

Infonuagique

TENDANCE TECHNOLOGIQUE

L'infonuagique, que le National Institute of Standards and Technology définit comme « la fourniture de ressources informatiques sur demande au moyen d'un réseau informatique », présente deux grands avantages : la flexibilité et l'extensibilité.

Par contre, elle entraîne des risques sur le plan de la sécurité, de la confidentialité, de l'accessibilité et de la pérennité. Des sondages indiquent que les entreprises recourent à l'infonuagique pour accélérer la mise en œuvre de fonctionnalités destinées à soutenir les unités administratives et à faire des économies.

Par ailleurs, si l'infonuagique offre beaucoup d'avantages, elle engendre aussi des coûts pour l'entreprise au chapitre de :

- **la confidentialité** : il faut redoubler de prudence et s'assurer que les fournisseurs de services infonuagiques protègent la confidentialité de l'information traitée ou stockée sur le nuage;
- **la conformité** : la réglementation et les exigences propres à un secteur, comme celles encadrant le secteur des cartes de paiement, peuvent empêcher l'utilisation de services en nuage, limiter le choix du type de nuages à utiliser ou imposer l'implantation de techniques de sécurité précises;
- **l'aspect juridique** : la contrefaçon des marques de commerce, la sécurité ainsi que le partage des sources de données d'une entreprise peuvent poser des problèmes;

- **la sécurité** : les problèmes potentiels de sécurité pourraient retarder l'adoption de l'infonuagique, principalement parce que les secteurs public et privé craignent la gestion des services à l'externe et le cohébergement des données de différents utilisateurs. Les solutions vont du chiffrement, notamment par infrastructure à clés publiques, à l'utilisation de différents fournisseurs de services infonuagiques en passant par le soutien juridique;
- **la durabilité** : en ce qui a trait aux modèles financier et technologique des fournisseurs;
- **la malveillance** : étant donné la quantité de données personnelles qu'elle contient, la plateforme infonuagique est une cible de choix pour les pirates informatiques du crime organisé. Des individus se faisant passer pour des clients légitimes peuvent acheter des services infonuagiques dans un but malveillant. En 2009, un cheval de Troie visant les services bancaires a utilisé illégalement le service bien connu Amazon comme vecteur de commandement et de contrôle pour publier des mises à jour de logiciels et des directives. Les entreprises ne veulent pas être associées accidentellement à de telles activités.

Selon un sondage analytique d'Information Week, les motifs de l'adoption d'un modèle SaaS sont la rapidité d'implantation (3,9 sur 5); la réduction des dépenses en immobilisations (3,5 sur 5) et la réduction des frais d'exploitation (3,4 sur 5).

Les gestionnaires doivent connaître les risques inhérents à l'infonuagique. Ils doivent savoir où sont stockées les données, si elles sont protégées adéquatement, si le fournisseur impartit à des sous-traitants qui pourraient ne pas avoir mis en place les contrôles prévus au contrat initial ou qui pourraient modifier ou mettre à

jour le logiciel, ce qui obligerait les entreprises clientes à effectuer des opérations coûteuses de modification, de mise à niveau et de conversion.

Description

L'infonuagique repose sur l'exploitation d'Internet et des notions de virtualisation pour créer un environnement dans lequel les personnes et les organisations peuvent acquérir de la capacité de stockage et de traitement.

Le nuage combine l'utilisation d'Internet avec la fourniture d'une gamme de services, comme :

- les logiciels-services (Software as a Service—SaaS) fournissent l'accès à des logiciels;
- les plateformes-services (Platform as a Service—PaaS) fournissent la plateforme informatique ou le dispositif de stockage;
- les infrastructures-services (Infrastructure as a Service—IaaS) fournissent l'infrastructure, le réseau et le dispositif de stockage.

Importance

Sur le plan conceptuel, l'infonuagique est similaire aux sociétés de services informatiques bien connus dans les années 1970 et 1980. L'infonuagique offre divers niveaux de services technologiques facturés à l'utilisation. Il convient d'en évaluer les enjeux commerciaux et techniques.

