

Annexe A
Énoncé des besoins
Services d'infonuagique publics

Table des matières

- 1. Besoin du gouvernement2
- 2. Buts, objectifs et fins2
- 3. Lois, instruments de politique et lignes directrices.....2

BROUILLON

1. Besoin du gouvernement

Le gouvernement du Canada a besoin de services d'infonuagique publics disponibles sur le marché afin de répondre aux besoins opérationnels d'un vaste éventail d'organisations gouvernementales.

L'accès à ces services sera rendu possible et géré par Services partagés Canada et soutenu par la collectivité des dirigeants principaux de l'information (DPI) du gouvernement du Canada (GC), afin de s'assurer que les services d'infonuagique sont utilisés à l'échelle du GC dans le respect des niveaux appropriés de gouvernance, de sécurité et d'intégration technique aux services de technologie de l'information (TI) existants, et d'intégration opérationnelle aux processus financiers et contractuels en place.

Cette approche permettra de réduire de façon importante le fardeau des divers ministères et organismes gouvernementaux, étant donné qu'une partie considérable des besoins associés à l'utilisation de services d'infonuagique commerciaux seront pris en charge par les fournisseurs de services d'infonuagique (FSI), ce qui facilitera l'accès à des services d'infonuagique approuvés pour utilisation par le GC.

2. Buts, objectifs et fins

Services partagés Canada (SPC) rendra possible, regroupera et rationalisera l'accès aux catalogues de services des FSI offerts pour être utilisés par d'autres organisations gouvernementales. Afin d'aider les organisations à fournir leurs services et à répondre à leurs besoins, tant en interne qu'à l'égard de la population canadienne, le Canada recherche l'accès aux services de FSI, et la prestation de ces services, par l'intermédiaire de catalogues de services en ligne.

Le but est de fournir un accès à des services d'infonuagique multiples pour le gouvernement du Canada. Conformément à l'énoncé des besoins, ces services doivent :

- a. être fournis sur demande;
- b. offrir une élasticité rapide;
- c. être fiables et disponibles 24 heures sur 24, 7 jours sur 7, 365 jours sur 365;
- d. être sécuritaires et conformes;

3. Lois, instruments de politique et lignes directrices

Le gouvernement du Canada doit respecter les dispositions des lois, politiques, lignes directrices et instruments suivants :

1. <i>Loi sur l'accès à l'information</i>	http://laws-lois.justice.gc.ca/fra/lois/A-1/index.html
2. <i>Loi sur les langues officielles</i>	http://laws.justice.gc.ca/fra/lois/O-3.01/index.html
3. <i>Loi sur la protection des renseignements personnels</i>	http://laws.justice.gc.ca/fra/lois/P-21/index.html
4. Politique de communication du gouvernement du Canada	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12316
5. Politique sur l'accès à l'information	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12453
6. Politique sur la gestion de l'information	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12742

7. Norme sur l'accessibilité des sites Web	http://tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601
8. Lignes directrices concernant la conservation des documents administratifs communs du gouvernement du Canada	http://www.collectionscanada.gc.ca/government/products-services/007002-3100.2-f.html#a
9. Norme sur la facilité d'emploi des sites Web	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?section=text&id=24227
10. Boîte à outils de l'expérience Web	http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/communications/ws-nw/wet-boew-fra.asp
11. Norme sur la protection de la vie privée et le Web analytique	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26761&section=text
12. Politique sur l'utilisation acceptable des dispositifs et des réseaux	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=27122
13. Politique sur la sécurité du gouvernement du Canada	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578
14. CST – ITSG-33, La gestion des risques liés à de la sécurité des TI : Une méthode axée sur le cycle de vie	https://www.cse-cst.gc.ca/fr/publication/itsg-33
15. CST – ITSG-22, Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada	https://www.cse-cst.gc.ca/fr/node/268/html/15236
16. CST – ITSG-38, Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones	https://www.cse-cst.gc.ca/fr/node/266/html/25034
17. CSTC – ITSG-31, Guide sur l'authentification des utilisateurs pour les systèmes TI	https://www.cse-cst.gc.ca/fr/node/267/html/22784

Livrables contractuels techniques et livrables contractuels de sécurité

Numéro	livrables contractuels
1.	L'entrepreneur doit livrer, activer, prendre en charge, gérer et faire fonctionner les services infonuagiques publics et qui comprend l'accès et la capacité à fournir des catalogues de services en ligne.
2.	L'entrepreneur doit avoir disponible des accords de niveaux de services publiés (ANS) et disponibles sur le marché.
3.	L'ENTREPRENEUR doit fournir au GC un compte global et la possibilité de créer des comptes auxiliaires pour les ministères clients du GC afin de permettre l'approvisionnement et l'utilisation de services d'infonuagique publics ainsi que l'accès aux catalogues de services publics en ligne.
4.	L'entrepreneur doit aviser et notifier le responsable technique du GC par téléphone et par courriel (7 jours x 24 heures x 365 jours), selon la priorité telle qu'indiquée par le GC, de tout incident suspecté ou réel relatif à la sécurité.
5.	L'ENTREPRENEUR doit signaler, dans les délais prévus de l'accord sur les niveaux de service (ANS) publié, tout incident de sécurité suspecté ou réel, y compris les suivants, sans s'y limiter : a) les risques d'attaque par déni de service; b) les logiciels malveillants; c) l'ingénierie sociale; d) l'intrusion ou l'accès non autorisé; e) la violation de la sécurité de l'information; fi) toutes autres violations de la sécurité ou cybermenaces ciblant le Canada, ou ayant des répercussions sur les services en nuage du GC (p. ex., des menaces venues de l'intérieur de la part de l'ENTREPRENEUR).
6.	L'entrepreneur doit fournir toutes les preuves associées à un incident de sécurité, y compris les registres et les enregistrements de vérification, dans l'heure suivant l'incident ou dans un délai précisé par le GC.
7.	Le fournisseur de l'ENTREPRENEUR doit travailler avec l'Équipe d'intervention en cas d'incident de sécurité en matière de TI (EIISTI) du Canada au confinement, à l'élimination et à la reprise en cas d'incident de sécurité informatique.
8.	L'entrepreneur doit mettre en œuvre un processus de vérification et d'enquête qui : a) ne permet qu'à des représentants désignés et préautorisés du Canada (p. ex., l'EISSTI de SPC) de demander et d'obtenir un accès discret et l'information associée aux données du GC (données de l'utilisateur, registres d'événements, contenu) aux fins de mener des enquêtes; b) ne doit pas divulguer cet accès aux utilisateurs finaux; et c) est approuvé par le GC.
9.	L'entrepreneur doit balayer toutes les données du GC pour déceler la présence de logiciels malveillants. Les serveurs doivent être dotés de mécanismes de protection actives ordinateurs hôtes qui recherchent activement les logiciels malveillants à une fréquence hebdomadaire.

10.	L'ENTREPRENEUR doit fournir une solution technique automatisée (par exemple, un pare-feu au niveau des applications Web) afin de surveiller tout le trafic vers les applications Web publiques et en provenance de celles-ci de sorte à détecter et à empêcher de façon continue les cyberattaques (failles de type injection, dépassements de mémoire tampon, script de site à site, etc.).
11	<p>L'entrepreneur doit s'assurer que l'intégrité des données du GC sont protégées à l'aide de solutions de chiffrement à moins de les protéger au moyen d'autres mécanismes alternatifs approuvés par le GC. L'intégrité des données du GC doit être maintenue afin d'empêcher et de détecter toute modification, copie ou destruction inappropriée (double saisie, authentification de message, signature numérique, totaux de contrôle, etc.).</p> <p>Cela inclut :</p> <p>a) la protection des données transmises entre les composantes de la solution et entre les systèmes autorisés afin de s'assurer que les informations sont intactes et qu'elles ne sont pas modifiées pendant le transfert, que ce soit à des fins malveillantes ou par accident; et</p> <p>b) la capacité d'exécuter des vérifications de l'intégrité des fichiers du système source au système cible pour l'échange de données et d'aviser les parties pertinentes lorsqu'une condition d'erreur est constatée (relativement à un message précis ou à des composantes de système).</p>
12.	<p>L'ENTREPRENEUR doit s'assurer que les solutions cryptographiques utilisées dans le cadre de la mise en œuvre de mesures de protection de la confidentialité ou de l'intégrité, ou encore d'un mécanisme d'authentification (p. ex. les solutions RPV, TLS, les modules logiciels, les IRC et les jetons d'authentification le cas échéant), implementés pour le GC utilisent les algorithmes cryptographiques, les tailles de clés cryptographiques, et les cryptopériodes approuvés par le GC.</p> <p>Cela comprend, sans toutefois s'y limiter :</p> <p>a) utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques et des cryptopériodes qui ont été approuvés par le CST et validées par le Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), et qui sont précisées dans la publication ITSB-111 (https://www.cse-cst.gc.ca/en/node/1428/html/25015) ou dans une version subséquente;</p> <p>b) être mise en œuvre sous forme d'un module cryptographique validé par le Programme de validation des modules cryptographiques (http://www.cse-cst.gc.ca/its-sti/services/industry-prog-industrie/cmvp-pvmc-fra.html) et conforme au niveau 1 de la norme FIPS 140-2, à tout le moins; et</p> <p>c) fonctionner sous un mode d'exploitation approuvé par la norme FIPS.</p> <p>La norme intitulée Federal Information Processing Standard (FIPS) 140-2 précise les exigences de sécurité auxquelles devra satisfaire un module cryptographique utilisé dans un système, un sous-système ou une composante de sécurité protégeant de l'information protégée. Avant d'utiliser tout module cryptographique, le fournisseur de services communs (FSC) doit fournir une copie du certificat de validation pertinent en vertu de la norme FIPS 140-2 ou, à tout le moins, le numéro du certificat de validation.</p>
13	La solution d'informatique en nuage de l'ENTREPRENEUR doit aussi prendre en charge le langage Security Assertion Markup Language 2.0 (SAML 2.0).

