Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Clauses contractuelles recommandées en matière de cybersécurité pour les services infonuagiques

Direction

TLP:CLEAR

Canada

Avant-propos

La présente publication intitulée *Clauses contractuelles recommandées en matière de cybersécurité pour les services infonuagiques (ITSM.50.104)* est un document NON CLASSIFIÉ, publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité).

Date d'entrée en vigueur

Le présent document entre en vigueur le *22 octobre 2024*.

Historique des révisions

Révision	Modifications	Date
1	Première version.	*22 Octobre 2024*

ISBN 978-0-660-73403-3
CAT D96-123/2024F-PDF

Vue d'ensemble

Étant donné que plus d'organisations adoptent des technologies et des services infonuagiques, il devient de plus en plus nécessaire de déterminer les clauses et les principes contractuels à l'appui pour veiller à ce que les attentes en matière de cybersécurité soient clairement comprises et documentées. Les clauses et les principes de cybersécurité sont des composantes de service importantes. Les deux doivent être combinés à des éléments contractuels fondamentaux, comme les accords sur les niveaux de service (ANS), les ordres de tâches et les normes de gouvernance.

Lorsqu'ils sont combinés, ces clauses et ces éléments contractuels fournissent un cadre de service pour s'assurer que votre organisation reçoit les services et les solutions auxquels vous vous attendez, et ils fournissent l'assurance nécessaire que les données et les identités sont sécurisées.

Cette publication décrit les domaines communs pour les marchés de services et d'approvisionnement infonuagiques du point de vue de la cybersécurité, tant pour le gouvernement que pour les autres organisations gouvernementales. Il faut tenir compte des recommandations fournies, de même que des principaux aspects fonctionnels et juridiques de l'approvisionnement de services, lorsque l'on travaille avec un fournisseur de services infonuagiques (FSI).

Table des matières

Liste des figures

1 Introduction

Les lignes directrices de la présente publication mettent en évidence d'importantes considérations en matière de sécurité pour votre organisation à mesure que vous précisez et passez en revue vos exigences contractuelles de services infonuagiques avec les FSI. Votre organisation devrait gérer les risques associés à l'approvisionnement et au recours aux services infonuagiques pour vos processus opérationnels essentiels. Il peut y avoir des lacunes dans les dispositions contractuelles si les composantes de cybersécurité d'un modèle d'approvisionnement de services infonuagiques sont gérées par des moyens traditionnels. Ces lacunes peuvent empêcher votre organisation de gérer les complexités associées aux services de cybersécurité modernes.

Bien que les FSI puissent présenter des conditions et des modalités de service fondamentales au départ, l'équipe de direction de votre organisation est responsable de démontrer et de vérifier que les modalités du contrat répondent aux besoins de sécurité opérationnelle de votre organisation. Les modalités doivent pouvoir s'adapter aux modifications futures afin de protéger les intérêts de votre organisation. Les modalités du contrat de service devraient également fournir à votre organisation les meilleurs résultats opérationnels possibles. Votre organisation doit prendre des mesures proactives pour veiller à ce que les dispositions de service comprennent des mécanismes de cybersécurité pour identifier, communiquer, atténuer et prévenir les risques.

Cette publication décrit les considérations communes en matière de cybersécurité pour l'évaluation des contrats de services infonuagiques et des risques en lien avec l'approvisionnement. Il est recommandé d'en tenir compte ainsi que des principaux aspects fonctionnels et juridiques de l'approvisionnement lorsque l'on travaille avec un FSI. Il faut également tenir compte de ces facteurs lorsque l'on fait appel à d'autres fournisseurs de services, comme un fournisseur de services gérés (FSG), un fournisseur de services de sécurité gérés (FSSG), un intégrateur des services (SI pour *Service Integrator*) ou un outil d'orchestration de services (SO pour *Service Orchestrator*).

Les clauses décrites dans la présente publication ne doivent pas être considérées comme des conseils juridiques. Elles fournissent plutôt un contexte pour votre organisation lorsque vous envisagez d'obtenir des services infonuagiques et qu'ils vous sont présentés par le fournisseur de services potentiel. Ces conseils peuvent aider votre organisation à savoir ce dont il faut tenir compte ou les questions à poser au moment de passer au nuage.

1.1 Portée

La présente publication fournit des conseils et des directives dans les domaines de l'approvisionnement de services infonuagiques. Dans tous les cas, l'application de ces directives peut incomber à la fois à votre organisation, en tant que consommateur, et au fournisseur de services. Les exemples énumérés ne sont pas une indication exhaustive des pratiques exemplaires, mais ils donnent un aperçu des clauses qui ont été utilisées avec succès par les partenaires du gouvernement et de l'industrie.

Avis de non-responsabilité : Le Centre de la sécurité des télécommunications et le Centre pour la cybersécurité ne recommandent ni n'approuvent l'utilisation d'aucune clause contractuelle particulière énumérée dans le présent document. Les renseignements fournis ne doivent être que des exemples de clauses contractuelles qui peuvent être utiles pour l'approvisionnement de services infonuagiques, et ils sont fournis à titre informatif seulement.

1.2 Documents d'orientation

Dans la préparation de ce document d'orientation, nous avons tenu compte des commentaires de divers documents de référence et cadres.

1.2.1 Ressources gouvernementales

La liste suivante présente des références aux politiques et aux documents d'orientation connexes qui ont été pris en compte dans l'élaboration de la présente publication :

- La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) [1]
- Lignes directrices sur la chaîne d'approvisionnement des technologies (TSCG-01) [2]
- Manuel de la sécurité des contrats de SPAC [3]
- FedRAMP Control – Specific Contract Clauses version 3.0 (en anglais seulement) [4]
- NIST SP 800-171 - Enhanced Security Requirements for Protecting Controlled Unclassified Information (en anglais seulement) [5]
- NIST SP 800-172- Enhanced Security Requirements for Protecting Controlled Unclassified Information: Supplementary (en anglais seulement) [6]

1.2.2 Ressources de l'industrie

De plus, nous avons tenu compte des normes et des cadres de l'industrie suivants :

- ISO 27001:2022 – Systèmes de management de la sécurité de l'information [7]
- ISO 27017:2015 – Code de bonnes pratiques pour les contrôles de sécurité de l'information [8]
- ISO 27018:2019 – Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII [9]
- Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing (en anglais seulement) [10]

1.2.3 Nomenclature recommandée

Toutes les ressources indiquées ci-dessus fournissent divers niveaux de détail et la nomenclature technique en ce qui a trait aux services infonuagiques. Du point de vue strictement contractuel, il y a des modalités qui vous aideront à obtenir des services infonuagiques en fonction d'un « moment précis » ou d'un « besoin futur ». La section 2.1 énumère les diverses formes d'intention dont votre organisation devra tenir compte en fonction des services infonuagiques requis. Dans certains cas, votre organisation devra peut-être savoir que certains services infonuagiques peuvent avoir besoin de temps pour être restructurés ou peuvent avoir des fonctions mises à jour dans une feuille de route. Votre organisation devrait tenir compte de vos besoins immédiats et de ceux qui peuvent être développés par étapes ou plus tard.

Votre organisation devrait établir les exigences obligatoires et cotées dont elle a besoin. Les exigences obligatoires sont celles que le fournisseur « doit » avoir ou « doit » fournir. Lorsque vous examinez les exigences cotées, votre organisation peut dire qu'elle « devrait » s'approvisionner, « peut » s'approvisionner ou « envisage » de s'approvisionner. Ces zones indiqueraient également que le fournisseur a déjà ces éléments en place. Dans les cas où les services sont sur une feuille de route ou ne sont pas encore en place, votre organisation devra chercher à utiliser des termes comme « volonté » ou « capable de réaliser » pour indiquer les attentes futures.

