chaque semaine de la phase de transition à la sortie;
- ✓ effectuer le suivi des projets, des migrations d'applications et des nouvelles implantations en matière de budget, d'échéancier, de biens livrables et de qualité;
- ✓ s'assurer que les obligations du PS sont pleinement exécutées;
- ✓ s'assurer de la qualité de ses biens livrables;
- ✓ informer l'OP de l'escalade de toute situation devenant impossible à maîtriser;
- ✓ collaborer étroitement à l'élaboration d'un bilan des projets, afin de maintenir ou d'améliorer le niveau de qualité en gestion de projet.

Période de chevauchement

Lors des deux (2) derniers mois de la période de transition à la sortie, une période de chevauchement entre le contrat en vigueur et le futur contrat de services devra permettre une transition entre le PS actuel et le futur PS.

Durant cette période de chevauchement, le PS devra :

- ✓ assurer la continuité des services existants;
- ✓ offrir une pleine et entière coopération à l'OP et au futur PS;
- ✓ effectuer un transfert de connaissances à l'OP, en répondant à toutes ses questions.

Le PS actuel devra assister le futur PS dans la résolution des incidents pouvant survenir lors de la transition.

o) Niveau de services et performance

Niveau de services

Les services exigés peuvent être de différents niveaux. Par exemple, L'OP peut demander un service 24/7 ou selon ses propres heures d'ouverture de bureau. Le niveau exigé doit être en relation avec l'utilisation faite de la solution infonuagique du PS.

En cas de problème

Le niveau de services requis peut être différent selon la situation. À titre d'exemple, des services 24/7 peuvent être catégorisés de la façon suivante, en fonction de la gravité du problème :

Gravité	Délais de retour d'appel	Délais de résolution
Gravité 1 : Problème urgent Événement affectant une majorité d'utilisateurs ou ayant un effet immédiat sur les services rendus à la clientèle de l'OP	xx minutes	xx h
Gravité 2 : Problème sectoriel Événement affectant un groupe d'utilisateurs, perturbant ainsi les opérations internes de l'OP ou occasionnant la dégradation des services pour une majorité d'utilisateurs	xx minutes	xx h
Gravité 3 : Dégradation importante Dégradation affectant un groupe d'utilisateurs ou problème empêchant un utilisateur de travailler	xx minutes	xx h
Gravité 4 : Problème unitaire Dégradation des services affectant un utilisateur ou problème touchant un utilisateur, mais qui peut être contourné ou dont la résolution peut être reportée	xx minutes	xx h

Note : Seul l'OP peut déterminer le niveau de gravité lors d'un appel de services. Le tableau précédent définit les niveaux de gravité des problèmes et présente les délais de résolution associés. Le délai de résolution est la période de temps écoulée entre l'heure de l'appel de services, y compris le délai d'attente, et l'heure à laquelle la solution est redevenue opérationnelle selon les niveaux de service attendus.

Niveau de performance et de disponibilité du service ou de la solution

Voici quelques exemples de méthodes de calcul :

- ✓ niveaux de services pour accéder à la solution exigée par l'OP;
- ✓ offrir les plages de services entre 8 h et 17 h, heure de l'Est, du lundi au vendredi inclusivement, avec un taux de disponibilité mensuelle de 99,5 %;
    - le taux de disponibilité sera calculé sur des périodes de référence d'un mois, la première période de référence débutant au moment de la mise en service et se terminant à la fin du mois courant, les périodes suivantes couvrant un mois civil et la dernière période se terminant à la date de fin du contrat;

- le taux de disponibilité est le nombre total d'heures de disponibilité réelle du site durant la plage de service, divisé par le nombre total d'heures couvertes par la plage de service, pour toute la durée de la période de référence;

- ✓ le service devra demeurer disponible hors de la plage de service indiquée précédemment, mais aucun taux de disponibilité n'est spécifié ou exigé;
- ✓ offrir sur demande des extensions de plages de services entre 17 h et 21 h, la semaine, et entre 8 h et 15 h, le samedi (demandées 24 heures ou plus à l'avance par l'OP);
- ✓ offrir un support téléphonique du lundi au vendredi inclusivement, entre 8 h et 17 h : réponse immédiate;
- ✓ la mise en production de tout changement apporté aux applications de la solution utilisée par l'OP doit se faire à l'extérieur des périodes de services, comprises entre 8 h et 17 h, et le PS doit aviser l'OP avant son implantation dans l'environnement de production;
- ✓ la documentation des nouvelles versions devra être préalablement fournie à l'OP.