- Les enjeux commerciaux ont trait à la viabilité, à la stabilité financière, à la performance passée et à d'autres questions dont il faut tenir compte avant de nouer une relation d'affaires.
- Les enjeux techniques ont trait à la satisfaction des besoins de l'entreprise en matière de fonctionnalité, de sécurité et de performance.

Pour les entreprises, l'infonuagique est un moyen abordable d'acquérir les capacités matérielles, logicielles, de communications et de traitement qui correspondent à leurs besoins.

Avantages commerciaux

Voici quelques-uns des avantages qu'offre l'infonuagique :

- les ressources informatiques sont « louées » pour répondre à des besoins variables au fil du temps;
- l'entreprise achète uniquement les ressources dont elle a besoin, et n'a pas à acquérir l'infrastructure et la capacité nécessaires en période de pointe;
- le fournisseur de services infonuagiques s'occupe de gérer l'infrastructure technologique, ce qui permet à l'entité de se concentrer sur ses activités commerciales;
- par sa nature, le nuage crée le stockage hors site, ce qui assure la disponibilité en cas de sinistre dans les locaux de l'entreprise;
- les données et les fonctions de traitement sont accessibles à partir de multiples emplacements;
- le fournisseur de services infonuagiques s'occupe des changements et des mises à niveau technologiques.

Enjeux et risques	Mesures d'atténuation possibles
<p>Il se peut que les entreprises ne connaissent pas l'emplacement actuel de leurs données ni le lieu où elles pourraient être stockées.</p>	<p>Exiger du fournisseur de services infonuagiques envisagé qu'il présente un rapport produit par une tierce partie sur ses activités relatives à la sécurité, aux contrôles, à la disponibilité et à la protection des renseignements personnels.</p>
<p>Le fournisseur de services infonuagiques peut impartir à son tour la capacité de traitement, le stockage en ligne ou l'archivage de l'information commerciale, ce qui peut :</p> <ul style="list-style-type: none"> • réduire la sécurité, la disponibilité ou la protection de l'information commerciale; • violer les lois et réglementations relatives aux renseignements personnels; • violer les obligations contractuelles entre l'entreprise et ses clients; • rendre plus difficile l'extraction des données de l'entreprise si le réimpartiteur éprouve des difficultés techniques ou financières. 	<p>S'assurer que toute entente entre les entreprises prévoit ce qui suit :</p> <ul style="list-style-type: none"> • interdire la réimpartition; ou • avant la réimpartition, l'entreprise doit approuver les aspects impartis; et • l'entreprise a le choix et la possibilité de revenir sur sa décision d'autoriser une réimpartition. <p>L'entreprise doit obtenir un exemplaire d'un rapport produit par une tierce partie indépendante sur la sécurité, le contrôle, la disponibilité, la politique de protection des renseignements personnels, les procédures, les solutions technologiques et leur efficacité opérationnelle.</p>
<p>Le stockage de certains renseignements dans le nuage pourrait contrevenir aux lois canadiennes, aux normes de l'industrie ou aux obligations contractuelles de l'entreprise.</p>	<p>L'entreprise doit préciser au fournisseur de services infonuagiques ses exigences particulières en matière de stockage des données.</p> <p>Le fournisseur de services infonuagiques doit accepter de respecter des exigences particulières dans une entente contractuelle.</p> <p>Le fournisseur de services infonuagiques doit fournir un rapport produit par une tierce partie sur la sécurité et, au besoin, sur la protection des renseignements personnels et la conformité avec les obligations contractuelles.</p>