2 Considérations générales en matière de cybersécurité

Afin d'établir les attentes en matière de sécurité dans les contrats de services infonuagiques d'entreprise, le modèle de service sélectionné influence le choix des services de sécurité disponibles. De plus, comprendre le modèle de responsabilité partagée peut fournir des précisions et des renseignements sur les options de contrôle de sécurité accessibles aux organismes clients. Par exemple, la gestion des mécanismes de contrôle d'accès dépend du client pour mettre en œuvre et déployer les fonctions de contrôle du système, tout comme elle dépend du FSI pour fournir l'infrastructure de soutien sous-jacente. Ces interactions sont établies dans les domaines de la sécurité logique; de la sécurité matérielle et physique; de la sécurité du personnel et de la sécurité des technologies de l'information (TI). Ces zones sont ensuite définies à l'aide d'un libellé contractuel précis accompagné de références à un profil ou à une superposition de contrôles de sécurité requis. Habituellement, les références à l'ITSG-33 [1], NIST 800-53, Security and Privacy Controls for Information Systems and Organizations [10], et à d'autres variantes, fournissent des catalogues de contrôle de sécurité et des références ou des suggestions pour des « profils de sécurité » précis. L'objectif est de réduire la probabilité d'événements à risque et de réduire l'incertitude au moyen d'exigences bien définies dans la gestion globale du contrat.

2.1 Principales considérations

Votre organisation devrait se concentrer sur plusieurs aspects principaux lorsqu'elle examine des modèles de services infonuagiques. Chaque domaine est incorporé dans une clause contractuelle spécifique. Toutefois, elles sont présentées ici comme un point à examiner lorsque l'on regarde la façon de catégoriser et de déterminer les types de services infonuagiques requis. Les premiers domaines à considérer sont les suivants :

- évaluation
- gestion des incidents
- gestion des clés
- protection des points terminaux
- gestion à distance
- gestion des accès privilégiés
- assurance cryptographique
- protection des données
- gestion de l'identité et de l'accès
- développement sécurisé
- tests de sécurité et validation
- sécurité des réseaux et des communications
- fédération
- fuite de renseignements
- enregistrement et vérification
- surveillance continue
- souveraineté des données
- résidence des données

Pour de plus amples renseignements sur la catégorisation et la classification des modèles de service, nous recommandons de consulter le Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.103) [11] du Centre pour la cybersécurité.

2.1.1 Sécurité et protection des données

La sécurité des données représente une attente de service de base dans le modèle de services infonuagiques. Pour assurer l'efficacité maximale des contrôles de sécurité des données, votre organisation devrait mettre en œuvre une approche de service à plusieurs niveaux. Les contrats de service doivent définir les responsabilités des FSI en ce qui concerne vos données et leurs limites en ce qui a trait aux droits de propriété intellectuelle sur les données organisationnelles, les données inférées ou les données construites de votre organisation. Les ententes contractuelles doivent faire la distinction entre les données inactives, les données en transit, le traitement et le stockage. Les exigences en matière de sécurité relatives aux protections de chiffrement, aux dépôts géographiques approuvés, aux limites des flux de transit et aux mesures de contrôle d'accès devraient être documentées. Les mesures d'atténuation mises en œuvre pour réduire ou éliminer les risques associés aux processus de récupération et de destruction des données devraient également être documentées. Vous devriez passer en revue les politiques en matière de résidence des données et les choix de service en ce qui a trait à l'environnement réglementaire particulier de vos activités. Il est possible que certains services et centres de données ne puissent pas résider au Canada, ce qui peut avoir une incidence sur la capacité de votre organisation à protéger les données conformément aux exigences législatives ou réglementaires.

Les risques associés aux technologies émergentes sont également une préoccupation croissante. Vous devriez envisager de limiter l'impact de ces technologies, comme l'intelligence artificielle (IA), l'apprentissage machine (AM) et l'informatique quantique sur vos données. Vous devez traiter les risques au moyen de clauses contractuelles proactives qui exigent des procédures, des exclusions ou des restrictions particulières à suivre lorsque vous utilisez vos données.

Exemple de structure et de libellé de clause

L'entrepreneure ou entrepreneur doit :

- mettre en œuvre le chiffrement des données inactives pour les services infonuagiques hébergeant les données de l'organisation lorsque le chiffrement des données inactives demeure en vigueur, ininterrompu et actif en tout temps, même en cas de défaillance de l'équipement ou de la technologie conformément à la protection cryptographique que le Centre pour la cybersécurité recommande dans le document Guide sur le chiffrement des services infonuagiques (ITSP.50.106) [12];
- transmettre les données de l'organisation de manière sécuritaire, en lui permettant de mettre en œuvre le chiffrement des données en transit pour toutes les transmissions de ses données, conformément à la protection cryptographique et à la sécurité des réseaux et des communications, comme recommandé par le Centre pour la cybersécurité;
- prendre les mesures appropriées pour s'assurer que son personnel n'a pas de droit permanent ou continu d'accès aux données de l'organisation, et que l'accès est limité au personnel du FSI ayant un besoin de connaître, y compris les ressources qui fournissent un soutien technique ou à la clientèle, en fonction de l'approbation appropriée;

- signaler à l'organisation cliente les violations intentionnelles ou accidentelles de la protection des données et des mécanismes cryptographiques, en fournissant de la documentation et des preuves sur les mesures prévues ou prises pour remédier à la situation;
- soutenir l'agilité cryptographique de manière à ce que la protection des données en transit ou inactives puisse rester à jour par rapport aux recommandations de protection cryptographique du CST et du Centre pour la cybersécurité, y compris l'utilisation de nouvelles normes pour atténuer la menace de l'informatique quantique. Pour obtenir de plus amples renseignements, consultez le document Conseils sur la mise en œuvre de l'agilité cryptographique (ITSAP.40.018) [13].

Références

- Mesures de protection du nuage du GC – Protection des données inactives [14]
- Mesures de protection du nuage du GC – Protection des données en transit [15]

2.1.2 Résidence et souveraineté des données

Les clauses contractuelles précisant la souveraineté des données et les exigences en matière de résidence devraient être documentées pour toutes les formes de services de données et de services infonuagiques dans les environnements réglementaires requis. Les contrats devraient obliger le FSI à informer le client lorsque les données organisationnelles sont transférées dans une région non approuvée. Les sorties de données des plateformes infonuagiques sont souvent conçues pour être coûteuses, alors qu'il existe des mesures incitatives pour faciliter les entrées de données vers la plateforme d'un FSI. Il faut éviter les modèles contractuels qui exposent votre organisation à des risques immobilisés et les ententes de conception qui garantissent l'accès aux données de votre organisation dans le cadre d'une structure de coûts raisonnable.

L'entrepreneure ou entrepreneur doit stocker et protéger les données de votre organisation, inactives, y compris les données sauvegardées ou conservées à des fins de redondance. Cela comprend la capacité d'isoler des données au Canada dans des centres de données approuvés. Un centre de données approuvé doit :

- satisfaire aux exigences de sécurité et aux certifications particulières définies par les exigences réglementaires de votre organisation;
- s'assurer que les données d'un client en particulier ne se trouvent pas sur un support physique;
- utiliser le chiffrement pour s'assurer qu'aucune donnée n'est inscrite sur le disque sous une forme non chiffrée, conformément à la protection cryptographique recommandée par le Centre pour la cybersécurité.

Exemple de structure et de libellé de clause

L'entrepreneure ou entrepreneur doit :

- prendre les mesures appropriées pour empêcher la transmission de données organisationnelles à l'extérieur des régions géographiques et de service convenues, sauf lorsque l'approbation de l'organisation est reçue;
- fournir la capacité et les outils nécessaires pour extraire toute l'information, y compris les configurations du système, les journaux d'activités et l'information sur le stockage des objets et des fichiers, afin que l'organisation puisse valider l'emplacement et l'enregistrement d'activité pour ses données.