À la demande de l'OP, le PS doit expliquer les raisons de la défaillance, en cas de problème au niveau de la disponibilité ou du niveau de services.

Procédure d'escalade

Voici un exemple de clause pouvant être incorporée aux documents d'appel d'offres :

Le PS doit inclure dans sa soumission la procédure d'escalade qu'il compte utiliser si les délais d'intervention ou de résolution mentionnés dans le tableau précédent sont dépassés. La procédure d'escalade doit préciser de quelle manière le PS entend réagir aux problématiques urgentes soulevées par l'OP. Le PS doit préciser les différentes étapes de la procédure, le niveau de connaissances des personnes impliquées à chacune des étapes, l'ordre dans lequel elles sont sollicitées et le moment où elles le sont. Le PS doit également indiquer le nom du responsable chargé de coordonner les activités et de participer aux différentes cellules de crise.

p) Pénalités (non entériné par la réglementation et le SCT)

Voici un exemple de clause pour des pénalités relatives au niveau de services requis au point N :

Si le PS ne respecte pas les niveaux de services requis, l'OP se réserve le droit d'imposer au PS les pénalités suivantes :

1. À la suite d'un problème de gravité 1, pour chaque tranche complète de xx minutes excédant le délai maximal de retour d'appel, une pénalité de xx $, et, pour chaque tranche complète de xxx minutes excédant le délai de résolution précisé dans les niveaux de services, une pénalité de xxx $;
2. À la suite d'un problème de gravité 2, pour chaque tranche complète de xx minutes excédant le délai maximal de retour d'appel, une pénalité de xx $, et, pour chaque tranche complète de xxx minutes excédant le délai de résolution précisé dans les niveaux de services, une pénalité de xxx $;
3. À la suite d'un problème de gravité 3, pour chaque tranche complète de xx minutes excédant le délai maximal de retour d'appel, une pénalité de xx $, et, pour chaque tranche complète de xxx minutes excédant le délai de résolution précisé dans les niveaux de services, une pénalité de xxx $;
4. À la suite d'un problème de gravité 4, pour chaque tranche complète de xx minutes excédant le délai maximal de retour d'appel, une pénalité de xx $, et, pour chaque tranche complète de xxx minutes excédant le délai de résolution précisé dans les niveaux de services, une pénalité de xxx $.

La durée d'un problème de disponibilité est la période de temps écoulée entre l'heure de l'appel de services, y compris le délai d'attente, et l'heure à laquelle la solution est redevenue opérationnelle selon les niveaux de services attendus.

Le délai de résolution d'un problème est établi par l'OP et correspond à la période écoulée (en heures et en minutes) entre l'heure de l'appel de services et l'heure à laquelle le composant faisant l'objet du problème est redevenu opérationnel, à la satisfaction de l'OP.

Aux fins de la présente section :

- ✓ le calcul de chaque pénalité se fait à la fin de chaque trimestre;
- ✓ le premier trimestre débute à la signature du contrat;
- ✓ la durée de tout problème de disponibilité ou de tout problème non résolu à la fin d'un trimestre est reportée dans le trimestre durant lequel le problème est résolu.

Malgré ce qui précède, le PS est passible, pour l'ensemble des pénalités prévues à la présente section, de pénalités totales ne pouvant excéder le montant trimestriel facturé par le PS pour l'utilisation de sa solution.