13.	L'ENTREPRENEUR doit fournir une solution technique automatisée (par exemple, un pare-feu au niveau des applications Web) afin de surveiller tout le trafic vers les applications Web publiques et en provenance de celles-ci de sorte à détecter et à empêcher de façon continue les cyberattaques (failles de type injection, dépassements de mémoire tampon, script de site à site, etc.).
14.	L'ENTREPRENEUR doit avoir la capacité de mettre en œuvre des certificats de clé publique délivrés en vertu d'une politique de certification approuvée par le GC ou par une autorité de certification approuvée par le GC. Ces certificats doivent être validés avant chaque utilisation.
15.	L'ENTREPRENEUR doit avoir la capacité de sécuriser et de crypter les canaux de communication qui sont utilisés pour la migration de serveurs physiques, d'applications ou de données vers des serveurs virtuels.
16.	<p>L'entrepreneur doit fournir une liste des emplacements (ville et province/état) des centres de données qui seront utilisés pour fournir les services inclus dans ce contrat. Pour les centres de données en dehors de l'Amérique du Nord, une liste de tous les pays dans lesquels les centres de données sont situés suffira.</p> <p>a) Pour chaque emplacement de centre de données, fournir la classification de niveau, utilisant le système de classification du Uptime Institute, LLC (basé aux E.U.) ou ses sociétés affiliées tel que décrit au https://uptimeinstitute.com/, ou toute autre normes de l'industrie avec lesquelles les centres de données sont conformes et que l'entrepreneur utilise pour classer les performances de disponibilité ou de performance de centre de données. L'entrepreneur est tenu de fournir les preuves de ces niveaux ou autre certifications indépendantes.</p>
17.	L'entrepreneur doit fournir et maintenir la documentation du système d'information et inclure toutes modifications apportées au système d'information / environnement de fonctionnement ou les problèmes identifiés lors de l'implémentation du plan ou de l'évaluation des contrôles de sécurité sur une base annuelle
18.	L'entrepreneur doit fournir la liste de leur personnel, identifiés par nom et le rôle, ayant les responsabilités d'administration de système, de surveillance et / ou de sécurité, qui devront recevoir les alertes de sécurité, les avis et les directives. Cette liste devra inclure l'autorité technique du GC et autres membres du personnel approuvé et spécifié par le GC.

1. Concept des opérations

1.1. But

Le concept des opérations a pour but de veiller à ce que l'infonuagique des documents non classifiés soit déployée et fonctionne selon les normes établies en infonuagique pour appuyer une gestion des risques efficace et trouver un équilibre entre la sécurité, les inscriptions et le soutien. De plus, le présent document expose la vision du mode et des conditions de fonctionnement du nouveau service.

Le lancement du projet d'infonuagique pour documents non classifiés permet d'établir une autorité d'approvisionnement centrale et de fournir aux ministères une méthode approuvée pour s'approvisionner en services d'infonuagique. De plus, les services d'infonuagique fournissent à SPC une méthode permettant d'établir la capacité informatique requise pour satisfaire la demande à l'aide de modèles financiers utilisateur-payeur semblables à ceux que l'on retrouve dans les services publics d'eau, d'électricité, de gaz et de téléphonie. Cette méthode permet aux gouvernements de passer d'un modèle de « dépenses d'investissement » (CAPEX) à un modèle de « dépenses d'exploitation » (OPEX), puisqu'il n'est pas nécessaire d'investir dans des infrastructures importantes, des services professionnels et du soutien.

Le contenu du présent document sera modifié pendant toute la durée du projet. La version 1.0 doit coïncider avec l'achèvement de la détermination des exigences.

1.2. Objectifs

L'objectif du projet d'infonuagique de documents non classifiés est de permettre aux ministères d'obtenir la capacité requise en infonuagique pour satisfaire la demande de solutions informatiques disponibles sur le marché et les mettre en œuvre. La première version du Programme d'activation du nuage sera axée sur un mécanisme d'approvisionnement qui facilitera l'adoption de services d'infonuagique (données non classifiées) par les ministères qui ont ce besoin. Services partagés Canada sera un agent habilitant qui gèrera les instruments de passation de marchés et facilitera l'adoption de l'infonuagique par son soutien en matière de réseau et de sécurité.

Les objectifs immédiats du Programme d'activation du nuage sont les suivants :

1. Fournir un mécanisme permettant aux ministères de choisir le nuage qui convient à leurs besoins opérationnels de façon à en maximiser les avantages comme l'élasticité, la disponibilité et la résilience.
2. Fournir la sécurité nécessaire pour que le Gouvernement du Canada gère les risques par des contrôles et des attestations de sécurité disponibles sur le marché.
3. Fournir des contrôles qui assureront l'enregistrement de toutes les données protégées et contrôlées par le gouvernement sur des serveurs situés au Canada (versions à venir).

1.3. Évaluation de la nature délicate des données

Responsables : Responsables ministériels des opérations ou du programme, chargés de projet ministériels, membres du personnel du Bureau du dirigeant principal de l'information (DPI) ou toute unité ministérielle ayant pour mandat de fournir des capacités en TI aux responsables opérationnels ministériels.

Activités : L'objectif de cette activité est de déterminer les catégories de sécurité correspondant aux activités opérationnelles sélectionnées qui seront imparties à un fournisseur de services infonuagiques.

On présume, à ce stade, que le ministère ou organisme responsable a établi les fonctions opérationnelles qui sont couvertes par la portée du projet et dont l'exécution se fera dans un environnement en nuage. Après avoir établi ces activités opérationnelles et les renseignements connexes, on définit une catégorie de sécurité qui indique le niveau le plus élevé de préjudice pouvant être causé par une menace portant atteinte aux objectifs de sécurité que sont la confidentialité, l'intégrité et la disponibilité.

Échéance : L'établissement des catégories de sécurité correspondant à l'activité opérationnelle est nécessaire pour confirmer le modèle de déploiement du nuage qui s'applique à l'impartition de l'activité en question et indiquer les contrôles de sécurité qui s'appliqueront sous la forme d'un profil de contrôle de sécurité. Cette activité doit s'accomplir tôt dans le cycle d'élaboration des systèmes que les ministères et les organismes utilisent et elle s'avère essentielle pour assurer l'approvisionnement et le déploiement des bonnes capacités d'infonuagique et créer les bons modèles de déploiement dans la stratégie d'adoption de l'infonuagique du GC.

Méthode : Mener les sous-activités énumérées ci-dessous et utiliser l'outil pour établir les catégories de sécurité (lien fourni). Cet outil est conçu pour saisir les renseignements produits par les sous-activités susmentionnées. Se servant d'une méthodologie normalisée, il saisit les renseignements sur les processus et les types de renseignements, établit les niveaux de préjudice et extrapole le seuil maximum de préjudice en matière de confidentialité, d'intégrité et de disponibilité, par rapport à un processus opérationnel ou un service devant être mis en œuvre dans le nuage.

1.4. Définir les processus opérationnels et les fonds de renseignements connexes

Il existe plusieurs sources permettant de définir et de décrire les processus opérationnels et les fonds de renseignements connexes, notamment :

- l'analyse de rentabilisation;
- le concept des opérations (CONOPS);
- les spécifications fonctionnelles provisoires;
- la documentation sur l'architecture d'entreprise qui décrit habituellement en détail les processus opérationnels d'une organisation et les fonds de renseignements connexes;
- les discussions et entrevues avec les analystes des activités ou d'autres personnes issues de communautés opérationnelles liées;
- les patrons de référence de services pour le modèle de référence stratégique du gouvernement du Canada (MRSG) du Secrétariat du Conseil du Trésor, qui peuvent également servir à définir et à décrire les processus opérationnels.

1.5. Évaluation des préjudices résultant d'une compromission

Idéalement, un ministère évalue les préjudices éventuels sur ses processus opérationnels et les fonds de renseignements connexes en faisant appel à des équipes multidisciplinaires regroupant des représentants du milieu des affaires, du monde juridique, de l'accès à l'information et de la confidentialité des données.

1.6. Établissement de la catégorie de sécurité pour l'activité opérationnelle

Une activité opérationnelle peut véhiculer un certain type d'information dont le niveau de préjudice serait bas en matière de confidentialité et un autre type d'information dont le niveau de préjudice serait moyen pour le même objectif de sécurité (ni l'un ni l'autre n'étant liés à l'intérêt national). Chacun de ces niveaux a une valeur et doit être consigné. Cependant, la catégorie de sécurité établie pour l'activité opérationnelle doit correspondre au niveau de préjudice le plus élevé.

Cette étape a pour résultat la catégorie de sécurité de l'activité opérationnelle, qui peut être exprimée à l'aide du même barème que celui des processus opérationnels individuels et des types d'information.

Concept de seuil maximum. L'établissement de la catégorie de sécurité pour une fonction opérationnelle qui sera prise en charge par le système d'infonuagique demande au responsable opérationnel d'envisager les catégories de sécurité de tous les types d'information qui seront traités ou enregistrés sur le nuage. Dans le cas d'un système d'information, le niveau de préjudice éventuel attribué aux objectifs respectifs en matière de sécurité (confidentialité, intégrité, disponibilité) est la valeur la plus élevée (seuil maximum) de toutes celles imputées aux catégories de sécurité établies pour chaque type de données résidant sur le système d'infonuagique.

1.7. Rédaction de l'énoncé sur la catégorisation de la sécurité

L'énoncé sur la catégorisation de la sécurité doit comprendre :

- une brève description des besoins opérationnels hébergés en infonuagique, du ou des processus lancés sur cette plateforme et des renseignements échangés;
- une description des préjudices attendus résultant d'une compromission;
- les niveaux de préjudices attendus en ce qui concerne la confidentialité, l'intégrité, et la disponibilité;
- les motifs de l'attribution des niveaux de préjudice;
- une déclaration d'acceptation explicite signée par les parties prenantes contenant la catégorisation du niveau de sécurité pour les processus opérationnels qui seront impartis à un fournisseur de services infonuagiques.

L'énoncé sur la catégorisation de la sécurité est rédigé dès l'achèvement de la catégorisation de la sécurité à la satisfaction de l'équipe du projet et des spécialistes en matière de sécurité participants.