Références

- Mesures de protection du nuage du GC – Emplacement des données [16]
- Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.105) [17]

2.1.3 Intégrité de la chaîne d'approvisionnement (ICA)

Les risques liés à la chaîne d'approvisionnement se rapportent aux activités des auteures et auteurs de menaces visant à exploiter les vulnérabilités de la chaîne d'approvisionnement dans le but de compromettre l'intégrité d'une ou de plusieurs composantes du système pour atteindre leurs objectifs généraux. Pour que les organisations puissent se protéger contre de telles menaces, les ententes contractuelles doivent tenir compte de la sécurité de la chaîne d'approvisionnement, dans la mesure des capacités de l'organisation, notamment les menaces provenant des points de fabrication, de transport, d'intégration et d'exploitation. Dans le cadre du processus d'approvisionnement en services infonuagiques, votre organisation doit effectuer des évaluations des risques liés à la chaîne d'approvisionnement et demander aux FSI de fournir des renseignements sur leurs plans de gestion des risques liés à celle-ci, les renseignements sur la propriété, les relations avec les filiales et les relations avec les tiers. En cas de préoccupation au sujet de la divulgation de ces renseignements ou d'une indication quant aux fournisseurs du FSI, il est recommandé de tenir des discussions sur l'assurance par un tiers par l'entremise d'une entité mutuellement convenue. Votre organisation peut également envisager d'utiliser la méthodologie harmonisée de l'évaluation des menaces et des risques [18] du Centre pour la cybersécurité ou l'outil ASTRA (logiciel d'analyse aux fins d'évaluation de la menace) pour effectuer des évaluations des menaces et des risques (EMR) et évaluer les risques associés à ses projets.

Exemple de structure et de libellé de clause

L'entrepreneure ou entrepreneur doit accepter ce qui suit :

- fournir les renseignements nécessaires pour que le client puisse effectuer une évaluation de la sécurité de la chaîne d'approvisionnement, y compris des renseignements sur la structure de propriété, l'enregistrement de la société, les investisseurs et les cadres supérieurs, les fournisseurs, les sous-traitants, les sous-traitants, les tiers-les relations entre les parties et toute autre information requise pour cette évaluation;
- soutenir l'évaluation de la sécurité de la chaîne d'approvisionnement en fournissant des renseignements sur l'équipement, les micrologiciels, les logiciels ou tout autre système, au besoin;
- maintenir un plan de gestion des risques de la chaîne d'approvisionnement qui décrit l'approche du FSI en ce qui a trait à la gestion des risques liés à la chaîne d'approvisionnement (GRCA) et démontre la manière dont l'approche de l'entrepreneur réduira et atténuera les risques liés à la chaîne d'approvisionnement;
- mettre en œuvre et maintenir des mesures de protection pour atténuer les menaces et les vulnérabilités de la chaîne d'approvisionnement des services de TI afin de maintenir la confiance dans la sécurité des sources des systèmes d'information et des composants de TI utilisés pour fournir les services.

Références

- La cybersécurité et la chaîne d'approvisionnement : évaluation des risques (ITSAP.10.070) [19]
- Menaces à la chaîne d'approvisionnement et espionnage industriel [20]
- Clauses contractuelles visant l'équipement et les services de télécommunications (TSCG-01L) [21]

- ISO/IEC 27036 – Cybersécurité — Relations avec le fournisseur (parties 1 à 4) [22]

2.1.4 Gestion de l'identité et de l'accès, accès privilégié et fédération

Les modèles infonuagiques de gestion de l'identité et de l'accès exposent des défis de sécurité uniques en raison de leur structure de services à responsabilité partagée. La façon dont les comptes d'utilisateur, les services de système et les entités sont identifiés, authentifiés ainsi que la façon dont leurs droits d'autorisation sont gérés peuvent nécessiter la coordination de plusieurs partenaires (client, FSI et fournisseur d'identité). Les clauses contractuelles utilisées pour gérer les services doivent définir clairement les responsabilités en matière de gestion des comptes pour toutes les parties. Les contrats de maintenance doivent documenter les mesures d'atténuation visant les utilisatrices ou utilisateurs, ou les systèmes non privilégiés ou non autorisés. La fédération des identités et des authentifiants devrait être limitée aux cadres de confiance convenus. L'accès non autorisé de tiers (utilisatrice/utilisateur ou système) aux données ou à l'instance infonuagique de votre organisation doit être restreint. Les ententes de service devraient rendre obligatoire la consignation des accès, et les périodes de conservation devraient être suffisantes pour faciliter les activités de vérification et d'intervention en cas d'incident. Les contrats de service doivent tenir compte des obligations du FSI en ce qui concerne les portes dissimulées des applications ou l'accès non autorisé par système (interfaces de programmation d'applications ou API).

Exemple de structure et de libellé de clause

Gestion de l'identité et de l'accès

L'entrepreneure ou entrepreneur doit fournir à votre organisation la capacité de soutenir l'accès sécurisé aux services infonuagiques, notamment :

- l'authentification multifacteur (AMF) résistante à l'hameçonnage, conformément au Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031) [23] à l'aide de justificatifs d'identité approuvés par le GC;
- l'accès basé sur les rôles et les comportements;
- les contrôles d'accès aux objets stockés;
- les politiques d'autorisation détaillées pour autoriser ou limiter l'accès.

L'entrepreneure ou entrepreneur doit avoir la capacité d'établir des valeurs par défaut à l'échelle de l'organisation pour gérer les politiques à l'échelle des locataires.

Gestion des accès privilégiés

L'entrepreneure ou entrepreneur doit utiliser des dispositifs d'extrémité sécurisés et fiables pour exécuter ses fonctions d'administration du système, comme un poste de travail à privilèges d'administrateur spécialisé conçu avec des configurations restreintes, des fonctionnalités du système et des contrôles de sécurité.

Fédération

L'entrepreneure ou entrepreneur doit veiller à ce que la fédération des mécanismes d'authentification, y compris l'identité de l'entreprise et les informations relatives aux attributs, soit protégée conformément à la norme NIST Digital Identity Standard

NIST SP 800-63-4 Digital Identity Guidelines : Federation and Assertions [25] ou à l'ITSP.30.031 [23] du Centre pour la cybersécurité.

Références

- Les 10 mesures de sécurité des TI : no 3 Gestion et contrôle des privilèges d'administrateur (ITSM.10.094) [24]
- Digital Identity Guidelines – NIST Special Publication 800-63-4 (en anglais seulement) [25]

2.1.5 Gestion et intervention en cas d'incident

Les clauses contractuelles qui gèrent les activités d'intervention en cas d'incident doivent mettre en œuvre une approche fondée sur les risques. Ces clauses doivent tenir compte des interruptions de service potentielles et des cibles de reprise de service prévues, surtout en raison de leur incidence sur la réglementation de l'industrie et les exigences en matière de reddition de compte. Votre organisation devrait envisager des clauses rendant obligatoire la divulgation de renseignements sur les incidents afin d'aider à évaluer l'incidence, la gravité et l'importance d'un incident qui peut nécessiter une notification et une surveillance réglementaires. Voici quelques exemples de ces types de clauses :

- avis lorsqu'un service est touché;
- divulgation de toute vulnérabilité connue et des correctifs connexes;
- fourniture d'information de journaux à une équipe de COS des entités aux fins d'ingestion.

Les caractéristiques supplémentaires ou la divulgation de renseignements précis sur le service entrent en ligne de compte pour les besoins et les capacités de votre organisation en matière de sécurité et de surveillance.

Les entités réglementées, ainsi que les organisations d'infrastructures essentielles qui offrent des services à l'appui de services nationaux essentiels ayant une incidence sur la sécurité nationale ou la sécurité publique peuvent nécessiter une surveillance supplémentaire. Une interruption de service peut entraîner des répercussions plus vastes sur la sécurité nationale et la sécurité humaine. D'un autre côté, des capacités d'intervention efficaces exigent une coordination entre de nombreuses entités internes et externes. Vos ententes contractuelles doivent définir clairement les responsabilités de tous les intervenants.

Exemple de structure et de libellé de clause

L'entrepreneure ou entrepreneur doit :

- Établir et maintenir une capacité de COS qui fonctionne selon l'heure de fonctionnement et le modèle de service définis de votre organisation, comme la couverture de service en tout temps.
- Établir et maintenir une équipe d'intervention en cas d'incident cybernétique qui peut être déployée par le FSI dans les limites des objectifs de service attendus de votre organisation.

Références

- Gérer les risques liés aux données du gouvernement du Canada dans le contexte des services infonuagiques (ITSM.50.109) [26]
- Guide sur la défense en profondeur pour les services fondés sur l'infonuagique (ITSP.50.104) [27]

2.1.6 Gestion des clés et de l'assurance cryptographique

L'accès au matériel et aux clés cryptographiques sensibles devrait être restreint. Les secrets comme les clés cryptographiques, les authentifiants de base de données, les API et les certificats représentent des composants sensibles qui nécessitent une surveillance approfondie. Le cycle de vie de ces composants et la façon dont ils sont gérés et déployés devraient être consignés dans les contrats de service. Les processus cryptographiques devraient utiliser les algorithmes cryptographiques les plus récents validés conformément à la norme FIPS ou approuvés par le Centre pour la cybersécurité. La sécurité des clés maîtresse du FSI a également une incidence sur la sécurité des clés propres à l'organisation liées à vos services.

Exemple de structure et de libellé de clause

L'entrepreneure ou entrepreneur doit :

- veiller à ce que les opérations cryptographiques et la protection des paramètres de sécurité essentiels (p. ex. clés cryptographiques) soient effectuées dans des modules cryptographiques certifiés par le Programme de validation des modules cryptographiques (PVMC); le module cryptographique devrait être configuré et utilisé dans un mode approuvé conformément à la politique de sécurité publiée par le PVMC;
- veiller à ce que la clé maîtresse ou les clés racines du FSI utilisées pour obtenir d'autres clés soient générées et gérées au moyen de processus sécurisés et approuvés et validés selon la norme FIPS 140 pour la génération, la distribution, le stockage et la gestion du cycle de vie des clés.

Références

- Guide sur le chiffrement des services infonuagiques (ITSP.50.106) [28]
- Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111) [29]

2.1.7 Sécurité des dispositifs de point d'extrémité et des supports

La résilience de l'infrastructure infonuagique dépend de la fiabilité des composants des appareils et des services logiciels connexes. Dans la mesure du possible, les contrats de service doivent tenir compte de la résilience des composants des appareils qui soutiennent les fonctions de service essentielles. Les ententes de service doivent tenir compte de la fiabilité, de la résilience, du rendement et des objectifs opérationnels des composants matériels et logiciels. Les ententes devraient traiter des restrictions d'accès aux supports amovibles, des procédures de destruction, du transport des supports et des limites de distribution.

Exemple de structure et de libellé de clause

L'entrepreneure ou entrepreneur doit :

- mettre en œuvre, gérer et surveiller des points d'extrémité renforcés par la sécurité avec des protections actives basées sur l'hôte afin de prévenir les maliciels, les attaques et les mauvais usages, conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles qui se trouvent dans la publication NIST 800-123 Guide to General Server Security [30], les objectifs repères du Center for Internet Security (CIS) [31], ou une norme équivalente approuvée par écrit par l'organisation;

- effacer, purger, éliminer ou détruire de façon sécuritaire les ressources, comme l'équipement, le stockage de données, les fichiers et la mémoire ou les dispositifs, qui peuvent contenir les données de votre organisation et veiller à ce que les données précédemment stockées ne puissent pas être instanciées à nouveau à partir de systèmes ou de dispositifs;
- concevoir et mettre en œuvre des mesures opérationnelles pour veiller à ce que les systèmes de communication de logiciel, de matériel et de réseau soutiennent les services redondants et résilients afin de résister aux interruptions, aux pannes de matériel et aux cyberévénements destructeurs;
- veiller à ce que les supports numériques et non numériques qui contiennent des données organisationnelles soient protégés par des mécanismes cryptographiques afin de protéger la confidentialité et l'intégrité de ces renseignements.

Références

- Configurer les dispositifs pour assurer leur sécurité [32]
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030) [33]
- La cybersécurité à la maison et au bureau – Sécuriser vos dispositifs, vos ordinateurs et vos réseaux (ITSAP.00.007) [34]
- Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001) [35]
- Application des mises à jour sur les dispositifs (ITSAP.10.096) [36]

2.1.8 Sécurité des réseaux et des communications

Les systèmes de communication (sans fil ou câblé) élargissent la capacité des plateformes infonuagiques à traiter les données et à fournir des ressources informatiques et de réseau sur demande. À mesure que les données passent d'un point à l'autre, les chemins de réseau, les dispositifs réseau, le plan de contrôle et l'interconnectivité avec d'autres services nécessitent des protections contre les vulnérabilités et les cyberattaques. Les plateformes infonuagiques nécessitent des composants de réseau fiables, des voies de communication sécurisées et des modèles de gouvernance pour offrir des services fiables. Les organisations clientes doivent s'assurer que les exigences des systèmes de communication fiables sont incluses dans les ententes de service avec les FSI.

Exemple de structure et de libellé de clause

L'entrepreneure ou entrepreneur doit :

- fournir la capacité d'établir des connexions sécurisées à sa plateforme, y compris la protection de la confidentialité, de l'intégrité et de la disponibilité, comme l'utilisation du protocole Transport Layer Security (TLS) pour le chiffrement des données en transit et le soutien mutuel du protocole TLS pour vérifier l'identité des clients et des services;
- permettre à votre organisation de mettre en œuvre des connexions dédiées ou privées à ses centres de données et de prendre en charge les charges de travail sensibles qui peuvent nécessiter de telles connexions;

- fournir des outils et des capacités pour évaluer l'efficacité des contrôles de sécurité et assurer la visibilité de l'application des contrôles de sécurité dans l'ensemble du parcours de transmission des données au moyen de technologies comme les registres d'activités et les rapports;
- valider la posture de sécurité et cerner et authentifier de façon unique les demandes avant d'établir une connexion réseau avec les ressources en nuage ou les locataires de l'organisation cliente.

Références

- Zones de sécurité de réseau en nuage (ITSP.80.023) [37]
- Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062) [38]
- Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.105) [17]

2.1.9 Surveillance continue (*Continuous monitoring*)

La surveillance continue de l'état et de la sécurité du service infonuagique est essentielle. La gestion des journaux, la surveillance du trafic réseau et la surveillance des composantes de service des applications ne sont que quelques-unes des activités connexes. Les journaux d'activités, les journaux de système, les journaux de vérification et les journaux d'événements sont des exemples de composants essentiels nécessaires pour effectuer la surveillance et l'analyse afin d'évaluer et de valider dans le nuage. La surveillance des mesures de rendement devrait également faire partie des capacités de production de rapports périodiques.

Exemple de structure et de libellé de clause

L'entrepreneure ou entrepreneur doit :

- surveiller activement et continuellement les menaces et les vulnérabilités à l'infrastructure de service, aux applications et aux services infonuagiques et aux données de votre organisation;
- procéder régulièrement à des analyses de vulnérabilité et à des tests de pénétration de l'infrastructure de l'entrepreneure ou entrepreneur et de ses sites de service. Ceci dans le but d'identifier les lacunes et d'y remédier afin d'empêcher l'accès non autorisé à des informations sensibles, le contournement des contrôles d'accès et l'élévation des privilèges, ainsi que l'exploitation des vulnérabilités pour accéder à des systèmes ou à des informations;
- consigner et détecter les événements de vérification, comme (i) les tentatives de connexion réussies et infructueuses au compte; (ii) la gestion des comptes; (iii) l'accès aux objets et la modification des politiques; (iv) les fonctions de privilège et le suivi des processus; (v) les événements du système et (vi) la suppression des données;
- mettre en œuvre des mesures de protection pour prévenir les attaques d'épuisement des services au moyen de mesures de sécurité comme les mesures de protection contre le refus de service.

Références

- Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085) [39]
- Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030) [40]

2.1.10 Développement sécurisé, test et validation

La gestion du cycle de vie du développement des logiciels et des systèmes touche plusieurs composantes de services infonuagiques. Le contrat de service doit établir ou décrire la gestion sécurisée du cycle de vie des logiciels, y compris la gestion des vulnérabilités, le cycle de gestion des correctifs et la sécurité des logiciels libres.

Exemple de structure et de libellé de clause

L'entrepreneure ou entrepreneur doit :

- fournir des renseignements pertinents sur les vulnérabilités de sécurité connues liées aux systèmes détenus ou contrôlés qui pourraient nécessiter des mesures de votre organisation pour les résoudre ou les protéger contre de telles vulnérabilités;
- gérer et appliquer les correctifs et les mises à jour liés à la sécurité en temps opportun et de façon systématique afin d'atténuer les vulnérabilités et de corriger tout problème signalé publiquement dans les services infonuagiques ou les bibliothèques utilisées par les services infonuagiques, et fournir des préavis de correctifs conformément aux engagements de niveau de service convenus.

Références

- Les 10 mesures de sécurité des TI no.2 Appliquer les correctifs aux systèmes d'exploitation et aux applications (ITSM.10.096) [41]
- Appliquer automatiquement les correctifs aux systèmes d'exploitation et aux applications [42]

2.2 Facteurs complémentaires à considérer

Les facteurs complémentaires à considérer servent d'exigences de base de services infonuagiques supplémentaires et de principes de sécurité à l'appui.

2.2.1 Risques pour les renseignements personnels

Votre organisation pourrait avoir des inquiétudes quant aux répercussions potentielles sur les renseignements personnels et des risques liés aux atteintes à la protection des données organisationnelles dans le nuage. Vous devriez tenir compte des questions de protection des renseignements personnels et de l'incidence sur la sécurité des données de votre organisation. Pour déterminer les mesures de protection des renseignements personnels nécessaires, votre organisation devrait examiner les contrôles de gestion (politiques et procédures) et les contrôles techniques du fournisseur de services. Vous devriez également envisager une évaluation indépendante des mesures de protection des renseignements personnels et de leur efficacité. Les évaluations des facteurs relatifs aux renseignements personnels doivent être prises en compte tout au long du cycle de vie des services infonuagiques pour s'assurer que les risques connexes sont bien gérés.

2.2.2 Sécurité du personnel

Votre organisation devrait confirmer que les enquêtes de sécurité et les vérifications des antécédents criminels sont effectuées pour les employées et employés du FSI dans le cadre de votre engagement contractuel. Le FSI devrait fournir la preuve de l'existence de politiques de filtrage du personnel, de contrôles de sécurité et d'un régime de conformité. Les

détails des habilitations de sécurité du personnel doivent être clairement documentés, et des procédures doivent être mises en place pour gérer le transfert et la cessation d'emploi du personnel. Dans le cas d'une transition de poste, les changements apportés aux identifiants et aux authentifiants doivent être effectués en temps opportun. Des ententes de non-divulgation doivent être en place pour les employées et employés du FSI qui ont accès aux données opérationnelles de l'organisation.

2.2.3 Sécurité physique

En raison de la nature du modèle de services infonuagiques, les considérations relatives à la sécurité physique ne sont pas souvent priorisées dans les ententes de service. Les exigences de sécurité pour vos données organisationnelles demeurent les mêmes, peu importe où elles se trouvent (sur place ou dans le nuage). Les ententes contractuelles doivent tenir compte des exigences en matière de sécurité physique pour soutenir vos biens et vos données au sein de l'infrastructure du FSI. Les clauses contractuelles doivent mettre l'accent sur les restrictions physiques concernant vos données et les renseignements sensibles de la Société.

Les contrôles de sécurité de la confidentialité des données, comme le chiffrement ou d'autres mécanismes de transformation des données, ne changent pas la classification de vos données. Vous devez vous assurer que vos exigences en matière de sécurité physique peuvent prendre en charge toutes les données et tous les biens qui sont traités. L'accès physique aux données ou aux ressources de votre organisation doit être limité au personnel autorisé. Les ententes contractuelles devraient traiter de la sécurité physique de l'infrastructure de communication, de la prévention de la modification et de l'altération des biens. Vous devez vous assurer que la surveillance de la sécurité évalue l'efficacité des mesures de sécurité physique et que les registres d'accès aux sites physiques sont à jour et vérifiés périodiquement.

2.2.4 Conservation et destruction des données

Les exigences en matière de conservation et de destruction des données devraient être définies de manière à ce que l'organisation, le FSI et les autres fournisseurs de services tiers comprennent leurs obligations en ce qui concerne les périodes de conservation des données, les processus de traitement des données et les processus de destruction. Votre organisation devrait s'assurer que les documents contractuels définissent les paramètres relatifs aux types de supports acceptables, à la durée de conservation des données, aux contrôles de protection des supports, aux mécanismes de nettoyage ou de destruction et aux méthodes de vérification de la destruction. Ces paramètres devraient être harmonisés avec la classification des données protégées. Les exigences de conservation et de destruction des données devraient s'appliquer à toutes les formes de données, y compris les formules structurées et non structurées. Des évaluations périodiques devraient être prévues pour confirmer que les obligations contractuelles sont respectées. Pour de plus amples renseignements, voir Nettoyage des supports de TI (ITSP.40.006) [43].

2.2.5 Intelligence artificielle

L'intelligence artificielle (IA) et les outils d'apprentissage machine (AM) stimulent des capacités novatrices et modifient la façon dont les applications et les services des systèmes sont fournis. Ceux-ci présentent des menaces et des défis uniques, en particulier en raison de la croissance de l'utilisation de modèles de langage de grande taille (LLM pour *Large Language Models*) et de l'IA générative. Les organisations devront peut-être porter attention aux répercussions sur la sécurité et la

protection des renseignements personnels des solutions fondées sur l'IA au sein de leur chaîne de valeur. L'IA est utilisée pour développer de nouveaux services et ces solutions sont formées à l'aide de données opérationnelles. Les outils d'IA non autorisés qui accèdent à vos données confidentielles et opérationnelles présentent des risques importants pour l'entreprise et les renseignements personnels. Les contrats de service doivent tenir compte des limites et des restrictions liées à l'accès à vos données par les outils d'IA.

2.2.6 Menace quantique

La cryptographie est un moyen efficace de protéger la confidentialité et l'intégrité de l'information et de défendre les systèmes de TI contre les auteures et auteurs de cybermenaces. L'informatique quantique menace de détruire une grande partie de la cryptographie que nous utilisons actuellement. Les ordinateurs quantiques utiliseront la physique quantique pour traiter efficacement l'information et résoudre des problèmes qui ne sont pas pratiques à résoudre à l'aide des capacités informatiques actuelles. Les ordinateurs quantiques actuellement disponibles ne sont pas assez puissants pour briser la cryptographie, mais la technologie progresse rapidement et pourrait être disponible d'ici les années 2030. Cependant, les auteures et auteurs de menaces peuvent maintenant voler des renseignements chiffrés et les conserver jusqu'à ce qu'un ordinateur quantique suffisamment puissant soit disponible pour déchiffrer, lire ou accéder aux renseignements, même bien après leur création.

Pour gérer les risques associés aux progrès de l'informatique quantique, votre organisation devrait évaluer la sensibilité des renseignements communiqués à votre fournisseur et déterminer leur durée de vie afin de cerner les renseignements qui pourraient être à risque, lesquels peuvent être intégrés à vos processus d'évaluation continue des risques. De plus, votre organisation devrait déterminer si l'organisation contractante a des plans pour contrer la menace quantique. Les ententes contractuelles devraient préciser que l'entrepreneure ou entrepreneur doit tenir à jour ses processus cryptographiques conformément aux lignes directrices Faire face à la menace que l'informatique quantique fait peser sur la cryptographie (ITSE.00.017) [44] du Centre pour la cybersécurité.

3 Conditions générales

Du point de vue de la sécurité, les éléments contractuels doivent être normatifs et conformes aux cadres et aux approches reconnus afin que le FSI puisse établir la manière dont il aborde et maintient la posture de sécurité indiquée par votre organisation. Dans de nombreux cas, le recours aux modalités d'un fournisseur donné, telles qu'elles sont énoncées dans un contrat ou un contrat de licence utilisateur final (EULA pour *End User Licensing Agreement*), peut être considéré comme acceptable. Toutefois, pour certaines organisations ayant des besoins particuliers ou pour celles qui sont liées par des autorités réglementées, il faudra peut-être négocier entre les équipes juridiques en utilisant certaines des clauses types indiquées dans le présent guide. Dans tous les cas, dans la mesure du possible, demandez un avis juridique si des sujets précis vous préoccupent.

3.1 Facteurs à considérer

Votre organisation devrait examiner les points suivants et en discuter avec un conseiller juridique et le fournisseur.

3.1.1 Protection des secrets commerciaux (comme le matériel breveté et l'image de marque légale)

Si votre organisation a des exigences réglementaires ou des considérations relatives à des partenariats ou à des coentreprises, vous devriez vous demander la manière dont ce type de renseignements est séparé ou sécurisé dans la location principale. Cela vous aidera à repérer les renseignements qui peuvent facilement être signalés et séparés des ordonnances générales d'information ou lorsqu'une retenue légale est indiquée. Toutes les modalités doivent également stipuler clairement que le placement de ces renseignements au sein du fournisseur de services ne signifie pas que votre organisation a autorisé la possession, la détention ou l'utilisation de ces renseignements, et qu'ils demeurent la propriété de votre organisation.

3.1.2 Propriété intellectuelle

Comme dans le cas des secrets commerciaux, la propriété intellectuelle n'est pas un enregistrement officiel comme un brevet, mais elle a une incidence directe sur la raison d'être ou le mandat de votre organisation et il faudra prendre d'autres mesures pour étiqueter, identifier et sécuriser. Toutes les modalités doivent également stipuler clairement que le placement de ces renseignements au sein du fournisseur de services ne signifie pas que votre organisation a autorisé leurs possession, détention ou utilisation, et qu'ils demeurent la propriété de votre organisation.

3.1.3 Indemnisation/limitation de responsabilité.

Dans tous les cas de l'approvisionnement, un certain niveau de responsabilité est requis et doit être clairement défini entre les parties. Le nuage offre une nouvelle dynamique à cet égard. L'attention portée à la façon dont le fournisseur assure la « sécurité du nuage » et la décrit dans les modalités est très importante. Il faut noter où la ligne de responsabilité entre en jeu pour la « sécurité dans le nuage », car c'est la responsabilité de votre organisation. Selon la location qui est utilisée, cela

peut devenir plus complexe lors de la conclusion d'un contrat avec un fournisseur de service géré, un intégrateur de service ou de système ou un orchestrateur de service. Une description plus détaillée de la propriété de la location se trouve à la section 3.2.

3.1.4 Soutien

Le modèle de soutien peut intéresser ou préoccuper les organisations réglementées. En général, les FSI sont de nature « mondiale », et ils indiquent que l'approche de « soutien continu ajusté aux fuseaux horaires » est utilisée pour obtenir une couverture mondiale, 24 heures sur 24, 7 jours sur 7, 365 jours par année. Cela signifie que toute la couverture des services est répartie entre plusieurs emplacements mondiaux couvrant un fuseau horaire spécifique. Pour toute organisation qui a des règlements sur l'endroit où les ressources de soutien ou les ressources contractuelles peuvent résider, il est recommandé de discuter avec le fournisseur.

3.1.5 Migration

Même s'il est toujours dans l'intention d'une organisation d'obtenir un partenaire de confiance, il peut arriver que le transfert de vos renseignements à un autre fournisseur soit considéré comme nécessaire ou peut-être même nécessaire. À cet égard, l'examen initial et les questions concernant la migration de l'information au début du contrat seraient examinés et discutés avec le fournisseur. Voici les mesures précises à prendre pour demander des renseignements :

- les charges d'entrée et de sortie pour le mouvement des données;
- le temps alloué pour les activités de migration une fois que cela est indiqué au fournisseur principal;
- la durée de présence des données dans la location une fois que l'information a été transférée.

Remarque : Le nettoyage ou l'élimination des données conformément aux directives Nettoyage des supports de TI (ITSP.40.006) [43] du Centre pour la cybersécurité. Vous devez plutôt utiliser le déchiquetage cryptographique et l'attestation du fournisseur qui indique à quel niveau d'assurance les données sont écrasées.

3.2 Propriété de location

Comme nous l'avons mentionné plus tôt, il existe des distinctions précises quant aux personnes qui assurent ou peuvent être responsables de la « sécurité du nuage » et de la « sécurité dans le nuage ». Il y a aussi la stipulation de l'endroit où votre organisation « héberge » vos renseignements. Cela peut se faire de deux façons précises :

- hébergement dans votre propre location (propriété/contrôlée);
- hébergement dans les locaux d'un fournisseur.

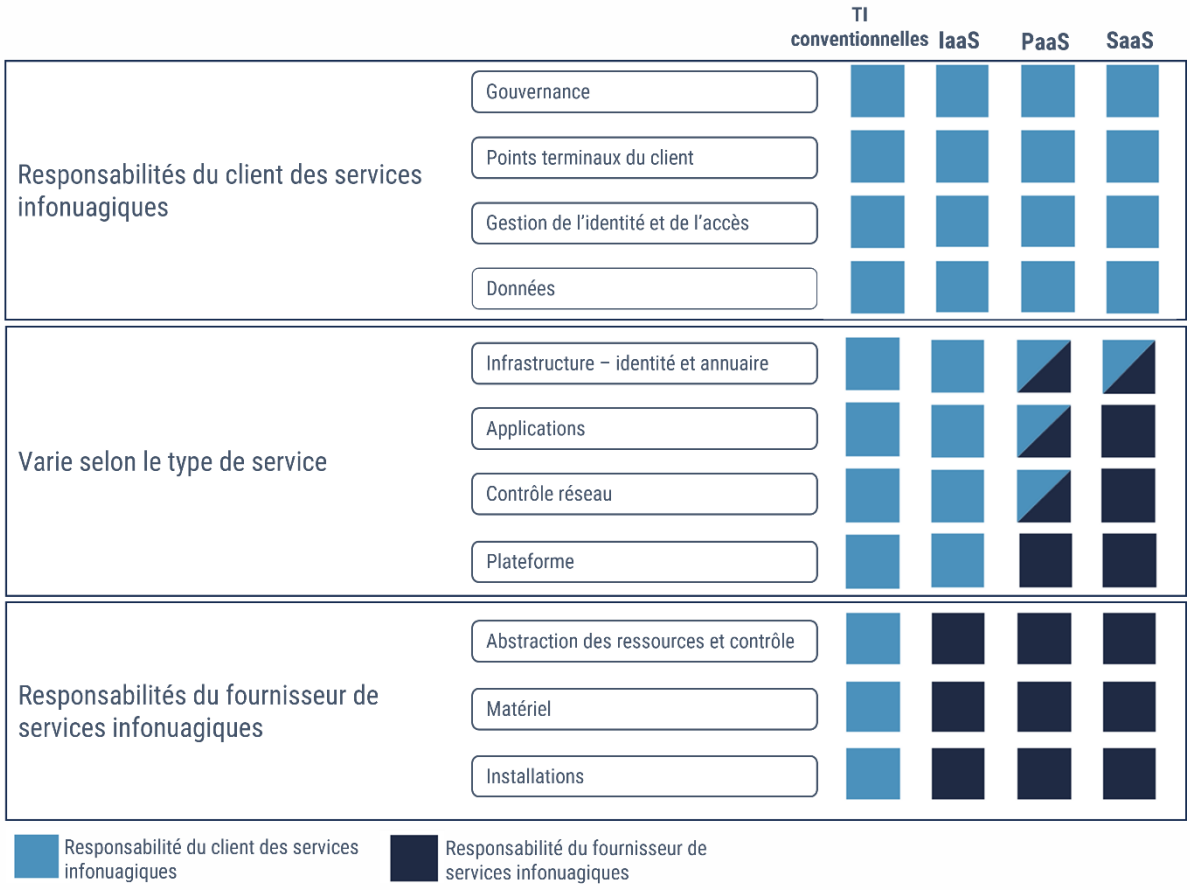
Votre organisation doit comprendre la différence entre un FSI et un FSG. La principale différence réside dans le contrôle exercé sur les données et le processus et qui en a le contrôle. Pour un FSG, le consommateur dicte la technologie et les procédures d'exploitation. Selon la MSP Alliance, les FSG présentent habituellement les caractéristiques distinctives suivantes :

- une certaine forme de service de centre des opérations du réseau (COR);
- une certaine forme de service de dépannage;
- la capacité à surveiller et à gérer à distance la totalité ou la majorité des objets pour le client;
- la capacité à entretenir de manière proactive les objets sous gestion pour le client;
- la capacité de fournir ces solutions au moyen d'une certaine forme de modèle de facturation prévisible, où le client sait avec une grande exactitude quelles seront ses dépenses habituelles de gestion des TI.

Avec un FSI, celui-ci dicte à la fois la technologie et les procédures opérationnelles mises à disposition du consommateur. Cela signifie qu'il offre une partie ou la totalité des composantes de l'informatique en nuage au moyen d'un logiciel-service (SaaS pour *Software as a Service*), d'une infrastructure-service (IaaS pour *Infrastructure as a Service*) ou d'un modèle de plateforme-service (PaaS pour *Platform as a Service*)[1].

Pour établir plus clairement les secteurs de responsabilité, la figure 1 fournit une description plus détaillée du modèle de responsabilité partagée.

Figure 1 : Modèle de responsabilité partagée



[1] *The official (ISC)2 Guide to the CCSP CBK*, 2016, Domain 1 Architectural Concepts and Design Requirements Domain, p. 4 (en anglais seulement).

Description de la figure : La figure 1 représente le partage des responsabilités entre une organisation de consommateurs de l'informatique en nuage et le FSI, en répartissant les responsabilités conformément au modèle de déploiement de l'informatique en nuage sélectionné. Que votre organisation et le FSI acceptent une IaaS, une PaaS ou un SaaS, vous aurez une combinaison de responsabilités uniquement pour votre organisation, uniquement pour le FSI et des responsabilités partagées entre les deux.

3.2.1 Location détenue ou contrôlée par une organisation (consommateur)

En ce qui concerne la propriété ou le contrôle de la location, l'organisation passe un contrat directement avec le FSI principal, y compris pour toute application PaaS ou SaaS. Dans ce contexte, votre organisation exerce donc un contrôle direct sur la configuration de la location et les zones requises, comme indiqué dans le modèle de responsabilité partagée, selon la solution qui a été conçue. Un aspect de la comparaison consiste à déterminer si votre organisation conclut un contrat avec un FSG ou un FSSG qui a accès au plan administratif de votre organisation. Bien que votre organisation possède et contrôle la location, vous donnez la capacité, par l'entremise de votre contrat avec le FSG ou le FSSG, d'administrer la location au nom de votre organisation. L'étendue du contrôle administratif dépend de l'intention de votre organisation. L'une des principales différences entre cette entente ou la location offerte par une autre entité est que votre organisation conserve le contrôle et que les secteurs de responsabilité seront négociés.

3.2.2 Fournisseur de services gérés et fournisseur de services de sécurité gérés

Le contexte de l'« hébergement » dans la location ou l'instance d'un fournisseur change la dynamique de ce dont votre organisation, en tant que consommateur, peut encore être responsable. Certains de ces domaines de responsabilité comprennent le contrôle de l'identité et de l'accès, ainsi que les données qui sont placées dans l'environnement. Le reste devient la responsabilité de l'entité qui héberge l'organisation. Les étapes supplémentaires que votre organisation peut prendre en plus de ce qui a déjà été discuté consistent à déterminer si vos données sont séparées au moyen de mesures logiques ou cryptographiques. Par le passé, des configurations matérielles distinctes (serveur) étaient une option, mais les environnements infonuagiques n'offrent pas cette capacité, à moins qu'une option « sans système d'exploitation » ne soit offerte. Cela complique la gouvernance des opérations de votre organisation, mais cela atténue les éléments de configuration et d'entretien de la location.

4 Conclusion

L'utilisation des services infonuagiques peut offrir beaucoup de souplesse et d'agilité à votre organisation. Il existe de nombreuses offres de services qui ont évolué au fil des ans, ce qui facilite la transition vers le nuage. Comme le présent document d'orientation le démontre, votre organisation doit examiner certains sujets de préoccupation et certaines questions avant, pendant et après la sortie d'un environnement infonuagique. Ce document vise à fournir des connaissances et des conseils généraux à toute organisation qui cherche à embarquer dans l'infonuagique et à contourner les pièges de l'utilisation des technologies infonuagiques. Comme indiqué, il ne s'agit pas d'un avis juridique.

Dans l'ensemble, le message clé est de travailler avec le FSI que vous avez choisi pour assurer une compréhension commune de votre engagement et de vous renseigner sur ce qui peut être fait pour répondre aux besoins particuliers de votre organisation.