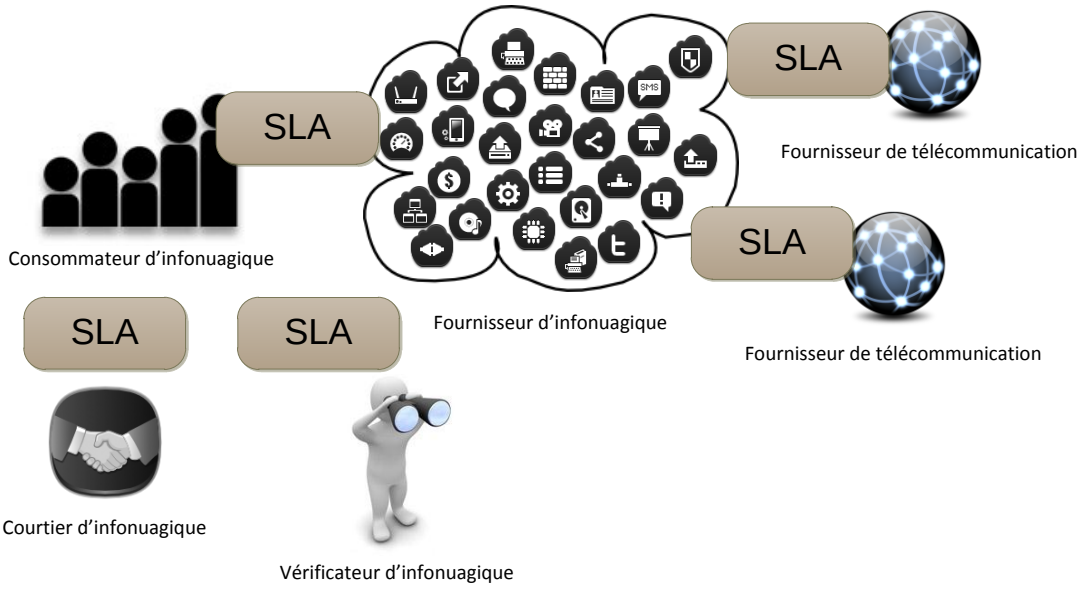
Toute somme due en vertu de la présente section pourra être déduite des sommes dues ou pouvant devenir dues au PS, par compensation, sans préjudice aux autres recours pouvant être exercés par l'OP. Le PS sera mis en demeure par le simple écoulement du temps prévu au contrat pour l'exécution de ses obligations.

Annexe 2 – Complément d'information sur les accords de niveau de service (SLA)

a) Comprendre les rôles et responsabilités

Les OP doivent reconnaître les activités et les responsabilités de chaque acteur engagé dans la prestation de leur environnement en nuage et de définir des niveaux de service attendus pour chacun. Il arrive qu'un fournisseur d'infonuagique utilise des services d'un fournisseur de télécommunication afin de livrer leurs services. En plus du SLA à convenir avec le fournisseur d'infonuagique, l'OP doit également préciser des attentes spécifiques à l'égard des fournisseurs de télécommunication.

Figure 1: Rôles et responsabilités du SLA



Tous les SLA traitant l'infonuagique seront uniques et basés selon les exigences de l'OP. Les exigences ne sont pas nécessairement limitées aux mesures quantitatives, mais peuvent également traiter des mesures qualitatives telles que les standards ou encore la protection des données.

b) Évaluer les politiques de l'entreprise

Données

Les politiques de données du fournisseur d'infonuagique, telles qu'exprimées dans un SLA, sont probablement les plus critiques pour l'OP et doivent être soigneusement évaluées.

Préservation des données

Les OP devraient assurer que le service offert en infonuagique prend en charge leur stratégie de conservation de données qui inclut des sources, ordonnancement, sauvegarde, restauration, contrôles d'intégrité, etc.

Redondance des données

Les OP doivent s'assurer qu'ils ont une stratégie de préservation des données appropriées qui traite de la redondance au sein du système et devraient pouvoir, à l'aide d'essais, démontrer la disponibilité du service.