Enjeux et risques	Mesures d'atténuation possibles
<p>La protection de l'information dans le nuage pourrait être inadéquate.</p>	<p>L'entreprise doit préciser ses exigences en matière de sécurité et de protection.</p> <p>L'entreprise doit préciser les normes à respecter (p. ex., ISO 27001/2, COBIT, PCI).</p> <p>Le fournisseur de services infonuagiques doit accepter de respecter des exigences particulières dans une entente contractuelle.</p> <p>Le fournisseur de services infonuagiques doit fournir un rapport produit par une tierce partie sur la sécurité et, au besoin, sur la protection des renseignements personnels et la conformité avec les obligations contractuelles.</p>
<p>L'information et les fichiers appartenant aux clients du fournisseur de services infonuagiques ne sont pas cloisonnés adéquatement.</p>	<p>Exiger du fournisseur de services infonuagiques qu'il garantisse le stockage des données critiques sur des appareils distincts.</p> <p>Chiffrer toutes les données commerciales stockées dans le nuage.</p>
<p>Enjeux résultant de l'impartition de certaines fonctions de TI précises à un tiers fournisseur de services infonuagiques.</p> <p>Il se peut que la responsabilité à l'égard des fonctions de TI confiée à un tiers, notamment la sécurité et la protection des renseignements personnels, soit mal définie ou traitée.</p>	<p>Conclure des contrats uniquement avec des fournisseurs de services infonuagiques viables et réputés.</p> <p>Clarifier la démarcation entre les processus et les technologies de l'entreprise (ordinateur et réseau) et les technologies et responsabilités du fournisseur de services infonuagiques, et veiller au bon fonctionnement des contrôles internes de l'entreprise jusqu'au point de démarcation.</p> <p>S'assurer que les politiques, procédures, processus d'affaires et solutions technologiques qu'emploie le fournisseur de services satisfont aux exigences de l'entreprise.</p>

Enjeux et risques	Mesures d'atténuation possibles
<p>Les sociétés n'ont plus besoin de posséder les applications ni les logiciels de base, ni d'obtenir des permis d'utilisation; elles peuvent maintenant louer les logiciels-services (SaaS) sur Internet en fonction de leurs besoins.</p> <p>Les logiciels loués pourraient être insuffisants pour répondre aux besoins de l'entreprise en matière de fonctionnalité, de sécurité ou de performance.</p> <p>Il se peut que le fournisseur de services infonuagiques refuse de modifier un logiciel pour répondre aux besoins particuliers d'un ou deux clients.</p>	<p>Définir les exigences d'affaires principales à satisfaire et y faire référence pour déterminer si les fournisseurs potentiels de services infonuagiques conviennent.</p> <p>Remanier les processus d'affaires pour les rendre conformes au modèle SaaS dans la mesure du possible afin de réduire les coûts et la personnalisation.</p> <p>Dans le cas de processus d'affaires ou d'exigences techniques exclusifs, vérifier si le fournisseur de services infonuagiques peut combler à coût abordable un besoin d'affaires particulier ou s'il peut remanier ses offres de services (processus et technologie) de façon à répondre effectivement aux besoins d'affaires.</p> <p>Envisager de modifier les processus d'affaires internes et la technologie pour créer une interface plus efficace avec le fournisseur de services infonuagiques.</p> <p>Déterminer de quelle façon des ponts temporaires (APS) pourraient être développés et entretenus au fil du temps.</p> <p>Évaluer les risques liés au maintien d'exigences de service non standards, particulièrement en cas de changement ou de mise à niveau technologique par le fournisseur de services infonuagiques.</p>
<p>L'entreprise qui « achète un service » n'est peut-être pas pleinement consciente des risques potentiels.</p>	<p>Inclure les risques commerciaux et technologiques dans l'évaluation du recours à un service fondé sur la technologie ou qui en dépend.</p> <p>S'assurer que l'entreprise a le droit d'auditer les projets et activités du fournisseur de services en matière de sécurité.</p> <p>Exiger par contrat du fournisseur de services infonuagiques qu'il présente un rapport d'audit produit par un tiers sur les contrôles relatifs aux risques financiers, d'exploitation et/ou réglementaires.</p> <p>Exiger par contrat du fournisseur de services infonuagiques qu'il divulgue les brèches de sécurité en temps opportun.</p>
<p>Il se peut que l'entreprise ne soit pas au courant des plans de continuité de l'exploitation et de reprise après sinistre du fournisseur de services infonuagiques.</p> <p>Il se peut que les plans de continuité de l'exploitation et de reprise après sinistre du fournisseur de services infonuagiques ne permettent pas de reprendre ou de restaurer le service selon les besoins de l'entreprise.</p>	<p>Effectuer un contrôle préalable rigoureux et prévoir des dispositions contractuelles de service et de reprise.</p> <p>Surveiller les niveaux de service et de conformité grâce aux rapports du fournisseur de services infonuagiques et/ou aux dispositions d'audit dans le contrat.</p> <p>Communiquer une fois par année les besoins et attentes de l'entreprise et modifier le contrat au besoin.</p>