5 Contenu complémentaire

5.1 Liste d'abréviations, d'acronymes et de sigles

Abréviation, acronyme ou sigle	Définition
AMF	Authentification multifacteur
API	Interface de programmation d'applications (*Application Programming Interface*)
ASTRA	Logiciel d'analyse aux fins d'évaluation de la menace (*Analytical Software for Threat Assessment*)
CIS	Centre for Internet Security
EMR	Évaluation des menaces et des risques
FIPS	Federal Information Processing Standard
FSG	Fournisseur de services gérés
FSSG	Fournisseur de services de sécurité gérés
FSI	Fournisseur de services infonuagiques
GIdA	Gestion des identités et de l'accès
IA	Intelligence artificielle
IaaS	Infrastructure-service (*Infrastructure as a Service*)
IDP	Fournisseur d'identité (*Identity Provider*)
LLM	Modèles de langage de grande taille (*Large Language Models*)
MHEMR	Méthodologie harmonisée de l'évaluation des menaces et des risques
NIST	*National Institute of Standards and Technology*
PaaS	Plateforme-service (*Platform as a Service*)
PVMC	Programme de validation des modules cryptographiques
SI	Intégrateur des services (Service Integrator)
SO	Outil d'orchestration des services (*Service Orchestrator*)
TI	Technologies de l'information
TLN	Traitement du langage naturel
TLS	Protocole de sécurité de la couche de transport (*Transport Layer Security*)

5.2 Glossaire

Terme	Définition
Authentification	Processus de vérification de l'identité déclarée par ou pour une entité de système.
Autorisation	Droits d'accès accordés à une utilisatrice ou un utilisateur, à un programme ou à un processus.
Contrat	Un contrat exécutoire est un accord délibéré (intention de créer des relations juridiques) constitué par une offre actuelle (offre d'acceptation) avec un ensemble de termes raisonnablement précis (certitude des termes) entre deux ou plusieurs parties compétentes (capacité) et inconditionnellement acceptées, qui s'appuie sur une considération mutuelle (contrepartie) pour accomplir un acte juridique volontaire (légalité de l'objet).

Évaluation des menaces et des risques	Processus qui permet d'établir les actifs du système et la façon dont ils peuvent être compromis, d'évaluer le niveau de risque que posent les menaces pour les actifs et de recommander des mesures de sécurité pour atténuer les menaces.
Infonuagique	Recours à des serveurs distants hébergés dans l'Internet. L'infonuagique permet à des utilisateurs d'accéder à un ensemble de ressources informatiques (comme des réseaux, des serveurs, des applications ou des services) sur demande et de n'importe où.
Informatique quantique	Un ordinateur quantique peut traiter un grand nombre de calculs simultanément. Tandis qu'un ordinateur classique travaille avec des « 1 » et des « 0 », un ordinateur quantique a l'avantage d'utiliser le « 1 », le « 0 » et des superpositions de « 1 » et de « 0 ».
Intelligence artificielle	Un sous-champ de l'informatique qui développe des programmes informatiques intelligents capables de donner l'impression d'une intelligence humaine (p. ex. résoudre des problèmes, tirer des leçons, comprendre une langue, interpréter des scènes visuelles).

5.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33), novembre 2012.
2	Centre canadien pour la cybersécurité, Lignes directrices sur la chaîne d'approvisionnement des technologies (TSCG-01), octobre 2010.
3	Services publics et Approvisionnement Canada (SPAC), Manuel de la sécurité des contrats.
4	United States Federal Risk and Authorization Management Program (FedRAMP), Control Specific Contract Clauses version 3.0 (en anglais seulement), décembre 2017.
5	National Institute of Standards and Technology, Enhanced Security Requirements for Protecting Controlled Unclassified Information (NIST SP 800-171) Revision 2, février 2020.
6	National Institute of Standards and Technology, Enhanced Security Requirements for Protecting Controlled Unclassified Information: Supplementary (NIST SP 800-172), février 2021
7	Organisation internationale de normalisation. ISO 27001:2022 – Systèmes de management de la sécurité de l'information.
8	Organisation internationale de normalisation. ISO 27017:2015 – Code de bonnes pratiques pour les contrôles de sécurité de l'information.
9	Organisation internationale de normalisation. Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII
10	Cloud Security Alliance (CSA). Security Guidance for Critical Areas of Focus in Cloud Computing Version 4.0, juillet 2017
11	Centre canadien pour la cybersécurité, Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.103), mai 2020.
12	Centre canadien pour la cybersécurité, Guide sur le chiffrement des services infonuagiques (ITSP.50.106), mai 2020.
13	Centre canadien pour la cybersécurité, Conseils sur la mise en œuvre de l'agilité cryptographique (ITSAP.40.018), mai 2022.
14	Gouvernement du Canada. Mesures de protection du nuage du GC – Protection des données inactives.
15	Gouvernement du Canada. Mesures de protection du nuage du GC – Protection des données en transit.
16	Gouvernement du Canada. Mesures de protection du nuage du GC – Emplacement des données

Numéro	Référence
17	Centre canadien pour la cybersécurité, Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.105), mai 2020.
18	Centre canadien pour la cybersécurité, Méthodologie harmonisée d'EMR.
19	Centre canadien pour la cybersécurité, La cybersécurité et la chaîne d'approvisionnement : évaluation des risques (ITSAP.10.070), juillet 2022.
20	Centre canadien pour la cybersécurité, Menaces à la chaîne d'approvisionnement et espionnage industriel.
21	Centre canadien pour la cybersécurité, Clauses contractuelles visant l'équipement et les services de télécommunications (TSCG-01L).
22	Organisation internationale de normalisation. ISO/IEC 27036 – Cybersécurité — Relations avec le fournisseur (parties 1 à 4).
23	Centre canadien pour la cybersécurité, Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031), avril 2018.
24	Centre canadien pour la cybersécurité, Les 10 mesures de sécurité des TI : no 3 Gestion et contrôle des privilèges d'administrateur (ITSM.10.094), juillet 2022.
25	National Institute of Standards and Technology, NIST SP 800-63-4 Digital Identity Guidelines: Federation and Assertions (Initial Public Draft), décembre 2022.
26	Centre canadien pour la cybersécurité, Gérer les risques liés aux données du gouvernement du Canada dans le contexte des services infonuagiques (ITSM.50.109), août 2022.
27	Centre canadien pour la cybersécurité, Guide sur la défense en profondeur pour les services fondés sur l'infonuagique (ITSP.50.104), mai 2020.
28	Centre canadien pour la cybersécurité, Guide sur le chiffrement des services infonuagiques (ITSP.50.106), mai 2020.
29	Centre canadien pour la cybersécurité, Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B - ITSP.40.111, septembre 2022.
30	National Institute of Standards and Technology, NIST 800-123 Guide to General Server Security.
31	Center for Internet Security, CIS benchmarks.
32	Centre canadien pour la cybersécurité, Configurer les dispositifs pour assurer leur sécurité, septembre 2019.
33	Centre canadien pour la cybersécurité, Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030), juin 2021.
34	Centre canadien pour la cybersécurité, La cybersécurité à la maison et au bureau – Sécuriser vos dispositifs, vos ordinateurs et vos réseaux (ITSAP.00.007), octobre 2020.
35	Centre canadien pour la cybersécurité, Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001), décembre 2020.
36	Centre canadien pour la cybersécurité, Application des mises à jour sur les dispositifs (ITSAP.10.096), mars 2021.
37	Centre canadien pour la cybersécurité, Zones de sécurité de réseau en nuage (ITSP.80.023), juin 2023.
38	Centre canadien pour la cybersécurité, Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062), octobre 2020.
39	Centre canadien pour la cybersécurité, Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085), décembre 2022.
40	Centre canadien pour la cybersécurité, Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030), octobre 2020.

Numéro	Référence
41	Centre canadien pour la cybersécurité, Les 10 mesures de sécurité des TI no.2 Appliquer les correctifs aux systèmes d'exploitation et aux applications (ITSM.10.096), août 2022.
42	Centre canadien pour la cybersécurité, Appliquer automatiquement les correctifs aux systèmes d'exploitation et aux applications, septembre 2019.
43	Centre canadien pour la cybersécurité, Nettoyage des supports de TI (ITSP.40.006), juillet 2017.
44	Centre canadien pour la cybersécurité, Faire face à la menace que l'informatique quantique fait peser sur la cryptographie (ITSE.00.017), mai 2020.