Localisation des données

Dans le cadre de la gestion de données, un examen attentif est requis au regard de la localisation des données et comment le fournisseur d'infonuagique répond aux exigences réglementaires. Il faut également porter une attention particulière au nombre de juridictions où les données seront entreposées. Dans le cas où le fournisseur d'infonuagique est présent dans plusieurs juridictions, l'OP doit se questionner sur la confiance qu'il a envers le fournisseur d'infonuagique à héberger les données dans le centre de traitement spécifié par celui-ci.

- ✓ les OP doivent s'assurer que lorsqu'un fournisseur choisit de fournir son service à partir d'un autre endroit, ce dernier s'engage à aviser l'OP du nouvel emplacement. Idéalement, le fournisseur d'infonuagique devrait obtenir l'approbation de l'OP avant de déplacer les données;
- ✓ saisie des données.

Dans certains cas, des pouvoirs légaux permettent aux forces de l'ordre de saisir les données de l'OP hébergées chez un fournisseur d'infonuagique. L'OP devrait également s'assurer qu'il peut récupérer ses données dans l'éventualité où le fournisseur d'infonuagique se place sous la loi de la protection des créanciers.

Confidentialité des données

La déclaration de confidentialité des données du fournisseur d'infonuagique devrait être intégrée au SLA. Cette déclaration devrait contenir de l'information sur la stratégie de rétention des données, sur la manière dont les données sont communiquées, sur la manière dont les données à caractère personnel sont stockées et utilisées, etc.

Garanties

Des objectifs mesurables sous forme de pourcentage de temps de garantie de fonctionnement du service doivent être définis.

Politique d'utilisation acceptable

Étant donné l'absence potentielle de relation directe entre le fournisseur d'infonuagique et l'OP, la politique d'utilisation décrira clairement comment l'OP peut utiliser un service d'infonuagique ainsi les actions que le fournisseur peut prendre en cas de violation.

Liste des services non-couvert

Dans le SLA, le fournisseur précisera dans quelles conditions l'accès à ses services est supporté. La SLA peut également indiquer ce qui est exclu et ce qui constitue un usage illégal. Dans le contexte actuel de l'offre infonuagique, cet élément est non-négociable et favorise généralement le fournisseur d'infonuagique.

Excès d'utilisation

Les OP devraient définir correctement leurs conditions d'utilisation, réduire la possibilité d'augmentation de son utilisation et examiner et comprendre les impacts de violation de leurs seuils d'utilisation. Une utilisation supérieure au contrat initial peut entrainer des coûts punitifs important.

Paiement

Le SLA doit préciser le mode de paiement et la fréquence. Il doit également préciser si le fournisseur exigence des paiements anticipés. L'OP doit être vigilent en cas de panne du service afin de réclamer un crédit.

Gouvernance

Les OP doivent vérifier qu'il y a un mécanisme en place pour être informé des changements à leur contrat par le fournisseur d'infonuagique. Un canal de communication doit être établi entre le(s) fournisseur(s) et les OP et les avis de modification doivent être transmis dans un délai raisonnable.

Support

Le fournisseur d'infonuagique doit préciser les niveaux de support en fonction du niveau de priorité d'une requête. Les éléments devant être mentionnés sont entre autre le temps de prise en charge, le temps de mise à jour du suivi et le temps cible de résolution.

Maintenance

Tous les systèmes requièrent une maintenance. Le SLA doit décrire, en pourcentage, le temps de disponibilité par exemple : 99,9% qui équivaut à 8,5 heures d'indisponibilité par an. Le SLA peut indiquer que ce temps n'inclus pas le temps requis pour la maintenance planifiée des systèmes. Ainsi, le fournisseur d'infonuagique peut avoir une interruption de service de 8,5 heures + le temps requis à la maintenance sans que l'OP ait droit à une indemnisation.