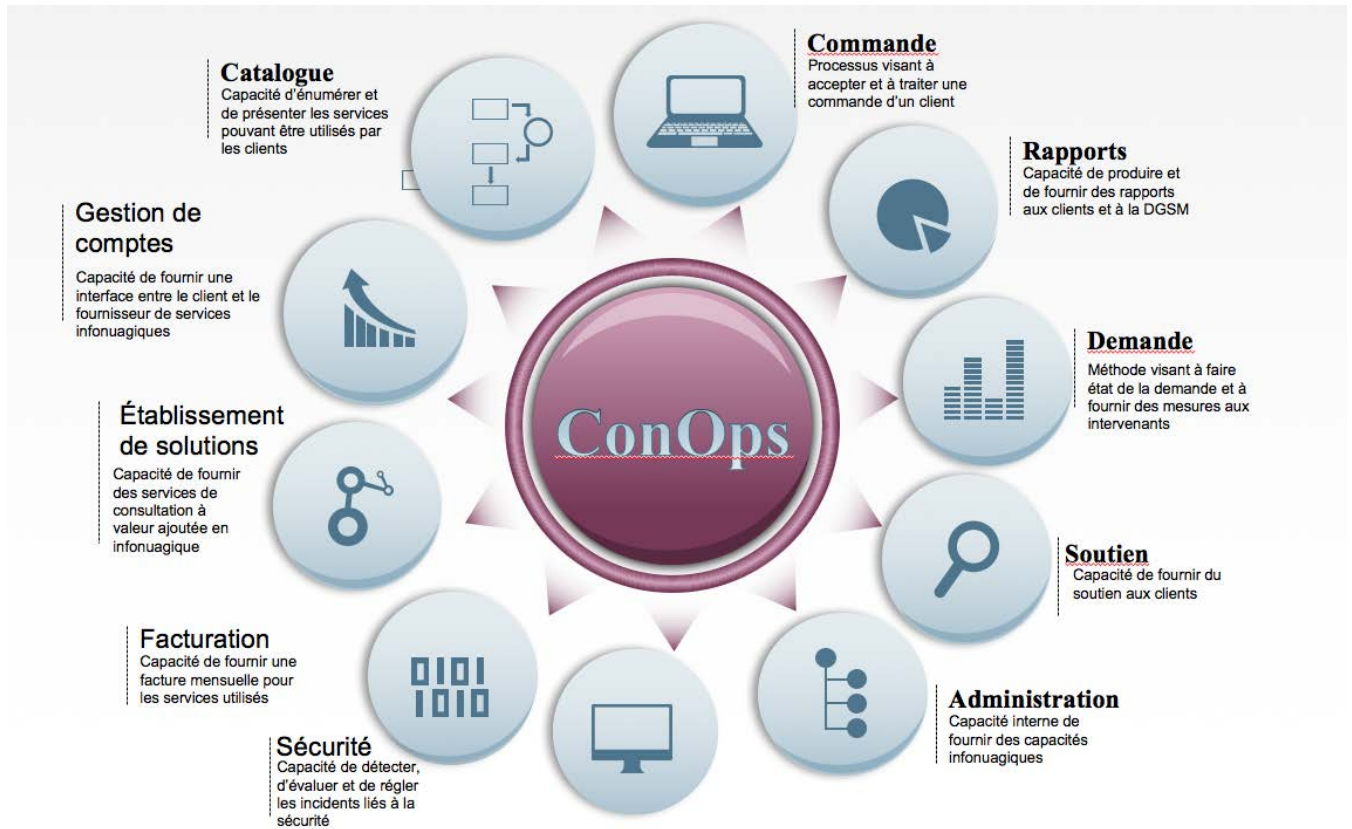
Il incombe aux ministères de valider la nature de leur accès aux services d'infonuagique requis aux termes du présent contrat, en précisant et en catégorisant les exigences, processus et renseignements opérationnels qui doivent être migrés ou hébergés dans le nuage en conformité avec la politique en place du GC qui est énoncée dans la directive du SCT sur la gestion de la sécurité ministérielle, Annexe C – Objectifs en matière de contrôles de sécurité (<https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16579§ion=html>).

Les ministères sont responsables de tout renseignement personnel qui se trouve sous leur garde. Aux termes de l'article 3 de la [Loi sur la protection des renseignements personnels](#), les renseignements personnels sont « les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable ». Il incombe aux ministères d'effectuer une évaluation des facteurs relatifs à la vie privée (EFVP) lorsqu'ils envisagent d'impartir des activités au cours desquelles on traite des renseignements personnels de Canadiens, ou au cours desquelles des organismes du secteur privé ont accès à de tels renseignements en vertu d'un contrat. Le document d'orientation du SCT intitulé « Prise en compte de la protection des renseignements personnels avant de conclure un marché » (<http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/p-prp/tpa-pcp/tpa-pcptb-fra.asp>) contient de plus amples renseignements à cet égard.

1.8. Déroulement des travaux

Ce qui suit vise à décrire le flux des activités pour le programme d'activation du nuage. Nous verrons d'abord les rôles et les responsabilités en détail, puis les processus fondamentaux dans le déroulement du programme.




Les processus suivants seront décrits :



1.8.1. Rôles et responsabilités

Le tableau suivant indique les rôles et responsabilités de chacun en ce qui a trait au déroulement des travaux.

Rôle	Description	Responsabilité
 Client	Il s'agit d'un ministère ou d'une entité gouvernementale qui obtient des services infonuagiques au moyen du mécanisme d'approvisionnement de SPC.	Il incombe au client de préparer la demande de services infonuagiques, de demander l'approbation du dirigeant principal de l'information (DPI) et du dirigeant principal des finances (DPF) et d'approvisionner les comptes auxiliaires nécessaires.
 Client DPI/DPF	SPC exige l'approbation du DPI et du DPF pour l'approvisionnement en services infonuagiques.	Le DPI et le DPF approuvent la demande de services infonuagiques déposée par le ministère.
 Fournisseur de services infonuagiques n	Le fournisseur de services infonuagiques est le fournisseur sélectionné par le client.	Il fournit les services conformément au service sélectionné par le client dans le catalogue du fournisseur.
 Programme d'infonuagique de SPC/Responsable technique	Le programme d'activation du nuage de SPC fait référence à l'unité opérationnelle interne qui a la responsabilité du fonctionnement du programme à SPC. Le responsable technique du programme d'infonuagique fournit l'interface avec SPC.	Le programme d'activation du nuage de SPC et le responsable technique gèrent les clients, le travail d'approvisionnement, l'interface avec les fournisseurs de services infonuagiques et les autres parties prenantes, le cas échéant.
 Administrateur de la DGSM	L'administrateur des fournisseurs de services infonuagiques est un des rôles du programme d'activation du nuage de SPC.	L'administrateur gère les comptes clients, fournit le soutien technique et administratif et approvisionne les clients au besoin.

 <p>Services des finances de SPC</p>	<p>L'équipe d'approvisionnement de SPC est l'organisation d'approvisionnement interne de SPC.</p>	<p>L'équipe d'approvisionnement de SPC est responsable du traitement de toutes les activités relatives à l'approvisionnement.</p>
 <p>COP de SPC</p>	<p>Le COP de SPC est le Centre des opérations de protection.</p>	<p>Il incombe au COP de traiter les incidents de sécurité et d'être l'initiateur des processus et procédures internes jusqu'à résolution de l'affaire. C'est le COP qui entre en liaison avec les parties intéressées, notamment le fournisseur de services infonuagiques.</p>
 <p>CER de SPC</p>	<p>Le CER de SPC est le centre d'exploitation de réseau.</p>	<p>Le CER a la responsabilité de traiter les demandes et les incidents liés au réseau. Il veille à assurer une connectivité de base entre les clients et le fournisseur de services infonuagiques. Il peut également être amené à participer à la résolution d'incidents de sécurité.</p>

1.8.2. Commande

SPC a élaboré un déroulement des commandes qui englobe l'intégration de clients dans le programme d'activation du nuage. Ce modèle est suivi lorsqu'un client indique avoir besoin d'un fournisseur de services infonuagiques (FSI) en particulier :



Responsable : Marc Contois

Outils : formulaire de suivi (doit être élaboré pour recueillir les renseignements sur les commandes), analyse de rentabilisation (prise en charge), courriel, document de gestion des demandes, formulaire de commande (Acquisitions et relations avec les fournisseurs [ARF])

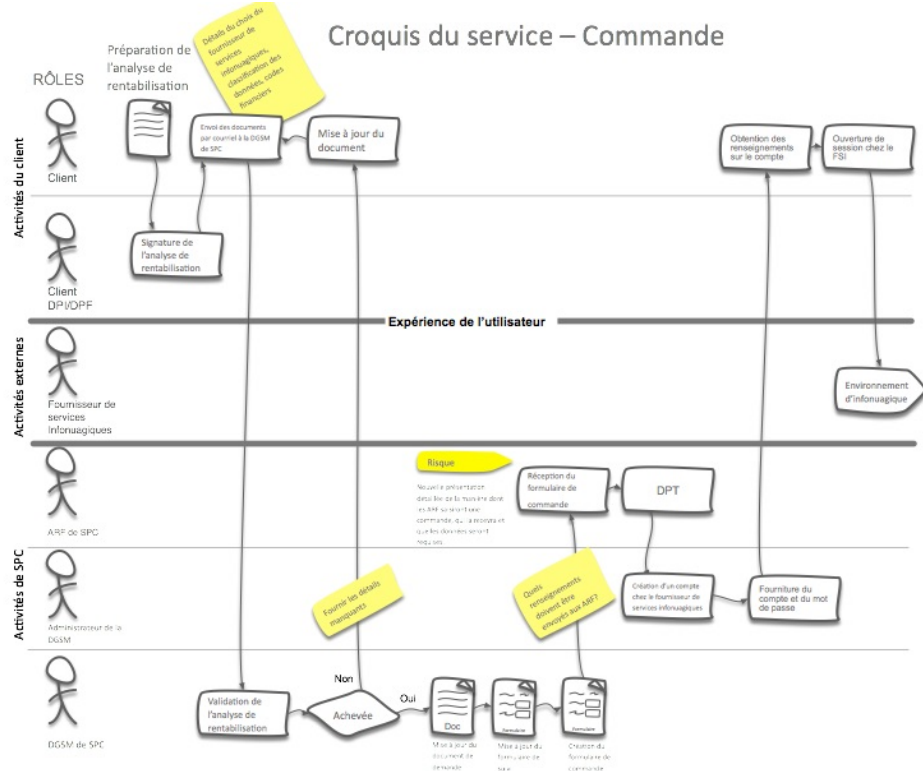
Accord sur les niveaux de service : à la suite de la réception, la commande sera traitée dans les deux jours ouvrables et envoyée aux ARF aux fins d'exécution

Fréquence du processus : sur demande, à la suite de la présentation d'une commande

Description du processus :

1. Réception de l'analyse de rentabilisation de la part du client par courriel par la Direction générale des services ministériels (DGSM).
2. La DGSM examine la proposition, vérifie la signature du Dirigeant principal de l'information (DGI) ou du Dirigeant principal des finances (DPF), vérifie les éléments financiers et la classification des données.
3. Si l'analyse de rentabilisation présente des lacunes sur le plan des renseignements, on la retourne au client, aux fins d'achèvement.
4. La DGSM saisit tous les renseignements pertinents dans la feuille de calcul Excel de gestion des demandes.
5. La DGSM saisit les renseignements sur la commande dans le formulaire de commande et l'envoie aux ARF.
6. Une commande dans laquelle figurent les précisions sur le client, les services visés par la commande, les codes financiers et les centres de coûts est envoyée aux ARF.
7. Les ARF traitent la commande et informent la DGSM que la création du compte peut être lancée.
8. Un administrateur de la DGSM crée un nouveau compte dans l'environnement des fournisseurs de services infonuagiques, crée le mot de passe et communique les données de connexion au client.
9. Le client peut ouvrir une session et créer son environnement.