Enjeux et risques	Mesures d'atténuation possibles
<p>Il se peut que le fournisseur de services infonuagiques dépende de tierces parties, comme des fournisseurs de télécommunications, et n'ait pas accès à leurs renseignements en matière de continuité de l'exploitation ou de reprise après sinistre.</p>	<p>S'assurer que le fournisseur de services infonuagiques peut effectivement évaluer la répartition ou le recours à des tierces parties.</p>
<p>Difficulté à extraire les données et les fichiers si l'entreprise annule les services du fournisseur de services infonuagiques.</p> <p>Difficulté pour l'entreprise de s'assurer que le fournisseur de services infonuagiques a supprimé tous ses fichiers et renseignements si elle annule les services du fournisseur de services infonuagiques.</p>	<p>Définir et documenter une stratégie de sortie dans le cadre de l'analyse de rentabilité du déplacement des données, du traitement ou du soutien vers un service infonuagique.</p> <p>Définir les exigences contractuelles garantissant le bon fonctionnement de la stratégie de sortie.</p> <p>Veiller à négocier les exigences de la stratégie de sortie dans le contrat et veiller à ce que le fournisseur de services infonuagiques continue de respecter ces exigences.</p>
<p>Le recours à un fournisseur de services infonuagiques peut créer une relation « exclusive » avec ce fournisseur, car il pourrait être difficile ou coûteux de l'abandonner.</p>	<p>Dans le cadre de l'analyse de rentabilité du transfert des données, du traitement ou du soutien vers un service infonuagique, définir et documenter les exigences technologiques minimales, et éviter la technologie ou les logiciels propres au fournisseur, sauf s'ils sont facilement accessibles auprès d'autres sources.</p> <p>Définir et négocier les exigences garantissant que le fournisseur de services infonuagiques est contractuellement obligé de maintenir des versions à jour de la technologie et des logiciels, et d'assurer le soutien des versions antérieures.</p> <p>Documenter une stratégie de sortie et déterminer si les offres du fournisseur de services infonuagiques satisfont aux exigences de la stratégie de sortie.</p>
<p>Les incidents ne font pas l'objet d'identification, de recours hiérarchique, de correction ni de signalement.</p>	<p>Avant de signer un contrat, évaluer les procédures de surveillance du fournisseur de services infonuagiques et la façon dont il identifie et traite les incidents, particulièrement les incidents touchant la sécurité, la protection des renseignements personnels, la disponibilité et la continuité.</p> <p>S'assurer que le fournisseur de services infonuagiques dispose d'un personnel qualifié en nombre suffisant pour traiter les incidents.</p> <p>Négocier contractuellement les critères de signalement des incidents et surveiller la performance du fournisseur de services infonuagiques en matière de traitement des incidents, d'identification de leurs causes et de mise en œuvre des solutions.</p>

Enjeux et risques	Mesures d'atténuation possibles
<p>Le fournisseur de services infonuagiques ne fournit pas de renseignements sur la sécurité et la protection des renseignements personnels.</p>	<p>Stipuler au contrat que le fournisseur de services infonuagiques doit fournir un rapport de type 2 conforme à la norme SSAE 16 (NCCM 3416) comprenant une liste des contrôles et une évaluation de leur efficacité opérationnelle.</p>

Les tableaux correspondant à chacune des tendances technologiques sont conçus pour éveiller l'intérêt et faire connaître certains des avantages, des risques, des enjeux ainsi que des stratégies et techniques d'atténuation des risques, mais ils ne visent pas à présenter une liste exhaustive des enjeux, des risques ou des solutions. Le lecteur est prié de faire appel à des professionnels pour l'aider à gérer ces technologies.

2012 © L'Institut Canadien des Comptables Agréés