Sous-contractant

Les OP doivent s'assurer que le SLA du fournisseur d'infonuagique immédiat est sans ambiguïté en déclarant que leur SLA s'applique au service complet sans égard aux fournisseurs sous-contractant du fournisseur immédiat

Mise à jour logicielle

Le fournisseur d'infonuagique peut transférer la responsabilité de mises à jour logicielles aux OP. Ce scénario peut être avantageux pour les fournisseurs puisque les mises à jour peuvent créer de l'instabilité. Le fournisseur peut également « pousser » la mise à jour. Les OP peuvent exiger, à l'intérieur du SLA, qu'un avis leur soit acheminé. À la réception de l'avis, les OP peuvent émettre une option refus « opt-out ».

Standard spécifique

Les industries réglementées, comme le gouvernement, les services financiers et les soins de santé, auront des normes spécifiques et généralement assez lourdes et coûteuses qui doivent être abordées dans la SLA d'infonuagique. Dans ces cas précis, il est important d'impliquer les ressources légales dans la négociation d'un SLA.

c) Identifier des objectifs de performance

Services offerts par les fournisseurs d'infonuagique en général correspondent à une des trois grandes catégories de modèles de services *: Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) et *Software as a Service* (SaaS). Pour chaque catégorie, il y a des différences significatives dans les objectifs de niveau de service et des indicateurs de performance clés qui seront éventuellement inclus dans le SLA. En général, les objectifs de PaaS et SaaS sont moins précis que les objectifs de l'IaaS étant donné que la variété des solutions et applications offertes par les fournisseurs est beaucoup plus large pour ces modèles de service.

IaaS

Les OP devraient retrouver les éléments suivant dans un SLA de catégorie IaaS :

- ✓ métrique de traitement : disponibilité, durée d'une panne, fréquence de redémarrage;

La performance du traitement est généralement exclue du SLA puisque que le fournisseur garantit seulement que les ressources demandées sont disponibles et non qu'elles sont suffisantes;

- ✓ métrique sur la réseautique : disponibilité, le nombre de paquets perdus, bande passante, latence;

Les mesures couvrent seulement les éléments sous la responsabilité du fournisseur d'infonuagique;

- ✓ métrique sur le stockage : disponibilité, entrée / sortie par seconde (IOPS), temps de récupération, latence.

PaaS

Les OP doivent faire la distinction entre les PaaS d'un environnement de développement et d'un environnement de production. L'état des métriques des PaaS ne sont pas encore matures et varient entre les fournisseurs d'infonuagique. L'absence de standard dans les interfaces de communications amène

des contraintes de « lock-in » avec un fournisseur. Certain standard (ex : OASIS TOSCA) font leur apparition et il est important de les inclure dans le SLA.

SaaS

L'offre du SaaS est très variée et il devient difficile d'identifier des éléments communs à inclure dans un SLA. En général, les éléments tel que la disponibilité mensuelle, le temps de réponse du service et les ajustements automatiques de la capacité de traitement fond partie d'un SLA pour un service d'infonuagique de type SaaS. L'entreposage des données selon des standards afin d'assurer une portabilité des données doit également être inclus dans le SLA.

En plus des modèles de services, les termes concernant les modèles de déploiement (privé, public, hybride) devrait également être inclus dans un SLA.

d) Évaluer les exigences en termes d'accès à l'information, de protection des renseignements personnelles ou autrement confidentiels et de sécurité

La mise en place d'un système de classification basé sur la criticité et la sensibilité des données est une étape cruciale afin d'assurer une sécurité suffisante. Ce plan devrait inclure des détails sur le propriétaire des données, niveaux de sécurité appropriés, des contrôles de protection et une description des exigences de conservation et destruction des données. Ce plan servira de base pour appliquer les contrôles d'accès, d'archivage ou l'encryptions. Les OP devraient inclure une clause au SLA permettant d'auditer le fournisseur d'infonuagique sur sa conformité aux règles de sécurités. Le fournisseur devrait également informer l'OP lorsque celui-ci subit une intrusion, peut-importe la nature de l'intrusion.

e) Identifier les exigences en matière de gestion des services

Audit

En termes d'audit, le SLA devrait permettre de fournir une évaluation impartiale sur la fiabilité du service d'infonuagique. Il permet également d'évaluer en détail l'efficacité des systèmes internes et des mesures du fournisseur d'infonuagique. Il fournit des outils pour comparer la qualité du service du fournisseur avec la concurrence. Finalement, il permet d'évaluer la capacité de l'OP d'interfacer avec le fournisseur d'infonuagique et d'offrir des services sans interruption.