- ### Hypothèses
- 1) Le client a achevé l'analyse de rentabilisation.
 - 2) La capacité du réseau du client est suffisante.
 - 3) Le degré d'intervention du client est faible.
 - 4) Le client a choisi le fournisseur de services infonuagiques.
 - 5) Le client a choisi des services du catalogue de fournisseurs de services infonuagiques.



Le responsable technique de SPC évalue la demande et vérifie les renseignements fournis dans la demande. Lorsque tous les renseignements ont été vérifiés, le responsable technique de SPC envoie la demande à l'équipe d'approvisionnement de SPC. L'équipe d'approvisionnement de SPC gère le contrat de services infonuagiques et évalue la demande. S'il s'agit d'une demande d'accès à un nouveau fournisseur de services pour ce client, l'équipe d'approvisionnement de SPC vérifie qu'il reste suffisamment d'espace libre avec ce fournisseur et lance une commande subséquente dans le cadre du contrat en fonction de l'espace demandé par le client. Lorsque tout est fait, l'équipe d'approvisionnement de SPC avise le fournisseur de services infonuagiques de la nouvelle demande de services. L'administrateur des fournisseurs de services infonuagiques de SPC en est informé et crée un compte client pour le fournisseur sélectionné. Ces identifiants sont ensuite fournis au client qui peut alors commencer à utiliser le service infonuagique.

Lorsque l'équipe d'approvisionnement de SPC reçoit une demande d'un client portant sur l'achat de services supplémentaires pour un fournisseur auprès duquel le client a déjà un compte, on a recours au processus d'achat de la section suivante.

1.8.3. Annulation du service



Responsable : Marc Contois

Outil : formulaire de suivi des annulations

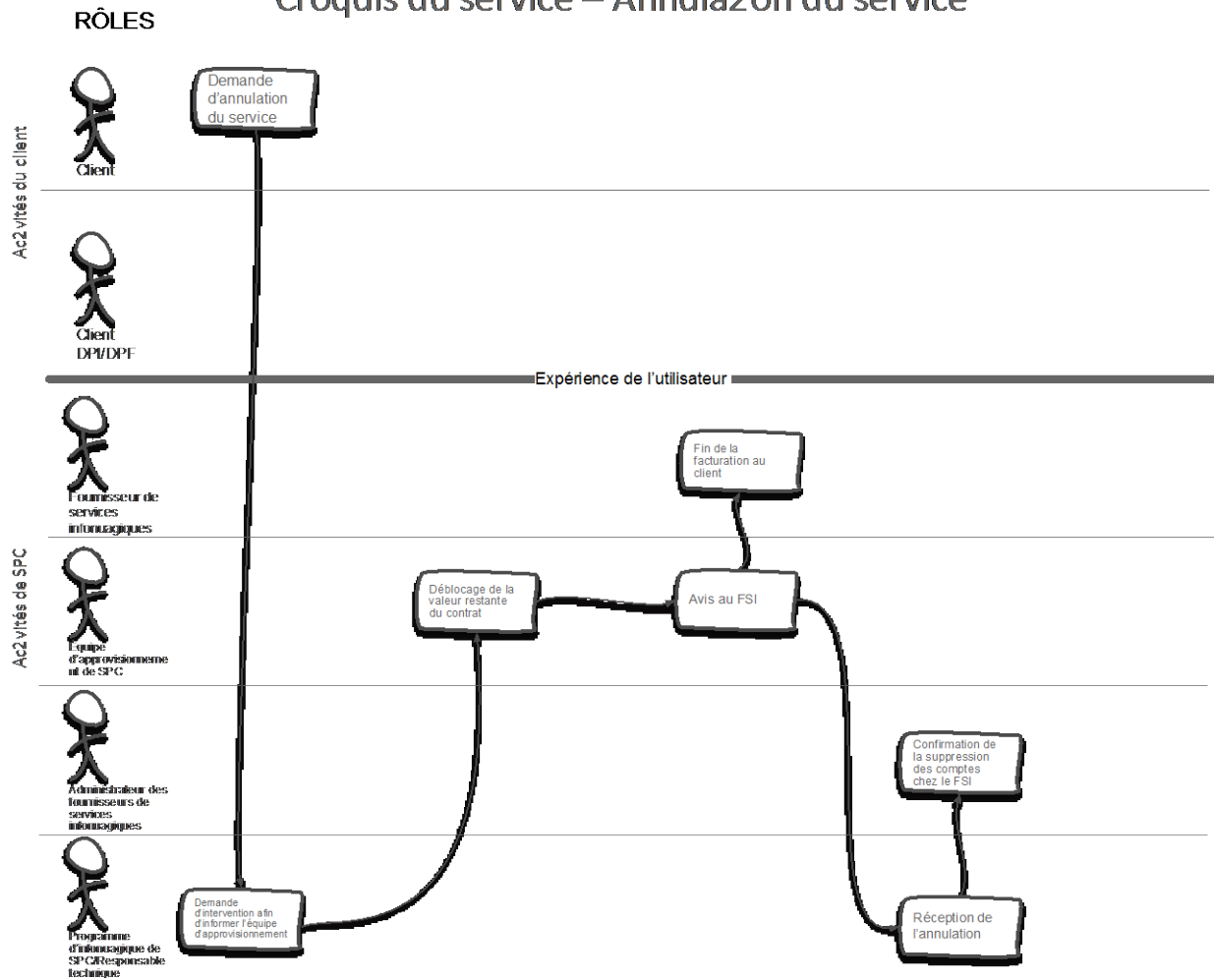
Accord sur les niveaux de service : à déterminer

Fréquence du processus : sur demande

Description du processus :

1. Le client informe le fournisseur de services infonuagiques qu'il souhaite résilier son service avec un fournisseur précis.
2. Le fournisseur de services infonuagiques informe l'équipe d'approvisionnement de Services partagés Canada (SPC).
3. L'équipe d'approvisionnement libère la valeur du marché et informe le fournisseur de services infonuagiques que l'engagement du client est achevé.
4. Elle informera la DGSM.
5. La DGSM fournit à l'administrateur de la DGSM les comptes à supprimer.

Croquis du service – Annulation du service



1.8.4. Rapports

Les clients qui décident d'annuler leur contrat auprès d'un fournisseur de services infonuagiques doivent d'abord informer par écrit le responsable technique de SPC de leur intention de mettre fin au service. Le responsable technique de SPC informe l'équipe d'approvisionnement de SPC du dernier jour de service. Il résilie le compte du client et débloque toute valeur restante du contrat pour la réaffecter au mécanisme d'approvisionnement. De plus, l'équipe d'approvisionnement de SPC informe le fournisseur de services infonuagiques de l'annulation et s'assure qu'aucune autre facturation n'a lieu. L'équipe d'approvisionnement de SPC fournira une confirmation écrite que le service est bien résilié au responsable technique de SPC, qui ouvre alors une session chez le fournisseur de services infonuagiques afin de supprimer les sous-comptes au nom du client.



Responsable : Marc Contois

Outil : tableau de bord des fournisseurs de services infonuagiques, interface de programmation d'applications des fournisseurs de services infonuagiques, Excel

Accord sur les niveaux de service : la DGSM doit être en mesure de fournir des rapports sur un éventail de paramètres dans les deux jours de la demande.

Fréquence du processus : sur demande

Description du processus :

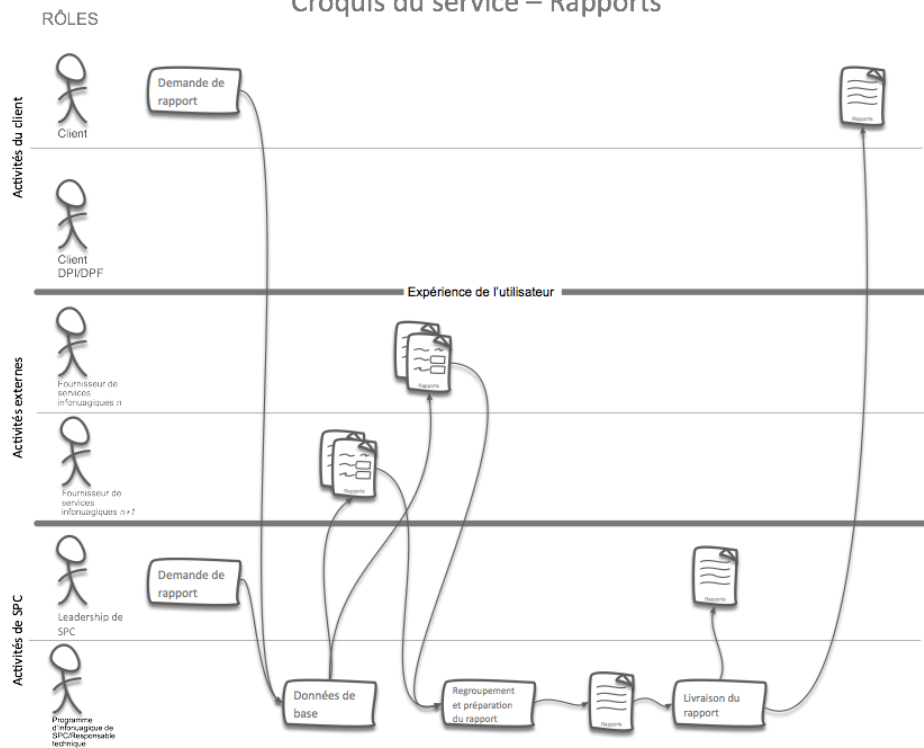
1. Une demande de production de rapport est envoyée à la DGSM.
2. La DGSM ouvre une session dans le tableau de bord des fournisseurs de services infonuagiques et produit les rapports.
3. Les rapports personnalisés reposant sur de nombreuses sources de données sont préparés dans Excel.
4. La DGSM prépare le rapport demandé et le présente au demandeur.

SPC

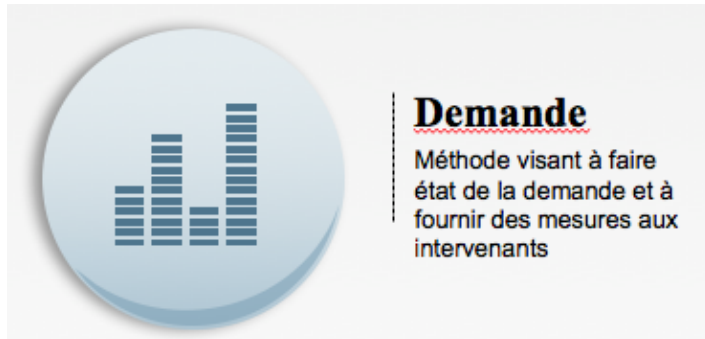
Hypothèses

- 1) Les fournisseurs de services infonuagiques fournissent un mécanisme permettant de produire des rapports en temps réel sur l'environnement.
- 2) L'utilisation de l'interface de programmation d'applications constituera une mise en œuvre à venir.

Croquis du service – Rapports



1.8.5. Demande



Responsable : Marc Contois

Outil : modèle de demande du client, modèle de cumul des demandes

Accord sur les niveaux de service : une demande est envoyée chaque mois aux ARF et au réseautage de SPC

Fréquence du processus : par commande, chaque mois

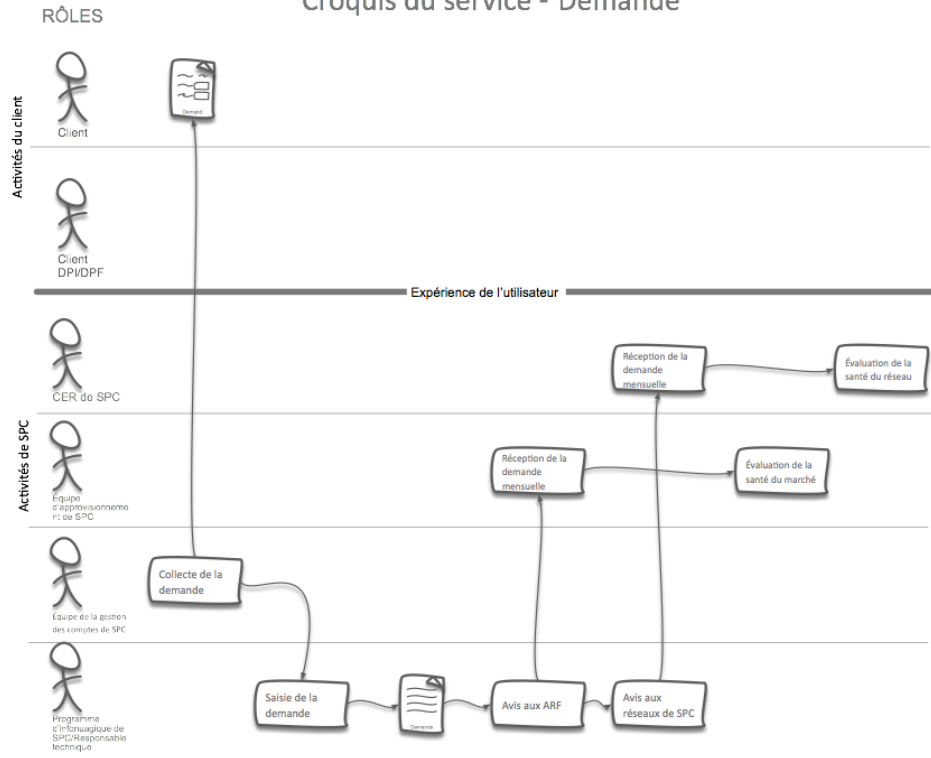
Description du processus :

1. Les gestionnaires de comptes de SPC présentent une enquête sur les demandes, chaque mois, aux clients.
2. Un formulaire est envoyé à un client pour prévoir les dépenses et le choix du fournisseur de services infonuagiques.
3. Les renseignements sont envoyés à la DGSM de SPC aux fins de collecte et de compilation.
4. Les renseignements sont saisis dans un modèle maître de demande.
5. Chaque mois, un résumé des demandes est envoyé aux ARF et aux Réseaux de SPC.
6. Les ARF et les Réseaux mènent une analyse pour faciliter la gestion de contrat et la demande relative au réseau.

Croquis du service - Demande

Assumptions

- 1) Le client désignera une ressource pour fournir les renseignements sur la demande.
- 2) L'équipe de la gestion des comptes de SPC communiquera avec le client pour recueillir les renseignements sur la demande, chaque mois.



1.8.6. Soutien



Responsable : Marc Contois

Outil : système de gestion des demandes du bureau de service

Accord sur les niveaux de service : les demandes sont réglées en 24 heures

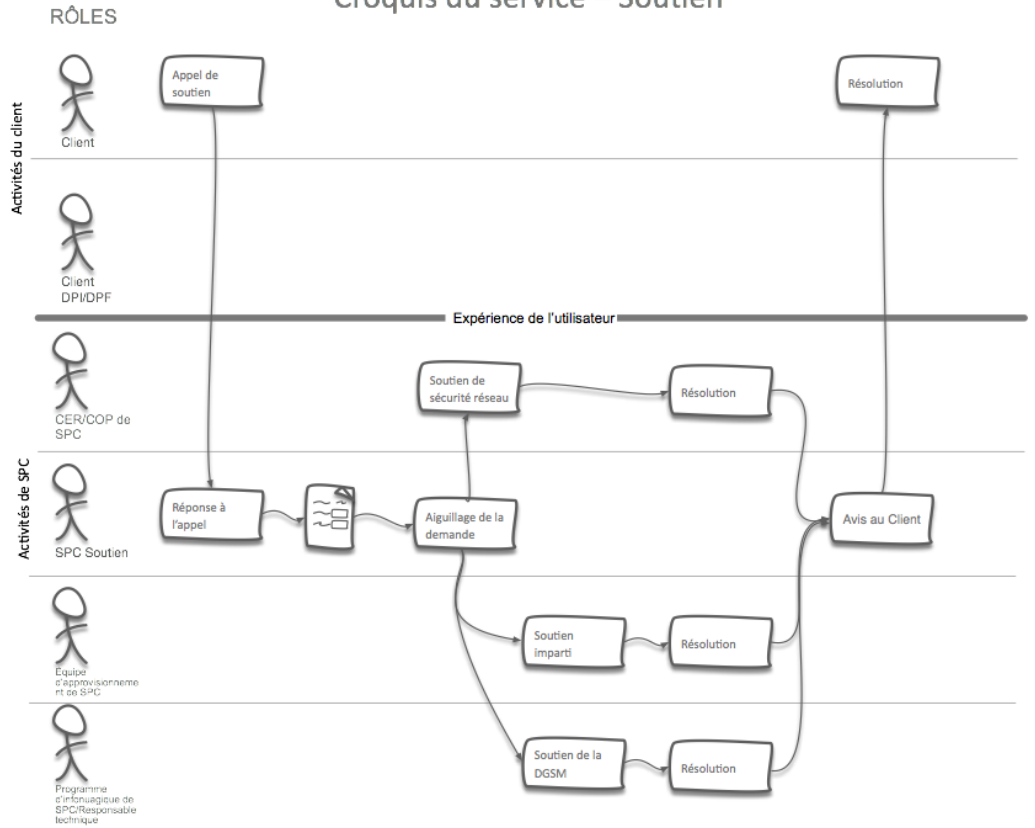
Fréquence du processus : sur demande

Description du processus :

1. Le client présente une demande de services auprès du bureau de service de SPC.
2. L'agent évalue l'appel et le transfère à l'organisation du réseau, à l'organisation de la sécurité, aux ARF ou à la DGSM.
3. La demande sera évaluée, traitée et résolue.
4. L'agent retourne la demande au bureau de service pour indiquer au client que la demande a été résolue.

Croquis du service – Soutien

- Hypothèses**
- 1) L'organisation de soutien de SPC créera une file d'attente pour la DGSM.
 - 2) Le soutien de première ligne prendra les appels de soutien et les aiguillera.
 - 3) Le soutien de première ligne avisera le client au sujet de la résolution.



1.8.7. Administration



Responsable : Marc Contois

Outil : tableau de bord d'administration des fournisseurs de services infonuagiques, formulaire d'ordre des travaux pour l'administration, formulaire pour le client

Accord sur les niveaux de service : à la suite de la réception, la commande sera traitée dans les deux jours ouvrables, et les données de connexion seront envoyées au client

Fréquence du processus : sur demande

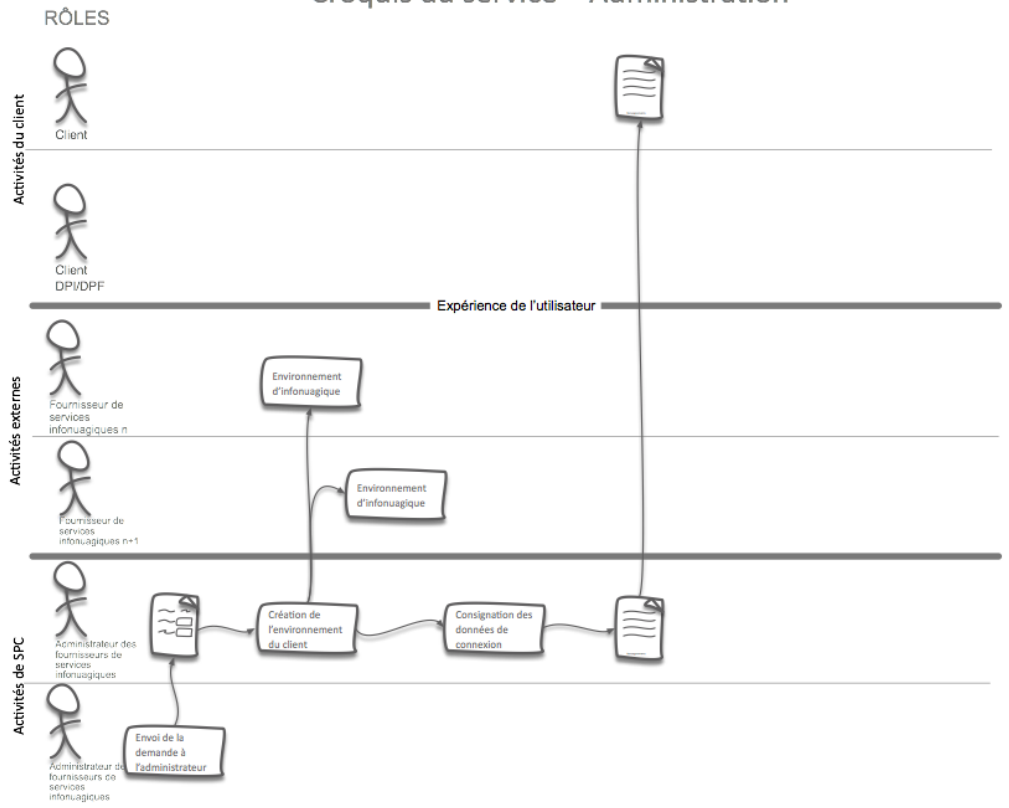
Description du processus :

1. La DGSM envoie un ordre des travaux à l'administrateur de la DGSM.
2. L'ordre présente les renseignements sur le compte qui doivent être présentés dans l'environnement des fournisseurs de services infonuagiques.
3. L'administrateur de la DGSM ouvre une session dans l'environnement des fournisseurs de services infonuagiques et crée les ressources nécessaires.
4. L'administrateur de la DGSM consigne l'environnement dans un formulaire.
5. Le formulaire est envoyé au client de manière sécuritaire.

Hypothèses

- 1) Un modèle maître de locataire sera utilisé.

Croquis du service – Administration



1.8.8. FACTURATION



Responsable : Marc Contois

Outil : facture du fournisseur de services infonuagiques, modèle de visualisation cumulative, modèle de facture de la DGSM, modèle de suivi des factures, compte de frais du courtier

Accord sur les niveaux de service : les factures doivent être livrées au service des finances de SPC dans les deux jours de leur réception de la part du fournisseur de services infonuagiques

Fréquence du processus : mensuelle

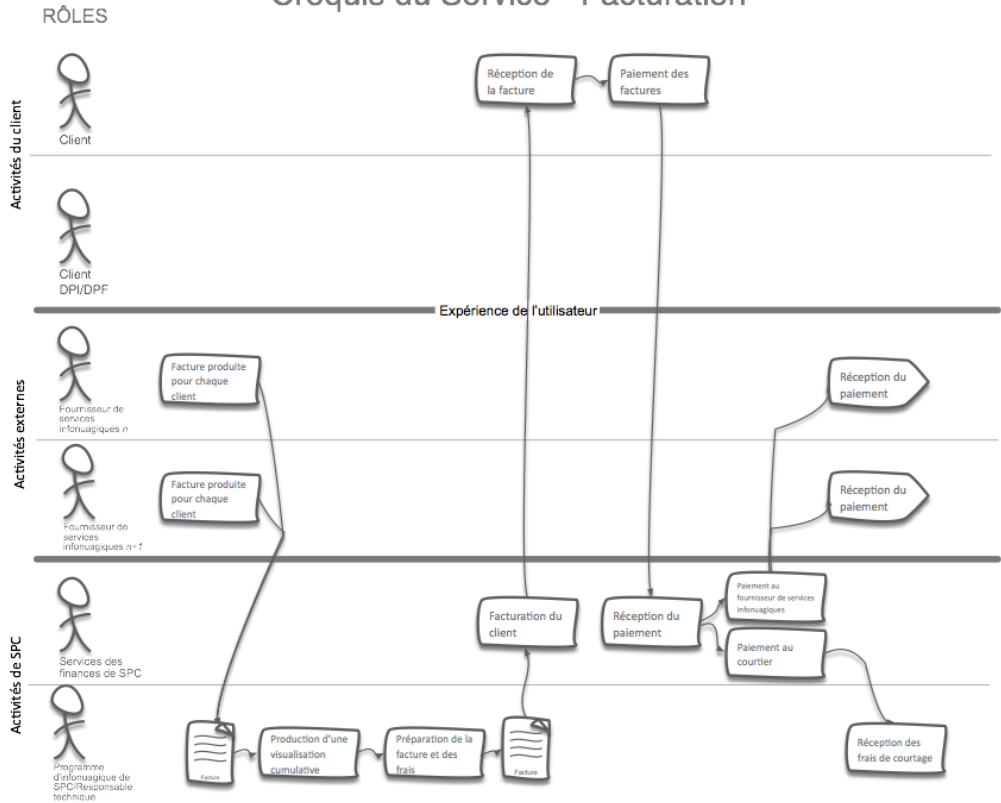
Description du processus :

1. Le fournisseur de services infonuagiques informe SPC par courriel qu'une facture est prête pour un client.
2. La DGSM ouvre une session dans la console du fournisseur de services infonuagiques, imprime la facture et saisit le total dans une feuille de calcul de suivi des factures.
3. La DGSM prépare une seule facture reposant sur un total partiel en fonction du fournisseur de services infonuagiques retenu.
4. La DGSM prépare une facture comprenant des frais de courtier de 10 %.
5. La DGSM envoie la facture au service des finances.
6. Le service des finances envoie la facture au client qui transfère les fonds au service des finances.
7. Le service des finances paie chaque fournisseur de services infonuagiques (le mécanisme doit être défini).
8. Le service des finances paie les frais de courtier au compte de la DGSM de SPC.

Hypothèse

- 1) SPC n'a pas de mandat et doit régler la facture pour le compte du client.
- 2) Le fournisseur de services infonuagiques présente une facture à SPC pour la totalité de l'utilisation mensuelle des services infonuagiques.
- 3) SPC reçoit la facture et y ajoute des frais de courtage de 10 %.
- 4) Le client reçoit la facture et paie sa partie de l'utilisation des services infonuagiques et les frais de courtage.
- 5) Le retard de paiement à un fournisseur de services infonuagiques constitue un risque plus élevé pour SPC.
- 6) Une facture à SPC pour chaque fournisseur de services infonuagiques.

Croquis du Service - Facturation



1.8.9. Établissement de solutions



Responsable : Marc Contois

Outil : catalogue de services de fournisseurs de services infonuagiques, modèle de solution personnalisée

Accord sur les niveaux de service : à déterminer

Fréquence du processus : sur demande

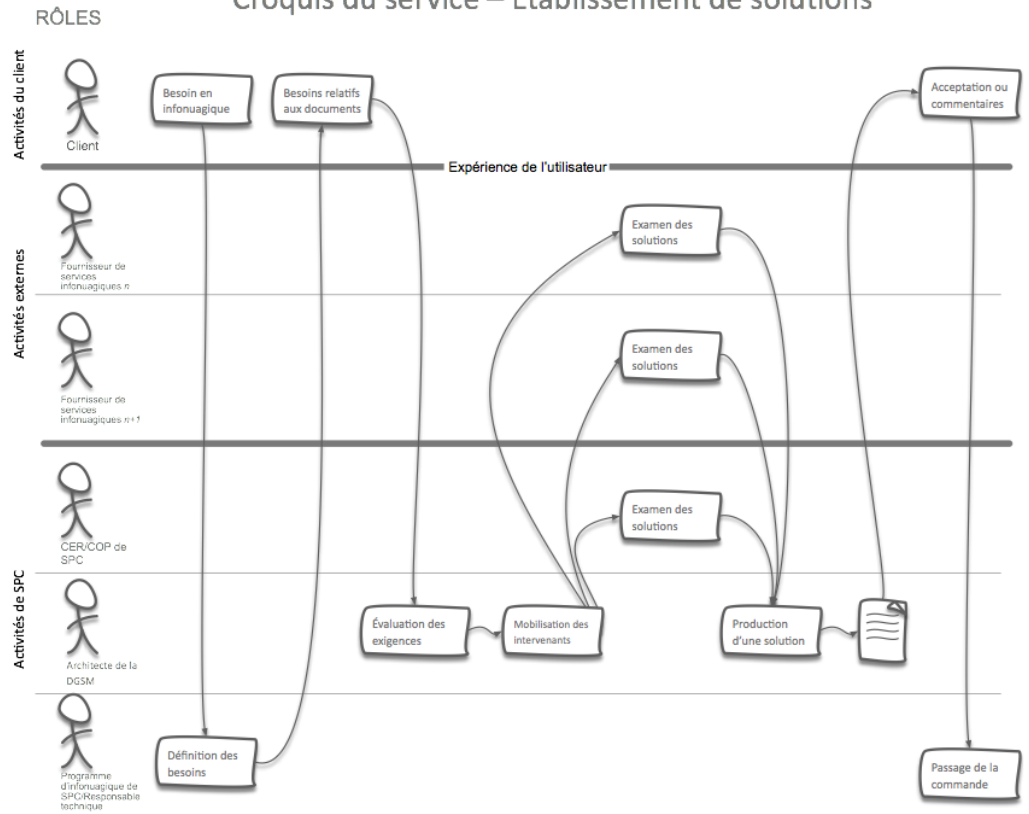
Description du processus :

1. Le client présente un besoin personnalisé à la DGSM.
2. La DGSM précise les besoins.
3. Les besoins sont présentés à un architecte d'infonuagique de la DGSM.
4. L'architecte d'infonuagique évalue les besoins et examine les solutions, allant de solutions de fournisseurs de services infonuagiques aux solutions de SPC.
5. L'architecte d'infonuagique prépare une solution et la présente au client.
6. Le client peut ensuite améliorer la solution, l'accepter ou la rejeter.
7. S'il l'accepte, le processus d'ordre est exécuté.

Hypothèses

- 1) La DGSM embauchera un expert-conseil en infonuagique pour élaborer des solutions personnalisées à degré d'intervention élevé avec le client.
- 2) Il s'agit d'une offre de service touchant l'état futur.

Croquis du service – Établissement de solutions



1.8.10. Gestion de comptes



Responsable : Marc Contois

Outil : information publicitaire sur les services de la DGSM, documents de formation pour la gestion de comptes

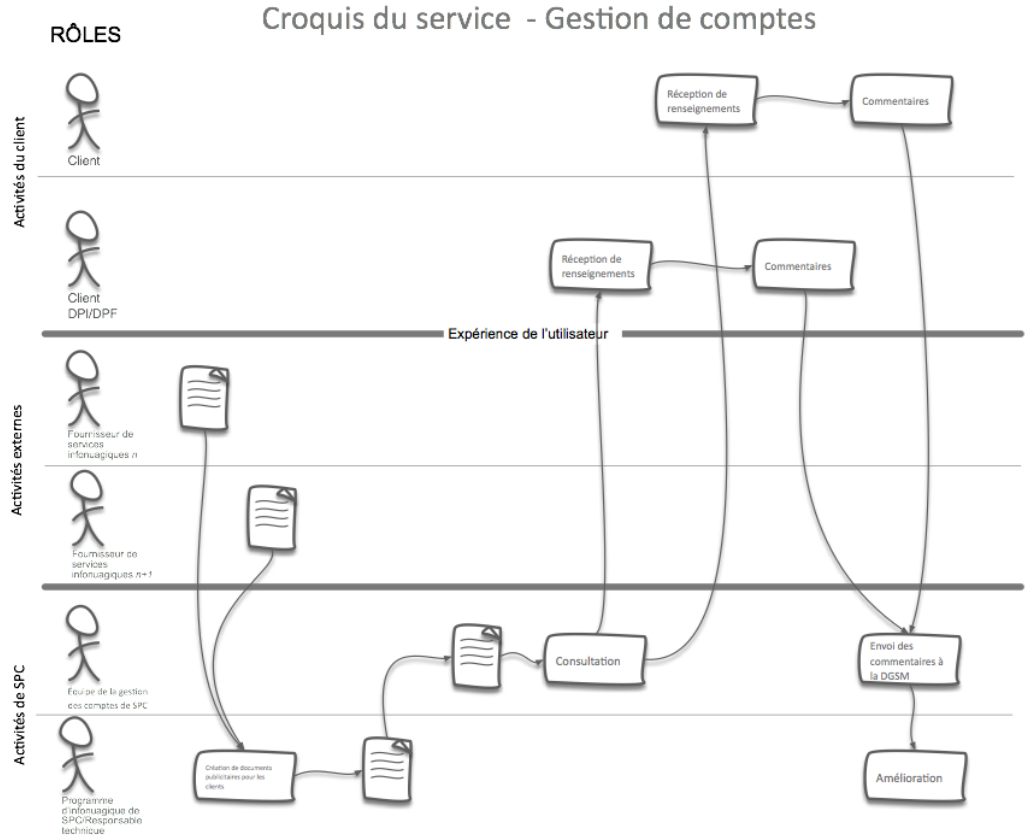
Accord sur les niveaux de service : la DGSM offrira des séminaires trimestriels pour présenter à la gestion de comptes une mise à jour sur les nouvelles capacités et les nouvelles caractéristiques

Fréquence du processus : trimestrielle

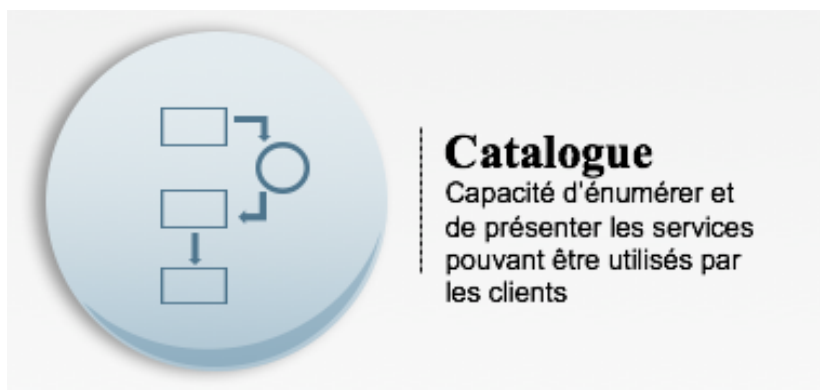
Description du processus :

1. La DGSM obtient des renseignements pertinents auprès des fournisseurs de services infonuagiques retenus.
2. La DGSM crée de l'information publicitaire sur le client et fournit des renseignements à jour à l'équipe de gestion de comptes.
3. La DGSM tient des séminaires pour définir l'étendue et l'ampleur des services offerts par l'intermédiaire de la DGSM.
4. L'équipe de gestion de comptes joue un rôle de prestation de services de consultation auprès des clients, répondant aux questions et aux demandes au sujet du service.
- 5.

Hypothèses	
1)	L'équipe de gestion de comptes de SPC acceptera le rôle de consultation auprès du secteur de service de la DGSM.
2)	La DGSM créera des documents aux fins de distribution aux clients.
3)	Le DGSM formera l'équipe de gestion de comptes.



1.8.11. Catalogue



Responsable : Marc Contois

Outil : catalogue de services de FSI, visualisation du catalogue de FSI

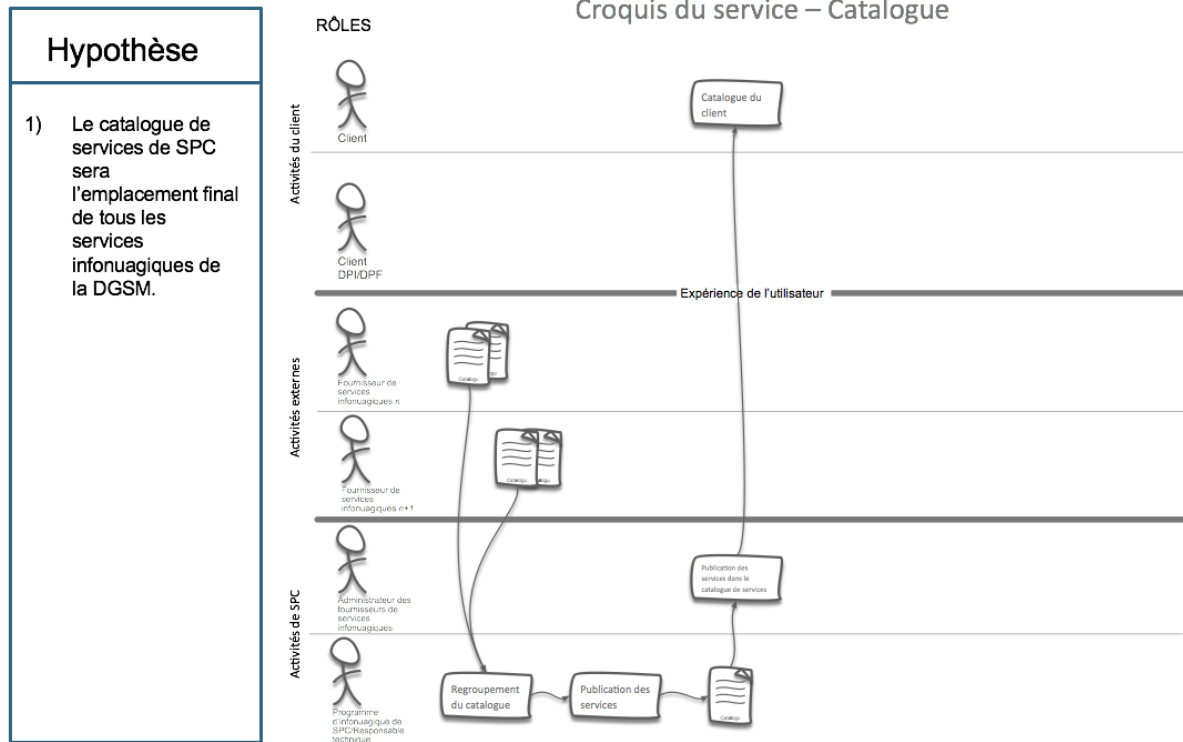
Accord sur les niveaux de service : le catalogue sera mis à jour chaque semaine.

Fréquence du processus : hebdomadaire

Description du processus :

1. La DGSM obtient le catalogue de chaque fournisseur de services infonuagiques.

2. La DGSM regroupe les catalogues selon un format de consultation compatible avec celui du catalogue des services de SPC.
3. L'administrateur de la DGSM publie le catalogue regroupé avec le catalogue des services de SPC.



1.8.12. Déroulement du soutien



Responsable : Marc Contois

Outil : système de gestion des demandes du bureau de service

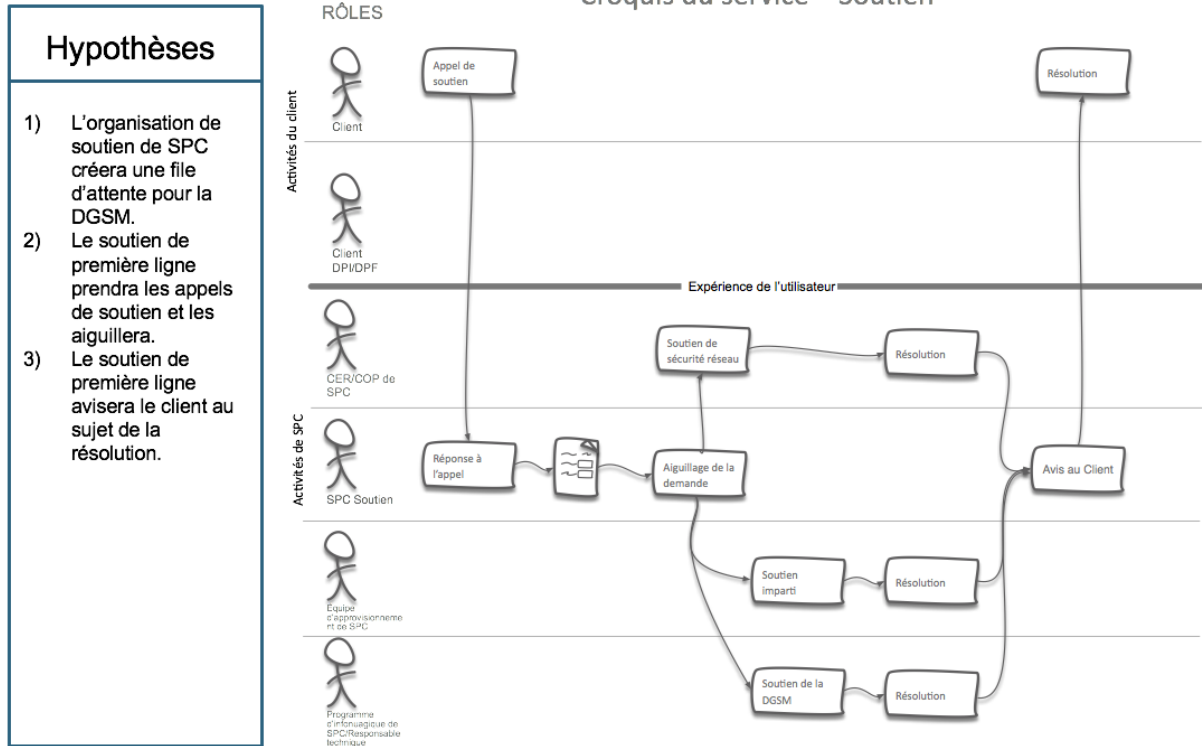
Accord sur les niveaux de service : les demandes sont réglées en 24 heures

Fréquence du processus : sur demande

Description du processus :

1. Le client présente une demande de services auprès du bureau de service de SPC.

2. L'agent évalue l'appel et le transfère à l'organisation du réseau, à l'organisation de la sécurité, aux ARF ou à la DGSM.
3. La demande sera évaluée, traitée et résolue.
4. L'agent retourne la demande au bureau de service pour indiquer au client que la demande a été résolue.



1.8.13. Déroulement d'incident de sécurité

Lorsqu'il détecte un incident de sécurité, le fournisseur de services infonuagiques doit communiquer ces renseignements au Centre des opérations de protection (COP) de SPC.



Responsable : Marc Contois

Outil : gestion des incidents,

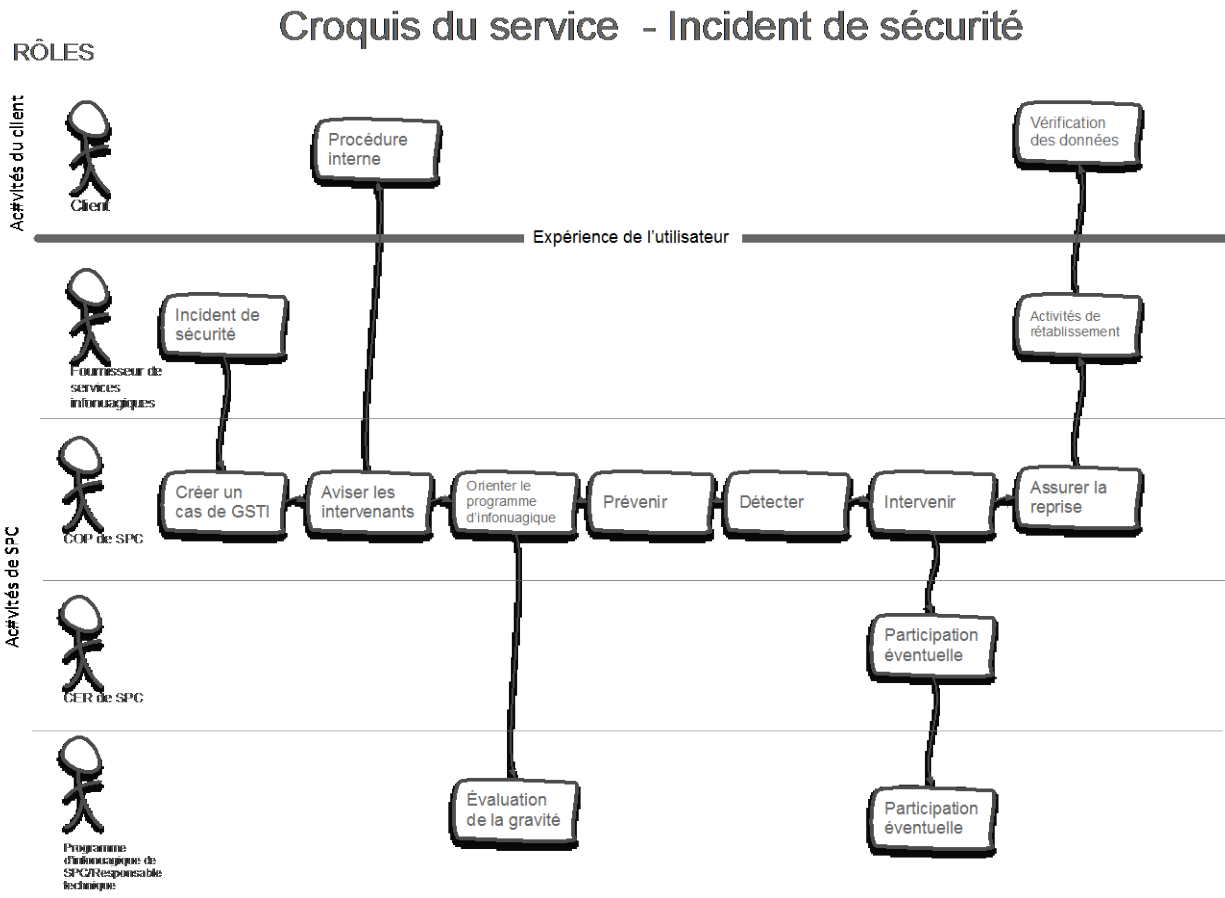
Accord sur les niveaux de service : à déterminer

Fréquence du processus : sur demande

Description du processus :

1. Un avis par courriel ou par téléphone est envoyé à des membres précis de la direction de SPC dans les 10 minutes qui suivent le début d'un incident de degré 1.
2. Le fournisseur de services infonuagiques tient une liste des personnes-ressources.

- Un processus d'acheminement au palier hiérarchique approprié fournit un mécanisme permettant de proposer d'autres moyens de résolution.



1.8.14. Incident de sécurité décelé par le client

Lorsqu'il décèle un incident de sécurité, le client doit communiquer ces renseignements au COP de SPC. Le COP de SPC fera participer les intervenants nécessaires, y compris le fournisseur de services infonuagiques, afin de résoudre l'incident.



Responsable : Marc Contois

Outil : gestion des incidents,

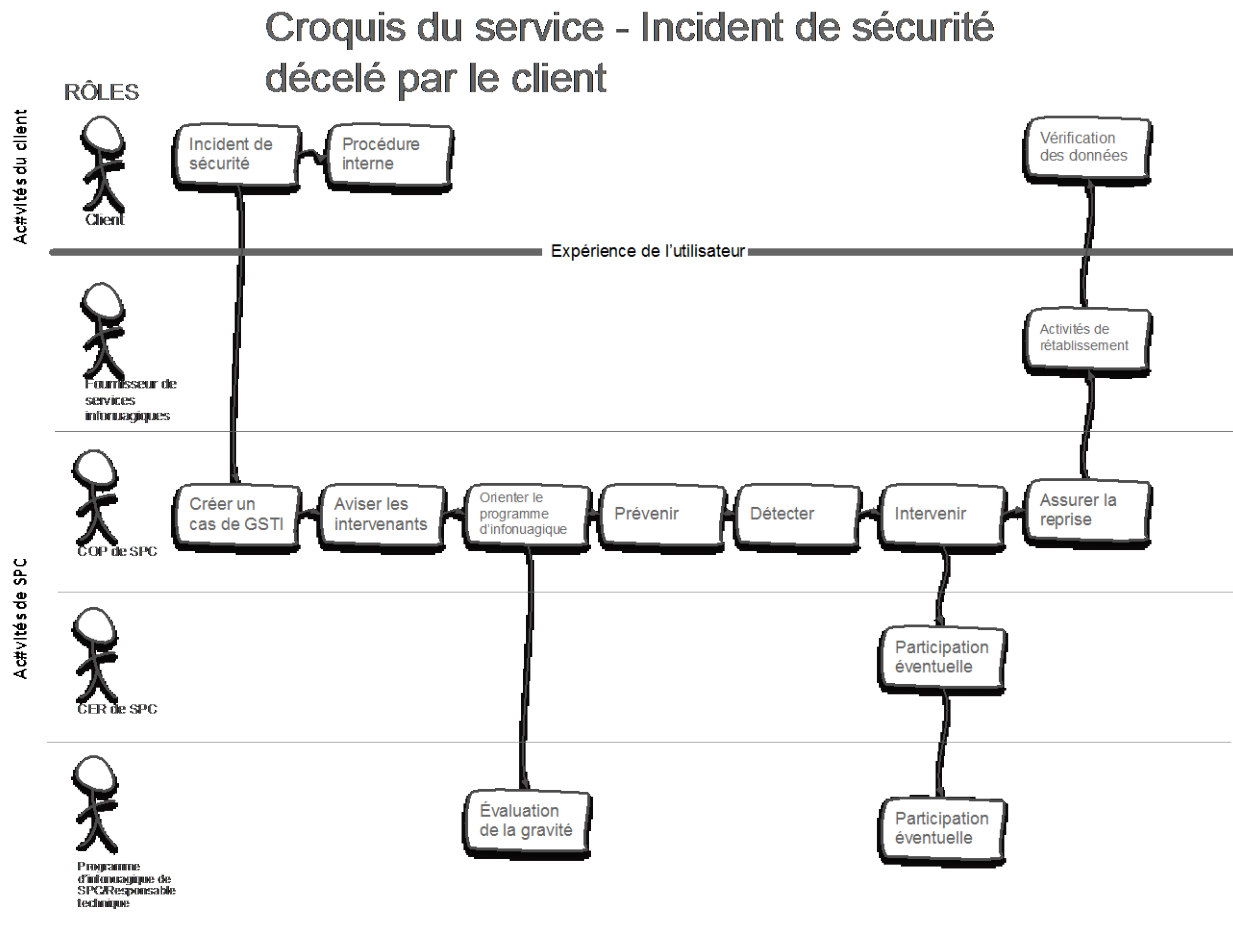
Accord sur les niveaux de service : à déterminer

Fréquence du processus : sur demande

Description du processus :

1. Un avis par courriel ou par téléphone est envoyé à des membres précis de la direction de SPC dans les 10 minutes qui suivent le début d'un incident de degré 1.
2. Le fournisseur de services infonuagiques tient une liste des personnes-ressources.
3. Un processus d'acheminement au palier hiérarchique approprié fournit un mécanisme permettant de proposer d'autres moyens de résolution.

1.8.15. Avis d'incident



Un avis par courriel ou par téléphone est envoyé à un groupe précis de membres de la direction de SPC dans les 10 minutes qui suivent le début d'un incident de degré 1. Le fournisseur des services infonuagiques tiendra à jour la liste des ressources approuvées qui recevront les avis.

1.8.16. Procédure de transfert à un niveau hiérarchique supérieur

Services partagés Canada offre un soutien en matière de transfert à un niveau hiérarchique supérieur pour les clients qui demandent de l'aide pour la gestion des incidents. Le responsable technique du programme d'activation du nuage de SPC intervient au nom des clients et communique avec le fournisseur de services infonuagiques afin de faciliter la résolution de l'incident. Les clients qui ont communiqué avec un fournisseur des services infonuagiques sans être parvenus à une résolution

satisfaisante peuvent dialoguer avec le bureau de service de SPC responsable de l'infonuagique. Le processus suivant devra être suivi :

1. Le client a communiqué avec le fournisseur de services infonuagiques concernant un incident et n'est pas parvenu à une résolution satisfaisante.
2. Le client communique avec le bureau de service de SPC.
3. Le bureau de service de SPC responsable de l'infonuagique évalue l'appel et donne des conseils dans la mesure du possible, ou transmet le problème au responsable technique du nuage de SPC.
4. Le responsable technique de SPC communique avec le client afin de comprendre l'incident.
5. Le responsable technique de SPC peut ensuite communiquer avec le fournisseur de services infonuagiques afin de lui transmettre l'incident et de le gérer avec lui.

En plus de servir de liaison avec les fournisseurs de services infonuagiques, le responsable technique de SPC peut également transférer l'incident à un niveau hiérarchique supérieur au sein de SPC. Cela peut avoir lieu lors de l'approvisionnement du réseau et des services de sécurité en vue d'améliorer l'échange d'information avec les fournisseurs de services infonuagiques.

1.8.17. Échéanciers en matière de transfert à un niveau hiérarchique supérieur

Tout incident devant être résolu qui dépasse ou qui devrait dépasser le seuil de niveau de service doit être transféré à un niveau hiérarchique supérieur et le représentant de SPC est informé par un courriel généré automatiquement ou par téléphone.

Le COP de SPC informe les parties concernées et exécute le processus interne de sécurité. Le COP communique avec le fournisseur de services infonuagique et d'autres intervenants pendant la durée de l'incident jusqu'à ce que l'on parvienne à le résoudre.

1.8.18. Gestion du rendement

Une évaluation plus approfondie de la structure de gestion du rendement sera réalisée au fur et à mesure de l'avancement du projet, toutefois, on a décidé que les fonctions de gestion du rendement seraient intégrées au groupe d'habilitation. Ce groupe sera responsable du contrôle de l'utilisation des services du fournisseur de services infonuagiques et disposera d'une série d'outils permettant de produire des rapports. On prévoit que le groupe d'habilitation surveillera certains aspects tels que l'utilisation, la fonctionnalité et les demandes de service.

Par ailleurs, l'accord sur les niveaux de service pour la fonction publique du fournisseur de services infonuagiques sera utilisé pendant le projet.