



CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

AVANTAGES ET RISQUES LIÉS À L'ADOPTION DES SERVICES FONDÉS SUR L'INFONUAGIQUE PAR VOTRE ORGANISATION

MARS 2020

ITSE.50.060

Ce document présente les avantages et les risques liés à l'utilisation de services fondés sur l'infonuagique qui fournissent des capacités de traitement informatique en tant que service plutôt que produit. Les fournisseurs de services infonuagiques (FSI) proposent des environnements informatiques évolutifs sur demande. Dans l'ensemble, les services fondés sur l'infonuagique offrent une plus grande souplesse que les solutions de TI locales, de même qu'un ensemble de capacités qui permettront de libérer les ressources de votre organisation. Par contre, de tels services ne protègent pas nécessairement les actifs qui sont stockés par leur intermédiaire. Il incombe toujours aux hauts responsables de protéger la confidentialité, l'intégrité et la disponibilité de l'information et des services de TI. Votre organisation sera appelée à établir toutes les exigences opérationnelles et de sécurité, et à gérer tous les risques connexes.



MODÈLES DE SERVICE INFONUAGIQUE

Logiciel en tant que service (SaaS pour *Software as a Service*) :

Votre organisation achète le droit d'utiliser les applications hébergées par le FSI, avec peu ou aucune visibilité de l'infrastructure sous-jacente;

Plateforme en tant que service (PaaS pour *Platform as a Service*) :

Votre organisation crée et exécute des applications personnalisées, tandis que le FSI offre les installations nécessaires pour concevoir, fournir et prendre en charge les applications et services;

Infrastructure en tant que service (IaaS pour *Infrastructure as a Service*) :

Vous pouvez accéder aux ressources informatiques de base (p. ex. les serveurs, le stockage de données, l'équipement de réseautage) et utiliser l'équipement du FSI pour déployer et exécuter les logiciels dont votre organisation a besoin.

AVANTAGES DE L'INFONUAGIQUE

Les services fondés sur l'infonuagique offrent un ensemble de capacités qui permettront de libérer les ressources de votre organisation. Selon le niveau de service sélectionné, le FSI est responsable des besoins en matériel, de la main-d'œuvre interne et des coûts de maintenance. Voici les avantages les plus couramment constatés :

- Les services offrent l'extensibilité nécessaire pour s'adapter automatiquement et rapidement à la demande de votre organisation;
- Les services sont offerts par abonnement; les frais que vous payez sont dictés par l'utilisation dont vous en faites;
- Les services de TI sont déployés sans que vous ayez à consacrer beaucoup d'efforts et de temps aux processus d'approvisionnement, de développement et de mise en œuvre internes;
- Votre organisation consacre moins de son budget de TI au développement et à la maintenance de logiciels et des infrastructures;
- Il est possible de réduire les coûts (p. ex., entretien, électricité, climatisation et licences) et de récupérer de l'espace précieux en faisant appel à des serveurs hors site;
- Les FSI sont responsables de la sécurité du nuage.

RISQUES

Dès le moment où elle fait appel à un service infonuagique, votre organisation cède tout contrôle direct sur plusieurs aspects de la sécurité et de la protection de ses renseignements personnels. En dépit de ce manque de contrôle, il incombe toujours à votre organisation de protéger la confidentialité, l'intégrité et la disponibilité de l'information et des services de TI conformément aux exigences légales, réglementaires et opérationnelles. Bien que la mise en œuvre des mesures de protection de la sécurité puisse faciliter la transition vers le nuage, les hauts responsables de votre organisation demeurent responsables de la gestion des risques associés à de tels services. Avant d'utiliser des services infonuagiques, vous devriez tenir compte des facteurs suivants :

- les manquements réels ou potentiels aux exigences imposées par les lois et les règlements (p. ex., la *Loi sur la protection des renseignements personnels*, la *Loi sur la protection des renseignements personnels et les documents électroniques* et l'*Orientation relative à la résidence des données électroniques* du Canada, et le *Règlement général sur la protection des données* de l'Union européenne);
- l'impact sur les ressources associées au déplacement, à la consolidation ou à la normalisation des services de TI locaux de votre organisation suivant l'adoption de services fondés sur l'infonuagique;
- la perte de contrôle direct et de visibilité des composants du nuage;
- le personnel de sécurité de votre organisation n'est pas familier avec les déploiements en nuage;
- les rôles et responsabilités pourraient être source de confusion au moment d'intervenir lors d'incidents s'ils ne sont pas clairement définis;
- l'organisation court le risque d'être contrainte à utiliser un service infonuagique en particulier en raison d'obligations financières ou de son incapacité à passer à un autre fournisseur de service.



Votre organisation est responsable de la sécurité et de la maintenance des actifs DANS le nuage.

SÉRIE HAUT DIRIGEANTS

© Gouvernement du Canada

Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

PROGRAMME D'ÉVALUATION DE LA SÉCURITÉ DES TI DU FSI

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) a mis en place un programme d'évaluation de la sécurité des TI dans le cadre duquel il évalue les processus et les contrôles de sécurité des FSI par rapport à un ensemble minimal d'exigences recommandées. Il importe de souligner que bien que le CCC examine les processus et contrôles actuellement employés par les FSI, il incombe à votre organisation d'établir ses exigences en matière de sécurité et de s'assurer que le FSI à qui il fait appel est en mesure de s'y conformer. Vous pouvez utiliser les résultats de cet examen (p. ex., les rapports sommaires) pour vous aider à prendre votre décision.

Pour de plus amples renseignements sur le programme d'évaluation de la sécurité des TI à l'intention des FSI, prière de se reporter à l'ITSM.50.100, *Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques*.



CONSEILS SUR LA MISE EN ŒUVRE DE SERVICES INFONUAGIQUES

Les organisations doivent adopter une approche structurée en matière de gestion des risques. Celle-ci devrait tenir compte de l'utilisation des services infonuagiques dans la réalisation des objectifs et des livrables de votre organisation.

Avant de s'engager, votre organisation devrait tenir compte des conseils suivants :

- Évaluez tout ce qui a été investi dans les logiciels jusqu'à présent, les coûts associés à l'exploitation des services locaux (p. ex., les centres de données, le matériel, les réseaux, les ressources) et la valeur qu'il serait possible d'ajouter par l'intermédiaire des nouvelles fonctions et fonctionnalités offertes par les services infonuagiques;
- Déterminez la valeur et le niveau de sensibilité de votre information; cet exercice vous permettra d'identifier l'information à stocker dans le nuage (p. ex. celle dont le niveau de sensibilité est faible) et d'assurer une protection adéquate des renseignements commerciaux et personnels sensibles;
- Examinez les efforts qui ont été déployés sur le plan de la sécurité, comme les rapports sommaires à l'intention des FSI pour en apprendre plus sur les contrôles et processus de sécurité d'un FSI en particulier;
- Demandez au FSI de fournir les certificats de sécurité et les attestations délivrés par les vérificateurs tiers de manière à avoir la preuve que le fournisseur a la posture de sécurité nécessaire pour se conformer aux exigences de votre organisation;
- Mettez en place des accords sur les niveaux de service afin de définir les rôles et les responsabilités, de documenter les exigences relatives au rendement du FSI et d'établir des sanctions pécuniaires en cas de sous-rendement;
- Passez en revue et gérez les contrôles de sécurité qui protègent les actifs qui sont stockés par l'intermédiaire d'un service infonuagique, notamment les passerelles des applications Web, les groupes de sécurité réseau et les contrôles de sécurité de base.



FACTEURS À CONSIDÉRER EN MATIÈRE DE RÉSIDENCE DES DONNÉES

On entend, par résidence des données, l'emplacement géographique où sont stockées les données. Votre organisation peut préciser un emplacement en fonction de ses exigences réglementaires et politiques.

La résidence des données est particulièrement importante pour ce qui est des renseignements personnels. Les exigences en matière de protection des renseignements personnels peuvent varier d'un pays à l'autre. Il incombe à votre organisation de veiller à ce que le FSI se conforme aux exigences liées à la résidence des données.

Si votre organisation relève d'un ministère ou organisme du gouvernement du Canada (GC), vous êtes tenu de vous conformer aux directives du Secrétariat du Conseil du Trésor du Canada et de stocker les données sensibles du GC dans les limites géographiques du Canada. En ce qui concerne les organisations non gouvernementales, on leur recommande de veiller à ce que toutes les données sensibles soient stockées au Canada, y compris l'information relative aux comptes et à la sécurité.

RESSOURCES SUPPLÉMENTAIRES

Vous trouverez plusieurs publications sur la sécurité infonuagique sur le site Web du CCC, notamment les suivantes :

- ITSM.50.062, *Gestion des risques liés à la sécurité infonuagique*;
- ITSM.50.100, *Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques*;
- ITSAP.50.110, *Qu'est-ce que l'infonuagique?*;
- ITSAP.50.111, *Modèles de l'infonuagique*;
- ITSAP.50.112, *Étapes pour gérer les fuites de données dans le nuage*.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à cyber.gc.ca.