Surveillance

Le SLA devrait inclure les éléments suivants :

- ✓ gestion de la performance du système en infonuagique (temps réponse des systèmes entre l'utilisateur et le système en infonuagique);
- ✓ performance en cas de charge;
- ✓ performance des systèmes en inter-infonuagique.

Mesure de consommation

Le SLA devrait inclure les éléments suivants :

- ✓ garantie de l'exactitude des mesures de consommations;
- ✓ la possibilité de séparer la méthode de mesure de différents services en fonction de leur modèle d'utilisation;
- ✓ la possibilité d'appliquer un système de taxation en fonction de l'endroit où le service est utilisé.

Approvisionnement rapide

Le SLA devrait inclure les éléments suivants :

- ✓ délais de livraison des services de base (nouvel utilisateur, nouveau poste, nouveau système, etc.);
- ✓ personnalisation des services livrés;
- ✓ disponibilité d'environnements d'essais;
- ✓ retrait de capacité une fois celle-ci devenu inutile.

Mise à niveau des services existants

Le SLA devrait inclure les éléments suivants :

- ✓ la responsabilité d'initier les demandes de mise à niveau;
- ✓ délais pour l'implantation de la mise à niveau;
- ✓ processus de résolution des problèmes suite à la mise à niveau;
- ✓ processus de retour arrière en cas de défaillance majeure suite à la mise à niveau.

f) Se préparer pour la gestion des bris de services

Cette section du SLA permet de définir ce qu'est un bris de service. Il faut noter que dans la majorité des cas, la responsabilité de démontrer qu'il y a eu un bris revient au consommateur (OP) et on au fournisseur de service d'infonuagique. Il est donc important que l'OP se dote d'outils afin de démontrer la durée et l'ampleur de la panne du service d'infonuagique. Finalement, la gestion d'un incident d'un service infonuagique s'intègre au processus de gestion des incidents de l'OP. Ce dernier a la responsabilité du processus de gestion des incidents. Le gestionnaire de l'incident doit pouvoir interagir avec le fournisseur d'infonuagique par un moyen de communication et des délais convenu dans le SLA.

g) Comprendre le plan de recouvrement en cas de sinistre

Le fait d'utiliser des services en infonuagique ne protège en rien l'OP contre un sinistre. Ce dernier doit inclure dans le SLA l'approche à utiliser en cas de sinistre. On entend par approche, entre autres, l'ordre de priorisation du retour des différents services portés en infonuagique.

h) Comprendre le processus de fin de contrat

Tout SLA doit inclure une section décrivant la fin de contrat. L'aspect le plus important est la récupération des données par l'OP. Ces derniers devraient également inclure les éléments suivants :

- ✓ le niveau d'assistance du fournisseur d'infonuagique dans le processus de fin de contrat, et ce, sans coûts additionnels;
- ✓ le fournisseur doit être responsable du retrait des données de l'OP et l'assister dans le processus de récupération des données;
- ✓ le format sous lequel les données sont retournées au OP doit également être précisé;
- ✓ un délai maximal au fournisseur d'infonuagique pour détruire les données de l'OP une fois celle-ci transmises;
- ✓ une assurance de la continuité du service tout le long du processus de fin de contrat.

Une fois les étapes complétées, l'OP doit exiger une confirmation écrite que le fournisseur de service à détruit l'ensemble des données lui appartenant.

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique