HEC Montréal

Établir les requis fonctionnels et technologiques en sécurité de l'information : le cas spécifique des *Cloud Access Security Brokers*

par

Andréanne Ostiguy

Sciences de la gestion

(Option Technologies de l'information)

Mémoire présenté en vue de l'obtention du grade de maîtrise ès sciences en gestion (M.Sc.)

Décembre 2016

© Andréanne Ostiguy, 2016

HEC MONTRÉAL

Comité d'éthique de la recherche

CERTIFICAT D'APPROBATION ÉTHIQUE

La présente atteste que le projet de recherche décrit ci-dessous a fait l'objet d'une évaluation en matière d'éthique de la recherche avec des êtres humains et qu'il satisfait aux exigences de notre politique en cette matière.

Projet # : 2016-2263

Titre du projet de recherche : Établir les besoins en sécurité de l'information: le cas spécifique des CASB

Chercheur principal :
Andréanne Ostiguy-Brunet
Étudiante M. Sc. - HEC Montréal

Directeur/codirecteurs :
Line Dubé
Professeur - HEC Montréal

Date d'approbation du projet : 18 avril 2016

Date d'entrée en vigueur du certificat : 18 avril 2016

Date d'échéance du certificat : 01 avril 2017

Maurice Lemelin
Président du CER de HEC Montréal

Sommaire

L'infonuagique est un mode d'impartition des technologies de l'information de plus en plus populaire auprès des organisations. Bien qu'elle permette une grande flexibilité et une implantation rapide, elle apporte aussi son lot de défis en sécurité de l'information. Parmi les défis recensés dans la littérature, on note ceux qui ont trait à la confidentialité, à l'intégrité et à la disponibilité des données imparties au fournisseur de services infonuagiques. D'ailleurs, le plus grand frein à l'adoption de l'infonuagique serait la perte de contrôle de l'organisation sur ses données imparties. En effet, d'un point de vue légal, même si les données sont stockées chez un fournisseur, l'organisation en conserve la responsabilité. Dans ce contexte, une nouvelle classe d'outils, les Cloud Access Security Brokers (CASB), a été proposée comme solution à certains des problèmes associés à l'utilisation de l'infonuagique. Cette classe d'outils émergente promet de faciliter et de centraliser la gestion des applications infonuagiques. Les CASB agissent comme un intermédiaire entre l'organisation cliente et le fournisseur d'applications infonuagiques. Ils permettent d'atteindre quatre objectifs de sécurité, soit d'identifier les applications infonuagiques utilisées au sein de l'entreprise, d'appliquer les politiques de gouvernance de sécurité, d'assurer la protection des données et de défendre l'organisation contre les menaces externes. Le mémoire se penche sur cette classe d'outils et son objectif est, dans un premier temps, de définir les besoins de sécurité d'une entreprise canadienne du domaine de la finance et de l'assurance afin de déterminer les requis technologiques et fonctionnels pour un CASB implanté dans une organisation de cette industrie. Dans un deuxième temps, ces requis ont été comparés aux fonctionnalités offertes par les CASB actuellement disponibles sur le marché pour ensuite discuter du potentiel de cette classe d'outils. L'étude permet de conclure que, même si les CASB offrent des fonctionnalités intéressantes, ils ont plusieurs limites et ne répondent que partiellement aux besoins typiques d'une organisation œuvrant dans le milieu de la finance et de l'assurance.

Mots-clés : infonuagique, sécurité de l'information, *Cloud Access Security Brokers*, CASB, requis de sécurité, *recherche action design,* finance et assurance.

Remerciements

Je tiens d'abord à remercier Line Dubé qui fut une directrice extrêmement dévouée, présente et patiente. J'ai eu beaucoup de chance de pouvoir travailler avec une personne aussi passionnée et attentive. Elle m'a appris l'importance de la rigueur en recherche et ses commentaires, ses suggestions et ses idées me furent d'une aide précieuse tout au long de la rédaction de ce mémoire. Je n'aurais jamais pu écrire un mémoire de cette qualité sans son soutien; j'ai une admiration et une reconnaissance sans borne à son égard.

Ensuite, je remercie Henri Barki et Suzanne Rivard pour leurs commentaires dans le cadre de l'Atelier de recherche; ce fut un grand honneur de les avoir comme professeurs. Je tiens à remercier aussi les professeurs Pierre-Majorique Léger et Sylvain Sénécal ainsi que toute l'équipe du Tech3Lab qui m'ont permis d'apprendre énormément et de découvrir la recherche TI en laboratoire. Je voudrais aussi souligner le travail acharné de tous les professeurs et enseignants du département de technologies de l'information à HEC Montréal. Tant au baccalauréat qu'à la maîtrise, j'ai eu la chance de pouvoir apprendre de ces gens passionnés et je ne garde que de bons souvenirs de mon passage dans leurs cours. Je souhaite également remercier les trois professeurs qui ont gentiment accepté de faire partie de mon jury.

Merci à l'entreprise qui m'a ouvert ses portes pendant près de trois mois pour ma collecte de données. Bien qu'elle doive rester anonyme, j'espère que les gens avec qui j'ai eu la chance de travailler se reconnaîtront. Leur professionnalisme, leur savoir-faire et surtout leur générosité ont grandement contribué à la réalisation de ce mémoire.

Je remercie aussi mes collègues à la maîtrise en TI à HEC Montréal, ils ont certainement rendu mon parcours aux études supérieures plus agréable. Un merci particulier à Cindy Nguyen qui partage le même intérêt que moi pour la sécurité de l'information et qui m'a souvent aidée lors de l'écriture en partageant des articles et des idées, en lisant mes ébauches ou bien en m'encourageant.

Finalement, l'écriture d'un mémoire est un exercice d'endurance parfois ardu et c'est pourquoi je tiens à remercier mes amis et ma famille pour leur soutien dans les derniers mois. Je remercie spécialement Chantal, Robert et ma mère qui, grâce à leur regard externe, ont rendu, je crois, ce mémoire plus accessible. Leurs commentaires et leurs suggestions furent toujours pertinents et leurs encouragements furent définitivement appréciés. J'ai beaucoup de chance d'être entourée d'autant de gens d'exception.

Table des matières

Liste des abréviations

Abréviation	Terme
API	*Application Programming Interface* ou Interface de programmation d'application
CASB	*Cloud Access Security Broker*
CEI	Commission électrotechnique internationale
CIA	*Confidentiality, Integrity and Availability* ou Confidentialité, intégrité et disponibilité
CSA	*Cloud Security Alliance*
DLP	*Data Loss Prevention* ou Protection contre la perte de données
IaaS	*Infrastructure as a Service*
ISO	Organisation internationale de la normalisation
NIST	*National Institute of Standards and Technology*
PaaS	*Platform as a Service*
PCI DSS	*Payment Card Industry Data Security Standard*
RAD	*Recherche action design*
RBAC	*Role-based Access Control* ou Contrôle des accès basé sur le rôle
SaaS	*Software as a Service*
SIEM	*Security Information and Event Management* ou Logiciel de gestion d'information et d'événements de sécurité
SLA	*Service Level Agreement* ou Entente de niveau de service
SSO	*Single Sign-on* ou Logiciel d'authentification unique
TI	Technologies de l'information

Liste des figures

Liste des tableaux

DANS LES ANNEXES

Chapitre 1: Introduction

1.1 Mise en contexte

L'importance du rôle des technologies de l'information (TI) au sein des organisations n'est plus à démontrer. Avec l'adoption croissante des TI viennent toutefois plusieurs risques en matière de sécurité de l'information, une problématique de plus en plus préoccupante pour beaucoup d'entreprises. En effet, malgré le niveau de sophistication des technologies de prévention dans le domaine de la sécurité de l'information, les brèches sont toujours présentes. Comme le montre un sondage global effectué en mai 2015, 79 % des répondants ont admis que leur entreprise avait subi au moins un incident de sécurité dans les douze mois précédents (PricewaterhouseCoopers, 2015). Certaines de ces brèches, comme celles de Sony ou de Target, ont été très médiatisées et elles ont occasionné des pertes de revenus de plusieurs millions de dollars en plus d'ébranler considérablement la confiance du public envers ces entreprises (Ponemon Institute, 2015). Les organisations, tant publiques que privées, ont donc un intérêt particulier à protéger leurs systèmes et leurs données. D'ailleurs, en ce sens, les investissements annoncés récemment en sécurité de l'information sont massifs.[1]

Plusieurs activités contribuent à accroître les risques en sécurité de l'information auxquels les entreprises font face. Parmi celles-ci, on retrouve les modes d'approvisionnement en services TI et plus spécifiquement l'infonuagique,[2] un mode d'approvisionnement de plus en plus populaire qui pose des défis particuliers en sécurité de l'information pour les entreprises qui l'adoptent. L'infonuagique est définie comme un « modèle qui permet un accès constant, pratique et sur demande à un bassin de ressources informatiques partagées (par exemple, des réseaux, des serveurs, du stockage, des applications et des services) qui peuvent être acquises et déployées rapidement avec un effort de gestion minimal » (traduction libre de Mell et Grance, 2011, p.2).

[1] Le gouvernement américain a récemment annoncé des investissements de 3,1 milliards de dollars américains en sécurité de l'information, une augmentation de 35 % par rapport à l'année précédente (Green, 2016). Dans la même veine, en juillet 2015, le gouvernement canadien a annoncé des dépenses supplémentaires de 142 millions de dollars sur cinq ans en cybersécurité (Mas, 2015). Les entreprises aussi augmentent leurs investissements : selon le sondage de PricewaterhouserCoopers, elles ont augmenté leur budget alloué à la sécurité de 24 % en 2015 par rapport à l'année précédente (PricewaterhouseCoopers, 2015).

[2] L'infonuagique ou l'informatique en nuage est la traduction française de *cloud computing* (Grand dictionnaire terminologique de la langue française, consulté le 13 février 2016, http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26501384).

Cette avenue s'avère intéressante puisque la technologie se développe à une grande vitesse et devient désuète tout aussi rapidement. En plus du désir de demeurer compétitives tout en minimisant les investissements et les coûts d'exploitation, cela force les entreprises à adopter une infrastructure technologique plus flexible qui permet de s'adapter rapidement aux changements de son environnement. L'infonuagique devient un maillon important de cette flexibilité, entraînant un changement important de paradigme pour la gestion des technologies et des risques en sécurité de l'information au sein des entreprises.

L'attrait principal de l'infonuagique pour les organisations est la rapidité et la facilité d'installation (Waters, 2005). Traditionnellement, lorsqu'une entreprise acquerrait un logiciel ou du matériel informatique, elle devait d'abord mettre en place l'infrastructure technologique nécessaire (serveurs, routeurs, réseaux et autres) en plus d'en assurer ensuite l'entretien et d'en faire les mises à jour. À présent, avec l'infonuagique, le déploiement devient beaucoup plus rapide puisqu'il peut se faire presque instantanément pour plusieurs utilisateurs (Hassan, 2011). Le concept de l'utilisateur payeur, un principe à la base de l'infonuagique, apporte une flexibilité qui permet aux organisations de répondre rapidement aux variations de la demande en ajoutant des ressources lorsque nécessaire (Zissis et Lekkas, 2012) et ce, en quelques minutes plutôt qu'en plusieurs semaines, comme c'est généralement le cas avec le modèle traditionnel (Armbrust *et al.*, 2010). Avec l'infonuagique, le parc informatique peut donc plus facilement suivre l'évolution des besoins de l'entreprise. Finalement, l'infonuagique permet aussi à l'organisation de réduire ses dépenses en acquisition et en exploitation d'infrastructure technologique en impartissant ces activités à un fournisseur externe pour lequel ces activités constituent le cœur de métier (Avram, 2014; Orman, 2016).

Malgré ses avantages indéniables, l'infonuagique est aussi une source importante de préoccupations en termes de sécurité de l'information pour bien des entreprises, à un point tel qu'elles seraient un frein à son adoption (Juels et Oprea, 2013). Ce mode d'approvisionnement pose certains défis en ce qui a trait à la confidentialité, l'intégrité et la disponibilité des données (Ali, Khan et Vasilakos, 2015). Comme l'organisation impartit une partie de ses activités et de ses données à une tierce partie, il y a un risque que la confidentialité et l'intégrité des données soient violées puisque celles-ci sont accessibles au fournisseur, à ses employés et à ses partenaires d'affaires (Ryan, 2013). La disponibilité et la pérennité des logiciels et des données reposent sur

la capacité du fournisseur externe à respecter des bonnes pratiques de gestion des TI. De plus, comme le partage des ressources informatiques est le principe à la base de l'infonuagique, une entreprise s'expose alors à la possibilité que la confidentialité de ses données soit mise en péril par les autres utilisateurs qui partagent le service (Ryan, 2013), ce qui est particulièrement vrai dans le cas spécifique de l'utilisation de l'infonuagique publique, contexte dans lequel les ressources d'un même fournisseur sont partagées entre différents clients (Rong, Nguyen et Jaatun, 2013).

En plus de ces défis, les normes et les lois auxquelles les organisations doivent se conformer en termes de sécurité de l'information ont aussi un impact sur les pratiques en sécurité et de là, sur les fournisseurs de services. Les organisations qui adoptent l'infonuagique doivent donc s'assurer que le fournisseur choisi réponde aux règles internes de sécurité, mais aussi qu'il respecte les lois et les normes auxquelles elles sont elles-mêmes assujetties (Rong *et al.*, 2013). Ainsi, l'aspect légal derrière le choix d'un fournisseur et de l'exploitation de services infonuagiques ajoute une couche de complexité.

Une des solutions potentielles pour remédier aux problèmes de sécurité liés à l'infonuagique réside dans l'émergence d'une nouvelle classe de logiciels appelée *Cloud Access Security Brokers* (CASB).[3] Cette nouvelle technologie est définie par la firme de recherche Gartner de la façon suivante :

> « Un intermédiaire, placé entre le client et le fournisseur de services infonuagiques, qui permet d'imposer le respect des politiques de sécurité lors de l'utilisation des ressources infonuagiques. Cet intermédiaire peut être lui-même un service infonuagique ou bien être physiquement mis en place sur les lieux de l'entreprise. » *(traduction libre de MacDonald et Firstbrook, 2012, p.4)*

Même s'il demeure transparent pour les utilisateurs, le CASB repose ainsi sur le principe qu'il est un intermédiaire représentant l'unique voie d'accès aux services infonuagiques. Pour l'instant, toutefois, les CASB évoquent plutôt une classe d'outils dont on connaît l'objectif global, mais pour laquelle les spécifications restent encore à être déterminées. Cette classe d'outils vise à accomplir quatre grands objectifs : 1) la visibilité, 2) la gouvernance et le respect de la conformité, 3) la

[3] Il ne semble pas exister de traduction française pour cette classe d'outils. L'acronyme CASB sera employé dans le texte.

sécurité des données et 4) la protection contre les menaces provenant de l'utilisation des services infonuagiques (Lawson, MacDonald et Heiser, 2015b). Les fonctionnalités de visibilité permettent à l'organisation de surveiller les activités faisant appel aux services infonuagiques, une nécessité considérant la prolifération d'outils et d'applications non autorisés[4] qui sont utilisés au sein des entreprises et le risque en sécurité que cette pratique représente (Silic et Back, 2014b). En ce qui a trait à la conformité, tel que mentionné précédemment, les entreprises sont sujettes à plusieurs lois et normes de sécurité et un CASB peut l'aider à s'y conformer, notamment en offrant des fonctionnalités de surveillance et de contrôle (Lawson *et al.*, 2015b). La sécurité des données est assurée par certains CASB qui offrent des fonctions de chiffrement qui permettent la protection des données échangées avec les fournisseurs de services infonuagiques (MacDonald et Firstbrook, 2012). Finalement, bien que la plupart des fournisseurs de services infonuagiques offrent des services de sécurité intégrés à leurs produits, les CASB ajoutent une couche supplémentaire de protection contre les menaces externes (Lawson *et al.*, 2015b).

Bien qu'ils tendent à viser ces quatre grands objectifs, les CASB sont encore une technologie en émergence : on ne sait pas trop comment chaque CASB se positionne par rapport à ces objectifs, les fonctionnalités ne sont pas universelles et elles varient selon les fournisseurs. À ce jour, la protection qu'offre chacune des solutions disponibles est souvent limitée à quelques applications infonuagiques spécifiques comme, par exemple, Salesforce ou Office 365 (Lawson, MacDonald et Lowans, 2015c). Pour cette raison, le choix d'une solution CASB est complexe puisqu'aucune ne répond à tous les besoins de l'entreprise. Il s'agit donc d'un choix à la pièce et on peut tout de suite entrevoir le défi cauchemardesque que cette classe d'outils représentera au point de vue de l'exploitation et de l'intégration avec les composantes technologiques actuelles de l'entreprise. D'autre part, le marché des CASB est encore très immature et les entreprises qui le composent sont principalement de petits joueurs comme des entreprises en démarrage[5] (Lawson *et al.*, 2015c). Cependant, les grandes entreprises de logiciels commencent de plus en plus à s'intéresser aux CASB et à pénétrer le marché, soit en faisant des acquisitions ou en établissant des

[4] Cette pratique est communément appelée *shadow IT*.

[5] Entreprise en démarrage est le terme français pour désigner une *startup* (Grand dictionnaire terminologique de la langue française, consulté le 17 mars 2016, http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=507728).

partenariats avec ces entreprises en démarrage (Lawson *et al.*, 2015c). Cet intérêt démontre le dynamisme et le potentiel prometteur de ce marché.

1.2 Objectif et questions de recherche

Dans ce contexte où l'infonuagique devient un mode d'approvisionnement de plus en plus adopté par les entreprises, il semble important de se pencher sur les risques de sécurité que représente cette façon de faire et surtout, sur les solutions permettant de faire face aux défis soulevés. La sécurité est d'ailleurs au centre des préoccupations des entreprises qui optent pour l'infonuagique (Goettelmann, Mayer et Godart, 2013). Bien que certains organismes comme l'Organisation internationale de normalisation (ISO) ou la Cloud Security Alliance (CSA) aient commencé à publier des normes spécifiques à la sécurité infonuagique et qui formulent des recommandations encadrant l'adoption de ces services, la façon de mettre en place ces normes est laissée à la discrétion des entreprises (Cloud Security Alliance, 2011; ISO/CEI 27017, 2015). Ainsi, l'établissement des besoins en sécurité infonuagique et la sélection des pratiques et des outils à mettre en place pour les combler représentent aujourd'hui un défi de taille pour les organisations (Heiser, 2015; Mouratidis, Islam, Kalloniatis et Gritzalis, 2013).

Dans ce contexte, les CASB offrent un potentiel attrayant pour les organisations qui souhaitent se protéger contre les risques engendrés par l'infonuagique. Aujourd'hui, toutefois, cette classe d'outils représente plus un principe que des solutions largement disponibles sur le marché et leur plein potentiel n'est pas encore défini ou même connu. En effet, les CASB entrent dans la catégorie des produits complexes et ambigus. Novak et Eppinger (2001) considèrent qu'un produit est complexe selon trois caractéristiques : 1) le nombre de composantes du produit, 2) l'envergure des interactions à gérer entre ces différentes composantes et 3) le degré de nouveauté du produit. Selon cette définition, les CASB peuvent être considérés complexes puisqu'ils ont généralement plusieurs fonctionnalités qui doivent non seulement interagir entre elles, mais aussi avec les autres systèmes de l'organisation (Lawson *et al.*, 2015c). De plus, ils ont un degré de nouveauté élevé comme le montrent l'immaturité du marché et le taux d'adoption encore faible. D'autre part, les CASB sont des produits ambigus, c'est-à-dire que « l'interprétation du produit […] et du marché change constamment » (traduction libre de Brun, Steinar Saetre et

Gjelsvik, 2009, p. 80), justement à cause du degré de nouveauté de cette classe d'outils et de son potentiel encore non défini.

Comme les CASB font partie de ces technologies que l'on peut qualifier d'émergentes, complexes et ambiguës, cela rend la définition des besoins et l'évaluation des fournisseurs éventuels difficiles pour l'entreprise souhaitant les adopter ou même seulement en évaluer le potentiel. Dans ce contexte, l'objectif de ce mémoire est donc de contribuer à une meilleure compréhension des CASB et de leur potentiel à répondre aux besoins en sécurité des organisations face à l'infonuagique. Le mémoire se concentre plus spécifiquement sur le cas des entreprises de l'industrie de la finance et de l'assurance. En effet, l'industrie à laquelle appartient une organisation pourrait avoir une incidence sur ses besoins en sécurité de l'information, ce qui pourrait mener à des requis fonctionnels et technologiques différents en termes de CASB.[6] L'industrie de la finance et de l'assurance représente un secteur de choix pour la présente étude parce qu'elle regroupe des entreprises qui se doivent d'être à la fine pointe de la technologie, qui détiennent de l'information hautement confidentielle sur leurs clients et partenaires d'affaires et qui sont tenues de respecter plusieurs lois et normes en ce qui a trait à la sécurité de l'information. Ces conditions, jumelées à la volatilité de son environnement et aux avantages potentiels des services infonuagiques dans un tel contexte, font en sorte que l'industrie symbolise un cas « extrême » duquel pourraient s'inspirer d'autres entreprises dont les besoins en sécurité pourraient s'avérer plus modestes.

Ainsi, les questions de recherche auxquelles tente de répondre cette étude sont les suivantes :

1. Quels sont les requis fonctionnels et technologiques pour un CASB utilisé par une organisation du domaine de la finance et de l'assurance au Canada[7]?

[6] Dans le cadre de ce mémoire, un besoin est une exigence (atteinte d'un objectif, réalisation d'un processus ou d'une tâche, etc.) identifiée comme étant manquante et nécessaire par l'organisation afin de protéger ses données. Un requis consiste plutôt en une fonctionnalité ou une spécification technique pour un outil qui permet de combler le besoin identifié.

[7] Selon Statistique Canada, « ce secteur comprend les établissements dont l'activité principale consiste à effectuer des opérations financières (c'est-à-dire des opérations portant sur la création, la liquidation ou la cession d'actifs financiers) ou à en faciliter l'exécution » (Statistique Canada (2012). « Système de classification des industries de l'Amérique du Nord (SCIAN) Canada », p. 369).

2. Quelles sont les fonctionnalités et les caractéristiques des CASB actuellement offerts sur le marché ?
3. Comment les solutions de type CASB actuellement offertes sur le marché répondent-elles aux requis identifiés ?

Afin répondre aux questions de recherche énoncées ci-dessus dans le contexte de l'établissement des fonctionnalités d'un produit complexe et ambigu, une approche basée sur la méthodologie de *recherche action design* (RAD) est adoptée. L'établissement des requis fonctionnels et technologiques s'est fait dans le contexte d'une grande entreprise canadienne évoluant dans le secteur choisi.

L'étude contribue à l'avancement des connaissances dans le domaine considérant que la littérature scientifique et professionnelle est plutôt limitée sur le sujet de la sécurité dans un contexte infonuagique et encore davantage sur les CASB. Comme cette technologie est récente et en constante évolution, il y a très peu d'information à ce sujet mis à part quelques articles de la firme de recherche Gartner qui en définit le principe de base. Le mémoire se penche donc sur la définition des CASB et la détermination de leurs requis, considérant qu'ils font partie d'une classe de produits complexes et dont la compréhension actuelle est limitée. Ce mémoire contribue ainsi à la littérature en établissant le bassin de fonctionnalités qu'un CASB peut offrir aux entreprises dans le domaine de la sécurité infonuagique. Les limites identifiées ouvrent la voie vers de nouvelles avenues où la recherche doit être approfondie.

Une fois la définition de cette classe d'outils établie, le mémoire permet de comprendre comment les CASB, dans leur forme actuelle, répondent aux besoins de sécurité de l'information des entreprises de la finance et de l'assurance. Il se penche sur le potentiel des CASB en tant qu'outil d'automatisation des processus de sécurité de ces entreprises. Quoique les entreprises de l'industrie de la finance et de l'assurance doivent répondre à des normes communes, il est clair que certains des éléments des résultats de la présente étude sont spécifiques à l'environnement contextuel de l'organisation étudiée. Ces éléments incluent l'infrastructure technologique de l'entreprise, le niveau de risque qu'elle est prête à assumer ou le contenu des contrats négociés avec les fournisseurs infonuagiques. Toutefois, considérant que les entreprises de ce secteur ont toutes des activités similaires, que la réglementation entourant les activités des firmes du milieu

de la finance et de l'assurance est très stricte et que le niveau de maturité technologique des entreprises de ce domaine est sensiblement le même, les résultats présentés dans l'étude sont en grande partie généralisables à l'échelle de l'industrie. Les entreprises de ce secteur pourront utiliser les requis identifiés pour les guider dans le processus de sélection ou de développement d'un CASB dans un contexte où l'élaboration des requis est basée sur des besoins qui sont généralement inconnus à cause de l'immaturité de la technologie. Au-delà des spécificités propres à l'industrie, le mémoire met en lumière d'autres caractéristiques organisationnelles qui pourraient avoir une influence sur les requis pour un CASB.

1.3 Structure du mémoire

À la suite du présent chapitre, la revue de la littérature permet d'établir les bases théoriques sur lesquelles s'appuiera ce mémoire ainsi que l'intervention en entreprise. Elle recense les écrits en sécurité de l'information, les défis présents dans un contexte d'utilisation de l'infonuagique et les normes encadrant ce mode d'approvisionnement. À la fin de la revue, les CASB sont présentés comme un outil potentiel pour mitiger les risques associés à certains des défis en sécurité infonuagique.

Le troisième chapitre décrit la méthodologie choisie pour ce mémoire, la *recherche action design*. Cette méthodologie, qui est un hybride entre la recherche action et le *design science*, permet de créer, grâce à l'intervention en entreprise, des artefacts permettant de répondre aux trois questions de recherche. Dans ce chapitre, chacune des étapes menant à la réalisation du mandat et à la formulation des réponses aux questions de recherche et la façon dont celles-ci sont appliquées spécifiquement dans ce mémoire sont expliquées.

Les résultats de l'intervention en entreprise, soit la grille des requis, sont présentés au quatrième chapitre du mémoire (artefact #1). En outre, afin de faciliter la discussion et pour répondre à la deuxième question de recherche, un recensement des fournisseurs actuels, de leurs produits et de leurs fonctionnalités est réalisé dans ce même chapitre (artefact #2).

Finalement, en cinquième partie du mémoire, une discussion permet de faire la lumière sur les écarts entre les requis de l'organisation à l'étude et les fonctionnalités des produits actuellement

en vente sur le marché (artefact #3). Cette analyse des écarts mène ensuite à un essai sur le potentiel des CASB comme outil de centralisation et d'automatisation de la sécurité de l'information. Le mémoire se conclut sur les contributions de l'étude, tant pour la pratique que pour la recherche, ainsi que sur ses limites.

Chapitre 2: Revue de la littérature

L'objectif premier de la revue de la littérature est de présenter le cadre dans lequel se fera subséquemment le travail d'élaboration des spécifications. Cette connaissance s'avère essentielle à une compréhension des défis en sécurité infonuagique et à la réalisation d'extrants pertinents.

En guise d'introduction, la revue de la littérature décrit l'infonuagique et ses caractéristiques. Ensuite, considérant que l'infonuagique pose certains défis de sécurité qui lui sont spécifiques, un recensement de ces défis est exposé. Il s'ensuit un inventaire des besoins en sécurité de l'information selon les normes en sécurité utilisées dans l'industrie de la finance et de l'assurance au Canada, s'affairant plus spécifiquement à présenter celles touchant l'infonuagique. Par la suite, les logiciels de type CASB y sont définis puisqu'ils représentent une solution possible à plusieurs des défis identifiés. Cependant, comme il s'agit d'une technologie nouvelle dans un marché immature, ce sont plutôt les principes généraux qui la sous-tendent qui y sont décrits. En dernier lieu, la revue de la littérature explore les raisons qui expliquent que les CASB sont des produits complexes.

La couverture de tous ces thèmes permet l'enrichissement de la réflexion sur la sécurité de l'information dans un contexte infonuagique. L'objectif de la revue de la littérature est donc de jeter les bases pour la suite du mémoire.

2.1 Méthodologie utilisée

Une première recherche d'articles et de comptes rendus de conférence a été effectuée dans les bases de données ABI/Inform Complete, EBSCOhost Business Source Complete et IEEE. La base de données de Google Scholar a été utilisée en complément. Les articles trouvés de cette façon concernent principalement les thèmes de la sécurité de l'information et de l'infonuagique. Malheureusement, comme les CASB sont une technologie émergente et que, selon nos recherches,[8] aucun article scientifique ou compte rendu de conférence n'a encore été écrit sur le sujet, le moteur de recherche Google a permis de trouver des articles professionnels sur cette classe d'outils. Les sites Internet des fournisseurs de CASB sont aussi une source importante

[8] En date du 19 août 2016.

d'information sur ces produits et leur fonctionnement. Les bases de données des firmes de recherche Gartner et Forrester ont été spécialement utiles pour trouver de la documentation sur les CASB en tant que tel puisque la plupart des informations sur le sujet proviennent de rapports publiés par ces organisations. Tous les articles recensés sont disponibles en format électronique.

En plus des articles, le site web de la bibliothèque de HEC Montréal a permis de rechercher de l'information sur la sécurité de l'information parmi sa collection de livres en format papier et numérique. Les mots-clés utilisés pour les recherches sont présentés dans un tableau disponible à l'annexe A.

Afin d'approfondir les connaissances en infonuagique et plus spécifiquement en sécurité, le principe de *backward search*, qui consiste à chercher parmi les travaux cités dans un article, et celui de *forward search*, qui vise à analyser les documents citant un article en particulier, ont été utilisés (Silic et Back, 2014a). Cependant, cette méthode de repérage n'a pu être appliquée dans les recherches sur les CASB puisque, tel que mentionné plus haut, aucune étude scientifique sur le sujet n'a pu être identifiée.

Finalement, les sites web des divers organismes comme ceux de la Cloud Security Alliance (CSA) et du National Institute of Standards and Technology (NIST) sont des sources de renseignements importantes sur les lignes directrices en sécurité infonuagique. Pour ce qui est des normes d'ISO et de la Commission électrotechnique internationale (CEI), elles sont disponibles en format papier à la bibliothèque de HEC Montréal.

2.2 L'infonuagique : définition et catégorisation

D'abord, comme l'infonuagique est au cœur de ce mémoire, il est important de bien la définir, d'en expliquer les principes de base et d'explorer les formes qu'elle peut prendre. Cette section se veut donc un survol de ce qu'est l'infonuagique et de ses différents types et modes de fonctionnement.

2.2.1 Définition de l'infonuagique

Bien que l'infonuagique ait connu un essor spectaculaire pendant la dernière décennie, le principe de base derrière ce concept n'est pourtant pas nouveau. En effet, dès 1961, John McCarthy, un professeur d'informatique à l'université Stanford, propose l'idée que l'informatique devienne éventuellement une commodité payable à l'utilisation comme l'électricité (Erl, Mahmood et Puttini, 2013; Hassan, 2011). L'infonuagique est le résultat de plusieurs avancées, particulièrement du gain d'efficacité de la technologie dû au développement rapide de la capacité des processeurs[9] (Marston *et al.*, 2011). Cette augmentation de la puissance des processeurs a notamment permis la réduction des coûts d'infrastructure et de là, la construction d'immenses centres de données contenant des milliers de serveurs, le tout contribuant ainsi à l'essor et à l'accessibilité de l'infonuagique (Armbrust *et al.*, 2009).

L'augmentation de la capacité des processeurs a permis plusieurs autres avancées en informatique comme la virtualisation, le principe à la base de l'infonuagique (Orman, 2016; Zissis et Lekkas, 2012). La virtualisation est la création d'une plateforme virtuelle ou d'une image d'un élément, que ce soit d'un système d'exploitation, d'un réseau ou d'un serveur de stockage (Laan, 2013). Ce type d'abstraction permet à l'ordinateur d'exécuter plusieurs processus en même temps sans qu'ils interfèrent entre eux (Orman, 2016). Ainsi, la virtualisation permet de partitionner un système en différentes machines virtuelles qui ont chacune leur propre système d'exploitation (Scarfone, Souppaya et Hoffman, 2011). De cette façon, différents utilisateurs peuvent partager la même infrastructure grâce à des machines virtuelles comme le montre la Figure 2.1. Celles-ci sont gérées par l'hyperviseur[10] dont le rôle est d'allouer les ressources disponibles de façon dynamique et de gérer les échanges d'instructions entre ces machines virtuelles (Gordon, 2016). Ainsi, grâce à la virtualisation, le fournisseur de services infonuagiques peut maximiser l'utilisation de ses ressources en les rendant simultanément disponibles à

[9] En 1965, Gordon Moore, qui est devenu plus tard un des fondateurs de l'entreprise de micro-processeurs Intel, a publié un article devenu célèbre dans lequel il a fait la prédiction que le nombre de composantes électroniques utilisées dans la fabrication de micro-processeurs doublerait tous les deux ans. Cette prédiction, qui est connue sous le nom de « Loi de Moore », s'est depuis réalisée et c'est ce qui a permis aux ordinateurs et autres appareils électroniques de se développer de façon exponentielle dans les cinq dernières décennies (Cross, 2016; Waldrop, 2016).

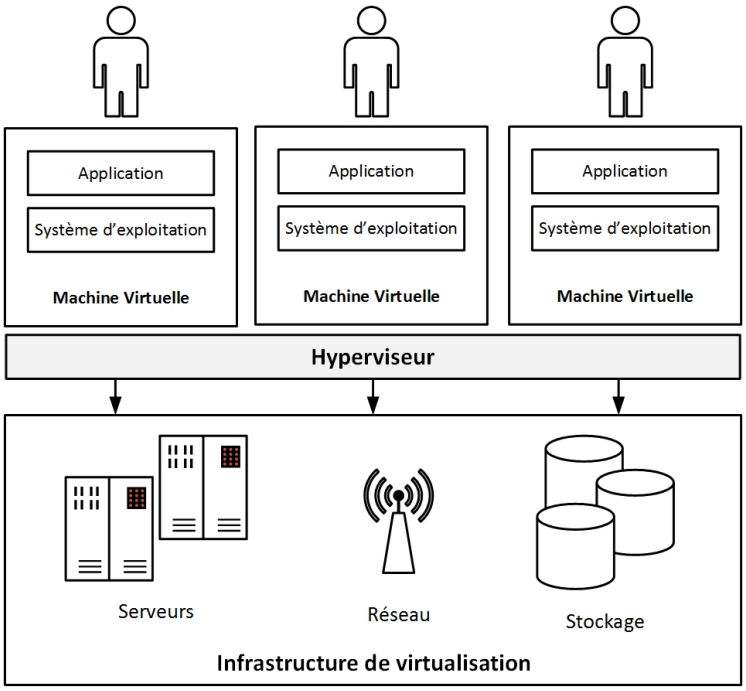
[10] L'hyperviseur est la traduction du terme anglais *hypervisor* (Grand dictionnaire terminologique de la langue française, consulté le 29 juin 2016, http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche= 8350552).

plusieurs utilisateurs qui sont isolés par les frontières virtuelles établies entre les différentes machines.

Un autre facteur qui a permis à l'infonuagique de prendre son essor est le développement des réseaux de communication à haute vitesse, rendant le partage de données plus facile et permettant de connecter les utilisateurs entre eux (Dwivedi et Mustafee, 2010). Cette avancée, jumelée à l'augmentation de la fiabilité des réseaux dans la deuxième moitié des années 1990 (Ball, Colbourn et Provan, 1995), a permis l'adoption et la démocratisation de l'Internet, créant un bassin grandissant de clients potentiels pour les services infonuagiques. Ainsi, les économies d'échelle rendues possibles par le partage des ressources, un principe à la base de l'infonuagique, se sont concrétisées, forçant les gros joueurs de l'industrie informatique à se tourner vers ce nouveau mode d'approvisionnement (Buyya *et al.*, 2009).

Figure 2.1 : Schéma de la virtualisation

(Adaptation de Laan, 2013, p.485)



Bien que le concept de l'infonuagique date des années 1960, le terme *cloud computing* n'est utilisé seulement que depuis les années 1990 (Erl *et al.*, 2013) et il provient du symbole de nuage qui est utilisé en informatique pour représenter l'Internet dans des diagrammes (Zissis et Lekkas, 2012). Il existe plusieurs définitions de ce qu'est l'infonuagique, mais la plupart des auteurs

s'entendent pour utiliser la définition du National Institute of Standards and Technology (NIST), un organisme du gouvernement américain qui veille à promouvoir l'innovation par la mise en place de normes et de métriques (NIST, 2016). Pour les besoins de cette étude, c'est cette définition qui sera utilisée. Ainsi, l'infonuagique est :

> « Un modèle qui permet un accès constant et sur demande à un bassin de ressources informatiques partagées (par exemple, des réseaux, des serveurs, du stockage, des applications et des services) qui peuvent être acquises et déployées rapidement en libre-service avec un effort de gestion minimal » (traduction libre de Mell et Grance, 2011, p.2).

Ainsi, toujours selon le NIST, l'infonuagique repose sur cinq grands principes :

1. **Accessibilité sur demande et en libre-service par l'utilisateur**

   Une fois que l'accord entre l'utilisateur et le fournisseur de services infonuagiques est conclu, l'utilisateur peut accéder au service infonuagique, au besoin et sans intervention humaine (Ali *et al.*, 2015).

2. **Accès par le réseau**

   Le service infonuagique doit être disponible en tout temps via le réseau Internet (Mell et Grance, 2011). Ainsi, avec l'essor des technologies mobiles, l'infonuagique a permis aux employés de l'entreprise d'avoir accès aux applications et aux données à partir de tout appareil disposant d'une connexion Internet.

3. **Mise en commun des ressources**

   Les ressources du fournisseur de services infonuagiques sont mises en commun et partagées dynamiquement entre ses clients grâce à la virtualisation. Cependant, cette architecture est transparente pour l'utilisateur final puisque le partage de ressources n'a pas d'impact sur ce dernier, chaque utilisateur étant isolé des autres par la virtualisation (Erl *et al.*, 2013). Cette colocation permet au fournisseur de maximiser l'allocation de ses ressources entre ses différents clients et d'ainsi rentabiliser son investissement.

4. **Élasticité et rapidité**

   L'utilisateur ne paie que pour le service qu'il utilise et peut rapidement ajouter ou réduire la quantité de ressources infonuagiques qu'il mobilise pour combler ses besoins (Ali *et al.*,

2015). L'infonuagique est donc un mode d'approvisionnement qui offre une grande flexibilité à l'entreprise l'adoptant puisqu'elle peut rapidement ajuster sa consommation de ressources informatiques et ne payer seulement que pour la quantité qu'elle utilise.

5. **Mesure de l'utilisation du service**

   Comme les services infonuagiques sont utilisés sur demande, leur utilisation varie constamment. Ces variations sont mesurées par le fournisseur de façon à allouer les ressources infonuagiques dynamiquement et ainsi optimiser leur utilisation (Mell et Grance, 2011). Elles servent aussi à établir la facturation puisque le service est payable à l'utilisation.

L'infonuagique est en fait un mode d'approvisionnement où le client impartit une partie ou la totalité de son infrastructure, de ses plateformes de développement ou de ses logiciels à un fournisseur. Contractuellement, un accord sur le niveau de service (*Service Level Agreement* ou SLA) permet au fournisseur et au client de s'entendre sur le type et la performance attendue du service, le partage des responsabilités, l'imputabilité et la gouvernance des données (Cloud Security Alliance, 2011; Takabi, Joshi et Ahn, 2010).

2.2.2 Types de services infonuagiques

Quoique la discussion précédente établisse les principes de base de l'infonuagique, il est nécessaire de comprendre que sa mise en œuvre peut varier. On reconnaît généralement qu'il existe trois différents types de services infonuagiques, l'*Infrastructure as a Service* (IaaS), la *Platform as a Service* (PaaS) et le *Software as a Service* (SaaS). Ces types sont importants puisqu'ils définissent les services rendus et la nature de ces derniers a une incidence sur les risques en sécurité de l'information. Afin de comprendre la répartition des responsabilités, il convient de se représenter l'architecture informatique en termes de couches. À la base, il y a la couche physique qui inclut le réseau physique, le stockage et les serveurs. Au-dessus, il y a la couche associée à la plateforme qui comprend le réseau virtuel, le système d'exploitation et le temps d'exécution. Finalement, la couche applicative contient les applications et les données. Pour chaque service infonuagique, la responsabilité et l'imputabilité pour la sécurité des différentes couches sont réparties différemment (Ouedraogo et Mouratidis, 2013). Ainsi, le SaaS héritera des

caractéristiques du PaaS et du IaaS alors que le PaaS héritera des caractéristiques du IaaS seulement (Aguiar, Zhang et Blanton, 2013; Cloud Security Alliance, 2011).

Le premier type est l'*Infrastructure as a Service* (IaaS) qui fournit le matériel (*hardware*) au cœur d'une architecture informatique, tel le stockage, la mémoire, le réseau et les processeurs et ce, généralement à l'aide de technologies de virtualisation (Ali *et al.*, 2015; Hassan, 2011; Mouratidis *et al.*, 2013). Elle permet donc au client de réduire les coûts d'installation et de maintenance de son parc informatique puisque son infrastructure, ou du moins une partie de celle-ci, est impartie à un fournisseur de services. La responsabilité de s'assurer que l'infrastructure et les images virtuelles soient sécuritaires revient au fournisseur puisque c'est ce dernier qui en a le contrôle (Cloud Security Alliance, 2011; Ouedraogo et Mouratidis, 2013). Cette pratique est donc intéressante pour une organisation qui ne souhaite pas investir massivement dans l'achat et la maintenance de matériel informatique (Erl *et al.*, 2013). Le fournisseur détenant actuellement la plus grande part du marché mondial pour l'IaaS est Amazon Web Services, une division du site de commerce en ligne Amazon.com. Vient ensuite Microsoft avec son produit Azure, puis une quinzaine d'autres fournisseurs, comme IBM, VMware et Rackspace, se partagent le reste du marché (Leong, Toombs et Gill, 2015).

Ensuite, il y a la *Platform as a Service* (PaaS) qui permet au client d'utiliser un ensemble d'outils ainsi qu'un environnement de développement d'applications (Ali *et al.*, 2015). La plateforme ainsi offerte permet aux programmeurs de développer, de tester et de mettre à jour des applications et ce, dans un environnement qui permet l'intégration de ces applications entre elles (Kepes, 2016). La compatibilité entre ces applications est donc assurée puisqu'elles utilisent le même langage, les mêmes librairies d'objets et le même ensemble d'outils qui sont tous offerts par le concepteur via le fournisseur de services infonuagiques. Il faut toutefois préciser que ces plateformes offertes en mode infonuagique sont généralement associées à un environnement logiciel spécifique. Donc, la PaaS fournit un écosystème qui permet à une organisation de développer et de déployer rapidement et économiquement des applications puisque l'organisation a accès à une variété d'outils de développement sans avoir à investir dans l'infrastructure sous-jacente (Cloud Security Alliance, 2011). Des exemples de PaaS sont *Google App Engine* de la compagnie américaine Google ou bien *Force.com* de l'entreprise Salesforce qui permettent aux clients de développer leurs propres applications compatibles avec leur

écosystème respectif et ensuite de les vendre ou de les partager avec le reste de la communauté (Kshetri, 2013).

Finalement, le dernier type de services infonuagiques est le *Software as a Service* (SaaS) qui permet au client d'utiliser les applications d'un fournisseur ainsi que de stocker les données qui y sont associées (Cloud Security Alliance, 2011). L'accès au logiciel peut se faire de diverses façons, mais la prédominante est par un navigateur web. Généralement, le logiciel est offert à coût récurrent sous forme de licence pour chacun des utilisateurs. Pour ce type de services infonuagiques, le client ne gère pas l'infrastructure et la plateforme nécessaires à l'utilisation du logiciel car cela est assumé par le fournisseur (Zissis et Lekkas, 2012). En contrepartie, cette façon de faire vient avec des risques de sécurité puisque toutes les données liées aux applications utilisées en mode infonuagique sont logées et traitées par le fournisseur (Ardagna, Asal, Damiani et Vu, 2015). Ainsi, contrairement au type IaaS, le client a moins de contrôle puisqu'il ne peut pas choisir quelles données sont stockées sur les serveurs du fournisseur. Pour certaines entreprises, cela représente une barrière à la transition vers des services infonuagiques parce qu'elles ne souhaitent pas perdre le contrôle sur leurs données (Hashizume, Rosado, Fernández-Medina et Fernandez, 2013). Il existe une panoplie de joueurs dans le marché des SaaS comblant autant des besoins d'affaires que des besoins personnels. D'ailleurs, selon la revue Forbes, la valeur du marché des SaaS s'élevait à 49 milliards de dollars américain l'an dernier (Columbus, 2015). Des exemples de SaaS sont des services de courrier électronique (ex : Gmail ou Outlook Web Access), de rédaction de documents (ex : Google Docs ou Office 365) ou des applications d'affaires (ex : Workday ou Salesforce).

Certains auteurs ou professionnels du milieu ajoutent d'autres catégories de services comme *Process as a Service*, *Hardware as a Service, Data as a Service*, etc. aux trois types de base qui font consensus. Cependant, ces additions peuvent se concevoir comme des sous-types plutôt que des types distincts de services. C'est pour cette raison que pour les besoins de ce mémoire, seuls l'IaaS, la PaaS et le SaaS sont considérés.

2.2.3 Modes d'implantation de l'infonuagique

Peu importe le type de services sélectionné, celui-ci peut être implanté selon quatre différents modes d'infonuagique. On reconnaît en général quatre modes d'implantation de l'infonuagique : public, privé, communautaire et hybride (Mell et Grance, 2011). Tout comme pour le type de services, le mode d'implantation aura un impact important sur le niveau de sécurité des données et des applications utilisées. Le choix d'un mode d'implantation dépendra des besoins de l'organisation en termes de contrôle, de sa tolérance au risque et de l'importance accordée aux données qui sont en cause (Mouratidis *et al.*, 2013).

L'infonuagique publique (*public cloud*) est un mode d'implantation par lequel l'infrastructure est disponible au grand public ou bien partagée entre plusieurs organisations (Rong *et al.*, 2013). Cette infrastructure appartient au fournisseur de services infonuagiques et les clients qui se procurent ses services se la partagent sans connaître l'identité des autres clients qui utilisent les mêmes ressources qu'eux. Il existe donc certains risques de sécurité associés à ce mode d'implantation puisque, comme les ressources sont partagées, une brèche ou une vulnérabilité pourrait potentiellement affecter tous les utilisateurs (Mouratidis *et al.*, 2013). Un autre risque provient du fait que, comme le service entre les différents clients n'est séparé que de façon virtuelle, il est plus facile pour un client malintentionné de profiter de son accès à l'infrastructure pour en exploiter une vulnérabilité et attaquer un autre client (Ouedraogo et Mouratidis, 2013). Malgré les risques, 88 % des entreprises utilisaient l'infonuagique publique en 2015, tous types de services confondus (RightScale, 2015).

Le second mode, l'infonuagique privée (*private cloud*), est considéré comme plus sécuritaire parce que les ressources infonuagiques sont utilisées par une seule entreprise (Ali *et al.*, 2015). Il y a deux possibilités : l'entreprise peut impartir ses ressources informatiques à une tierce partie qui lui fournira une infrastructure dédiée ou bien, l'entreprise peut elle-même mettre en place et gérer ses ressources infonuagiques. Dans le cas où le service est géré par une tierce partie, l'infonuagique privée ressemble beaucoup à de l'hébergement dédié dans un centre de données puisque les ressources sont consacrées seulement à l'organisation et ne sont pas partagées avec d'autres. La différence avec l'hébergement dédié, dans ce cas, réside surtout dans les principes de base de l'infonuagique qui permet l'accessibilité sur demande et en libre-service, l'élasticité et la rapidité. Ainsi, dans le cas de l'infonuagique privée, il n'est pas nécessaire de renégocier avec

le fournisseur chaque fois que des ressources informatiques sont requises ; l'utilisateur n'a qu'à en faire la demande et les ressources sont généralement disponibles en quelques minutes (Bittman, 2016). Les mêmes précautions de sécurité que pour l'hébergement dédié s'appliquent alors.

Dans le second scénario de l'infonuagique privée, l'entreprise gère, par l'entremise de son département TI, l'achat, l'installation et la maintenance du matériel informatique. Les différentes unités d'affaires agissent comme les clients du département TI qui les approvisionnent selon leurs besoins (Cloud Special Interest Group et PCI Security Standards Council, 2013). Il s'agit donc plutôt d'un mode de livraison des ressources informatiques internes plutôt qu'un mode d'approvisionnement. Même si ce mode de livraison peut exercer une grande pression sur les pratiques de gestion internes, les risques de sécurité rattachés à un tel mode de livraison sont très similaires à ceux d'une infrastructure traditionnelle puisque les données demeurent dans l'enceinte de l'entreprise et sont sous son contrôle en tout temps (Gordon, 2016). Puisque ce mémoire traite de la sécurité dans un contexte d'impartition infonuagique, seul le premier cas de figure dans lequel l'organisation impartit le service à un fournisseur externe sera considéré lorsqu'il sera question de l'infonuagique privée.

Même si elle permet une sécurité accrue, l'infonuagique privée commande généralement un coût plus élevé que pour le mode public. Dans le cas où l'entreprise gère elle-même le service, elle doit posséder et gérer son infrastructure et en assumer tous les frais. Dans le cas où elle fait affaire avec une tierce partie, le coût d'avoir un service dédié et les ressources qui l'accompagnent, s'avère plus élevé que pour le mode d'implantation public. Selon un sondage récent, c'est environ 63 % des organisations qui utiliseraient le mode d'implantation privé, les deux scénarios confondus (RightScale, 2015).

Le troisième mode, l'infonuagique communautaire (*community cloud*), ressemble beaucoup au mode privé, sauf qu'au lieu d'avoir des ressources dédiées à une seule entreprise, elles sont partagées parmi un regroupement d'entreprises qui se connaissent et qui ont des objectifs de sécurité ou d'affaires similaires (Zissis et Lekkas, 2012). Généralement, une tierce partie agit comme fournisseur de services infonuagiques pour la communauté. L'avantage d'implanter ce mode d'infonuagique pour un groupe d'entreprises est de profiter d'une sécurité plus grande que

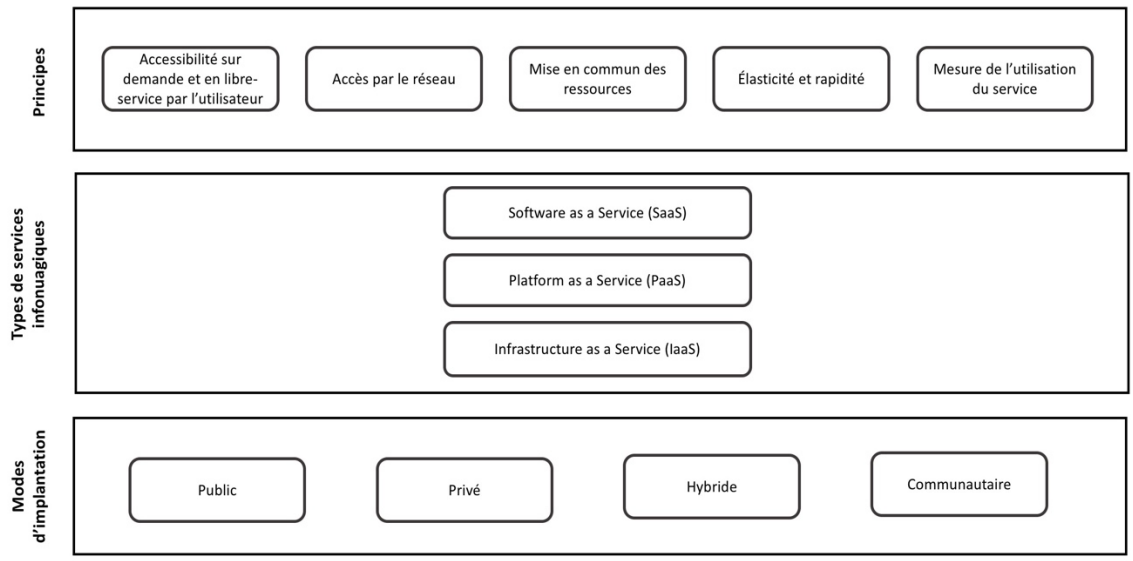
pour l'infonuagique publique car une relation de confiance est déjà établie entre les entreprises faisant partie de la communauté. Elles partagent aussi le coût élevé de l'infrastructure. Cependant, le risque qu'un des clients essaie d'exploiter une vulnérabilité de l'infrastructure est toujours présent.

Finalement, le mode hybride est, comme son nom l'indique, une combinaison des modes privé et public. La mise en place de ce mode implique que l'entreprise fait le choix d'avoir une partie des services livrée dans un mode privé, soit à l'interne ou bien avec l'aide d'un fournisseur, alors que l'autre partie est déployée par l'infonuagique en mode public (Laan, 2013). Le mode hybride permet à l'entreprise de minimiser ses coûts grâce au mode public tout en conservant un certain contrôle sur les données qu'elle juge critiques grâce au mode privé (Rong *et al.*, 2013).

La figure suivante offre un résumé des principes, des types de services et des modes d'implantation de l'infonuagique.

Figure 2.2 : Définition de l'infonuagique, des types et des modes d'implantation

(Traduction libre de Cloud Security Alliance, 2011, p.13)



À la lumière des sections précédentes, on constate que l'infonuagique est un mode d'approvisionnement complexe et que les options sont nombreuses. Loin d'être mutuellement exclusifs, les types de services et les modes d'implantation peuvent être combinés. Le choix de

l'un ou l'autre dépend de plusieurs facteurs, dont la sécurité et l'usage qui en sera fait. Les entreprises ont donc souvent recours à plusieurs fournisseurs pour combler leurs besoins en TI et mitiger les risques de sécurité. La multiplication des types de services et des modes de déploiement fait en sorte que les options quant au choix d'un service infonuagique sont très nombreuses. En outre, les logiciels, les plateformes et l'infrastructure de ces différents fournisseurs choisis doivent avoir un certain degré de compatibilité entre eux. Tous ces services doivent être compatibles pour assurer la fluidité de l'échange de l'information, la collaboration et pour éviter de créer des silos au sein de l'entreprise. Tout cela facilite l'utilisation pour l'utilisateur final pour qui le tout est transparent. L'interopérabilité entre les différents services infonuagiques permet aussi de changer rapidement de fournisseur ou d'ajouter des composantes sans devoir y consacrer de grands efforts d'ingénierie (Cloud Security Alliance, 2011). Ainsi l'augmentation du nombre de services et de fournisseurs infonuagiques risque de rapidement devenir un casse-tête de gestion pour les organisations (Overby, 2016) et cela est sans compter les mesures qui doivent être mises en place pour s'assurer que le tout est sécuritaire.

2.3 Défis spécifiques de sécurité de l'information dans un contexte infonuagique

L'objectif de cette section est d'approfondir le thème de la sécurité de l'information dans un contexte infonuagique puisque ce mode d'approvisionnement donne naissance à des défis spécifiques qu'on ne retrouve pas dans une infrastructure traditionnelle.

Les organismes ISO et CEI définissent la sécurité de l'information de la façon suivante : « [elle] préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate » (ISO/CEI 27001, 2013, p.v). Ainsi, on note que la sécurité de l'information ne se traduit pas en termes technologiques, mais prend la forme d'un processus (Mitnick et Simon, 2002) ; la technologie est un outil qui permet de mettre en place et de gérer les différents processus liés à la sécurité. Ces processus couvrent plusieurs dimensions, allant de la protection physique des locaux de l'entreprise, jusqu'à la gestion des risques et le contrôle des accès (Silic et Back, 2014a). L'objectif de la sécurité de l'information est de « s'assurer de la

continuité des affaires et de minimiser les dommages à l'organisation en limitant les impacts des incidents de sécurité » (traduction libre de von Solms et van Niekerk, 2013, p.98).

Au cœur du concept de la sécurité de l'information se trouvent trois notions : la confidentialité, l'intégrité et la disponibilité de l'information.[11] La confidentialité est la capacité d'une entreprise de limiter l'accès à l'information seulement aux personnes autorisées, alors que l'intégrité est le fait d'être en mesure de préserver la structure et le contenu de l'information dans son entièreté (Ardagna *et al.*, 2015). Finalement, la disponibilité permet de s'assurer que l'information est accessible en continu lorsque requise par une personne autorisée (Ardagna *et al.*, 2015).

Le contexte d'impartition infonuagique crée plusieurs défis de sécurité. Certains sont similaires à ceux qu'on retrouve dans une infrastructure traditionnelle, alors que d'autres sont spécifiques à l'infonuagique. Le tableau suivant dresse un inventaire des défis de sécurité répertoriés dans la littérature, classés selon la triade de la CIA en sécurité de l'information. On peut y voir que les défis de confidentialité touchent surtout la gestion des accès aux données tant du côté du client que du fournisseur. Le défi d'assurer l'intégrité des données utilisées dans un environnement infonuagique réside quant à lui dans les moyens à mettre en place pour prévenir la modification non autorisée. Finalement, les défis en termes de disponibilité comprennent principalement les mesures à prendre pour assurer la surveillance du service et la gestion des incidents de sécurité.

[11] On réfère souvent à ces concepts par le terme CIA, l'acronyme pour les mots anglais *Confidentiality, Integrity* et *Availability*. Cet acronyme sera utilisé dans ce texte lorsqu'il est question de ces concepts.

Tableau 2.1 : Les défis de sécurité de l'information dans un contexte infonuagique

Objectifs de sécurité	Défis de sécurité	Auteurs
Confidentialité	Limiter l'accès aux données confidentielles de l'organisation par les employés du fournisseur de services infonuagiques.	Asghar, Ion, Russello et Crispo (2013); NIST Cloud Computing Standards Roadmap Working Group (2013); Rong *et al.* (2013); Ryan (2013); Takabi *et al.* (2010); Zissis et Lekkas (2012)
	Contrôler l'identité et les accès pour s'assurer que seules les personnes autorisées du côté du client accèdent aux services infonuagiques et aux données.	Aguiar *et al.* (2013); Ali *et al.* (2015); Asghar *et al.* (2013); Cloud Security Alliance (2011); Damiani *et al.* (2007); Dorey et Leite (2011); Kapsalis, Hadellis, Karelis et Koubias (2006); NIST Cloud Computing Standards Roadmap Working Group (2013); Rong *et al.* (2013)
	Limiter les risques liés à la virtualisation et au partage des ressources infonuagiques avec d'autres clients (surtout pour l'infonuagique publique et hybride).	Aguiar *et al.* (2013); Ali *et al.* (2015); Hashizume *et al.* (2013); Ouedraogo et Mouratidis (2013); Rong *et al.* (2013); Ryan (2013); Takabi *et al.* (2010); Zissis et Lekkas (2012)
	Établir une relation de confiance avec le fournisseur.	Kanwal, Masood, Shibli et Mumtaz (2015); NIST Cloud Computing Standards Roadmap Working Group (2013); Zissis et Lekkas (2012)
Intégrité	S'assurer que les données ne soient pas altérées par le fournisseur de services.	NIST Cloud Computing Standards Roadmap Working Group (2013); Rong *et al.* (2013); Zissis et Lekkas (2012)
	Prévenir la perte de données et la modification ou la suppression non autorisées, soit lorsqu'elles sont stockées chez le fournisseur ou en transit entre le client et le fournisseur ou vice versa.	Aguiar *et al.* (2013); Mouratidis *et al.* (2013); Ryan (2013); Zissis et Lekkas (2012)
Disponibilité	Gérer les incidents et les attaques dans un contexte de partage de l'imputabilité et des responsabilités.	Ab Rahman et Choo (2015); Aceto, Botta, Donato et Pescapè (2013); Khansa et Zobel (2014); NIST Cloud Computing Standards Roadmap Working Group (2013)
	Surveiller et contrôler la qualité du service et de la performance / mettre en place des indicateurs de performance.	Aceto *et al.* (2013); Aguiar *et al.* (2013); Armbrust *et al.* (2009); Kanwal *et al.* (2015)

Il ressort du Tableau 2.1 que les défis de la sécurité de l'information s'appliquent aux trois types de services, les SaaS, les PaaS et les IaaS puisqu'ils reposent surtout sur la relation avec le fournisseur. Le contexte d'impartition auquel est associée l'infonuagique pose certains problèmes liés à la gestion de la relation avec le fournisseur. Effectivement, l'organisation cliente souhaite s'assurer que les données qui sont confiées au fournisseur seront traitées et stockées de façon aussi sécuritaire que si elle ne les impartissait pas. Puisque les données sont stockées chez le fournisseur, le client doit s'assurer que seules les personnes autorisées auront accès à ses données tant de son côté que du côté du fournisseur (Takabi *et al.*, 2010). Au-delà de la gestion des accès, l'organisation voudra aussi s'assurer qu'elle aura accès à ses données en tout temps et que le fournisseur n'altérera ou n'effacera pas les données qui lui sont confiées. Tous ces défis sont propres à n'importe quel contexte d'impartition informatique, pas seulement pour l'infonuagique.

Puisque l'entreprise est légalement responsable de la bonne gestion de ses données, il semble normal qu'une des plus grandes inquiétudes de celles qui décident de faire le saut vers l'infonuagique soit la perte de contrôle sur leurs données (Al Morsy, Grundy et Müller, 2010; Ardagna *et al.*, 2015; Dorey et Leite, 2011). En effet, comme les données utilisées dans un contexte infonuagique peuvent être traitées ou entreposées chez le fournisseur, l'entreprise n'a pas autant de contrôle qu'avec une infrastructure traditionnelle, ce contexte dans lequel elle décide elle-même où ses données sont logées et qui y a accès. Certaines entreprises ont donc peur de perdre le contrôle sur la confidentialité et l'intégrité de leurs données en déplaçant leurs activités vers le mode infonuagique.

Le présent chapitre s'est ouvert sur les mécanismes qui ont permis l'essor de l'infonuagique et parmi ceux-ci, il y avait la virtualisation qui permet de partager des ressources informatiques en créant des machines virtuelles. La virtualisation n'a pas que des avantages et amène son lot de défis de sécurité parce qu'il doit y avoir une ségrégation entre les machines virtuelles afin d'assurer la confidentialité des données de chacun des clients (Aguiar *et al.*, 2013; Ali *et al.*, 2015). Si les machines virtuelles ne sont pas isolées de façon convenable, un des clients pourrait, par inadvertance, avoir accès aux données d'une autre organisation qui partage la même infrastructure ou bien pourrait planifier une attaque (Aguiar *et al.*, 2013). En effet, lorsqu'une machine virtuelle est compromise, les autres alors deviennent vulnérables aux attaques (Ali *et al.*,

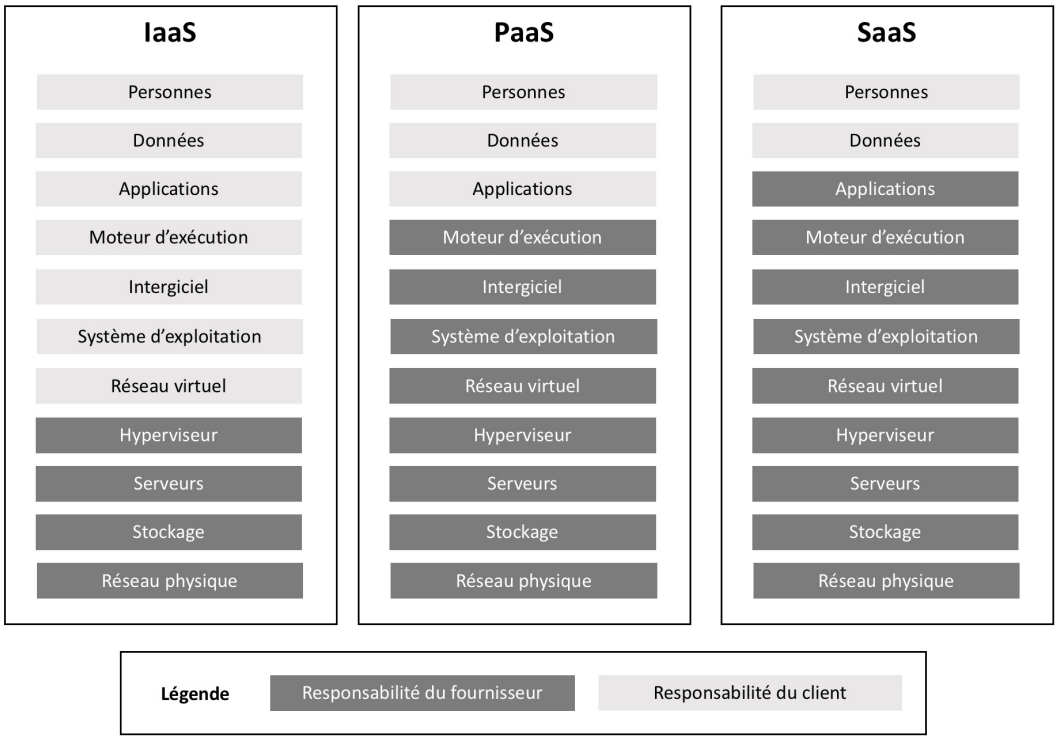
2015). La mise en commun des ressources du fournisseur est donc une autre source d'inquiétude pour les clients.

Tous les défis mentionnés dans les paragraphes précédents sont liés à la relation de confiance que le client a avec son fournisseur. La confiance signifie que l'organisation a la certitude que le fournisseur sera en mesure de fournir le service selon les termes entendus, y compris les requis touchant la sécurité (Zissis et Lekkas, 2012). Les frontières de responsabilité entre l'organisation cliente et le fournisseur permettent de définir la division des responsabilités entre les deux parties, un aspect essentiel de la sécurité infonuagique (NIST Cloud Computing Standards Roadmap Working Group, 2013). Il est important de mentionner que le concept de confiance n'est pas spécifique à l'infonuagique, mais à toutes les relations avec des fournisseurs qui manipulent des données confidentielles.

La division des responsabilités dans une relation d'impartition infonuagique est d'ailleurs la source de plusieurs défis. La Figure 2.3 montre comment les responsabilités sont séparées entre le client et le fournisseur selon les types de services. Tel que mentionné précédemment, l'infrastructure informatique peut être illustrée comme étant constituée de plusieurs couches qui sont toutes liées entre elles. On y voit que les responsabilités varient d'un type de services à l'autre : le type SaaS donnant la plus grande partie des responsabilités au fournisseur, alors que pour le IaaS, la majeure partie des responsabilités incombe plutôt à l'organisation. Les responsabilités dans un environnement infonuagique doivent être très bien définies afin de s'assurer que le fournisseur ait mis en place des mécanismes de sécurité, des processus de gestion des vulnérabilités et de la surveillance suffisants pour les couches sur lesquelles il exerce son contrôle. De plus, en cas d'incident, puisque le contrôle entre les multiples couches est divisé, le client et le fournisseur doivent avoir des processus intégrés qui leur permettent de travailler ensemble pour remédier à l'incident. Par exemple, le client et le fournisseur s'entendront sur les personnes à contacter en cas d'incident, le canal de communication à privilégier, les étapes à exécuter, les personnes responsables, etc. La gestion des vulnérabilités et des incidents de sécurité doit donc se faire en partenariat, ce qui peut représenter un certain défi de collaboration et de communication, surtout considérant qu'un fournisseur d'infonuagique publique peut avoir jusqu'à des milliers de clients qui se partagent ses ressources informatiques (Munteanu,

Edmonds, Bohnert et Fortis, 2014). On peut imaginer la complexité des processus de gestion des incidents dans un tel contexte.

Figure 2.3 : Partage des responsabilités selon le type de services infonuagiques[12, 13]
(Traduction libre de Riley, 2016, p.3)



En conclusion, les défis de sécurité spécifiques à l'infonuagique sont en grande partie liés à la virtualisation, à la division des responsabilités et au contrôle des données. Ces défis ne sont pas nécessairement plus complexes que les défis qu'on retrouve dans une infrastructure traditionnelle ; ils sont simplement différents. À cause de la relative nouveauté de l'infonuagique, ces défis font souvent peur aux organisations, mais il existe cependant des solutions qui peuvent être mises en place pour y faire face et mitiger les risques associés à l'infonuagique.

[12] Le terme moteur d'exécution utilisé dans la figure est la traduction du mot anglais *runtime*. Il s'agit de la « version minimale d'un langage de programmation, contenant le code nécessaire à l'exécution des applications qui ont été développées avec ce langage » (Grand dictionnaire terminologique, de la langue française, consulté le 25 novembre 2016, http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8385820)

[13] Le terme intergiciel utilisé dans la figure est la traduction du mot anglais *middleware*, communément utilisé pour désigner des logiciels intermédiaires entre les applications d'un système (Grand dictionnaire terminologique, de la langue française, consulté le 29 juin 2016, http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8354286).

2.4 Solutions proposées pour faire face aux défis en sécurité infonuagique

Plusieurs solutions ont été proposées tant par le milieu académique que par l'industrie pour tenter de surmonter les défis liés à l'infonuagique. Comme mentionné précédemment, la sécurité est définie par des processus qui sont appuyés par des outils technologiques. Pour refléter cette définition, les solutions recensées dans la littérature ont été divisées en deux grandes catégories, soit les solutions liées aux processus de l'organisation et celles qui sont de nature technologique. Dans le cas des solutions processuelles, on parle d'activités qui visent à bonifier les processus de sécurité actuellement en place dans l'organisation. Pour ce qui est des solutions technologiques, elles correspondent à des fonctionnalités, des systèmes, des outils ou des logiciels qui peuvent aider à améliorer la sécurité des services infonuagiques.

Le tableau ci-dessous présente les solutions recensées dans la littérature pour tenter de mitiger les risques de sécurité liés à l'utilisation de services infonuagiques. On y voit que les solutions processuelles sont liées au choix du fournisseur, à la mise en place de normes et de certifications ainsi qu'à la surveillance et aux audits pour s'assurer que le fournisseur se conforme aux exigences du contrat. Parmi les solutions techniques, il y a le chiffrement qui revient très fréquemment dans la littérature, les mécanismes de gestion des accès, les mécanismes de protection imbriqués dans le matériel informatique ou le navigateur web, et l'utilisation de tiers de confiance. Tous ces éléments sont expliqués plus en détail à la suite du Tableau 2.2.

Tableau 2.2 : Les solutions proposées en sécurité de l'information dans un contexte info-nuagique

Type de solution	Nom de la solution	Auteurs
Processuelle	Choix du fournisseur	Dorey et Leite (2011); Ouedraogo et Mouratidis (2013); Patiniotakis, Verginadis et Mentzas (2015); Tang et Liu (2015)
	Mise en place de normes et obtention de certifications	Ab Rahman et Choo (2015)
	Audits et mise en place de mécanismes de contrôle et de surveillance pour assurer la gouvernance	Aceto *et al.* (2013); Ouedraogo et Mouratidis (2013); Rebollo, Mellado, Fernández-Medina et Mouratidis (2015); Rong *et al.* (2013); Tang et Liu (2015)
Technique	Mécanismes de contrôle des accès et d'authentification	Asghar *et al.* (2013); Dorey et Leite (2011); Gordon (2016); Hashizume *et al.* (2013); Kapsalis *et al.* (2006); Wang, Yi, Bertino et Sun (2016); Zissis et Lekkas (2012)
	Chiffrement des données	Ali *et al.* (2015); Cloud Security Alliance (2011); Damiani *et al.* (2007); Dorey et Leite (2011); Hashizume *et al.* (2013); Rong *et al.* (2013); Ryan (2013); Wang *et al.* (2016); Zissis et Lekkas (2012)
	Mécanismes de sécurité imbriqués dans le matériel (*hardware-anchored security*)	Ryan (2013)
	Mécanismes de sécurité imbriqués dans le logiciel de navigation web	Aguiar *et al.* (2013)
	Utilisation de tiers de confiance (*Trusted cloud computing platform / Trusted third party)*	Hashizume *et al.* (2013); Rizvi, Cover et Gates (2014); Zissis et Lekkas (2012)

Parmi les solutions liées aux processus de l'organisation, on recommande d'abord de réduire les risques en amont lors de la sélection du fournisseur. Pour ce faire, les auteurs suggèrent des cadres de référence, des méthodes de sélection ou des listes d'éléments essentiels à considérer pour le choix d'un fournisseur. De plus, certaines entreprises décident de procéder à un audit du fournisseur potentiel avant la signature du contrat afin de s'assurer de ses bonnes pratiques. Les audits permettent aussi de s'assurer de la conformité du fournisseur aux lois en vigueur (Cloud Security Alliance, 2011). Alternativement, pour s'assurer que le fournisseur est légitime, de plus en plus d'organismes proposent des certifications de qualité. Ces certifications ne remplacent pas

les principes de vérification diligente que devrait mener le client avant de faire affaire avec un fournisseur, mais elles peuvent être utiles pour effectuer un tri parmi l'abondance dans l'offre de services infonuagiques.

Au-delà des processus effectués avant la signature du contrat avec le fournisseur, plusieurs auteurs recommandent de conduire des audits aussi pendant la prestation des services afin de s'assurer que ceux-ci correspondent aux requis dans les clauses de l'entente avec le fournisseur (*service level agreement* ou SLA). Comme on impartit un service vers un fournisseur externe, il est important de conserver une certaine visibilité sur les pratiques de ce dernier et sur les données de l'organisation. Le client doit s'assurer que le fournisseur fait l'objet d'un audit externe, indépendant et fréquent en plus d'exiger d'avoir la preuve de conformité qui en résulte afin de s'assurer que les clauses de performance du définies dans le SLA soient bien respectées (Tang et Liu, 2015).

En ce qui a trait à la deuxième grande catégorie de solutions, celle touchant l'aspect technologique, la gestion des accès est primordiale pour assurer un contrôle sur les personnes qui peuvent voir ou traiter les données. Le client est responsable de gérer les accès de ses employés aux services infonuagiques et aux données associées. Cela va de soi pour tous les systèmes et non pas spécifiquement dans le cas de l'infonuagique. La solution infonuagique choisie doit être compatible avec les outils internes ainsi que les mécanismes et les politiques de gestion des identités comme le service d'annuaire[14] de l'organisation, les privilèges d'accès et les différents groupes d'utilisateurs auxquels sont associés ces privilèges. Avec la multiplication des services infonuagiques dans l'entreprise, cette intégration devient essentielle pour éviter les multiples connexions à chacun des services (Dorey et Leite, 2011) et ainsi éviter, au niveau de la gestion des accès, d'avoir à gérer individuellement les comptes et les permissions pour chacun des services. Sans cette intégration, on peut imaginer le cauchemar que représenterait la gestion des comptes de milliers d'employés pour des centaines d'applications. L'intégration simplifie l'utilisation des services pour les utilisateurs et les administrateurs et fait en sorte que les employés n'ont pas à se souvenir de plusieurs identifiants et mots de passe. De plus, l'intégration des politiques d'accès

[14] Le service d'annuaire est « un service centralisé qui regroupe les noms et les adresses des utilisateurs, ainsi que les adresses des ordinateurs et des ressources accessibles sur un réseau » (Grand dictionnaire terminologique de la langue française, consulté le 3 septembre 2016, http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8362254). Un des services d'annuaire les plus connus est l'*Active Directory* de Microsoft.

de l'entreprise aux services infonuagiques facilite l'arrivée de nouveaux employés puisqu'ils reçoivent automatiquement les accès aux applications dont ils ont besoin selon le poste qu'ils occupent. Pour les mêmes raisons, le processus de retrait des accès est plus simple lorsqu'un employé quitte l'organisation.

Toujours d'un point de vue technique, le chiffrement des données est de loin la solution qui revient le plus souvent dans la littérature. Il s'agit d'une procédure par laquelle la donnée est convertie, grâce à l'utilisation d'une clé de chiffrement, dans un format qui ne peut être compris que par les personnes possédant cette clé (Yi, Paulet et Bertino, 2014). À titre d'exemple, chaque lettre d'un fichier texte serait remplacée par un caractère différent selon un algorithme et une clé établie à l'avance. Le récipiendaire du fichier devra connaître cet algorithme et posséder la clé pour déchiffrer le fichier et ainsi consulter le contenu original. Des logiciels informatiques font automatiquement le chiffrement et le déchiffrement des fichiers, ce qui permet d'augmenter le niveau de confidentialité des données, à condition que les clés demeurent secrètes.

Ensuite, les mécanismes de protection présentement utilisés pour sécuriser les échanges de données confidentielles via les sites Internet et qui sont directement imbriqués dans le navigateur peuvent contribuer à protéger principalement les SaaS et même les PaaS, puisque l'accès à la plupart de ces services se fait grâce à un navigateur. Ces mécanismes se traduisent par l'utilisation de certificats numériques qui permettent, d'une part, d'authentifier le fournisseur et, d'autre part, de valider son identité (Winnard, von dem Bussche, Choi et Rossi, 2016). Pour ce faire, on doit avoir recours à une tierce partie de confiance (*trusted third party*). Cette tierce partie est aussi appelée une autorité de certification et gère l'émission de certificats numériques. L'utilisation de certificats numériques se fait selon le processus suivant : le fournisseur de l'application infonuagique doit d'abord se procurer, auprès d'une autorité de certification reconnue, un certificat numérique qui est chiffré avec la clé privée de l'autorité de certification[15] (Dubé et Bernier, 2011). Ce certificat contient plusieurs informations dont le nom du détenteur (donc du fournisseur) et sa clé publique. Si on suit la logique du chiffrement asymétrique, cela

[15] Il existe deux types de clés de chiffrement : privée et publique. La clé privée est secrète sauf pour son propriétaire alors que la clé publique « est connue de tous les partenaires qui veulent échanger avec le propriétaire de la clé privée » (Dubé et Bernier, 2011, p.253). Un système de chiffrement qui utilise les deux types de clés est appelé asymétrique. Pour le chiffrement asymétrique, « [si] un message est codé avec une clef publique, seul celui qui détient la clé privée qui lui est liée peut le décoder » (Dubé et Bernier, 2011, p.253).

implique qu'il faut détenir la clé publique de l'autorité de certification pour déchiffrer le certificat numérique et pour voir son contenu. Les clés publiques des principales autorités de certification sont déjà connues des navigateurs web ce qui leur permet de déchiffrer le certificat numérique reçu et ainsi s'assurer que la clé publique qui sera utilisée provient bel et bien du fournisseur de services (Dubé et Bernier, 2011). Un échange de clé privée s'ensuivra ce qui permettra de lancer une session pendant laquelle les échanges entre l'utilisateur et le fournisseur seront sécurisés (Bella, Giustolisi et Lenzini, 2013).

Les solutions présentées dans le tableau précédent s'appliquent aux trois types de services infonuagiques. La seule exception sont les mécanismes de sécurité imbriqués dans le navigateur qui s'emploient principalement pour les SaaS et les PaaS puisque les applications infonuagiques sont souvent accédées à l'aide d'un navigateur Internet. Toutes les solutions s'appliquent autant au mode privé qu'au mode public.

Un autre élément qu'il est important de rappeler ici sont les raisons principales pour lesquelles les entreprises se tournent vers l'impartition : soit parce qu'elles n'ont pas les capacités de rendre elles-mêmes le service ou bien parce qu'il est moins coûteux et plus avantageux de l'impartir. L'infonuagique permet une grande flexibilité et un déploiement rapide. Or, si une organisation ne peut faire confiance à son fournisseur de services infonuagiques et qu'elle met en place un grand nombre de processus ou de mécanismes de sécurité pour protéger les services impartis, cela va à l'encontre de l'objectif de base de l'infonuagique. L'organisation en question se trouve à investir un nombre important de ressources dans la gestion de ce service alors, qu'à la base, elle souhaitait plutôt le confier à un fournisseur. Ainsi, bien que plusieurs solutions de sécurité existent, elles ne sont souvent pas alignées avec les objectifs principaux de l'infonuagique qui sont la réduction des coûts, la flexibilité et la rapidité. En outre, en suivant cette logique, plus le nombre de services infonuagiques est élevé, plus cela risque de représenter un casse-tête pour la gestion de la sécurité. C'est pour cette raison qu'une solution comme les CASB représente un si grand potentiel pour la sécurité des organisations. Ils permettraient de centraliser et d'automatiser la gestion des processus de sécurité liés à l'utilisation des services infonuagiques.

L'infonuagique pose donc certains défis en ce qui a trait à la sécurité de l'information. Plusieurs entreprises sont nerveuses à l'idée de céder une partie du contrôle de leurs TI à un fournisseur.

Cependant, il ne faut pas oublier que, contrairement à la plupart des organisations clientes, les fournisseurs infonuagiques devraient posséder une expertise particulière en sécurité de l'information puisqu'ils se doivent d'assurer un niveau de sécurité qui correspond aux exigences de leurs clients car leur capacité à attirer de nouveaux clients et à les retenir pour assurer leur profitabilité en dépend. Par contre, peu importe le type ou le mode d'implantation, le client conserve toujours la responsabilité de ses données (Riley, 2016) et il est de sa responsabilité de s'assurer que le fournisseur mette en place les mécanismes nécessaires pour les protéger (Aceto *et al.*, 2013). Le choix d'un fournisseur est, en conséquence, très important et ne doit pas être fait à la légère. Malgré tout, il ne faut pas voir l'infonuagique comme une solution plus risquée qu'une infrastructure traditionnelle, mais plutôt accepter que les risques soient différents et choisir des solutions processuelles et technologiques en conséquence. Chaque entreprise est différente et ses besoins en sécurité le sont aussi. Il est essentiel qu'avant de prendre toute décision liée à l'impartition de ses TI, que ce soit pour l'infonuagique ou pour une solution plus traditionnelle (comme l'hébergement), l'organisation fasse un inventaire de ses besoins afin de faire un choix qui assure un niveau de risque avec lequel elle est confortable (Mouratidis *et al.*, 2013).

2.5 Aperçu des normes actuelles de sécurité infonuagique

En plus des solutions proposées, il existe des pratiques d'excellence en sécurité de l'information qui aident les entreprises à adopter des comportements sécuritaires dans un contexte d'impartition infonuagique. Ces pratiques sont souvent présentées sous forme de normes ou de lignes directrices et elles sont complémentaires aux solutions présentées dans la section précédente. L'examen de ces pratiques aide à comprendre les objectifs globaux que les CASB visent à atteindre. Les paragraphes suivants présentent quelques-unes de ces normes parmi les plus populaires qui peuvent aider les entreprises à mettre en place un cadre de gouvernance en sécurité de l'information.

Le développement et la publication de normes se sont faits progressivement. Suite à l'augmentation du taux d'adoption de l'infonuagique dans les organisations pendant la deuxième moitié des années 2000, les entreprises et les professionnels du milieu des TI ont pris conscience de la nécessité de développer des cadres de référence et des outils pour guider les entreprises se tournant vers ce mode d'approvisionnement. En effet, même s'il existait à l'époque des lois et des

normes relatives à l'impartition de services TI, aucune n'adressait les spécificités de l'infonuagique,[16] laissant les fournisseurs et les clients s'autoréguler (Borenstein et Blake, 2011).

Devant la lenteur des gouvernements à légiférer en matière d'infonuagique, certains organismes à but non lucratif ont tenté d'ajuster le tir en publiant des normes ou des lignes directrices qui visent directement ou englobent les services infonuagiques. L'objectif derrière la mise en place de normes et de lignes directrices est de faciliter l'adoption de l'infonuagique en la rendant sécuritaire et en simplifiant l'interopérabilité entre les différents fournisseurs (Cloud Security Alliance, 2011; Rojas, 2014). Le résultat est, qu'à ce jour, il existe une quinzaine d'organismes qui ont publié des lignes directrices relatives à l'infonuagique (European Telecommunication Standards Institute, 2013). Les efforts en ce sens sont donc très fragmentés ce qui s'explique par l'absence d'un organisme international largement reconnu qui réglementerait et encadrerait l'utilisation de l'infonuagique (Emison, 2013). Dans ce contexte où il règne beaucoup de confusion, tant les clients que les fournisseurs de services infonuagiques se retrouvent laissés à eux-mêmes pour identifier les pratiques à adopter et pour développer des cadres de gouvernance de sécurité liés l'utilisation de l'infonuagique.

Dans le but de demeurer succinct, seules les recommandations de trois organismes sont présentées dans ce mémoire : 1) les lignes directrices de la Cloud Security Alliance (CSA), 2) les normes de l'Organisation internationale de la normalisation (ISO) développées conjointement avec la Commission électrotechnique internationale (CEI) et 3) les recommandations du National Institute of Standards and Technology (NIST). Elles ont toutes trois été choisies principalement parce que ce sont les normes et les lignes directrices les plus fréquemment adoptées par les entreprises pour encadrer leur utilisation de l'infonuagique (Tang et Liu, 2015). Il faut noter que ces normes ont été développées en parallèle et qu'elles montrent souvent des similitudes.

Les recommandations émises sont généralement issues du bon sens en matière de gestion de la relation avec les fournisseurs ou de la sécurité des TI. Elles se veulent un langage commun entre

[16] Il faut toutefois noter que maintenant il existe notamment la *Loi sur la protection des renseignements personnels dans le secteur privé* au Québec et, l'équivalent canadien, la *Loi sur la protection des renseignements personnels et les documents électroniques* pour les autres provinces. Ces lois n'abordent pas spécifiquement le cas de l'infonuagique, mais les données échangées dans un environnement infonuagique y sont tout de même assujetties.

les fournisseurs et les clients afin que l'adoption de services infonuagiques se fasse de façon sécuritaire. La mise en place de normes dans une industrie permet d'assurer la compatibilité entre les services et de créer des bases uniformes pour évaluer leur sécurité et leur qualité (Rojas, 2014). Ce dernier point augmente la confiance envers le mode d'impartition qu'est l'infonuagique et a le potentiel de faciliter son adoption.

Plusieurs organisations utilisent ou s'inspirent de ces normes pour établir leurs exigences de gouvernance en termes de sécurité infonuagique. Ces normes sont souvent perçues dans le milieu comme un certain gage de qualité et c'est ce qui pousse souvent les organisations à s'y conformer (Cavusoglu, Cavusoglu, Son et Benbasat, 2015; Siponen et Willison, 2009). À cause du type d'information souvent confidentielle qu'elles traitent, les organisations du domaine de la finance et de l'assurance sont nombreuses à mettre en œuvre des normes pour encadrer leur utilisation de l'infonuagique dans une logique essentielle de gestion des risques. Il est nécessaire de faire l'examen de ces normes et de ces lignes directrices afin de pouvoir comprendre les pratiques de sécurité de l'information mises en place dans les organisations dans un contexte infonuagique et comment le tout pourrait se traduire en termes de fonctionnalités pour les CASB.

Les prochains paragraphes décrivent brièvement chacun des organismes et le contenu de leurs normes ou lignes directrices. En premier lieu, celles de la Cloud Security Alliance sont présentées puisqu'elles furent chronologiquement le premier effort visant à établir des pratiques exemplaires pour ce mode d'impartition. Ce sont des lignes directrices spécifiques à l'infonuagique, mais faites à un très haut niveau. Dans un deuxième temps, les normes ISO/CEI sont présentées. Les normes en sécurité de l'information de cet organisme datent déjà de plusieurs années, mais ce n'est que récemment qu'il les a mises à jour par le biais de deux documents spécifiques à la sécurité dans un contexte d'utilisation de l'infonuagique. Les dernières recommandations, celles du National Institute of Standards and Technology, proviennent de plusieurs publications discutant de divers sujets liés à l'infonuagique comme la virtualisation ou l'implantation de services infonuagiques.

2.5.1 Lignes directrices de la Cloud Security Alliance (CSA)

Devant la popularité grandissante des services infonuagiques dans les années 2000, l'industrie des TI a ressenti le besoin de mettre en place des moyens d'uniformiser les pratiques. De ce besoin est née la Cloud Security Alliance (CSA), un organisme international sans but lucratif, formé de fournisseurs, de clients et même d'individus qui ont un intérêt envers la sécurité infonuagique (Messmer, 2009). Cet organisme vise à proposer et à promouvoir des pratiques d'excellence en sécurité infonuagique (Cloud Security Alliance, 2016a). La réputation de la CSA a grandi au fil des années, notamment grâce à l'adhésion de membres notoires qui participent aux travaux comme Microsoft, VMware ou Cisco (Cloud Security Alliance, 2016b).

En 2009, la CSA a publié le document intitulé *Security Guidance for Critical Areas of Focus in Cloud Computing,* formulant des recommandations en sécurité infonuagique. Ces lignes directrices, qui en sont présentement à leur troisième version, sont disponibles gratuitement sur le site Internet de la CSA.[17] Celles-ci sont divisées en quatorze sections portant sur différents aspects de la sécurité infonuagique et chacune des sections est développée et révisée par un groupe d'experts en la matière (Cloud Security Alliance, 2011).

La première section de ces lignes directrices explique toute l'architecture technologique sous-jacente à l'infonuagique en définissant les types de services et les modes d'implantation. Les trois sections suivantes discutent des implications de gouvernance, de conformité et juridiques associées à l'utilisation des services infonuagiques. La cinquième section aborde les risques pour la sécurité des données. La section suivante évoque tous les problèmes de compatibilité qui peuvent survenir entre les services infonuagiques, mais aussi avec les autres systèmes déjà en place dans l'organisation. Dans cette section, la CSA fait valoir l'importance d'utiliser des technologies standards pour stocker et traiter les données. Les quatre sections qui suivent discutent respectivement de la continuité des affaires, de l'exploitation des centres de données, de la gestion des incidents et du développement sécuritaire. La onzième section porte sur le chiffrement et la gestion des clés de chiffrement, un élément très important lorsqu'il est question d'assurer la confidentialité des données. La section suivante discute de la gestion des identités et des accès aux services infonuagiques alors que la treizième section offre des recommandations

[17] https://cloudsecurityalliance.org/ (page consultée le 26 octobre 2016).

pour mitiger les risques associés à la virtualisation. Finalement, la dernière section s'intitule *Security as a Service* et offre des recommandations pour l'impartition des processus de sécurité infonuagique à une tierce partie. L'Annexe B présente chacune des quatorze sections contenues dans les lignes directrices de la CSA avec des exemples de quelques recommandations pour chacune.

Les lignes directrices de la CSA se veulent d'abord éducatives beaucoup plus que normatives. Elles sont formulées à un haut niveau : elles ne suggèrent pas de moyens techniques pour assurer la protection de l'environnement infonuagique. Elles ne proposent pas, par exemple, un algorithme de chiffrement spécifique, mais se contentent de recommander de suivre les meilleures pratiques du marché. Donc, il s'agit plutôt d'un guide à l'intention des gestionnaires qui sont en charge des décisions quant à l'impartition de services. Elles mentionnent les points importants à prendre en considération d'un point de vue légal, des processus et de la protection des données. Le peu de profondeur des lignes directrices de la CSA en fait un bon point de départ pour une organisation qui souhaite en apprendre davantage sur la sécurité de l'information dans un contexte infonuagique, mais elles n'expliquent pas comment opérationnaliser les pratiques de sécurité.

En plus du document présentant les lignes directrices, la CSA a publié une matrice qui permet aux entreprises qui souhaitent se tourner vers l'infonuagique de déterminer le niveau de risque d'un fournisseur (Cloud Security Alliance, 2014). Cette matrice se base sur les lignes directrices de la CSA, mais elle fait aussi le lien avec d'autres normes de l'industrie comme celles d'ISO/CEI ou avec des articles de lois spécifiques comme la *Loi sur la protection des renseignements personnels et les documents électroniques* du gouvernement canadien. Le document de la CSA, disponible gratuitement sur son site Internet,[18] propose plus d'une centaine de contrôles et indique à quel type de services infonuagiques ils s'appliquent. De plus, il spécifie si la responsabilité de se conformer au contrôle incombe au client ou au fournisseur. Cette matrice peut donc s'avérer d'une aide précieuse pour une entreprise qui tente d'élaborer ses propres exigences de sécurité infonuagique. Néanmoins, bien que l'objectif de cette matrice soit d'aider à mettre en place les lignes directrices de la CSA qui elles s'avèrent plutôt théoriques, elle contient plus de 150 questions à poser à un fournisseur de services infonuagiques avant de signer une entente avec

[18] Le lecteur intéressé par le détail de cette matrice peut la retrouver à l'adresse suivante : https://cloudsecurityalliance.org/group/cloud-controls-matrix/ (page consultée le 28 août 2016).

celui-ci. Il s'agit donc d'un document très lourd et difficile à mettre en œuvre puisque toutes les questions ne s'appliquent pas à tous les contextes organisationnels possibles. Certains contrôles sont de nature très technique et on peut imaginer la difficulté de devoir passer au travers d'un tel document avec chacun des fournisseurs de services avec lesquels une organisation souhaiterait faire affaire.

2.5.2 Normes ISO/CEI 27017 et 27018

L'Organisation internationale de la normalisation (ISO) et la Commission électrotechnique internationale (CEI) sont deux organismes indépendants, mais qui, par des comités techniques conjoints, élaborent des normes internationales encadrant différents domaines (ISO/CEI 27001, 2013). Les comités techniques sont composés d'experts proposés par les 163 pays membres d'ISO (ISO, 2016a, c).

Le développement des normes doit suivre un processus transparent et ces normes doivent faire consensus auprès des membres (ISO/CEI, 2016). Pour cette raison, ces normes sont très respectées dans une variété de domaines, dont les TI (ISO, 2016b). Comme ISO est un organisme à but non-lucratif, il finance ses travaux avec les cotisations de ses membres et avec la vente de ses normes (ISO, 2016d).[19]

Puisque les normes touchent à différents domaines, elles sont regroupées en plusieurs familles auxquelles on a attribué un numéro. Ainsi, toutes les normes liées à la sécurité de l'information dans les entreprises comportent le numéro 27000. La norme 27001 mentionne les exigences liées à la sécurité de l'information dans les entreprises alors que la norme 27002 présente les bonnes pratiques pour mettre en place ces exigences (ISO/CEI 27001, 2013; ISO/CEI 27002, 2013). Ces deux normes ont été publiées en 2005, puis révisées en 2013. Elles ne sont pas spécifiques à une technologie en particulier, mais s'appliquent plutôt à l'ensemble des TI.

Par la suite, comme l'infonuagique implique certaines différences par rapport à l'informatique traditionnelle et dans le but de refléter ces différences, ISO/CEI a émis en 2015, une nouvelle norme 27017 qui est spécifique à l'infonuagique et basée sur les recommandations déjà

[19] Une copie des normes est disponible à la bibliothèque Myriam et J.-Robert Ouimet de HEC Montréal.

contenues dans la norme 27002 (ISO/CEI 27017, 2015). En plus de cette dernière, il existe aussi une norme 27018 qui se penche sur la protection des données personnelles dans un environnement d'infonuagique publique (ISO/CEI 27018, 2014).

Les deux nouvelles normes (27017 et 27018) constituent en quelque sorte une interprétation des travaux précédents, appliquée spécifiquement au contexte infonuagique. Elles sont en quelque sorte des addendas à la norme 27002, c'est-à-dire que tous les contrôles de 27002 s'appliquent aussi à l'infonuagique, en plus des recommandations spécifiques contenues dans chacune des normes 27017 et 27018. Le tableau de l'Annexe C relève les recommandations spécifiques à l'infonuagique qui sont tirées de ces deux dernières normes. Les normes ISO/CEI adoptent un point de vue objectif puisqu'elles tiennent compte autant des responsabilités et des obligations du client que celles du fournisseur. Par contre, comme ce mémoire se concentre sur la perspective de l'organisation qui adopte les services infonuagiques, l'Annexe C ne contient que la perspective du client.

Les normes ISO/CEI en termes de sécurité infonuagique sont divisées en quatorze sections couvrant plusieurs fonctions de l'entreprise, allant des ressources humaines à l'exploitation. Il faut garder en tête qu'elles suivent la même structure que la norme 27002 qui se voulait un guide complet sur la sécurité de l'information organisationnelle. Plusieurs des sections sont semblables à celles de la CSA, par exemple : la gouvernance en sécurité, la conformité, la gestion des accès, la gestion des incidents et de la continuité des affaires, la sécurité physique et le chiffrement. D'ailleurs, les recommandations dans ces sections se ressemblent beaucoup pour les deux organismes. Les normes ISO/CEI sont cependant un peu plus précises que les lignes directrices de la CSA, donnant plus d'exemples de pratiques à mettre en place. Toutefois, les normes ISO/CEI demeurent elles aussi à un haut niveau et n'expliquent pas comment mettre en pratique les recommandations qu'elles contiennent, laissant le tout à la discrétion du lecteur.

L'Annexe C présente cette norme et est divisée selon les quatorze sections proposées par l'organisme. Pour chacune des sections, les recommandations provenant de la norme 27017 sur les contrôles à mettre en place lors de l'utilisation de l'infonuagique sont présentées. À la suite des recommandations de la norme 27017, celles provenant de la norme 27018 sur la protection des données personnelles utilisées par les services infonuagiques sont répertoriées. Il est fréquent

qu'aucun nouveau contrôle ne s'applique pour la norme 27018 soit parce qu'ils ne sont pas pertinents à la section ou bien parce qu'ils sont déjà couverts dans les autres travaux d'ISO/CEI.

2.5.3 Recommandations du NIST

En dernier lieu, le NIST est un organisme du gouvernement américain qui propose des normes et des métriques standards pour encadrer l'utilisation de la technologie (NIST, 2016). Leurs travaux incluent la rédaction de plusieurs rapports nommés « publications spéciales » qui sont rédigées par des comités formés de chercheurs des différentes agences du gouvernement américain, des universités ainsi que de l'industrie et qui se réunissent pour se pencher sur des sujets spécifiques. Ensuite, ces publications traversent une période de consultation publique pendant laquelle les suggestions du public sont reçues (NIST Joint Task Force, 2013). À la base, les publications du NIST ont comme principal auditoire les agences du gouvernement américain, mais comme elles sont libres d'accès,[20] plusieurs entreprises se basent sur celles-ci pour établir leurs politiques de gouvernance (PricewaterhouseCoopers, 2014; Proctor, Thielemann, Perkins et Pratap, 2016). Elles n'ont cependant aucune valeur légale puisque le NIST n'est pas un organisme réglementaire et, en conséquence, mis à part les agences du gouvernement américain, aucune compagnie n'est tenue de s'y conformer.

Étant donné la clientèle première pour laquelle elles sont développées et, bien que les lignes directrices publiées par le NIST soient très détaillées et élaborées de façon rigoureuse, elles s'appliquent surtout dans un contexte gouvernemental. Il peut donc être ardu de les mettre en place pour une entreprise canadienne qui n'est pas soumise aux mêmes lois et réglementations ou qui n'a pas les mêmes objectifs de sécurité que les agences fédérales américaines (Bradbury, 2014).

Les publications spéciales, un peu comme les normes ISO/CEI, sont regroupées en plusieurs familles auxquelles on a attribué un numéro. Ainsi, les publications de la famille SP 500 touchent les systèmes d'information alors que les publications SP 800 ont trait à la sécurité de l'information. Il faut mentionner que le NIST ne travaille pas en vase clos et tient compte des normes ISO/CEI

[20] Les publications spéciales du NIST sont disponibles à l'adresse suivante : http://csrc.nist.gov/publications/PubsSPs.html (page consultée le 26 octobre 2016).

dans la rédaction de ses publications spéciales. Certains éléments contenus dans les publications touchant la sécurité de l'information peuvent être liés aux différentes recommandations de la norme ISO/CEI 27001 sur la sécurité des systèmes d'information ce qui permet d'harmoniser les deux documents. Contrairement à ISO/CEI, les publications du NIST « fournissent un niveau de détail additionnel spécifiquement pour le gouvernement fédéral [américain] et ses fournisseurs » (traduction libre de NIST Joint Task Force, 2013, p.H-1). L'annexe H de la publication spéciale *SP 800-53 : Security and Privacy controls for Federal Information Systems and Organization* établit d'ailleurs la correspondance entre les contrôles du NIST et ceux d'ISO/CEI 27001 (NIST Joint Task Force, 2013).

Comme le NIST s'est intéressé très tôt à l'infonuagique, plusieurs publications spéciales de ces deux familles (SP 500 et SP 800) traitent du sujet. L'Annexe D dresse l'inventaire des publications spéciales qui offrent des recommandations portant sur la sécurité de l'information dans un contexte d'utilisation de l'infonuagique. Comme les normes ISO, les publications spéciales du NIST adoptent la perspective tant du client que du fournisseur. Encore une fois, pour les besoins de cette étude, seules les recommandations faites aux clients des services infonuagiques y sont présentées. De plus, les recommandations spécifiques au gouvernement américain n'y ont pas été incluses puisqu'elles n'ont pas d'application dans le contexte d'une organisation qui évolue dans l'industrie de la finance et de l'assurance au Canada.

L'Annexe D répertorie six publications spéciales qui remplissent les critères énoncés ci-haut. Elles sont présentées par ordre numérique croissant plutôt que par ordre chronologique de publication. Les deux premières publications, SP 500-291 et SP 500-293, sont en fait des guides pour aider les organismes du gouvernement américain dans son adoption sécuritaire des services infonuagiques et offrent des recommandations de sécurité de base. La troisième publication, SP 500-316, s'adresse plus aux fournisseurs en faisant des recommandations sur la façon d'améliorer l'expérience utilisateur des services infonuagiques. Néanmoins, elle contient certaines recommandations pour les clients et c'est pour cette raison qu'elle a été incluse dans l'annexe. Par la suite, la publication SP 800-125 offre des recommandations pour mitiger les risques de sécurité associée à la virtualisation, un principe à la base de l'infonuagique. Le tout est suivi de la publication spéciale 800-144 qui fut la première du NIST à proposer des lignes directrices spécifiques à l'infonuagique en 2011. En dernier lieu, la publication SP 800-146 est un

document récapitulatif sur la définition et les caractéristiques de l'infonuagique ainsi que sur les opportunités et les risques qui y sont associés.

Contrairement aux deux autres normes et lignes directrices présentées précédemment, les recommandations du NIST ne sont pas divisées par section, mais par sujet à l'intérieur des différentes familles de publications spéciales. Conséquemment, certaines recommandations se retrouvent dans plusieurs publications du NIST, mais cela permet aussi une plus grande profondeur pour chacun des thèmes abordés. Puisque le NIST est un organisme dont la mission est d'encadrer l'utilisation de la technologie, leurs recommandations offrent aussi plus de détails techniques que celles de la CSA et d'ISO/CEI, notamment en ce qui a trait à la sécurité entourant la virtualisation et à l'utilisation du chiffrement.

2.5.4 Analyse des points à retenir des normes et des lignes directrices présentées

Suite à la présentation des recommandations faites par les trois organismes, quelques observations peuvent être mentionnées. D'abord, on remarque beaucoup de similitudes entre les thèmes abordés par les trois organismes. Chacun couvre les grandes lignes de la sécurité de l'information dans un contexte infonuagique, mais avec quelques nuances. Le point qui ressort des trois lignes directrices est la mitigation des risques associés à l'infonuagique plutôt que la mise en place de solutions techniques spécifiques à la sécurité infonuagique (mis à part le chiffrement). On insiste sur la division des responsabilités entre le client et le fournisseur et la nécessité pour le client de vérifier que le fournisseur a mis en place les processus et les mécanismes de sécurité jugés suffisants. Ces processus incluent la gestion des incidents, des accès, des vulnérabilités et de la continuité des affaires. Il y est aussi question de la gouvernance et des politiques de sécurité de l'entreprise qui doivent être adaptées au contexte d'utilisation infonuagique. On inclut aussi des recommandations par rapport au chiffrement qui semble être le moyen à privilégier lors de l'utilisation de l'infonuagique pour assurer la confidentialité des données.

Bien que les thèmes couverts par les trois organismes soient similaires, l'approche de chacun pour les aborder diffère. Les normes d'ISO/CEI sont très assertives et offrent peu de place à l'interprétation, contrairement à la CSA qui est beaucoup plus vague dans ses recommandations.

Les lignes directrices de cette dernière se lisent plutôt comme des suggestions de pratiques à mettre en place, à la discrétion de l'entreprise qui les adopte. Pour ce qui est des recommandations du NIST, elles se distinguent par leur aspect plus technique. Contrairement à ISO/CEI et la CSA qui ciblent principalement les gestionnaires qui prennent des décisions à un haut niveau, le NIST propose des recommandations un peu plus ancrées dans le quotidien qui incluent des éléments plus techniques.

Malgré qu'elles puissent être utilisées pour guider les entreprises dans l'adoption de pratiques sécuritaires, les normes existantes sont loin de représenter une solution à tous les risques liés à l'utilisation de l'infonuagique puisqu'elles ont quelques limites. Tel que mentionné auparavant, un des problèmes associés à l'infonuagique est qu'il n'existe aucune norme universellement acceptée ou d'organisme régulateur. ISO/CEI est probablement l'organisme qui se rapproche le plus de cet objectif, mais considérant que sa mise à jour pour l'infonuagique est très récente, il risque de s'écouler encore quelques années avant que leurs normes soient globalement acceptées et mises en œuvre dans les organisations. On se retrouve donc avec plusieurs recommandations d'organismes différents qui ont tenté de mettre à jour leurs normes existantes afin de les adapter à l'infonuagique. Cette situation fait en sorte qu'il n'y a pas de consensus sur les pratiques qu'il est préférable d'adopter. Comme aucun des organismes présentés n'a de pouvoir légal, l'adhésion à leurs normes ou lignes directrices se fait de façon volontaire. En conséquence, les entreprises qui tentent de mettre en place des politiques de gouvernance encadrant l'utilisation de l'infonuagique peuvent donc choisir des éléments de chacune des lignes directrices existantes afin de créer des politiques qui conviennent à leur situation. De la même façon, un fournisseur peut aussi opter pour l'adoption des normes qu'il préfère ou bien n'en adopter aucune. Du côté du fournisseur de services, sa motivation à adopter ces pratiques est souvent en fonction des exigences des clients ou bien elle est issue de son obligation de se conformer à certaines lois. L'adoption de normes requiert un engagement de la part du fournisseur à octroyer les ressources nécessaires, à adapter ses processus pour assurer le respect des normes et à se soumettre à des audits, ce qui a un impact sur ses activités et ses coûts.

Ensuite, malgré que les normes présentées dans cette section offrent des recommandations aux entreprises en termes de sécurité, leur plus grande limite est qu'elles n'offrent que peu de détails sur la façon dont elles doivent être mises en œuvre. En effet, ces normes sont plutôt des

recommandations de haut niveau, des principes ou des conseils alors que la façon de les mettre en place est laissée à la discrétion et à l'interprétation des organisations. On note néanmoins un effort de la CSA en ce sens avec l'élaboration de sa matrice, celle-ci ayant pour but de faciliter la mise en place de ses recommandations. Le problème est que, tel que mentionné précédemment, ce document est lourd et comporte beaucoup de questions, ce qui rend son opérationnalisation difficile. Les entreprises sont donc laissées à elles-mêmes pour créer des politiques et des processus leur permettant de se conformer à ces normes. De surcroît, la plupart des normes et des lignes directrices sont assez récentes et les ressources qui permettent d'accompagner les entreprises dans leur application sont encore assez limitées. On peut penser que, dans le futur, l'industrie de la consultation et de la certification se développera davantage afin d'aider les entreprises à se conformer à ces normes.

De surcroît, la mise en œuvre de tels cadres de sécurité de l'information engendre nécessairement certains coûts pour l'entreprise qui doit adapter ses processus pour s'y conformer. L'organisation doit être en mesure de justifier les coûts ainsi générés. Comme la sécurité de l'information est souvent perçue comme une dépense plutôt qu'un investissement et que les bénéfices qui en découlent sont surtout intangibles, il peut être difficile de justifier les investissements en sécurité (Johnson, 2009). La mise en place des contrôles de sécurité peut aussi créer des délais, des barrières à l'adoption et une certaine frustration pour les employés si les contrôles sont trop nombreux ou s'ils affectent la performance du processus d'approvisionnement informatique. Ces façons de faire vont donc à l'encontre des principes de rapidité et de flexibilité de l'infonuagique et c'est pourquoi l'application de normes peut devenir un exercice assez laborieux.

Une autre entrave à l'adoption des normes spécifiques à l'infonuagique est le contexte d'affaires de l'entreprise qui cherche à les adopter. L'industrie canadienne de la finance et de l'assurance est déjà hautement réglementée et les entreprises de ce domaine doivent déjà se conformer à plusieurs lois et lignes directrices (ex : la Loi canadienne sur les banques, les accords de Bâle, la norme *Payment Card Industry Data Security* (PCI DSS), etc.). Les normes des trois organismes présentés ici n'ont pas été développées spécifiquement avec le contexte de cette industrie en tête. L'adhésion à un ensemble de normes, comme celles présentées dans cette section, peut s'avérer complexe puisque le tout devra se faire dans le respect des lois actuelles qui ont préséance.

Bien que les normes et lignes directrices représentent un pas dans la bonne direction en ce qui concerne la sécurité des services infonuagiques, elles ne sont pas suffisantes pour les organisations qui ont grandement besoin de mécanismes et de processus de sécurité qui s'intègrent à ceux qu'elle a déjà en place. Leur mise en œuvre est souvent longue et difficile parce qu'elles exigent des changements de processus qui risquent de rencontrer de la résistance de la part des employés et des gestionnaires.

Suite à la lecture des sections précédentes, on se rend compte que les défis liés à l'utilisation de l'infonuagique sont nombreux. D'abord, le nombre de services et de technologies disponibles associés à l'infonuagique est mirobolant, rendant la sélection de fournisseurs et de services complexes. La nature même de ce mode d'approvisionnement crée certaines inquiétudes quant à la confidentialité, à l'intégrité et à la disponibilité des données ainsi qu'à la sécurité de l'infrastructure dans un contexte où les ressources sont partagées. L'objectif de l'infonuagique est d'impartir un service que l'organisation cliente ne souhaite pas gérer elle-même. Toutefois, avec la multiplication des contrôles, des accès et des comptes engendrée par la croissance du nombre de services utilisés, la gestion associée à l'infonuagique peut devenir lourde. À tous ces contrôles s'ajoute la conformité aux lois auxquelles l'entreprise doit se soumettre, l'obligeant à mettre en place des contrôles manuels pour chacun des services qu'elle impartit. Les CASB incarnent donc une piste de solution pour l'application de ces lois puisqu'ils proposent différentes fonctionnalités qui permettent de renforcer la sécurité liée à l'utilisation des services infonuagiques, en plus de proposer des mécanismes pour l'application des politiques de sécurité de l'entreprise. Ils ont ainsi le potentiel de centraliser et d'automatiser la gestion de la sécurité des applications infonuagiques utilisées au sein de l'organisation.

2.6 Les *Cloud Access Security Brokers* (CASB) : une solution complexe et ambiguë

Les sections précédentes démontrent bien l'ampleur du défi en sécurité infonuagique pour les organisations qui décident d'opter pour ce mode d'approvisionnement. Bien que plusieurs solutions existent pour tenter de surmonter les défis, elles sont souvent disparates et leur compatibilité, entre elles et avec les systèmes existants, est loin d'être démontrée. Par conséquent, plusieurs entreprises spécialisées en sécurité ont commencé à offrir des solutions

qui facilitent la gestion de la sécurité infonuagique. Ces produits, les *Cloud Access Security Brokers* ou CASB, présentent un grand potentiel pour l'avenir de la sécurité, mais ils sont encore très émergents. L'objectif de cette section est donc de mieux comprendre cette classe d'outils en présentant leurs objectifs de base, leur fonctionnement et les conditions actuelles du marché. Cette présentation mettra la table pour le travail empirique à venir.

2.6.1 Les principes généraux

Les *Cloud Access Security Brokers* représentent une classe de produits de sécurité infonuagique définie en 2012 par la firme de recherche Gartner (MacDonald et Firstbrook, 2012). Comme les produits qui la constituent sont relativement nouveaux et que le marché est très fragmenté, il règne une certaine confusion autour de la définition et des fonctionnalités des CASB (Coles, 2016b; N. Leong, 2016). D'ailleurs, une autre firme de recherche, Forrester, utilise les termes *Cloud Access Security Intelligence*, *Cloud Data Protection* ou *Cloud Security Gateway* pour désigner des produits qui ont sensiblement les mêmes caractéristiques que la classe d'outils décrite par Gartner. Puisque la définition et la catégorisation de Forrester sont moins précises que celles de Gartner, ce sont plutôt celles de cette dernière qui seront retenues comme point de départ pour les besoins de cette étude. C'est aussi la définition que semblent avoir adoptée les professionnels et les entreprises de l'industrie lorsqu'ils réfèrent à ce genre de produit.

Ces logiciels offrent des fonctionnalités visant à remplir quatre grands objectifs de sécurité et sont disponibles en deux modes de fonctionnement, soit en tant qu'intermédiaires vers l'interface d'application (API)[21] du service infonuagique ou par *proxy*. En fonction des fournisseurs, ils peuvent être implantés en mode infonuagique ou en mode local, donc installés physiquement sur les lieux de l'organisation. Dans le cas où ils sont implantés en mode infonuagique, ils sont vendus à un coût récurrent par utilisateur. Ce coût, à partir de cinq dollars par mois, varie en fonction des fournisseurs, mais aussi selon la version utilisée puisque certains fournisseurs offrent plusieurs versions de leur produit, chacune offrant un ensemble de fonctionnalités différentes.

[21] L'interface de programmation d'application est la traduction française des termes *Application Programming Interface* (Grand dictionnaire terminologique de la langue française, consulté le 1 décembre 2016, http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26508293).

2.6.1.1 Les objectifs de sécurité

À la base, les CASB reposent sur quatre catégories de fonctionnalités qui permettent à l'organisation de réaliser différents objectifs de sécurité des applications infonuagiques : la visibilité, la conformité et la gouvernance, la sécurité des données et la protection contre les menaces (Lawson *et al.*, 2015b; Lawson *et al.*, 2015c). La littérature offre déjà des pistes quant aux fonctionnalités généralement offertes par cette classe d'outils. Même si l'étude permet de creuser les requis fonctionnels pour un CASB dans un contexte spécifique, il est difficile de se faire une idée claire du potentiel d'un CASB sans cet examen détaillé de cette classe d'outils. Le Tableau 2.3 présente les différentes fonctionnalités recensées et associées avec chacun des grands objectifs. Les paragraphes qui suivent ce tableau décrivent davantage ces fonctionnalités.

Tableau 2.3 : Fonctionnalités des CASB[a]

Objectifs de sécurité	Fonctionnalités
Visibilité	• Identification des applications infonuagiques utilisées dans l'entreprise. • Identification des appareils autorisés et non autorisés utilisant le réseau de l'entreprise. • Vue consolidée de l'utilisation d'applications infonuagiques dans un tableau de bord.
Conformité et gouvernance	• Gestion des accès basée sur le type de données (publiques, privées ou confidentielles)[22] et sur le rôle de l'utilisateur. • Traçabilité des activités infonuagiques par la création de journaux des activités. • Gabarits qui imposent les politiques de protection des données afin d'assurer la conformité à certaines lois ou normes comme *Sarbanes-Oxley* ou *Payment Card Industry* (PCI DSS).
Sécurité des données	• Prise en considération de la classification des données pour déterminer l'action de sécurité appropriée. • Chiffrement des données basé sur leur classification. • Application des politiques de protection contre la perte de données (DLP).[23]
Protection contre les menaces	• Analyse du comportement des utilisateurs et identification de comportements anormaux ou à risque. • Détection de contenu suspect dans les données ou les fichiers échangés via les applications infonuagiques. • Blocage des appareils non autorisés ou refus d'accès aux applications infonuagiques.

[a] Contenu tiré de : Cser, Balaouras et Dostie (2015a); Lawson, MacDonald et Deshpande (2015a); Lawson *et al.* (2015b); Lawson *et al.* (2015c); MacDonald et Firstbrook (2012); MacDonald et Lawson (2015); Reed et Lowans (2016).

Visibilité

Le premier objectif, celui de la visibilité, est aujourd'hui essentiel puisque les employés utilisent divers appareils pour accéder aux applications d'affaires et aux données d'une entreprise, que ce soit des ordinateurs, des tablettes ou des téléphones (Lowans, Heiser et Buchanan, 2016). Ces appareils ne sont pas nécessairement ceux fournis par la compagnie et appartiennent plutôt à

[22] Il existe différentes taxonomies pour identifier le niveau de confidentialité des données. Les catégories varient d'une organisation à l'autre, mais les trois proposées ici sont généralement les plus acceptées. Une donnée publique correspond à de l'information qui, si elle est divulguée sans autorisation, n'aura pas d'impact sur la réputation ou la sécurité de l'organisation, de ses employés, de ses clients et de ses partenaires. Dans le cas d'une donnée privée, sa divulgation à l'extérieur de l'organisation peut causer un impact modéré sur la réputation et la sécurité de l'organisation, mais sans affecter ses activités. Une donnée confidentielle peut avoir un impact sur les activités de l'organisation et causer un préjudice grave à la réputation et à la sécurité de l'entreprise, de ses employés, de ses clients et de ses partenaires (Carnegie Melon University, 2016).

[23] La protection contre la perte des données (ou *Data Loss Protection* en anglais) est un ensemble de technologies qui permettent de gérer les données et d'en prévenir la fuite hors des frontières de l'organisation. Ces technologies permettent à l'organisation d'opérationnaliser ses politiques de protection des données (Elastica, 2014).

l'employé,[24] ce qui rend leur surveillance et leur contrôle plus difficiles pour l'organisation. Cette prolifération du nombre d'appareils a causé ce qu'on appelle le *shadow IT* ou l'utilisation d'appareils ou d'applications non autorisés par le département TI d'une organisation (Silic et Back, 2014b). Cette pratique semble inévitable à notre ère d'ubiquité des technologies et n'est pas limitée qu'à l'infonuagique, mais elle pose tout de même différents risques de sécurité. En effet, sans moyen de surveillance et de contrôle, les entreprises sont incapables de savoir qui accède à leur réseau, leurs données et leurs applications, comment ces personnes y accèdent et quelles données y sont échangées (MacDonald et Lawson, 2015). S'ajoutent à cela les risques d'infection que ces appareils non autorisés et non protégés peuvent introduire dans l'écosystème informatique (Silic et Back, 2014b). L'organisation est donc vulnérable aux attaques de l'interne ou de l'externe et aux pertes de données, entre autres celles qui contiennent de l'information confidentielle. Comme elle demeure responsable de ses données (et non pas le fournisseur de services infonuagiques), l'entreprise s'expose alors à de sérieux risques légaux et a donc intérêt à savoir quelles applications et appareils sont utilisés par ses employés, dans quel environnement et à bien analyser les risques qui y sont liés.

Certains CASB ont des fonctionnalités qui permettent de surveiller l'activité en lien avec les services infonuagiques afin de dresser un inventaire de toutes les applications SaaS et de tous les appareils utilisés par les employés de l'organisation. Ces fonctionnalités permettent aussi aux entreprises de repérer l'utilisation par ses employés d'appareils ou d'applications non autorisés et de les signaler (Lawson *et al.*, 2015b). Cette information est généralement agrégée dans un tableau de bord qui montre l'activité par utilisateur et par appareil. Cette consolidation de l'information peut donc aider l'organisation à prendre des décisions concernant ses politiques d'utilisation en termes de sécurité et de gouvernance TI (Reed et Lowans, 2016).

Conformité et gouvernance

Le second objectif, la conformité et la gouvernance en sécurité, est atteint grâce à l'intégration et la centralisation des politiques de protection des données de l'entreprise. Le CASB peut analyser les données utilisées par les services infonuagiques pour en identifier la classification (ex : données publiques, privées ou confidentielles). Ensuite, il peut appliquer les mécanismes de

[24] Ce phénomène par lequel les employés utilisent leurs appareils personnels dans le cadre de leur travail plutôt que ceux fournis par l'entreprise est communément appelé *Bring Your Own Device* (BYOD).

protection appropriés ou bien limiter l'accès à certains types de données qu'aux personnes autorisées (MacDonald et Firstbrook, 2012).

Certains CASB offrent aussi des gabarits de politique se collant à certaines lois comme Sarbanes-Oxley ou PCI DSS (Lawson *et al.*, 2015a; Lawson *et al.*, 2015b). Les gabarits indiquent au CASB comment traiter chacune des données de l'application selon sa nature. Par exemple, la norme PCI DSS oblige les organisations à chiffrer tout numéro de carte de crédit lors d'une transaction (PCI Security Standards Council, 2013). Si on met en place le gabarit PCI DSS pour un CASB, toutes les données transitant par l'application infonuagique seront analysées et celles qui contiennent des numéros de cartes de crédit seront alors obligatoirement chiffrées. Les gabarits permettent tout simplement d'appliquer automatiquement les exigences associées à une certaine loi (ou à une pratique interne) aux données correspondantes. De cette façon, il est beaucoup plus facile pour l'organisation de se plier aux lois en vigueur et on s'assure que les politiques sont appliquées de façon uniforme à toutes les données des applications infonuagiques. Au-delà de l'imposition des politiques de gouvernance, les CASB enregistrent dans des journaux toutes les activités liées aux applications SaaS comme les connexions, les utilisateurs, les données transférées vers le service, etc. Ces journaux permettent donc de garder une trace, ce qui peut s'avérer très utile en cas de litige, d'audit ou d'une investigation suite à une attaque.

Sécurité des données

En troisième lieu, les entreprises qui adoptent des services infonuagiques demeurent responsables des données qui y sont échangées ou stockées (Cloud Security Alliance, 2011). Même si la plupart des fournisseurs de SaaS intègrent des dispositifs de sécurité à leurs produits, cela n'est pas toujours suffisant pour répondre aux normes et aux besoins de certaines organisations. Plusieurs organisations prennent elles-mêmes en charge la sécurité pour mieux protéger la confidentialité, l'intégrité et la disponibilité des données utilisées dans l'environnement infonuagique. Les CASB peuvent aider l'entreprise à atteindre un plus haut niveau de sécurité avec des mécanismes de chiffrement, de segmentation en unités [25] ou de protection contre la perte de données.

[25] La segmentation en unités est la traduction française de *tokenization*. Il s'agit d'un processus par lequel une donnée sensible est remplacée par un élément équivalent, mais sans valeur exploitable (Gartner, 2016).

Actuellement, seuls quelques fournisseurs SaaS offrent le chiffrement des données (Lowans, 2016). De plus, le chiffrement ne se fait pas nécessairement au niveau de chaque champ individuel, mais au niveau de la base de données en partageant la clé avec plusieurs clients (Lowans, 2016). Le CASB offre une solution à ce problème en identifiant le type de chaque donnée transigeant par l'application infonuagique et, si elle répond aux critères définis par la politique de gouvernance, il la chiffrera avant qu'elle ne soit envoyée vers le fournisseur (Cser *et al.*, 2015a; Lawson *et al.*, 2015b). Lorsque la fonctionnalité de chiffrement est disponible pour un CASB, les données sont chiffrées individuellement au niveau du champ et directement dans l'application. Ainsi, une personne ne possédant pas la clé ne verra que des champs chiffrés en ouvrant l'application ou en cas de vol du disque dur ou d'identifiants de connexion (Kahol, 2015). Les CASB permettent donc de chiffrer les données du côté du client, s'assurant que le fournisseur de services n'ait pas accès à ces données, ce qui respecte les recommandations en termes de chiffrement des organismes normatifs présentés à la section précédente. L'inconvénient du chiffrement par CASB plutôt qu'avec les mécanismes présents dans l'application est une possible perte de fonctionnalité du SaaS, notamment dans le traitement des données ou la recherche parmi celles-ci (Lowans, 2016).

Un dernier mécanisme de protection des données offert par les CASB est la protection contre la perte des données (*Data Loss Prevention* ou DLP). Ces fonctionnalités sont utilisées de pair avec les politiques de gouvernance décrites précédemment. Si une donnée est jugée trop sensible pour être utilisée par un certain SaaS, le CASB bloquera le transfert (Lawson *et al.*, 2015c). Afin de mieux illustrer ce point, imaginons qu'un employé a un document contenant une liste de noms, de dates de naissance et d'adresses des employés de son département. Il souhaite télécharger ce document sur l'application de partage de fichiers Dropbox afin de le rendre disponible à un collègue du département des ressources humaines. Puisque les CASB sont en mesure de reconnaître certains types de données dans des documents contenant des données structurées ou non, le CASB de l'exemple pourrait intercepter le transfert et le bloquer si l'entreprise a mis en place des politiques qui empêchent le partage de données confidentielles sur Dropbox. En plus, le CASB pourrait, par exemple, émettre une alerte dans le tableau de bord pour informer l'administrateur que l'employé a tenté de partager des données confidentielles par le biais d'une application non autorisée. La protection contre la perte des données permet donc de minimiser les risques de fuite de données hors des frontières de l'organisation.

Protection contre les menaces

La dernière dimension prise en charge par les CASB est la protection contre les menaces. Les CASB peuvent être configurés pour récolter, soit automatiquement ou manuellement selon le produit, les journaux générés par les pare-feu et les *proxys* que l'entreprise a déjà en place (Microsoft, 2016a). Cette configuration leur permet de recevoir de l'information sur le trafic circulant sur le réseau puis de l'analyser, grâce à des algorithmes d'analytique, pour identifier les tendances dans l'utilisation des SaaS par les utilisateurs (Cser, Holland, Balaouras et Dostie, 2015b). Grâce à cette information sur l'utilisation, le CASB est en mesure de détecter des activités suspectes liées aux applications infonuagiques ou aux appareils utilisés et d'émettre des alertes en conséquence (Lawson *et al.*, 2015a). Les CASB peuvent aussi supprimer ou mettre en quarantaine des documents jugés suspects afin de protéger l'entreprise contre les virus ou autres logiciels malicieux (Lawson *et al.*, 2015b; Lawson *et al.*, 2015c). Ces fonctionnalités ressemblent beaucoup à celles déjà offertes par les pare-feu ou les anti-virus, avec la différence qu'elles sont spécifiques à l'infonuagique et qu'elles offrent un niveau d'analyse et de protection plus granulaire s'appliquant à chaque champ de l'application utilisée (Coles, 2016a; Kirti, 2016). On peut donc choisir d'appliquer des protections à des champs spécifiques dans une application infonuagique plutôt qu'à l'application entière, ce qui permet d'accélérer le traitement des données et de réduire la latence lors de l'utilisation.

Les quatre objectifs de cette classe d'outils présentés dans cette section peuvent être utilisés pour catégoriser les produits en sécurité de l'information présentement offerts sur le marché. Comme il le sera démontré plus tard, ce ne sont pas tous les CASB qui proposent des fonctionnalités permettant d'atteindre les quatre grands objectifs. L'immaturité de cette classe d'outils explique en partie cette variabilité, mais les deux modes de fonctionnement d'un CASB peuvent aussi l'expliquer. Ces deux derniers sont décrits plus en détail dans la prochaine section.

2.6.2 Les modes de fonctionnement des CASB

Il existe deux modes de fonctionnement possibles pour les CASB : le mode en tant qu'intermédiaire vers une interface de programmation d'application (API) ou par *proxy*. Chacun des deux offre des fonctionnalités et un niveau de protection différents. Certains CASB fonctionnent seulement selon l'un des deux modes, alors que d'autres intégreront les deux

(Lawson *et al.*, 2015c). La prochaine section résume ce que sont ces deux modes, les fonctionnalités qu'ils permettent, leurs avantages et leurs limites.

2.6.2.1 Intermédiaire vers l'interface de programmation d'application (API)

Une interface de programmation d'application (API) est un ensemble de commandes et de protocoles qui permettent à une application spécifique d'interagir avec d'autres applications (Proffitt, 2013). À titre d'exemple, c'est grâce à une API qu'un utilisateur peut se connecter à un site web grâce à son identifiant Facebook plutôt que de devoir créer un compte sur le site en question. Facebook met donc à la disposition des concepteurs de site web une API qui leur permet d'interagir avec les applications de Facebook. Les API sont donc des blocs de code qui peuvent être réutilisés selon les besoins.

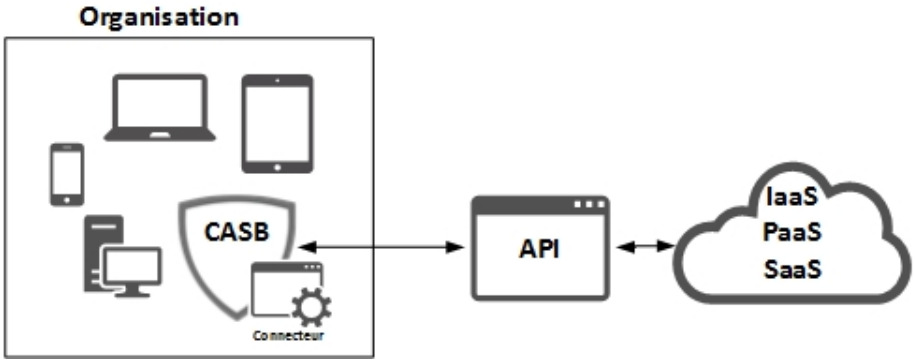
Les fournisseurs SaaS permettent généralement à leurs clients d'accéder aux API disponibles pour leur application. Ces API permettent au client de bénéficier de certaines fonctionnalités, définies dans le code de l'API par le fournisseur, mais qui ne sont pas disponibles dans l'application de base (Proffitt, 2013). De son côté, le client doit, pour y avoir accès, programmer une commande pour l'appel à l'API. Une fois que la commande d'appel est lancée, il peut alors utiliser les fonctionnalités ou obtenir l'information offerte par l'API en question. Dans les cas où il y a plusieurs API disponibles pour une même application, le client doit recommencer ce processus pour chacune des API auquel il souhaite avoir accès. L'éventail de ce qu'il est possible de faire varie selon l'API et la volonté du fournisseur, mais peut inclure, par exemple, le contrôle des accès à l'application ou la récolte des données de connexion et d'utilisation (Lawson *et al.*, 2015b; Thomas et Moyer, 2016).

Les lignes précédentes mettent en évidence le rôle que le client a à jouer s'il souhaite avoir accès aux fonctionnalités ou à l'information offertes par les API. La programmation de la commande d'appel à l'API doit se faire manuellement dans le langage de programmation spécifique choisi par le fournisseur (Malinverno, 2014). Il n'existe malheureusement pas de norme quant au langage utilisé pour programmer des API, donc chaque fournisseur est libre de programmer la sienne dans le langage qu'il choisit (Lawson *et al.*, 2015c). Conséquemment, l'utilisation des API requiert des connaissances dans le langage informatique dans lequel l'API qu'on souhaite utiliser

est programmée.[26] Pour l'organisation cliente, cela rend la gestion et le contrôle de la sécurité des services SaaS plutôt complexes parce qu'il faut avoir recours à des ressources possédant les connaissances techniques nécessaires. Les CASB résolvent ce problème puisqu'ils agissent comme un intermédiaire qui permet d'automatiser la programmation de la commande d'appel aux API de certaines applications spécifiques et de centraliser la présentation de l'information concernant ces applications (Sookasa, 2016).

La Figure 2.4 montre comment le CASB interagit avec un API de l'application infonuagique, grâce à un connecteur inclus dans le produit du fournisseur de CASB. Les CASB n'ajoutent donc pas de nouvelles fonctionnalités, mais permettent plutôt d'obtenir un accès automatisé et standardisé aux fonctionnalités offertes par les API du fournisseur puisque leurs connecteurs contiennent le code requis pour lancer la commande d'appel. Ainsi, le client élimine le besoin de programmer manuellement chacune de ces commandes d'appel pour les API qu'il souhaite utiliser.

Figure 2.4 : Mode de fonctionnement d'un CASB en tant qu'intermédiaire vers l'API
(Adaptation de Lawson *et al.*, 2015b, p.10)



Afin d'illustrer les propos précédents, supposons qu'une organisation implante un CASB en mode d'intermédiaire vers l'API pour l'application Salesforce. Cette application populaire de gestion de la relation avec les clients permet, entre autres, de faire des suivis auprès des clients actuels ou

[26] Ce qui est décrit dans le paragraphe est le fonctionnement de base d'un API. Il faut cependant mentionner que les fournisseurs de services infonuagiques sont conscients que leurs clients ne disposent pas toujours des ressources ou des connaissances requises pour programmer une commande d'appel à l'API. Certains offrent donc des connecteurs qui sont essentiellement de petits programmes informatiques permettant de simplifier la programmation de la commande d'appel. L'installation de ces connecteurs ne requiert que quelques connaissances de bases en programmation et la documentation nécessaire est largement disponible sur les sites Internet des fournisseurs de services infonuagiques (Google, 2016; Microsoft, 2016d; Salesforce, 2016a).

potentiels. En premier lieu, l'organisation devra définir, dans la console d'administrateur du CASB, les politiques de protection des données qu'elle souhaite mettre en place. Elle peut choisir d'utiliser un gabarit prédéterminé qui est fourni avec le CASB ou de personnaliser les politiques selon ses besoins. Imaginons, pour simplifier cet exemple, que la seule règle qu'elle met en place est le chiffrement des dates de naissance. À présent, supposons qu'un employé de l'organisation souhaite créer une nouvelle fiche de client (aussi appelé *contact* dans Salesforce). Suite à sa connexion à l'application Salesforce, l'employé tape les informations du nouveau contact dans chacun des champs requis, par exemple, le nom, l'adresse, le numéro de téléphone, la date de naissance et le numéro de carte de crédit. Une fois les données entrées, celles-ci sont enregistrées sur les serveurs de Salesforce et sont considérées « au repos » jusqu'à ce qu'un utilisateur les sollicite.[27] Le CASB, à certains intervalles donnés, lancera la commande d'appel vers l'API de Salesforce, ce qui lui permettra de faire un balayage des données au repos et de reconnaître celles qui correspondent aux dates de naissance pour ensuite les chiffrer tel que l'impose la politique de protection des données définie par l'organisation. Le lancement de la commande d'appel pour le balayage des données au repos se fait périodiquement et non pas en temps réel lorsque les données sont saisies dans l'application par l'utilisateur. Il peut donc y avoir un certain délai entre le moment où la donnée est créée et celui où elle est chiffrée par le CASB. L'utilisation d'un CASB fait alors simplement en sorte que cette commande est programmée et lancée automatiquement, plutôt que de devoir faire appel à une ressource technique spécialisée dans la programmation d'API spécifique à Salesforce.

Le grand avantage des CASB qui agissent comme intermédiaires vers l'API est qu'ils permettent d'appliquer des mesures de contrôle à un niveau très granulaire défini par l'entreprise (Kirti, 2016), c'est-à-dire jusqu'au niveau de chacun des champs utilisés par une application. Si un module du CASB est disponible pour l'application en question, ce dernier sera en mesure de lancer un appel à l'API pour faire un balayage des données au repos dans la base de données de l'application afin d'en identifier la nature et d'appliquer à chaque donnée les politiques de

[27] L'application Salesforce inclut, dans son offre de base, une technologie qui masque seulement les champs standards et chiffre jusqu'à 175 caractères dans des champs personnalisés avec des clés de 128 bits et l'algorithme *Advanced Encryption Standard (AES).* Pour bénéficier du chiffrement des champs standards avec un algorithme 256-bits AES, soit le plus puissant actuellement disponible sur le marché, le client doit débourser des frais supplémentaires et cette option n'est pas offerte pour toutes les éditions de Salesforce (Kohgadai, 2016; Salesforce, 2016b).

protection qui sont définies par l'organisation, mais toujours dans le respect des limites de l'API qui sont imposées par le fournisseur de l'application (Kirti, 2016). Ces contrôles peuvent être du chiffrement ou de la segmentation en unités selon le niveau de confidentialité requis. Les objectifs de conformité aux politiques de gouvernance, de sécurité des données et de prévention des menaces sont tous réalisables principalement par le mode API (mais toujours dans les limites de ce qu'offre l'API en question) (Lawson *et al.*, 2015a). De plus, ils n'affectent pas la performance de l'application et sont donc transparents pour l'utilisateur (Kirti, 2016). Leur puissance de protection est donc très grande, mais limitée à quelques applications pour lesquelles un module du CASB est disponible.

Il existe certaines limites aux CASB qui agissent en tant qu'intermédiaire vers l'API. La première est qu'ils sont disponibles que pour certaines applications et celles-ci varient selon le fournisseur de CASB. Donc le chiffrement ou l'application des politiques de protection des données au repos n'est possible que pour certaines applications spécifiques protégées par le CASB. L'offre varie d'un produit à l'autre, mais pour l'instant, les applications les plus communes disponibles avec les CASB sur le marché sont Box, Dropbox, Google Apps, Office 365, Salesforce et ServiceNow (Bitglass, 2016b; CloudLock, 2016; Elastica, 2016; FireLayers, 2016; Microsoft, 2016b; Netskope, 2016; Palerra, 2016; Palo Alto Networks, 2016; Skyhigh Networks, 2016). Il faut donc que le client achète le module spécifique à l'application qu'il souhaite protéger pour bénéficier des avantages du CASB qui joue le rôle d'intermédiaire vers l'API. Donc, si par exemple, une organisation utilise Office 365, Salesforce et ServiceNow, elle devra acheter trois modules différents et il n'est pas garanti que le fournisseur de CASB qu'elle choisira offre un module pour chacune de ces trois applications. Un autre point négatif mentionné plus tôt est que le mode en tant qu'intermédiaire vers l'API ne permet pas une protection en temps réel des données contrairement au mode par *proxy* puisqu'un appel doit être fait vers l'API du fournisseur après le traitement de la donnée (Schuricht et Hafid, 2016).

2.6.2.2 Mode par *proxy*

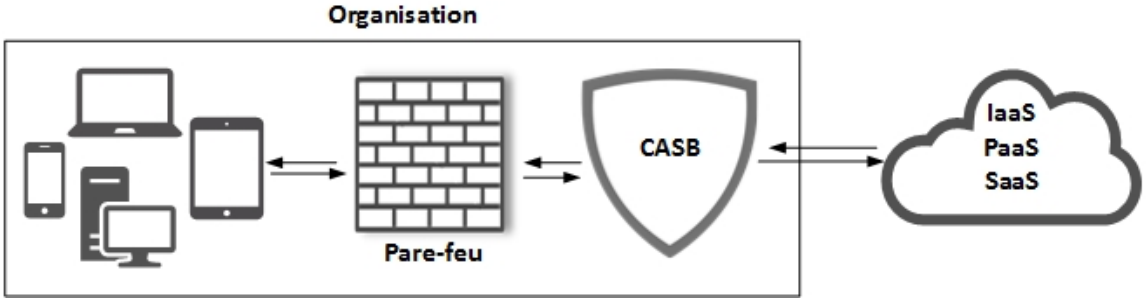
Le terme *proxy* est utilisé en informatique pour désigner un intermédiaire entre deux éléments (Microsoft, 2016f). En ce qui a trait aux CASB en mode *proxy*, cela signifie que celui-ci agit comme une passerelle pour tout le trafic passant entre l'organisation et le réseau externe, un peu comme

le ferait un pare-feu. La Figure 2.5 est une illustration simplifiée de l'intégration du CASB avec les pare-feu de l'entreprise pour intercepter et analyser le trafic. Il permet donc la protection des données en transit, contrairement au mode en tant qu'intermédiaire vers l'API qui est limité à la protection des données au repos (Coles, 2016a). Ainsi, le trafic provenant de l'application vers l'utilisateur (et vice-versa) est redirigé en temps réel vers le CASB et ensuite traité selon l'analyse faite par le CASB et selon les règles qui y ont été configurées (Lawson *et al.*, 2015b).

Il existe deux sous-groupes de fonctionnalités pour les CASB par *proxy*. Le *reverse proxy* permet de découvrir et de gérer les appareils non autorisés sur le réseau de l'organisation, donc tout ce qui touche au BYOD. Le *forward proxy*, pour sa part, permet de gérer les appareils autorisés, c'est-à-dire les appareils fournis par l'organisation. Pour ce faire, l'organisation doit s'assurer de configurer les pare-feu de façon à ce que tout le trafic du réseau soit redirigé vers le CASB et les paramètres de *proxy* (*proxy settings)* de chaque appareils doivent être modifiés en conséquence (Bitglass, 2016a; Kirti, 2016). Lorsque les deux groupes de fonctionnalités sont utilisés, le CASB est en mesure de détecter toutes les activités en lien avec l'utilisation infonuagique sur son réseau, que les appareils soient autorisés ou non.

Figure 2.5 : Mode de fonctionnement d'un CASB par *proxy*

(Adaptation de Lawson *et al.*, 2015b, p.9)



Le plus grand avantage du mode par *proxy* est qu'il offre la protection et l'analyse des données échangées pendant qu'elles sont en transit. Les CASB utilisant ce mode ressemblent beaucoup au pare-feu et d'ailleurs, ils s'y intègrent (Lawson *et al.*, 2015a). Cependant, contrairement au pare-feu qui bloquera simplement l'accès au réseau interne de l'entreprise (Gordon, 2016), le CASB peut mettre en place certains mécanismes de sécurité, selon l'analyse qu'il fait des données

comme, par exemple, d'exiger un mot de passe ou l'authentification de l'utilisateur, de refuser l'accès ou bien d'appliquer un filigrane sur un document (Lawson *et al.*, 2015b).

Les CASB disponibles en mode *proxy* ont des limites, la plus grande étant la complexité associée à leur installation et à l'effort d'ingénierie qui y est rattaché. En effet, comme ils doivent s'intégrer aux autres composantes de sécurité et doivent être configurés de façon à ce que tout le trafic du réseau y soit dirigé, leur mise en place est plus complexe que pour le mode d'intermédiaire vers l'API. De plus, ils peuvent avoir un impact sur la performance en créant de la latence, spécialement si le trafic sur le réseau est élevé (Kirti, 2016; Lawson *et al.*, 2015b). Finalement, un autre inconvénient du CASB par *proxy* est qu'il devient un point de panne unique[28] car tout le trafic doit obligatoirement y passer (Lawson *et al.*, 2015a).

Comme chacun des deux modes a des avantages et des inconvénients, il peut être difficile de n'en choisir qu'un seul. Le mode d'intermédiaire vers l'API permet une protection beaucoup plus grande des données, mais celle-ci n'est limitée qu'à quelques SaaS et n'est pas en temps réel. Le mode par *proxy* permet de surveiller tout le réseau de l'entreprise afin d'obtenir une vision d'ensemble de toutes les applications et de tous les appareils qui y sont utilisés, menant à un plus grand contrôle sur le *shadow IT.* Cependant, il est limité dans la gamme de ses mécanismes de protection. Il n'est donc pas surprenant de voir de plus en plus de fournisseurs qui combinent les deux modes, celui d'intermédiaire vers l'API et celui par *proxy*, afin d'offrir plus de fonctionnalités (Lawson *et al.*, 2015a). Un CASB hybride permet donc d'offrir toutes les fonctionnalités possibles par les deux modes. D'ailleurs, la firme Gartner recommande de choisir un CASB qui prend en charge les deux modes afin d'avoir accès à un plus large spectre de fonctionnalités de sécurité (Lawson *et al.*, 2015b).

2.6.3 L'état du marché et la complexité du produit

Le marché des CASB est en pleine émergence et en période de consolidation (Lawson *et al.*, 2015c; Reed et Lowans, 2016). Le marché est présentement constitué d'une quinzaine de joueurs,

[28] Un point de panne unique est la traduction française de l'expression *single point of failure* qui signifie qu'à elle seule, une composante peut causer une panne généralisée de tout le système informatique d'une entreprise ; dans ce cas-ci, de tous les systèmes utilisés en mode infonuagique. (Grand dictionnaire terminologique de la langue française, consulté le 17 mai 2016, http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8419768).

principalement des entreprises en démarrage, mais plusieurs grosses entreprises de logiciels ont fait des acquisitions dans les deux dernières années afin de mieux se positionner dans ce marché (Cser *et al.*, 2015b). Par exemple, Microsoft a acheté la petite entreprise de CASB Adallom en 2015 (Cser *et al.*, 2015b). Toujours en 2015, la firme BlueCoat a acheté Elastica et Perspecsys, deux fournisseurs de CASB. BlueCoat a par la suite été rachetée en juin 2016 par l'entreprise de sécurité Symantec (Baker, 2016). Ces changements causent une certaine volatilité et incertitude dans ce marché. De plus, bien qu'on semble s'entendre sur la définition de Gartner pour catégoriser les CASB, en investiguant les fournisseurs actuels, on se rend compte que plusieurs tentent de faire passer leurs produits de sécurité pour des CASB alors que tel n'est pas le cas. Au total, il semble donc y avoir beaucoup de confusion autour des CASB et de leurs fonctionnalités. Cette volatilité et consolidation du marché ainsi que la confusion autour de la définition même du produit expliquent la difficulté à bien le comprendre. Au-delà de cela, l'immaturité du produit fait en sorte que les CASB sont appelés à se développer et à évoluer au cours des prochaines années. En conséquence, il est possible que d'ici quelques années, ces produits changent radicalement et offrent des fonctionnalités différentes de celles qui les définissent actuellement.

Un autre aspect qui rend le choix d'une solution de type CASB difficile pour une entreprise est la complexité du produit. En effet, la section précédente montre que les CASB ont plusieurs fonctionnalités possibles et qu'ils peuvent être implantés selon différents modes. En conséquence, les CASB entrent dans la définition de Novak et Eppinger (2001) de produits complexes qui sont caractérisés selon les trois points suivants :

1. **Le nombre de composantes du produit**

   Les CASB ont des fonctionnalités qui tentent de d'atteindre quatre objectifs, soit la visibilité, la conformité, la sécurité des données et la protection contre les menaces. Cependant, ces quatre dimensions ne sont pas toutes présentes pour chacun des CASB sur le marché et les mécanismes pour chaque dimension varient d'une solution à l'autre selon le mode d'implantation par *proxy* ou en tant qu'intermédiaire vers l'API. De plus, le nombre d'applications infonuagiques qui peuvent être sécurisées avec les CASB est présentement limité (Lawson *et al.*, 2015a) et les modules sont vendus à l'unité selon les applications pour lesquelles on souhaite assurer la protection. De ce fait, seules ces applications pour lesquelles il existe un module de CASB correspondant bénéficient des

protections comme le chiffrement ou la gestion des accès basée sur le type de données (MacDonald et Firstbrook, 2012). Une entreprise qui utilise plusieurs applications infonuagiques devra potentiellement acquérir plusieurs modules ou CASB pour les sécuriser. En outre, comme les fournisseurs du marché sont en consolidation, le nombre de composantes ou de mécanismes de sécurité d'un produit et la façon de les implanter risquent de changer rapidement selon la demande et les progrès technologiques.

2. **L'envergure des interactions à gérer entre les différentes composantes**

   Une des faiblesses des CASB est leur intégration avec l'infrastructure technologique de l'entreprise (Reed et Lowans, 2016). Tel que mentionné plus haut, la plupart des CASB se vendent en différents modules et ceux-ci doivent non seulement être compatibles entre eux, mais aussi avec les autres composantes de l'architecture. Comme l'entreprise a probablement déjà certains mécanismes et processus de sécurité tels des pare-feu, des logiciels de gestion d'information et d'événements de sécurité (*Security Information and Event Management* ou SIEM), des logiciels d'authentification ou bien des logiciels de gestion d'appareils mobiles (*Mobile Device Management* ou MDM), il faut que le CASB puisse s'intégrer à ces processus et à ces outils afin de ne pas créer de silos supplémentaires. Ce dernier point complexifie la sélection et l'implantation, mais surtout l'exploitation de ces solutions dans le temps, en plus d'augmenter les coûts, le nombre de ressources et les compétences requises.

3. **Le degré de nouveauté du produit**

   L'infonuagique telle qu'on la connaît aujourd'hui est un phénomène relativement nouveau et la sécurité de l'information dans un contexte infonuagique est encore plus récente. La définition des CASB ne date d'ailleurs que de 2012 (Lawson *et al.*, 2015b), montrant l'immaturité et la nouveauté du produit. Les fonctionnalités, les caractéristiques et les modes de fonctionnement des CASB ne sont pas encore bien définis et risquent d'évoluer dans les années à venir.

En terminant, bien que les CASB soient une solution à haut potentiel pour centraliser la gestion de la sécurité infonuagique, l'immaturité du marché et la complexité du produit rendent son adoption difficile. On se rend compte que ces produits, malgré les arguments de marketing des fournisseurs, sont loin de représenter une solution tous azimuts en sécurité de l'information. Il

s'agit plutôt d'un outil qui permet de centraliser certains mécanismes et activités de sécurité, ne remplaçant pas les logiciels et les outils actuellement en place. L'intégration des CASB avec ces outils est donc d'une très grande importance pour éviter de créer des silos dans les activités de sécurité de l'organisation, ajoutant une lourdeur dans l'exploitation de ces solutions.

Le quatrième chapitre de ce mémoire présente les requis en termes de CASB pour une entreprise du domaine de la finance et de l'assurance. Il s'agit du premier artefact réalisé et il permet de synthétiser l'information recueillie et analysée lors de la collecte de données. De plus, les CASB actuellement disponibles sont ensuite répertoriés et l'inventaire de leurs fonctionnalités est dressé afin de mieux comprendre l'offre et de la comparer aux requis de l'organisation (artefact 2). Finalement, un troisième tableau présente l'écart entre l'offre du marché et des requis technologiques et fonctionnels de l'organisation (artefact 3). La méthodologie choisie pour développer ces trois artefacts est décrite plus en détail dans le chapitre suivant.

Chapitre 3: Méthodologie

Le chapitre qui suit a pour objectif de décrire la méthodologie de *recherche action design* (RAD) adoptée pour ce mémoire. D'abord, une définition de la *recherche action design* appliquée aux technologies de l'information et des principes qui la sous-tendent seront exposés. Ensuite, le choix de cette méthodologie dans le contexte du mémoire sera justifié. Subséquemment, les étapes et les activités de la méthodologie sont détaillées, suivi de la façon dont elles ont été opérationnalisées pour l'atteinte des objectifs de ce mémoire.

3.1 Définition de la *recherche action design* (RAD)

Les technologies de l'information visent à étudier l'adoption et la gestion des technologies à un niveau individuel et organisationnel et sont souvent décrites comme une science appliquée (Iivari, 2007) puisque les théories qui en émergent devraient s'appliquer à un milieu organisationnel. Cependant, la réalité est toute autre et plusieurs professionnels se plaignent du manque de pertinence de la recherche académique pour la pratique (Benbasat et Zmud, 1999). En effet, le domaine des TI semble avoir de la difficulté à allier la théorie avec son application dans le contexte organisationnel (Benbasat et Zmud, 2003). Par conséquent, certaines méthodologies qui placent l'organisation au centre du processus de recherche, comme la recherche action, le *design science* et, plus récemment, la *recherche action design*, ont été proposées afin de remédier à ce problème.

La méthodologie adoptée pour le présent mémoire est la *recherche action design* qui a été proposée par Sein *et al.* (2011) en tant qu'approche hybride, à la croisée de la recherche action et du *design science*. La recherche action est une méthode par laquelle le chercheur étudie activement le changement organisationnel, c'est-à-dire qu'il participe au changement tout en l'étudiant (Baskerville et Myers, 2004). Le *design science*, pour sa part, cherche à résoudre des problèmes humains et technologiques par la conception d'artefacts qui se veulent innovateurs et utiles pour l'organisation (Hevner et Chatterjee, 2010). L'artefact créé à l'issue du *design science* peut prendre plusieurs formes telles qu'un construit, un modèle ou une instanciation (Hevner, March, Park et Ram, 2004). Plus précisément, Gregor et Hevner (2013) indiquent que les artefacts peuvent inclure des outils de modélisation ou de prise de décision, des stratégies de gouvernance ou des méthodes pour l'évaluation de technologies de l'information.

Une des limites du *design science* est toutefois qu'il ne tient pas bien compte du contexte organisationnel à partir duquel est créé l'artefact, donnant ainsi raison aux détracteurs qui accusent la recherche en TI de manquer de pertinence pour la pratique (Sein *et al.*, 2011). Ainsi, la méthode de *recherche action design* proposée par Sein *et al.* (2011) met l'accent sur l'intervention dans l'organisation afin de produire un artefact qui permettra de résoudre la problématique à l'étude. La résolution de ce problème organisationnel se fait grâce à des activités itératives d'intervention et d'évaluation, incorporées aux activités de développement de la solution (l'artefact) (Sein *et al.*, 2011). En effet, contrairement au *design science* dans lequel l'activité d'évaluation de l'artefact se fait à la toute fin de sa conception, la RAD propose que l'évaluation soit intégrée en continu lors du développement de l'artefact. Il en résulte donc une méthode itérative et dynamique qui tient compte de la rétroaction des membres de l'organisation à l'étude *pendant* la conception de l'artefact afin de garder les deux (l'artefact et les besoins organisationnels) bien alignés. Il faut noter que, malgré quelques différences, la méthode de Sein *et al.* (2011) est fortement influencée du *design science* tel que décrit par Hevner *et al.* (2004) et par Peffers *et al.* (2007) et que, comme présenté dans les prochaines sections, certains de ses principes s'appliquent aussi à la RAD.

Ainsi, la RAD est particulièrement adaptée au contexte de ce mémoire pour plusieurs raisons. D'abord, selon Hevner *et al.* (2004), la recherche inspirée du *design science* est idéale dans les cas où les requis et les contraintes sont instables et proviennent d'un contexte environnemental mal défini. Les CASB entrent dans cette catégorie puisque, comme mentionné dans la revue de la littérature, ils sont des produits complexes et ambigus, ce qui sous-tend que leurs fonctionnalités et leurs requis changent à mesure que se développent le marché, les connaissances et les besoins organisationnels. La *recherche action design* tient compte de cette instabilité dans les requis et permet une grande flexibilité puisque le développement de l'artefact est un processus itératif et dynamique qui s'alimente du contexte organisationnel et de la rétroaction des utilisateurs cibles (Sein *et al.*, 2011).

Ensuite, peu importe le type de CASB qu'une entreprise choisit, ce dernier devra interagir avec toutes les autres composantes de l'infrastructure de l'organisation, ajoutant une couche de complexité au problème de la définition des requis. La RAD tient compte de cette complexité

d'interaction entre les composantes puisque lors de son intervention, le chercheur devra comprendre le fonctionnement actuel de l'organisation afin d'en saisir les spécificités et de proposer un artefact qui s'intègre à ce contexte (Sein *et al.*, 2011).

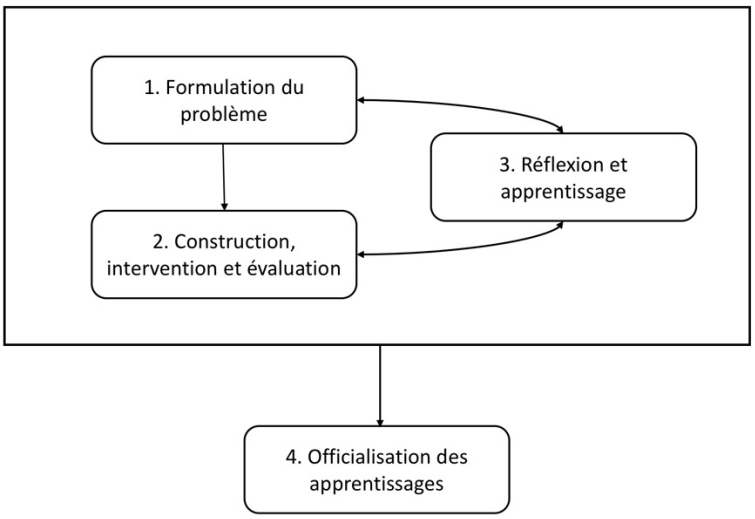
De plus, la sécurité de l'information, dans un contexte infonuagique, représente une inquiétude pour plusieurs organisations (Juels et Oprea, 2013). Les CASB sont perçus comme une solution potentielle aux problèmes de sécurité infonuagique, mais la définition des besoins qui y sont rattachés est présentement difficile à réaliser. D'ailleurs, cette problématique a été énoncée très clairement lors d'un entretien avec la direction du département de sécurité de l'information de l'entreprise participante. Leur participation à des forums d'échange où les défis de l'heure de leur industrie sont discutés montre que cela représente une problématique véritablement ancrée dans la réalité des organisations de cette industrie. Cette situation correspond à une des directives émises dans l'article de Hevner *et al.* (2004) pour faire une utilisation appropriée d'une approche tirée du *design science*.

Finalement, puisque les trois artefacts produits dans le cadre de ce mémoire sont en partie liés au contexte organisationnel dans lequel se déroule l'étude, l'approche de *recherche action design* proposée par Sein *et al.* (2011) est parfaitement appropriée. Les auteurs argumentent que leur méthodologie permet : 1) la résolution d'un problème organisationnel spécifique grâce à l'intervention du chercheur et 2) l'évaluation d'un artefact qui résout le problème rencontré dans le contexte particulier de l'organisation (Sein *et al.*, 2011). Considérant que l'étude se déroule au sein d'une entreprise du domaine de la finance et de l'assurance et que la collaboration des employés est requise afin de construire un ou des artefacts qui aident à résoudre leur problématique, la méthodologie de *recherche action design* semble donc toute désignée.

3.2 Description de la méthodologie

La présente section a pour objectif de présenter de façon détaillée la méthodologie adoptée pour ce mémoire. Pour ce faire, dans un premier temps, les grandes lignes de la méthodologie telle que décrite par Sein *et al.* (2011) sont exposées. La Figure 3.1 ci-dessous illustre la séquence de ces étapes. La section subséquente présente la façon dont les étapes préconisées ont été traduites dans l'approche méthodologique utilisée lors de la réalisation du présent mémoire.

Figure 3.1 : Processus de recherche selon la méthodologie de *recherche action design*
(Adaptation de Sein *et al.*, 2011, p.41)



3.2.1 La RAD selon Sein *et al.* (2011)

La méthodologie de *recherche action design* se décline en quatre étapes. Elles sont présentées dans la présente section avec une description des éléments importants qui ont été appliqués dans ce mémoire.

Étape 1 : Formulation du problème

La première étape consiste à étudier un problème. Sein *et al.* (2011) identifient deux façons de formuler le problème : soit en s'inspirant de la pratique comme c'est le cas ici ou soit en s'inspirant de la théorie. Les tâches effectuées lors de cette première étape sont les suivantes :

1.1. Identifier et conceptualiser l'opportunité de recherche.

Une problématique de recherche, ancrée dans la réalité organisationnelle d'une entreprise, est formulée à cette étape. Une des lignes directrices de Hevner *et al.* (2004) concernant les méthodologies dérivées du *design science* est de s'assurer de la pertinence du problème à l'étude. La problématique énoncée au Chapitre 1 du mémoire ainsi que les questions de recherche découlent de discussions avec des gestionnaires seniors de l'entreprise participante, ce qui démontre l'importance et la pertinence du problème. Les

CASB représentent une avenue de grand intérêt pour cette entreprise, mais dû au fait qu'ils sont très émergents et encore ambigus, il est difficile pour l'organisation de cerner ses besoins pour ce genre d'outil. Cette étude a donc pour but d'établir les fonctionnalités qu'un CASB devrait posséder pour une utilisation optimale dans le contexte d'une entreprise du domaine de la finance et de l'assurance. Conséquemment, les résultats du mémoire auront une application très pratique puisqu'ils répondent directement à un problème organisationnel. Malgré cela, certains éléments de ce problème pourront aussi être généralisés à plusieurs autres entreprises de l'industrie qui doivent se soumettre aux mêmes règles en termes d'impartition infonuagique.

1.2. Formuler la question de recherche.

La ou les questions de recherche clarifient les objectifs précis de l'étude.

1.3. Présenter le problème en tant qu'exemple d'une classe de problèmes.

Le problème énoncé aux étapes précédentes doit pouvoir être généralisé de façon à contribuer à la pratique et à la recherche. Le principe derrière la méthodologie RAD n'est pas d'agir en tant que consultant qui résout le problème précis d'une organisation, mais plutôt de tenter de générer des connaissances pouvant être généralisées à une classe de problèmes (Sein *et al.*, 2011) et être appliquées dans d'autres entreprises. Le présent mémoire tente de contribuer à définir une classe d'outils considérée comme émergente et d'ainsi aider les entreprises à prendre des décisions éclairées en la matière. Bien que l'étude se déroule au sein d'une seule organisation, une partie des résultats pourront être généralisés à toute l'industrie de la finance et de l'assurance canadienne puisque les entreprises qui la constituent ont des besoins très similaires en termes de sécurité de l'information à cause de la rigidité des normes et des lois les régissant. De plus, le monde de la sécurité de l'information dans cette industrie est très petit, ce qui signifie que les connaissances générées par ce mémoire pourront y être diffusées rapidement et facilement.

1.4. Identifier les contributions théoriques et les avancées technologiques potentielles.

La recherche de type RAD devrait contribuer à l'avancée des connaissances dans le domaine, ce qui rejoint la quatrième ligne directrice de Hevner *et al.* (2004). Ces connaissances doivent être identifiées dès le début du projet de recherche. La question

de la définition des besoins dans le contexte de produits complexes et ambigus comme les CASB mérite d'être explorée. Aucune étude n'existe pour l'instant sur ce type de technologie qui représente toutefois un fort potentiel pour assurer la sécurité des entreprises dans un contexte d'impartition infonuagique. Le mémoire vient donc combler un vide dans ce domaine.

1.5. S'assurer de l'engagement de l'organisation participante.

Un des principes à la base de la *recherche action design* est le développement d'un artefact par l'entremise d'une intervention en entreprise. Pour ce faire, la collaboration de l'organisation est vitale du début jusqu'à la fin du projet. Non seulement le chercheur devra être présent physiquement sur les lieux de l'entreprise, mais selon la méthodologie RAD, il devra interagir avec les employés et avoir accès à la documentation nécessaire afin de bien comprendre l'environnement organisationnel.

1.6. Identifier les rôles et responsabilités.

Il est important que l'organisation et le chercheur s'entendent sur les objectifs du projet de recherche, les rôles, les attentes et les responsabilités de chacun avant que l'intervention en entreprise ne débute afin d'éviter tout malentendu ou conflit pendant la réalisation de l'étude. Comme la nature de l'étude implique l'accès à de la documentation hautement confidentielle sur les processus et les exigences de sécurité de l'entreprise, il est très important que les attentes et les responsabilités face au chercheur soient bien établies a priori. C'est donc aussi à cette étape que la documentation nécessaire à l'étude sera identifiée et que l'entreprise devra s'assurer que le chercheur y ait accès.

Étape 2 : Construction, intervention et évaluation

La seconde étape est celle de « Construction, intervention et évaluation » qui tente de résoudre le problème défini à l'étape précédente. À ce point-ci, la collaboration de l'entreprise à l'étude est essentielle afin de favoriser le partage d'expériences et de savoirs entre le chercheur et l'organisation. De plus, le chercheur et les membres de l'organisation s'influencent mutuellement pour tenter de développer un artefact qui résoudra le problème. En outre, à cette étape s'effectue l'évaluation de l'artefact produit pour s'assurer qu'il réponde aux objectifs énoncés.

Contrairement au *design* science qui considère cette activité comme séquentielle à la création de l'artefact, la méthode de *recherche action design* intègre l'évaluation à la construction de l'artefact, faisant ainsi du design une activité itérative qui est alimentée par la contribution des membres de l'organisation participante. D'ailleurs, cette étape consiste en plusieurs cycles de construction, d'intervention et d'évaluation qui utilisent le savoir généré lors du cycle précédent pour améliorer l'artefact.

2.1. Trouver les cibles de création de savoir.

Les cibles de création de savoir sont les représentants organisationnels qui seront intrinsèquement intégrés en continu au processus d'élaboration de l'artefact. En effet, la participation des membres de l'entreprise est essentielle à la création de savoir puisque c'est grâce à leurs intrants, leurs suggestions et leur rétroaction continus que le chercheur pourra développer un artefact utile et pertinent.

2.2. Choisir la source de la conception.

Cette étape peut être, à un extrême, dominée par le développement de l'artefact technologique ou, à l'autre, par l'organisation lorsque la source d'innovation provient de l'intervention elle-même (Sein *et al.*, 2011). Tout comme l'affirment les auteurs, le développement d'un outil de structuration de la décision, dans le cas présent, un outil de compréhension et d'analyse des CASB, tient plus de l'innovation au niveau de l'organisation elle-même. En effet, même si un artefact visible sera créé, le processus de l'intervention lui-même, et toute la réflexion et la participation qu'il suscitera, sera la source d'un apprentissage organisationnel important. Tel que le disent Sein *et al.* (2011), il est alors de la plus grande importance de bien choisir et d'intégrer avec soin les membres de l'organisation au processus de réalisation de l'intervention. On peut parler, dans ce cas précis, d'un processus de co-construction de la connaissance.

2.3. Exécuter le cycle de construction, d'intervention et d'évaluation.

Cette étape se base sur le principe d'influence mutuelle entre le chercheur et les membres de l'organisation. Le chercheur amène des connaissances théoriques alors que les membres de l'entreprise ont un savoir spécifique au contexte organisationnel, ce qui permet d'avoir deux perspectives différentes sur le problème à l'étude (Sein *et al.*, 2011). Afin de développer l'artefact, le chercheur doit se baser sur la théorie, mais il doit surtout

tenir compte de l'environnement organisationnel, d'où l'importance de la rétroaction des utilisateurs et des employés. De plus, les auteurs mentionnent l'importance d'intégrer les activités d'évaluation à celles de construction et d'intervention afin de raffiner le design de l'artefact.

2.4. Évaluer s'il y a un besoin de répéter des cycles supplémentaires.

La méthodologie RAD se veut itérative, ce qui signifie que les activités de construction, d'intervention et d'évaluation effectuées précédemment servent de base aux subséquentes. Cependant, le chercheur doit être en mesure d'évaluer s'il est adéquat d'effectuer un cycle supplémentaire ou bien de s'arrêter pour éviter de tomber dans le piège des itérations perpétuelles.

Étape 3 : Réflexion et apprentissage

La troisième étape s'appelle « Réflexion et apprentissage » et elle s'effectue en même temps que les deux étapes précédentes. En effet, le chercheur se doit de constamment remettre en question ses conclusions afin de générer des solutions au problème. Au fur et à mesure qu'il avance dans son étude, il accumule du savoir spécifique à l'organisation qu'il applique ensuite à la création de l'artefact. Le processus doit être adapté aux nouvelles connaissances acquises lors de l'intervention au sein l'entreprise. Les activités qui caractérisent cette étape sont les suivantes :

3.1. Réfléchir à la conception et au design pendant le projet.

Comme le mentionnent Hevner *et al.* (2004) dans leurs lignes directrices en matière de *design science*, le design doit être perçu comme un processus de recherche. Il doit être central à toutes les activités de recherche et le chercheur doit constamment penser à la façon dont ses interventions influencent la conception de l'artefact final. Il doit aussi garder en tête que l'artefact conçu devra s'appliquer à une classe de problèmes et non pas seulement à l'organisation à l'étude.

3.2. S'assurer du respect des principes de recherche.

La rigueur, telle que le font valoir Hevner *et al.* (2004), est essentielle dans toute méthodologie de recherche. Le chercheur se doit donc d'appliquer la méthodologie dans son intégralité et de respecter les principes énoncés aux étapes précédentes.

3.3. Analyser les résultats des interventions selon les buts énoncés.

Les objectifs de l'étude sont énoncés avant d'entamer l'intervention en milieu organisationnel, à l'Étape 1 : Formulation du problème. À la fin de son mandat, le chercheur fait une réflexion sur ces objectifs et évalue s'ils ont été atteints. Si ce n'est pas le cas, il doit tenter d'identifier les causes et proposer des explications.

Étape 4 : Officialisation des apprentissages

Finalement, la dernière étape est celle d'« Officialisation des apprentissages ». À ce point-ci, la solution qui a été développée pour répondre aux besoins spécifiques d'une organisation doit être généralisée à une classe de problèmes dans un domaine particulier. En effet, bien que le propre de la *recherche action design* soit qu'elle se déroule dans une organisation spécifique, les problèmes qu'elle tente de résoudre ne sont pas généralement spécifiques à cette organisation, mais devraient pouvoir être généralisés à un domaine ou une industrie. Les activités réalisées lors de cette étape sont :

4.1. Transférer les apprentissages en concepts pour une classe de problèmes du domaine à l'étude.

Il est difficile de faire des généralisations lorsque la méthode RAD est employée dû au fait que le développement de l'artefact est intimement lié à l'environnement organisationnel dans lequel se déroule l'étude. Cependant, le chercheur devrait pouvoir tirer de son artefact, un ensemble de fonctionnalités ou de caractéristiques qui s'appliquent à une classe de problèmes à plus haut niveau que le problème spécifique de l'organisation étudiée (Sein *et al.*, 2011).

4.2. Partager les résultats avec les professionnels du milieu.

Les connaissances générées par la recherche en TI se doivent d'être applicables dans les organisations (Benbasat et Zmud, 1999). Par conséquent, une des activités de la *recherche action design* est de partager le savoir acquis avec des professionnels de l'industrie afin qu'ils puissent en bénéficier et éventuellement l'appliquer dans le cadre de leur travail.

4.3. Exprimer les apprentissages à la lumière des théories sur lesquelles se base l'étude.

Cette activité s'applique surtout dans le cas où le problème a été formulé en s'inspirant de la théorie plutôt que de la pratique. Elle représente une réflexion et une discussion sur les modèles théoriques utilisés lors du projet de recherche et les apports que ce projet a sur ces modèles.

4.4. Formaliser les résultats pour la diffusion.

La formalisation peut se faire de plusieurs façons, notamment par la publication d'un article, d'une thèse, d'un mémoire ou par la participation à des conférences académiques où est présentée l'étude.

3.2.2 Détails de l'application de la RAD dans le présent mémoire

S'inspirant des étapes de l'approche présentée par Sein *et al.* (2011), le Tableau 3.1, présenté à la page suivante, offre une description des activités qui ont été effectuées à chacune des étapes de la méthodologie de *recherche action design* utilisée pour la réalisation de ce mémoire. Dans la dernière colonne, on y retrouve, les chapitres du mémoire qui correspondent à chacune des étapes.

Tableau 3.1 : Étapes méthodologiques du présent mémoire

Étapes selon Sein *et al.* (2011)	Sous-étapes selon Sein *et al.* (2011)	Dates	Activités réalisées dans le cadre de ce mémoire	Extrant(s) des activités
1. Formulation du problème	1.1. Identifier et conceptualiser l'opportunité de recherche.	Février 2016	• Discussions avec des professionnels de l'organisation participante afin de mieux cibler leurs défis en sécurité infonuagique. • Recherches sommaires sur la problématique choisie afin de définir les grandes lignes du projet de recherche.	Chapitre 1 : Introduction
	1.2. Formuler la question de recherche.	Février 2016	• Réalisation d'une revue de la littérature sur : 1) infonuagique et des défis qui l'accompagnent ; 2) solutions possibles et 3) CASB. • Formulation des questions de recherche.	
	1.3. Présenter le problème en tant qu'exemple d'une classe de problèmes.	Mars 2016	• Rédaction de la problématique. • Réflexion sur la contribution potentielle du projet, à savoir comment les résultats pourraient être généralisés à d'autres organisations.	
	1.4. Identifier les contributions et avancées technologiques potentielles.	Mars 2016	• Raffinement des questions de recherche et de la problématique. • Rédaction des contributions potentielles de l'étude.	
	1.5. S'assurer de l'engagement de l'organisation.	Mars et avril 2016	• Obtention du consentement de l'organisation. • Entente sur la participation monétaire et logistique de l'organisation participante. • Signature de l'entente de confidentialité avec l'organisation participante. • Approbation de l'étude par le Comité d'éthique de la recherche de HEC Montréal.	
	1.6. Identifier les rôles et les responsabilités.	Avril 2016	• Établissement des grandes lignes du projet de recherche et comment le tout serait opérationnalisé au sein de l'organisation participante (échange de courriels avec le directeur superviseur de l'organisation).	
		Mai 2016	• Rencontre avec le directeur superviseur en entreprise pour établir les attentes et les frontières du projet. • Rencontre avec les membres de l'organisation participante pour expliquer l'étude et ses objectifs. • Négociation de l'accès à la documentation confidentielle sur les pratiques de sécurité de l'entreprise.	
2. Construction, intervention et évaluation	2.1. Trouver les cibles de création du savoir.	Mai 2016	• Jumelage avec un employé de l'organisation (parrain) pour faciliter l'intégration et l'organisation de rencontres avec les spécialistes et les experts au sein de l'organisation. • Identification des personnes clés de l'entreprise (spécialistes et experts) qui sont intégrées de près au développement des artefacts.	Chapitre 2 : Revue de la littérature
	2.2. Choisir la source de conception.	Mai 2016	• L'organisation est au cœur de cette étape ; s'assurer de conserver l'engagement des personnes identifiées.	

Tableau 3.1 : Étapes méthodologiques du présent mémoire (suite)

Étapes selon Sein *et al.* (2011)	Sous-étapes selon Sein *et al.* (2011)	Dates	Activités réalisées dans le cadre de ce mémoire	Extrant(s) des activités
2. Construction, intervention et évaluation (suite et fin)	2.3. Exécuter le cycle de construction, d'intervention et d'évaluation.	Mai à août 2016	• Étude des normes et des meilleures pratiques en sécurité de l'information afin de préparer l'intervention en entreprise (étude approfondie de la littérature). • Identification des défis spécifiques à la sécurité infonuagique de l'entreprise. • Observation participante au sein de l'entreprise (participation aux réunions d'équipe, prise de notes et conversations informelles) permettant de comprendre en action les défis rencontrés. • Inventaire et documentation des processus et des activités de sécurité de l'entreprise ainsi que des principes qui les sous-tendent (grâce à des rencontres d'équipe, la consultation de la documentation de l'entreprise, des entrevues informelles avec des responsables de la sécurité de l'information, des architectes, des spécialistes en cryptographie et des conseillers en gouvernance de la sécurité). • Identification des requis fonctionnels et technologiques pour un CASB qui serait éventuellement utilisé au sein de l'organisation participante et développement de la grille de requis présentée dans les résultats (artefact #1). • Rencontre avec spécialistes (conseillers en gouvernance, responsables de sécurité, architectes de sécurité) de l'organisation participante pour recueillir leur rétroaction suite aux rencontres avec les fournisseurs. • Présentation informelle hebdomadaire de la grille des requis en sécurité au parrain afin d'évaluer le travail effectué et d'établir les étapes suivantes et les spécialistes à rencontrer. • Consultation de la documentation de Gartner et de Forrester afin de faire le choix final des douze fournisseurs de CASB qui seront analysés dans le cadre de l'étude. • Documentation des fonctionnalités des CASB disponibles sur le marché en faisant une analyse approfondie des sites web des fournisseurs (et de tous les documents qu'ils contiennent comme, par exemple, des fiches techniques de produit, des livres blancs et du matériel de marketing). • Organisation de trois rencontres virtuelles avec deux fournisseurs de CASB parmi les douze sélectionnés. • Échange de courriels avec deux autres fournisseurs de CASB parmi les douze sélectionnées. • Développement d'une grille recensant les fonctionnalités et les caractéristiques des CASB choisis (artefact #2) grâce à l'analyse de l'information recueillie.	Chapitre 4 : Résultats
	2.4. Évaluer s'il y a un besoin de répéter des cycles.	Mai à août 2016	• Évaluation du travail accompli et des artefacts en développement grâce à des discussions avec les employés de l'organisation. • Présentation informelle de l'évolution du travail au directeur superviseur en entreprise toutes les quatre semaines pour recueillir sa rétroaction. • Développement d'une grille permettant d'analyser les écarts entre les requis de l'organisation et les caractéristiques des produits sur le marché (artefact #3 : Tableau 5.1).	Chapitre 4 : Résultats et Chapitre 5 : Discussion

Tableau 3.1 : Étapes méthodologiques du présent mémoire (suite)

Étapes selon Sein *et al.* (2011)	Sous-étapes selon Sein *et al.* (2011)	Dates	Activités réalisées dans le cadre de ce mémoire	Extrant(s) des activités
3. Réflexion et apprentissage	3.1. Réfléchir à la conception et au design pendant le projet.	Mai à août 2016	• Observation participante au sein de l'entreprise (participation aux réunions d'équipe et conversations formelles et informelles) permettant de valider la compréhension des requis, des artefacts en développement et la pertinence des solutions formulées afin de garder les livrables alignés sur une interprétation juste des requis compris et documentés.	Chapitre 4 : Résultats
	3.2. S'assurer du respect des principes de recherche.	Avril 2016	• Rédaction du chapitre sur la méthodologie du mémoire.	Chapitre 3 : Méthodologie
		Mai à août 2016	• Respect des étapes qui sont énoncées dans la méthodologie de Sein *et al.* (2011) et contenues dans la déclaration approuvée par le Comité d'éthique de HEC. • Documentation de toutes les interactions en entreprise (agenda et prise de notes).	
	3.3. Analyser les résultats de l'intervention selon les buts énoncés.	Mai à août 2016	• Suite à la rétroaction des employés de l'organisation et du directeur superviseur, évaluation du premier et du second artefact selon les objectifs de l'organisation et selon les objectifs de l'étude afin de déterminer s'ils ont été atteints. • Formalisation de l'analyse menant au développement de l'artefact #3 suite aux commentaires des membres de l'organisation sur les deux premiers artefacts. • À la fin de l'intervention, rencontre avec le directeur superviseur afin de faire le bilan sur les apprentissages et acquis faits pendant l'intervention.	Chapitre 4 : Résultats
		Août à octobre 2016	• Rédaction du chapitre de la Discussion dans lequel sont présentées une analyse des résultats ainsi qu'une discussion sur le potentiel et les limites des CASB pour l'organisation à l'étude et pour d'autres entreprises de la même industrie. • Discussions des résultats et de l'analyse avec la directrice de recherche.	Chapitre 5 : Discussion
4. Officialisation des apprentissages	4.1. Transférer les apprentissages en concepts pour une classe de problèmes du domaine à l'étude.	Septembre et octobre 2016	• Réflexion sur les apprentissages que d'autres entreprises peuvent tirer de l'exercice fait. • Rédaction de la section des Contributions à la pratique et à la recherche appliquée du chapitre de conclusion.	Chapitre 6 : Conclusion et Projet d'article
	4.2. Partager les résultats avec les professionnels du milieu.	Août 2016	• Présentation formelle ? de l'artefact #1 sur les requis technologiques et fonctionnels en sécurité infonuagique aux membres de l'entreprise participante afin de présenter les conclusions préliminaires de l'intervention. • Présentation aux membres de l'organisation de l'offre de CASB (artefact #2) et des constats par rapport à l'implantation potentielle d'un CASB selon l'analyse des écarts entre les besoins et l'offre du marché (artefact #3). • Présentation aux étudiants de la M.Sc. en TI dans le cadre du cours d'Atelier de recherche en systèmes d'information. Cette présentation a permis de familiariser les futurs professionnels au concept de CASB comme classe d'outils de sécurité infonuagique. • Rédaction d'un projet d'article sur l'étude.	

Tableau 3.1 : Étapes méthodologiques du présent mémoire (suite et fin)

Étapes selon Sein *et al.* (2011)	Sous-étapes selon Sein *et al.* (2011)	Dates	Activités réalisées dans le cadre de ce mémoire	Extrant(s) des activités
4. Officialisation des apprentissages (suite et fin)	4.3. Exprimer les apprentissages à la lumière des théories sur lesquelles se base l'étude.	Septembre et octobre 2016	• Rédaction de la discussion du Chapitre 5 qui démontre les écarts entre les requis de l'organisation et les fonctionnalités des CASB (artefact #3).	Chapitre 5 : Discussion et Projet d'article
	4.4. Formaliser les résultats pour la diffusion.	Décembre 2016	• Dépôt du mémoire. • Soumission du plan pour un article.	

Chapitre 4: Résultats

Le résultat de la première étape de la méthodologie RAD, la « Formulation du problème », a été présenté en introduction à ce mémoire. La revue de la littérature (Chapitre 2) a permis d'entamer la deuxième étape, soit la « Construction, intervention et évaluation » en établissant les bases nécessaires à la planification de l'intervention en entreprise. Le Chapitre 4 présente maintenant les résultats de l'intervention en entreprise. L'intervention en soi correspond aux deuxième et troisième étapes de la méthodologie, c'est-à-dire qu'elle a permis de construire la grille des requis fonctionnels et technologiques et d'ensuite poser un regard critique sur le travail accompli grâce à la rétroaction des employés de l'organisation afin d'évaluer en continu le travail pour décider si d'autres itérations étaient nécessaires.

4.1 Mise en contexte

Avant de présenter les résultats de l'intervention en entreprise, il convient de rappeler le contexte dans lequel a eu lieu la collecte de données.

Le développement des artefacts s'est fait au sein du département de sécurité de l'information d'une grande[29] entreprise canadienne qui offre une gamme complète de produits et de services financiers aux particuliers et aux entreprises. Comme les processus et l'information partagés par l'entreprise pendant la réalisation de l'étude sont de nature sensible, celle-ci souhaite conserver l'anonymat. La participation de l'entreprise était volontaire et la direction du département de sécurité se sentait démunie face au potentiel de cette classe d'outils. Son intérêt pour le projet était sincère, à un point tel qu'elle était prête à accorder à un petit groupe de professionnels intéressés par les CASB, le temps nécessaire pour participer à l'atteinte des objectifs du présent mémoire. Notons que j'ai été rémunérée à titre de stagiaire pendant la collecte de données qui s'est étalée sur une période de trois mois pendant l'été 2016.

Le département de sécurité de l'information de l'entreprise à l'étude s'occupe de la gestion des identités et des accès, des politiques de gouvernance en sécurité, de la prévention de la fraude et

[29] Selon le Ministère de l'innovation, des sciences et du développement économique du Canada, une entreprise de grande taille emploie plus de 500 employés rémunérés (Ministère de l'innovation, sciences et développement économique Canada, page consultée le 26 mai 2016, https://www.ic.gc.ca/eic/site/061.nsf/fra/ 02803.html).

de la mise en place de processus de sécurité dans tous les départements et tous les points de services. Le mandat à réaliser en entreprise était d'établir les besoins et les exigences en sécurité de l'information dans un contexte d'impartition infonuagique. Ce mandat ne constituait pas un exercice théorique, mais répondait à un réel besoin de l'organisation. En participant à la réalisation de ce mandat, l'entreprise souhaitait vraiment en apprendre davantage sur les CASB et les fonctionnalités qui y sont rattachées afin de voir s'ils pourraient combler ses besoins en sécurité. La liste des besoins et des exigences s'est par la suite traduite, pour ce mémoire, en une liste de requis technologiques et fonctionnels d'un CASB qui serait utilisé par l'organisation, tel que l'indique la première question de recherche de l'étude. En conséquence, les résultats de ce mémoire seront utiles à l'organisation pour l'aider à comprendre cette nouvelle classe d'outils, pour la guider dans le choix d'une solution CASB ou bien pour établir les requis à inclure dans un appel d'offres pour ce type de logiciel.

L'organisation à l'étude a émis le désir de se tourner davantage vers l'infonuagique dans les prochaines années, reconnaissant l'importance grandissante de ce mode d'approvisionnement. Néanmoins, comme nous l'avons vu dans la revue de la littérature, pour beaucoup d'entreprises, l'infonuagique, de par sa nouveauté, impose un lot de défis tant au niveau du choix d'une solution appropriée, qu'au niveau légal ou encore de la sécurité. En effet, les processus actuels d'approvisionnement en services TI de l'entreprise ont été créés pour la gestion des fournisseurs de services traditionnels et le virage vers l'infonuagique implique plusieurs changements. De surcroît, considérant que l'organisation étudiée œuvre dans le domaine de la finance et de l'assurance, elle détient énormément d'informations confidentielles sur ses clients, sur ses employés et sur ses partenaires et elle a l'obligation légale de les protéger en tout temps. Si elle décide d'impartir à des fournisseurs de services infonuagiques le traitement et le stockage de ces données, elle voudra d'abord s'assurer que toutes les précautions soient prises pour conserver leur confidentialité, leur intégrité et leur disponibilité.

Avec l'augmentation continuelle de la consommation de services infonuagiques, l'entreprise se voit confrontée à la lourdeur associée à la gestion de la sécurité infonuagique. Elle étudie donc la possibilité d'acquérir un CASB pour faciliter la gestion de ces services et assurer la mise en place des politiques de gouvernance en sécurité de l'information pour ce mode d'approvisionnement. Comme elle entrevoit une augmentation du nombre de services infonuagiques utilisés dans les

prochaines années, elle souhaite dès maintenant centraliser, standardiser et, autant que possible, automatiser la sécurité associée à ce mode d'approvisionnement pour en faciliter la gestion.

4.2 Les requis en sécurité infonuagique de l'organisation à l'étude

Cette section vise à présenter les résultats de l'intervention. D'abord, les activités méthodologiques correspondant à l'étape de « Construction, intervention et évaluation » sont détaillées. Le tout est suivi des résultats qui comprennent d'abord les requis technologiques et fonctionnels pour un CASB dans le contexte de l'organisation étudiée et ensuite, la description des fournisseurs actuels de CASB et des fonctionnalités offertes par leurs produits.

4.2.1 Description détaillée de l'étape méthodologique de « Construction, intervention et évaluation »

L'étape de « Construction, intervention et évaluation » vise à développer les artefacts qui constituent les extrants ou les livrables du projet de recherche. Un des aspects importants de la méthodologie RAD de Sein *et al.* (2011) est le principe du développement par itérations qui demande une réflexion de la part du chercheur suite aux commentaires des membres de l'organisation. Cette réflexion permet de peaufiner l'artefact afin de le rendre le plus pertinent possible pour l'entreprise, mais aussi pour le domaine cible.

L'objectif du présent mémoire est le développement de trois artefacts : 1) la grille des requis technologiques et fonctionnels de l'entreprise, 2) la grille d'évaluation des fournisseurs actuels et 3) la grille des écarts entre les deux premiers artefacts (les requis et l'offre). Chacun des trois répond à la définition d'un artefact de Gregor et Hevner (2013) et de Hevner et Chatterjee (2010), c'est-à-dire qu'ils ont été développés en tenant compte du contexte organisationnel et de façon itérative, soit en y intégrant en continu la rétroaction des employés. Bien que l'organisation eût un intérêt à en apprendre davantage sur les CASB et que certains de ses membres ont participé aux rencontres avec les fournisseurs, le plus important pour elle était d'abord d'inventorier ses besoins et les requis nécessaires en matière de sécurité de sécurité de l'information dans un contexte infonuagique. Ainsi, les prochains paragraphes s'attardent principalement aux deux premiers artefacts dont le développement fut directement influencé par l'environnement

organisationnel ainsi que la rétroaction de ses membres. La réalisation de ces deux artefacts s'est faite en parallèle puisque les discussions concernant les caractéristiques et fonctionnalités des CASB ont alimenté la réflexion et les commentaires sur les requis de sécurité de l'organisation. Pour ce qui est du troisième artefact, son développement a pu se faire à la suite des deux autres puisque la grille présentée est en fait la formalisation de l'analyse des écarts entre le contenu de l'artefact #1 et celui de l'artefact #2.

La première activité de l'étape de « Construction, intervention et évaluation », soit l'identification des cibles de création de savoir, a été effectuée dans la première semaine de l'intervention en entreprise. D'abord, un jumelage a été fait avec un conseiller en gouvernance de la sécurité qui avait comme tâche de mettre en place les exigences entourant l'utilisation de l'infonuagique en termes de sécurité. Ce parrainage a facilité, d'une part, l'intégration dans l'équipe et, d'une autre part, l'identification des cibles de création du savoir. Il convient de rappeler que, selon Sein *et al.* (2011), les cibles de création du savoir sont les représentants organisationnels qui sont intégrés au développement de l'artefact. Dès le début de l'intervention, certaines personnes ont pu être identifiées comme telles. Elles incluent plusieurs employés de différents groupes au sein du département TI, soit des architectes de sécurité, des conseillers en gouvernance de la sécurité, des responsables en sécurité de l'information de certaines unités d'affaires et des gestionnaires du département de sécurité. En tout, douze spécialistes ont été rencontrés individuellement ou en petits groupes tout au long de l'étude. Certaines de ces personnes ont été identifiées dès le début de l'intervention en entreprise grâce au parrain, alors que d'autres ont plutôt été proposées par les gens interviewés selon une technique d'échantillonnage appelée « boule de neige » (Kumar, 2014).

Une fois les principales cibles de création du savoir identifiées, il a été possible de commencer le premier cycle de « Construction, d'intervention et d'évaluation » pour reprendre les termes propres à la méthodologie RAD. En premier lieu, il était important de se familiariser avec la documentation liée aux processus et aux exigences de sécurité de l'organisation. Celles-ci sont divisées en positionnements et en encadrements. Les premiers sont des documents qui consignent les bonnes pratiques en sécurité pour une technologie ou un domaine d'activité spécifique. Les positionnements sont de nature plus suggestive que normative, contrairement aux encadrements. Ces derniers contiennent plutôt des exigences et des pratiques qui doivent

obligatoirement être mises en place dans toute l'organisation, sans exception. Les positionnements et les encadrements sont divisés en plusieurs domaines ou thèmes et ils représentent environ 150 pages de documentation. Certaines pratiques et certains contrôles contenus dans ces documents s'appliquent aussi à un contexte d'impartition infonuagique et ils ont servi de base à l'identification des requis présentés dans le Tableau 4.2. En plus de la documentation spécifique au contexte organisationnel, les normes présentées dans la revue de la littérature du Chapitre 2 ont servi de fondements théoriques.

Une fois que les bases théoriques furent jetées, il a été possible de commencer à organiser les rencontres avec les personnes identifiées comme « cibles de création du savoir ». Ces rencontres avaient pour but de cerner les requis technologiques et fonctionnels que devrait avoir un CASB implanté dans l'organisation et qui ont ensuite été consignés dans une grille. Dans l'esprit de la méthodologie de *recherche action design*, l'élaboration de cette grille s'est fait en plusieurs itérations, à la suite d'observations et de discussions tenues dans l'entreprise. Au final, l'objectif était d'intégrer plusieurs perspectives afin d'obtenir un portrait aussi complet que possible des besoins de sécurité de l'information de l'organisation à l'étude et, par la suite, de traduire ces besoins en requis fonctionnels et technologiques. Comme le veut la méthodologie, l'important était aussi de respecter continuellement le cycle d'identification et de validation afin de garder les artefacts produits bien ancrés dans la réalité terrain.

Ainsi, chaque itération s'est déroulée comme suit. Chacune des personnes rencontrées avait un champ d'expertise spécifique comme, par exemple, la relation avec les fournisseurs, la cryptographie (la discipline liée au chiffrement et à la protection de l'information) ou la gestion des vulnérabilités. Elles ont été consultées pour recueillir leurs recommandations spécifiques à leur domaine d'expertise en lien avec l'utilisation de l'infonuagique, mais elles ont aussi pu donner leur opinion sur l'entièreté du document de requis. Cela a permis d'obtenir des points de vue variés sur la grille des requis présentée dans ce mémoire. Ces rencontres ont varié en durée, allant de trente minutes à une heure et demie selon les cas et se sont étalées sur les trois mois qu'a duré le mandat. Elles se déroulaient généralement de la façon suivante : d'abord les grandes lignes du projet de recherche étaient expliquées, ensuite le document de requis (la version en cours de développement) était sommairement présenté, les recommandations spécifiques au

champ d'expertise de la personne étaient recueillies et, si le temps le permettait, les commentaires sur les autres sections du document étaient récoltés.

À la suite de chacune des rencontres, une analyse de l'information récoltée devait être menée. Cette étape cruciale a permis de distinguer les faits des opinions des professionnels rencontrés et de comprendre comment leurs propos pouvaient être traduits en requis pour un CASB. De plus, chaque expert s'exprimait sur son domaine et n'avait pas la même vue d'ensemble qu'avait le chercheur. Il fallait donc comprendre comment les propos de chacun s'intégraient à l'ensemble des requis à l'échelle de l'organisation, donc au-delà de leur champ d'expertise spécifique. Ce travail de réconciliation et d'analyse de l'information a permis de dresser un portrait global des requis pour l'ensemble de l'organisation. Par la suite, le document était mis à jour et envoyé par courriel à la personne rencontrée pour vérifier que ses observations avaient été bien documentées ou pour obtenir d'autres suggestions, le cas échéant.

Dans le cadre de ces itérations, lorsque jugé nécessaire, certains spécialistes ont été rencontrés plus d'une fois. À la fin du mandat, une dernière itération a eu lieu dans le cadre d'une rencontre avec deux directeurs, dont le directeur principal du département de sécurité. Cette présentation des résultats, d'une durée de près de deux heures tenue le 17 août 2016, a permis de recueillir les derniers commentaires quant au contenu présenté dans la section suivante du mémoire (artefacts #1, #2 et #3).

Le Tableau 4.1 présente les différentes personnes rencontrées selon leur titre (l'emploi du masculin a été privilégié), le nombre de rencontres formelles qui ont eu lieu avec chacune d'entre elles et les dates de chacune de ces rencontres. Il est à préciser que le parrain a participé à toutes ces rencontres, sauf celles du 17 août à cause d'un conflit d'horaire.

Tableau 4.1 : Sommaire des rencontres avec les spécialistes de l'organisation

Titre des professionnels rencontrés	Nombre d'entrevues	Date
• Directeur de l'équipe de gouvernance de sécurité	1	25 mai 2016
• Chef de l'équipe de gouvernance • Directeur de l'équipe de gouvernance de sécurité	3	31 mai 2016 10 juin 2016 7 juillet 2016
• Architecte de sécurité 1 • Architecte de sécurité 2	1	1 juin 2016
• Chef de l'équipe de gouvernance • Conseiller en gouvernance spécialisé dans la relation avec les fournisseurs et la gestion des incidents	1	2 juin 2016
• Chef de l'équipe responsable des tests d'intrusion et des balayages de vulnérabilités	1	6 juin 2016
• Conseiller en gouvernance spécialisée dans la gestion des identités et des accès	1	15 juin 2016
• Responsable en sécurité de l'information spécialisé dans les technologies utilisées dans l'organisation	1	16 juin 2016
• Responsable en sécurité de l'information spécialisé en cryptographie	1	22 juin 2016
• Architecte de sécurité 3	1	23 juin 2016

• Groupe d'intérêt CASB
  ○ Architecte de sécurité 2
  ○ Architecte de sécurité 3
  ○ Chef de l'équipe de gouvernance
• Responsable en sécurité de l'information spécialisé dans les technologies utilisées dans l'organisation
	1	27 juillet 2016

• Chef de l'équipe de gouvernance • Directeur de l'équipe de gouvernance de sécurité • Directeur principal du département de sécurité	1	17 août 2016

Mis à part ces rencontres, un comité informel de gens intéressés à en apprendre davantage sur les CASB a été constitué à la fin juin. Dans le tableau précédent, ce comité est nommé « Groupe d'intérêt CASB » et il comprend deux architectes de sécurité, le chef d'équipe et un conseiller de gouvernance (le parrain) et un responsable de la sécurité de l'information. Ces gens ont participé à trois rencontres virtuelles avec les fournisseurs de CASB (qui n'ont pas été incluses dans le tableau puisqu'elles n'ont pas eu d'impact sur le développement de la grille des requis) et à une discussion de groupe à la suite des rencontres avec les fournisseurs pour discuter des CASB dans le contexte organisationnel spécifique de leur employeur. L'analyse des propos tenus lors de cette conversation du 27 juillet 2016 a été spécialement utile pour cerner les besoins de l'organisation spécifiquement en termes de requis fonctionnels et technologiques pour un CASB.

En plus des requis, ce chapitre présente aussi un tableau des fonctionnalités des CASB actuellement sur le marché. Ces fonctionnalités ont été identifiées suite à l'examen de diverses sources comme les pamphlets d'information des fournisseurs, des appels ou des échanges de courriels avec des représentants des fournisseurs et des documents disponibles sur Internet. De plus, tel que mentionné au paragraphe précédent, trois rencontres virtuelles ont été organisées avec deux fournisseurs afin qu'ils présentent leur produit et en fassent la démonstration.

4.2.2 Présentation des résultats

La grille ci-dessous reprend en partie les défis répertoriés dans la littérature et présentés précédemment dans le Tableau 2.1 afin de faire l'inventaire des requis fonctionnels et technologiques en sécurité de l'information d'une organisation de l'industrie de la finance et de l'assurance dans un contexte infonuagique (artefact #1). Cette grille représente aussi la réponse à la première question de recherche qui visait à identifier les requis fonctionnels et technologiques pour un CASB utilisé dans l'industrie de la finance et de l'assurance. Ces requis représentent l'idéal pour un CASB dans le respect des frontières fixées par les quatre grands objectifs que cette classe d'outils entend remplir (voir la section 2.6.1.1).

Le Tableau 4.2 présente les requis qui sont séparés d'abord selon les requis fonctionnels des CASB et ensuite selon les requis technologiques. Le titre de chacune de ces sections est dans une cellule grisée pour mieux marquer la distinction. Ensuite, les notions de confidentialité, d'intégrité et de disponibilité (CIA) sont reprises dans la colonne de gauche. À celles-ci s'ajoute celle de la gouvernance qui englobe la conformité aux lois et aux normes ainsi que l'imputabilité. Une dernière section, nommée « Autres », correspond aux requis qui ne conviennent à aucune des quatre premières catégories, mais qui s'avèrent tout de même essentiels. On se souviendra que la confidentialité est la capacité de limiter l'accès aux données aux seules personnes autorisées ; l'intégrité est l'habileté de préserver la structure et le contenu des données alors que la disponibilité permet de s'assurer que les données sont accessibles aux personnes autorisées en tout temps (Ardagna *et al.*, 2015). La gouvernance, pour sa part, consiste en l'ensemble des politiques, des moyens et des processus mis en place pour assurer l'imputabilité et le contrôle sur les activités de l'organisation (von Solms et von Solms, 2009). Ensuite, dans la grille, pour chaque

requis global identifié, des requis plus spécifiques sont recensés. En italique, sous chacun des besoins spécifiques, on retrouve une définition ou une précision qui donne plus de détails sur le requis en question et la façon dont il s'applique aux CASB. Finalement, les crochets dans les deux dernières colonnes à droite montrent pour quels types de services et pour quels modes d'implantation le requis s'avère pertinent.

Tableau 4.2 : Requis de sécurité de l'organisation dans un contexte infonuagique

Objectifs de sécurité	Requis globaux	Requis spécifiques	Type de service			Mode d'implantation	
			SaaS	PaaS	IaaS	Public	Privé (via un tiers)
Requis fonctionnels							
a. Confidentialité	a.1. Gestion de l'identité et des accès pour s'assurer que seules les personnes autorisées aient accès.	a.1.1. Fédération des identités. • *La fédération des identités permet de gérer l'identité et les attributs d'un utilisateur au travers de différents systèmes (Rountree, 2013). Dans le cas de l'infonuagique, comme plusieurs services sont généralement utilisés, la fédération des identités permet d'avoir un identifiant unique pour tous les services. Le CASB doit intégrer la fédération des identités pour les services infonuagiques.*	✓	✓	✓	✓	✓
		a.1.2. Intégration des politiques de gestion des accès et des privilèges de l'entreprise. • *Les privilèges et les autorisations associés à chaque utilisateur doivent pouvoir être intégrés au CASB afin qu'il les applique à chacun des services infonuagiques. Cette fonctionnalité évite une gestion individuelle des accès pour chaque service.*	✓	✓	✓	✓	✓
		a.1.3. Authentification multi-facteur pour les comptes à hauts privilèges (comptes bénéficiant de privilèges d'administrateur ou à haut risque de sécurité pour l'organisation). • *L'authentification d'un utilisateur peut se faire selon trois catégories : ce qu'il sait (ex : un mot de passe), ce qu'il possède (ex : une carte bancaire) ou ce qu'il est (ex : une mesure biométrique comme l'empreinte digitale). L'authentification multi-facteur exige au moins deux facteurs parmi les trois catégories (Rountree, 2013). L'authentification multi-facteur doit être faite par le CASB pour les comptes à hauts privilèges.*	✓	✓	✓	✓	✓

Tableau 4.2 : Requis de sécurité de l'organisation dans un contexte infonuagique (suite)

Objectifs de sécurité	Requis globaux	Requis spécifiques	Type de service			Mode d'implantation	
			SaaS	PaaS	IaaS	Public	Privé (via un tiers)
a. Confidentialité (suite)	a.1 Gestion de l'identité et des accès pour s'assurer que seules les personnes autorisées aient accès (suite et fin).	a.1.4 Contrôle des accès basé sur le rôle (*Role-based Access Control* ou RBAC). • *Le RBAC permet à l'administrateur du système de créer différents rôles basés sur le poste occupé par les employés. Les permissions sont ensuite attribuées à ces rôles. Les utilisateurs sont assignés à un rôle et obtiennent les permissions liées à ce rôle. Le RBAC facilite donc l'arrivée d'employés puisqu'on n'a pas à créer un profil d'accès pour chaque nouvel employé, on n'a qu'à l'assigner à un rôle qui lui donnera automatiquement les accès dont il a besoin pour accomplir son travail (Chen, Violetta et Yang, 2013). En termes de requis pour un CASB, le RBAC doit être intégré afin de simplifier la gestion des permissions accordées pour la création, la modification ou la suppression des données utilisées dans l'environnement infonuagique. Ces permissions sont attribuées à des groupes spécifiques d'utilisateurs selon leur rôle et le type d'accès nécessaires.*	✓	✓	✓	✓	✓
	a.2 Empêcher l'accès aux données confidentielles des clients par le fournisseur ou par les autres clients du même service infonuagique.	a.2.1 Chiffrement des données confidentielles au repos. • *Les données d'une organisation sont généralement classées selon trois catégories : publiques, privées ou confidentielles. Les données confidentielles sont celles dont la divulgation à des personnes non autorisées est susceptible de causer des dommages graves à l'organisation et à sa réputation. Parmi les données qui sont habituellement classées confidentielles, il y a les numéros de cartes de crédit, les numéros d'assurance sociale, les dates de naissance, les numéros d'identification personnels, etc. Ces données confidentielles, lorsqu'elles ne sont pas utilisées ou en transit, donc au repos, doivent être chiffrées en tout temps. Ces fonctions doivent être accomplies par le CASB choisi par l'organisation.*	✓	✓	✓	✓	✓
		a.2.2 Chiffrement de toutes les données en transit, incluant celles échangées entre les machines virtuelles. • *Les données en transit sont celles échangées entre différents systèmes ou services. Elles doivent être constamment protégées grâce à des protocoles de chiffrement et ce, peu importe leur catégorie (publiques, privées ou confidentielles). Le CASB choisi doit donc chiffrer les données en transit.*	✓	✓	✓	✓	✓

Tableau 4.2 : Requis de sécurité de l'organisation dans un contexte infonuagique (suite)

Objectifs de sécurité	Requis globaux	Requis spécifiques	Type de service			Mode d'implantation	
			SaaS	PaaS	IaaS	Public	Privé (via un tiers)
a. Confidentialité (suite et fin)	a.2 Empêcher l'accès aux données confidentielles des clients par le fournisseur ou par les autres clients du même service infonuagique (suite et fin).	a.2.3 Le chiffrement ne doit pas affecter la performance des fonctions de recherche ou de tri des données utilisées par l'application. • *Le fournisseur de services doit déchiffrer les données pour pouvoir les traiter. Si l'utilisateur souhaite effectuer des opérations comme de la recherche ou un tri sur les données, elles doivent donc être déchiffrées au préalable. Selon les meilleures pratiques discutées dans la revue de la littérature, le fournisseur ne devrait jamais avoir accès aux données en texte brut. Le CASB doit effectuer ces opérations sans déchiffrer les données afin d'assurer leur confidentialité.*	✓	✓	✓	✓	✓
		a.2.4 Utilisation d'algorithmes standards, éprouvés et à jour pour le chiffrement. • *Après un certain temps, les algorithmes ne sont plus considérés valides, soit parce qu'un algorithme plus sécuritaire a été développé ou bien parce qu'ils ne sont plus assez puissants par rapport aux développements en termes de capacité machine. Les algorithmes utilisés par le CASB doivent remplir ce requis.*	✓	✓	✓	✓	✓
		a.2.5 Identification des appareils autorisés ou non qui utilisent des services infonuagiques. • *L'organisation doit être en mesure d'identifier tous les appareils utilisés sur son réseau. Ces derniers incluent les appareils autorisés, donc généralement ceux fournis par l'organisation, et les appareils non autorisés. Le CASB doit identifier les appareils non autorisés et en empêcher ou en restreindre l'accès aux services infonuagiques. Après la configuration des pratiques d'accès, il faut que cela soit fait de façon automatique pour éviter des efforts de gestion supplémentaires.*	✓	✓	✓	✓	✓
		a.2.6 Identification des applications infonuagiques qui sont utilisées dans l'organisation. • *Les employés ne passent pas nécessairement par le département TI pour utiliser ou installer une application sur leurs appareils (Lowans et al., 2016). Ils peuvent même y accéder directement à partir d'un navigateur web. Il devient donc essentiel pour l'organisation de se doter de moyens pour identifier quelles applications sont utilisées par les membres de l'entreprise afin d'évaluer le niveau de risque auquel elles exposent l'organisation et pour appuyer les décisions de la direction à savoir si elle autorise ou non l'utilisation de ces applications. Le CASB doit inventorier l'utilisation des services en continu.*	✓			✓	

Tableau 4.2 : Requis de sécurité de l'organisation dans un contexte infonuagique (suite)

Objectifs de sécurité	Requis globaux	Requis spécifiques	Type de service			Mode d'implantation	
			SaaS	PaaS	IaaS	Public	Privé (via un tiers)
b. Intégrité	b.1 Altération des données.	b.1.1 Chiffrement des données. • *Les algorithmes de chiffrement permettent de conserver l'intégrité des données et d'empêcher toute personne ne possédant pas la clé d'altérer ces données.*	✓	✓	✓	✓	✓
c. Disponibilité	c.1 Gestion des incidents et des attaques.	c.1.1 Automatisation de la surveillance (journaux des accès et surveillance des incidents ou des anomalies) pour les couches sous le contrôle de l'organisation. • *L'infonuagique implique une division des responsabilités entre l'organisation et son fournisseur de services. Il est donc essentiel que chacune des parties mette en place des mécanismes de surveillance pour les couches de l'infrastructure qui sont sous son contrôle. Devant le nombre grandissant d'applications infonuagiques utilisées par l'organisation, l'automatisation de la surveillance, grâce à un CASB, devient crucial pour minimiser les efforts visant à accomplir ce processus.*	✓	✓	✓	✓	✓
		c.1.2 Centralisation des informations liées aux services infonuagiques (nom du fournisseur, nature du service, responsabilités, systèmes reliés, etc.) dans un répertoire afin de pouvoir répondre rapidement aux incidents. • *Les personnes qui utilisent les services infonuagiques ne sont généralement pas les personnes qui s'occupent de leur gestion ou de leur surveillance et de la gestion des incidents. La création d'un répertoire centralisé contenant les informations sur les services infonuagiques utilisés par l'entreprise permet d'avoir rapidement toute l'information nécessaire lors d'un incident. Le CASB peut servir de répertoire des services infonuagiques, à condition qu'on s'assure que l'accès à ce répertoire soit bien géré et octroyé aux bonnes personnes selon les politiques de gestion des accès.*	✓	✓	✓	✓	✓

Tableau 4.2 : Requis de sécurité de l'organisation dans un contexte infonuagique (suite)

Objectifs de sécurité	Requis globaux	Requis spécifiques	Type de service			Mode d'implantation	
			SaaS	PaaS	IaaS	Public	Privé (via un tiers)
d. Gouvernance	d.1 Surveillance et imputabilité.	d.1.1 Suivi et journalisation de la création, de la modification et de la suppression de données utilisées par les applications infonuagiques. • *Le suivi est essentiel pour des raisons de conformité et en cas de poursuite judiciaire. La journalisation des actions effectuées sur les données permet de garder une trace et d'assurer une certaine imputabilité. Le CASB doit suivre les données au travers de leur cycle de vie.*	✓	✓	✓	✓	✓
		d.1.2 Journalisation des connexions et des autorisations et détection de comportements anormaux. • *Cela permet de s'assurer de la conformité et de l'imputabilité lors de l'utilisation des services infonuagiques. Les journaux peuvent être utilisés en tant que preuve lors d'un litige ou encore pour remonter le fil des événements lors d'un incident. De plus, le journal des connexions permet de déceler les anomalies comme, par exemple, les tentatives de connexions multiples à un compte. Le CASB doit alimenter en continu ces journaux.*	✓	✓	✓	✓	✓
	d.2 Conformité.	d.2.1 Conformité avec la réglementation et les normes de sécurité de l'information en vigueur au Canada (ex : Loi de la protection des renseignements personnels, Loi sur les banques, etc.). • *L'industrie de la finance et de l'assurance canadienne est très réglementée et l'utilisation des services infonuagiques doit respecter les lois auxquelles l'entreprise est assujettie. Les CASB permettent d'opérationnaliser le suivi des lois, notamment grâce à l'utilisation de gabarits intégrés. Ces gabarits permettent de s'assurer que le traitement approprié est appliqué aux différentes catégories de données selon les stipulations d'une loi spécifique. L'organisation n'a qu'à choisir le gabarit associé à la loi en question pour que le CASB automatise la protection des données en conséquence. Un CASB utilisé par une organisation du domaine de la finance et de l'assurance au Canada doit avoir des gabarits de lois canadiennes. Sans ces gabarits, le CASB doit être configuré manuellement, ce qui peut exiger d'importantes ressources.*	✓	✓	✓	✓	✓

Tableau 4.2 : Requis de sécurité de l'organisation dans un contexte infonuagique (suite et fin)

Objectifs de sécurité	Requis globaux	Requis spécifiques	Type de service			Mode d'implantation	
			SaaS	PaaS	IaaS	Public	Privé (via un tiers)
Requis technologiques							
e. Disponibilité	e.1 Gestion des incidents et des attaques.	e.1.1 Alertes en temps réel en cas d'attaque ou d'anomalie et intégration avec les outils du centre de surveillance de la sécurité de l'organisation. • *L'organisation doit être rapidement avisée en cas d'attaque ou d'anomalie. Les alertes devraient être en temps réel afin de permettre de rapidement mettre en place le plan de réponse aux incidents et de limiter les impacts négatifs. Le centre de surveillance de la sécurité a déjà plusieurs outils qui lui permet de faire un suivi des événements de sécurité. Les alertes et les métriques fournies par le CASB doivent donc s'intégrer à celles déjà en place au centre de surveillance de la sécurité qui est responsable de la gestion des incidents et de la mise en place du plan de réponse.*	✓	✓	✓	✓	✓
f. Autres	f.1 Intégration.	f.1.1 Compatibilité avec les composantes de l'architecture d'entreprise actuelle. • *Tout outil assurant la sécurité des services infonuagiques, incluant les CASB, doit s'intégrer aux interfaces, aux logiciels, aux systèmes, aux environnements de développement et aux équipements informatiques de l'entreprise afin d'être aussi transparent que possible pour les utilisateurs.*	✓	✓	✓	✓	✓
		f.1.2 Intégration avec les mécanismes de sécurité (ex : logiciel de gestion des événements en sécurité de l'information, logiciel d'authentification unique, logiciel de gestion des appareils mobiles, pare-feu, etc.) déjà en place dans l'organisation, sans les compromettre. • *Le CASB doit pouvoir s'intégrer aux outils en place, à moins qu'il ne possède des fonctions semblables qui pourraient lui permettre de remplacer l'outil existant.*	✓	✓	✓	✓	✓
		f.1.3 Déploiement local (et non pas en mode infonuagique). • *Le déploiement local, donc l'installation sur les lieux de l'entreprise, est considéré comme plus sécuritaire parce qu'il n'oblige pas l'organisation à transmettre les données utilisées par les services infonuagiques au fournisseur de CASB. L'organisation conserve ainsi le contrôle sur cet aspect de ses données.*	✓	✓	✓	✓	✓

Dans l'esprit de la méthodologie RAD, le tableau précédent représente le premier artefact venant répondre à la première question de recherche qui vise à comprendre quels sont les requis fonctionnels et technologiques pour un CASB utilisé au sein d'une entreprise de la finance et de l'assurance. L'élaboration de cette grille de requis, tel que mentionné plus tôt, a nécessité plusieurs discussions avec différents spécialistes de l'organisation. L'analyse de ces discussions a permis d'abord de faire ressortir les principaux besoins en sécurité de l'information et, par la suite, ces besoins ont pu se traduire en requis fonctionnels et technologiques. On rappelle que selon la définition donnée en introduction de ce mémoire, un besoin est une exigence identifiée comme étant manquante et nécessaire par l'organisation alors qu'un requis consiste en une fonctionnalité ou une spécification technique pour un outil qui permet de combler le besoin identifié. Ce sont ces requis, tels que définis dans le cadre de l'organisation étudiée, qui sont présentés dans le tableau précédent.

Au total, toutefois, il y a deux grands besoins qui sont ressortis de tout ce travail, soit la nécessité de comprendre l'ampleur du phénomène de prolifération des applications infonuagiques et des appareils non autorisés et les besoins de chiffrement des données sensibles de l'entreprise. Parmi tous les besoins énoncés, ce sont ces deux derniers qui sont considérés comme prioritaires et sont ceux auxquels l'entreprise souhaite s'attaquer en premier. D'autres besoins importants sont aussi ressortis des discussions et de l'analyse des résultats et ils font partie du tableau, notamment la gestion des identités et des accès, la surveillance des applications infonuagiques et la compatibilité des CASB avec les composantes de l'infrastructure. Les paragraphes qui suivent abordent plus en détails les deux besoins prioritaires, puis les autres besoins et comment chacun s'est traduit en requis spécifiques pour un CASB.

4.2.2.1 Le *shadow IT*

Le premier besoin prioritaire, celui d'évaluer le phénomène du *shadow IT*, provient entre autres de l'offre mirobolante d'applications SaaS sur le marché. Le *shadow IT* n'est pas nouveau ni spécifique à l'infonuagique, mais le nombre grandissant d'applications SaaS, disponibles souvent à peu de coût, a contribué à l'exacerber. La facilité d'accès aux applications fait en sorte que les employés peuvent facilement omettre de passer par le département de TI de l'organisation pour télécharger une application (Lowans *et al.*, 2016) ou bien peuvent y accéder par le biais d'un

navigateur web, toujours à l'insu du département de TI. Il est donc logique de souhaiter inventorier l'utilisation de l'infonuagique avant de penser à mettre en place des contrôles de sécurité (par exemple, une politique d'utilisation des services externes) pour encadrer son emploi. En effet, il est impossible pour une entreprise de penser à contrôler un phénomène dont elle ne connaît même pas l'ampleur et de tenter de mettre en place des mécanismes de protection si elle ne connaît pas les applications utilisées par ses employés et leur contexte d'utilisation. Sans visibilité sur l'utilisation des applications SaaS, l'entreprise ne peut analyser le niveau de risque associé à chacune de ces applications, ne peut s'assurer de sa conformité aux lois auxquelles elle est assujettie et n'est donc pas en mesure prendre une décision éclairée quant à leur utilisation. Par conséquent, la mise en place de politiques concernant le *shadow IT* et de mécanismes permettant de surveiller et de contrôler l'utilisation d'appareils non autorisés au sein de l'organisation passe d'abord par une évaluation de l'ampleur du phénomène.

Une autre conséquence du *shadow IT* est justement la protection des données échangées entre les employés et les applications non autorisées. Ces applications ne bénéficient pas nécessairement des mêmes contrôles et mesures de protection que celles qui sont autorisées par l'entreprise, ce qui la rend vulnérable aux fuites ou aux vols de données. Plusieurs employés ont l'habitude d'utiliser certaines applications infonuagiques pour leur usage personnel (Lowans *et al.*, 2016) et les utilisent donc de la même façon au travail, ne réalisant pas qu'ils exposent leur employeur à des risques de sécurité. L'organisation, de son côté, ne sait pas quelles données se retrouvent dans ces applications et perd la traçabilité de ses données utilisées dans ce contexte. Ainsi, la protection des données transitant par des applications non autorisées est ardue. Pour s'assurer de les protéger contre la fuite ou la perte, l'organisation a avantage à savoir quelles données sont transmises à des applications infonuagiques, d'où l'importance de mettre en place des mécanismes permettant d'accomplir cette tâche.

Une fois que l'entreprise a identifié les applications infonuagiques utilisées par ses employés, un des besoins qui en découlera sera la centralisation de la gestion de toutes ces applications. En effet, l'infonuagique offre une variété de services qui permettent d'accomplir n'importe quelle tâche corporative. Autrefois, une entreprise adoptait un progiciel de gestion intégrée qui était utilisé par tous les départements. À présent, grâce à son accès et à son implantation faciles, l'infonuagique permet à chaque département de personnaliser ses TI et d'utiliser les applications

qui correspondent davantage à ses besoins. Cette multiplication des applications rend leur gestion par le département TI beaucoup plus complexe, puisqu'il se retrouve à présent à jongler avec des centaines d'applications plutôt qu'avec seulement une poignée. Dans un tel contexte, il est important de trouver des moyens pour centraliser la gestion des services infonuagiques. Cette centralisation permet à l'organisation de mettre en place une gouvernance d'entreprise en sécurité de l'information, d'être plus efficace dans sa surveillance des services et plus proactive en cas d'incident de sécurité.

Ce besoin de s'attaquer au problème du *shadow IT* dans l'organisation s'est traduit en deux requis de la section « Confidentialité » du Tableau 4.2, soit les lignes a.2.5 et a.2.6. En effet, le CASB mis en place dans l'entreprise doit détenir des fonctionnalités d'identification des applications et des appareils non autorisés. De surcroît, les CASB ont le potentiel d'aider à rationaliser les efforts de gestion liés à la multiplication des services infonuagiques utilisés. Ils agissent comme une console centrale de gestion où sont répertoriés les services utilisés et les événements de sécurité s'y produisant. Cette vue d'ensemble permet d'appuyer la direction dans sa prise de décision et d'être plus agile dans sa gestion des services infonuagiques.

4.2.2.2 Le chiffrement des données utilisées dans un environnement infonuagique

Mis à part la prise en charge du problème de *shadow IT*, le second grand besoin prioritaire qu'a formulé l'entreprise à l'étude est la nécessité de chiffrer les données utilisées dans l'environnement infonuagique. La grille précédente présente plusieurs requis liés au chiffrement (a.2.1 à a.2.4 et b.1.1) parce que lorsqu'il est fait au niveau de la donnée, il représente un mécanisme de protection très puissant. Il empêche toute personne ne possédant pas la clé de voir la donnée en texte brut, incluant les employés du fournisseur ou les autres clients qui partagent les ressources de ce dernier. La cryptographie est un domaine complexe et il existe actuellement plusieurs protocoles différents de chiffrement. Il convient donc de bien s'informer sur les pratiques d'un fournisseur dans ce domaine avant de signer un contrat avec celui-ci ; par exemple, demander quel algorithme de chiffrement il utilise, comment il assure la gestion des clés et où celles-ci sont stockées.

Les politiques associées au chiffrement varieront selon les principes de gouvernance mis en place au sein de l'organisation, la valeur et la classification des données. Cependant, selon les meilleures pratiques prônées par le NIST et la CSA, les deux organismes recommandent tous deux de chiffrer les données à la source, avant de les envoyer vers le fournisseur de services infonuagiques, puis de s'assurer que le fournisseur n'ait pas accès aux clés de chiffrement pour protéger la confidentialité et l'intégrité des données (Badger *et al.*, 2014; Cloud Security Alliance, 2011). Cela n'est malheureusement pas toujours possible, surtout dans les cas d'applications SaaS qui peuvent nécessiter que le fournisseur ait accès aux données non chiffrées pour que l'application puisse en faire le traitement (Rizvi *et al.*, 2014). Pour contrer cela, une solution appelée chiffrement homomorphique a été proposée (Dorey et Leite, 2011; Hashizume *et al.*, 2013; Tebaa, El Hajji et El Ghazi, 2012). Cette technique permet de réaliser des opérations comme l'addition ou la multiplication sans avoir à déchiffrer les variables, alors que le résultat de l'opération sort en texte brut (non chiffré). Les données n'ont donc pas à être déchiffrées pour être traitées. Malheureusement, cette approche est théoriquement possible, mais en pratique, elle n'est pas applicable. Elle requiert une puissance de calcul beaucoup trop élevée pour être viable dans un contexte organisationnel (Naone, 2011). En conséquence, les entreprises qui souhaitent chiffrer leurs données doivent faire le compromis de partager les clés avec le fournisseur pour qu'il puisse traiter les données pendant qu'elles sont utilisées dans l'application ou lorsqu'elles sont au repos.

Pour ce qui est des données en transit du client vers le fournisseur ou vice-versa, elles doivent toujours être chiffrées pour les protéger au cas où elles seraient interceptées (requis a.2.2 du tableau précédent). Le chiffrement en transit est possible et il existe, depuis plusieurs années, des protocoles éprouvés pour le faire (Paar et Pelzl, 2009).

On constate donc que, même si une organisation souhaitait appliquer le chiffrement à toutes ses données, peu importe leur état, la technologie n'est pas encore à point, ce qui limite les efforts en ce sens. Les CASB, grâce à leur objectif de sécurité des données permettent de chiffrer certaines données, en transit ou au repos, selon les préférences de l'entreprise. Pour cette raison, le besoin de chiffrement s'est traduit en plusieurs requis pour un CASB.

4.2.2.3 Autres besoins non-prioritaires et les requis correspondants

Outre les deux grands besoins de prise en charge du phénomène de *shadow IT* et de chiffrement des données, d'autres besoins moins prioritaires en sécurité infonuagique sont ressortis de l'étude et de ceux-ci ont découlé différents requis pour un CASB. Parmi ceux-ci, il y a la gestion des identités et des accès, la surveillance et la compatibilité.

La gestion des identités et des accès

Le premier besoin non-prioritaire, la gestion des accès et des identités est un processus central aux organisations. Les requis associés à ce besoin se retrouvent au début du Tableau 4.2, soit aux lignes a.1.1 à a.1.4.

Le grand défi en gestion des identités est de créer un identifiant par utilisateur qui lui permettent d'accéder à toutes les applications, les plateformes et les systèmes dont il a besoin pour accomplir son travail. L'utilisation d'un identifiant unique à travers ces systèmes s'appelle la fédération des identités et elle permet non seulement de faciliter la vie de l'utilisateur, mais aussi celle des responsables de la gestion des identités. Considérant la multiplication des applications due à l'essor de l'infonuagique, la fédération des identités est devenue essentielle pour simplifier le processus de gestion des identités et des accès (requis a.1.1 du tableau précédent). Elle se fait généralement à l'aide de logiciels spécialisés qui, jumelés au service d'annuaire de l'organisation, permettent aux utilisateurs de ne s'identifier qu'une seule fois au début de leur session de navigation par exemple.

Un autre concept très important lié à la gestion des identités est le contrôle des accès basé sur le rôle (*Role-based Access Control* ou RBAC, décrit à la ligne a.1.4). Il permet la création de groupes qui sont tous liés à un rôle dans l'organisation. Pour chacun des groupes, on lui attribue les accès requis pour accomplir le travail. Disons, par exemple, qu'on crée un groupe « Ventes ». On associera toutes les applications utilisées par les gens du département des ventes à ce groupe. Ensuite, on ajoutera des membres à ce groupe, soit les vendeurs. À chaque fois qu'un nouveau vendeur est embauché, on n'aura qu'à l'ajouter au groupe « Ventes » plutôt que de passer en revue la liste des applications utilisées par les vendeurs et de lui accorder les accès pour chacune. Le RBAC permet de sauver du temps et de réduire le nombre d'erreurs d'accès pour chacun des

employés. Le CASB qui permet le RBAC peut plus facilement gérer l'accès aux applications infonuagiques et aux données associées grâce à l'utilisation de ces groupes d'utilisateurs.

La surveillance des applications infonuagiques

Ensuite, il y a la surveillance qui n'est pas spécifique à l'infonuagique, mais qui s'applique à tous les services impartis à des tierces parties. Néanmoins, la multiplication des systèmes et des applications qui a été évoquée précédemment entraîne avec elle une augmentation du nombre de journaux d'activités produits par chacune des applications. Ces journaux sont généralement fournis à l'organisation cliente à une fréquence déterminée dans le contrat, mais parfois, certains fournisseurs de services d'infonuagique publique refusent de distribuer les journaux à leurs clients, de peur de compromettre l'information des autres clients qui partagent la même infrastructure. Si, par contre, le fournisseur partage ses journaux, l'organisation doit avoir les ressources nécessaires pour analyser ces données afin d'en déceler les événements liés à la sécurité et d'y apporter les correctifs nécessaires. Or, à cause de la quantité de données que cela représente, peu d'entreprises ont réellement la maturité et la capacité de surveiller tous les services infonuagiques qu'elles utilisent. Il leur faut donc un moyen d'automatiser le processus de surveillance afin de récupérer rapidement les journaux, de les analyser afin d'en tirer des indicateurs de sécurité pertinents, de créer des tableaux de bord et d'avoir des alertes automatiques en cas d'incident. Ce besoin s'est traduit en plusieurs requis liés à la surveillance qui sont décrits aux lignes c.1.1, d.1.1, d.1.2 et e.1.2 du tableau 4.2. Ces requis pour un CASB permettraient à l'organisation d'être beaucoup plus agile et proactive dans sa gestion de la sécurité, surtout considérant que les incidents qui ne sont pas détectés et traités rapidement peuvent avoir des conséquences graves pour l'entreprise.

La compatibilité

En dernier lieu, la compatibilité est un besoin essentiel lorsqu'il est question de l'infonuagique. En effet, une majorité d'organisations a déjà des outils de sécurité en place et les nouveaux services devraient s'intégrer à ceux-ci pour éviter de dupliquer les efforts et de créer des silos pour la sécurité de chaque service utilisé. En plus d'être contre-productif, cela est coûteux et va à l'encontre des principes de flexibilité et de rapidité à la base de l'infonuagique. Les CASB doivent donc être compatibles avec les mécanismes de sécurité déjà présents dans l'entreprise pour faciliter les échanges d'informations entre eux (requis f.1.2).

En conclusion de cette section, les deux besoins prédominants et prioritaires qui ressortent de l'étude sont la gestion du *shadow IT* et le chiffrement des données utilisées par les services infonuagiques. Au-delà de ces deux éléments, la gestion des accès permet de s'assurer que seules les personnes autorisées ont accès aux données nécessaires, que ce soit du côté du fournisseur ou du client. Ensuite, la coopération entre l'organisation cliente et le fournisseur de services infonuagiques est aussi essentielle afin de s'assurer que toutes les couches de l'infrastructure sous-jacente au service font l'objet d'une surveillance et que chacun connaît son rôle et ses responsabilités. Finalement, la compatibilité entre les différents services infonuagiques demeure un élément essentiel pour faciliter l'adoption des services, obtenir une plus grande flexibilité et permettre les échanges de données entre les services. Ces besoins ont permis d'identifier différents requis fonctionnels et technologiques pour un CASB dans le contexte de l'organisation à l'étude. Ces requis, exposés dans le Tableau 4.2, représentent, pour l'organisation, un premier pas dans sa réflexion sur l'infonuagique et les moyens nécessaires pour assurer son utilisation sécuritaire. L'étape suivante consiste à s'informer sur l'offre actuelle, puis de s'interroger sur la façon dont elle peut combler les requis identifiés.

4.3 L'offre actuelle des fournisseurs de CASB

En parallèle à l'analyse des requis organisationnels, une analyse de l'offre actuelle a été effectuée dans le but de répondre à la seconde question de recherche. Cette dernière visait à inventorier les fonctionnalités et les caractéristiques des produits sur le marché. Les prochains tableaux dressent cet inventaire. En premier lieu, le « Market Guide » publié par Gartner et certains rapports de Forrester ont servi de base pour établir la liste des produits disponibles sur le marché, soit environ une vingtaine de fournisseurs. De cette liste, seuls les CASB offrant des fonctionnalités d'au moins deux des quatre familles d'objectifs (la visibilité, la gouvernance et la conformité, la protection des données et la protection contre les menaces) ont été retenus. En effet, le CASB est actuellement un mot à la mode dans l'industrie TI et plusieurs fournisseurs semblent vouloir profiter de l'intérêt que suscite cette classe d'outils pour mousser leurs ventes. Il était donc important de faire un tri et de retirer certains produits qui ne semblaient pas vraiment faire partie de la classe des CASB, mais qui se révèlent plutôt être des logiciels de sécurité qui tentent de se

faire passer pour un CASB. Suite à ce tri, douze fournisseurs ont été retenus afin de procéder à une analyse plus approfondie des fonctionnalités de leur produit.

Pour collecter l'information sur les produits et les fournisseurs, les sites web de ces derniers, des articles de presse et des rapports des firmes Gartner et Forrester ont été consultés. La liste complète des références est disponible dans une section à part et identifiée comme telle dans la bibliographie à la fin de ce mémoire. De plus, des appels et des démonstrations avec deux fournisseurs ont été organisés et des courriels ont été échangés avec deux autres pour obtenir des précisions sur leurs produits. Le sommaire des résultats de cette collecte d'information se retrouve au Tableau 4.3. Ce dernier présente les fournisseurs de solutions CASB par ordre alphabétique et incluent une brève description de l'entreprise, des fonctionnalités offertes par le CASB et finalement, s'il y a lieu, l'historique des acquisitions par d'autres joueurs du milieu.

Par la suite, le Tableau 4.4 présente ces mêmes fournisseurs selon les fonctionnalités de leur produit CASB. Les fonctionnalités sont divisées d'abord selon les objectifs globaux de sécurité présentés tout au long du mémoire soit la confidentialité, l'intégrité, la disponibilité et la gouvernance. Ensuite, ces catégories sont divisées selon les quatre grands objectifs de sécurité des CASB présentées dans la revue de la littérature (Chapitre 2) : la visibilité, la sécurité des données, la protection contre les menaces et, la conformité et la gouvernance. Cette catégorisation permet d'étendre l'examen des CASB sur le marché à la suite des discussions déjà présentes dans la littérature et présentées au Chapitre 2. Les fonctionnalités reprennent les termes utilisés par les fournisseurs de CASB dans la documentation liée à leurs produits.

Finalement, le Tableau 4.5 reprend la même structure que le tableau précédent, mais cette fois-ci avec les caractéristiques du produit plutôt que ses fonctionnalités. Parmi les caractéristiques, on retrouve le mode de déploiement, les logiciels protégés par les différents modules du CASB et les logiciels de l'organisation qui sont compatibles.

Il est important de spécifier ici que le but de l'exercice n'est pas de faire la promotion de l'un ou l'autre des produits présentés, mais plutôt de comprendre l'état actuel du marché. Il est à noter que l'information contenue dans les Tableaux 4.3, 4.4 et 4.5 est à jour en date du 19 août 2016, soit la fin de l'intervention en entreprise.

Tableau 4.3 : **Sommaire des fournisseurs de CASB et de leurs principales caractéristiques**[b]

Fournisseur	Description et caractéristiques
Bitglass	• Entreprise américaine fondée en 2013 et située en Californie. • Offre des fonctionnalités de visibilité, de gouvernance, de sécurité des données et de protection contre les menaces. • Sa technologie de chiffrement est brevetée et permet d'exécuter certaines opérations de recherche sur des données chiffrées.
BlueCoat (Elastica)	• Elastica est une firme fondée en 2012 en Californie. • En 2015, BlueCoat a fait l'acquisition de deux fournisseurs de CASB, Perspecsys en juillet et Elastica en novembre (Wright, 2015). Elastica est demeuré un produit à part entière alors que la technologie de chiffrement développée par Perspecsys a été intégrée dans l'offre de produits de sécurité de BlueCoat. • En juin 2016, BlueCoat a été acheté par l'entreprise de cybersécurité Symantec qui n'a pas encore dévoilé sa vision pour son produit de type CASB (Baker, 2016). • Elastica offre des fonctionnalités de visibilité, de gouvernance et de protection contre les menaces, mais n'offre pas le chiffrement des données.
CensorNet	• Entreprise britannique fondée en 2007 et qui offre un CASB depuis 2015. • Son CASB permet l'identification des applications infonuagiques, certaines fonctionnalités de gouvernance et de protection contre les menaces. • Contrairement aux autres CASB, CensorNet ne se vend pas par modules spécifiques pour différentes applications. Sa solution se veut universelle pour toutes les applications infonuagiques, mais le niveau de protection est par conséquent plus limité.
CipherCloud	• Entreprise américaine fondée en 2010. • Son CASB offre des fonctionnalités associées aux quatre objectifs des CASB, incluant le chiffrement des données.
CloudLock	• CloudLock a été fondée en 2011 au Massachusetts. • En août 2016, Cisco a annoncé l'acquisition de CloudLock pour la somme de 293 millions de dollars américains (Clark et Laryea, 2015). • Ce CASB offre des fonctionnalités remplissant chacun des quatre objectifs de sécurité.
FireLayers	• Entreprise américaine qui offre un CASB depuis 2014. • Le produit offert par FireLayers offre des fonctionnalités limitées de visibilité et de protection contre les menaces et des fonctionnalités complètes de gouvernance. Elle n'offre cependant pas de chiffrement. • La documentation disponible sur ce produit est limitée et malgré des courriels envoyés au fournisseur, il a été impossible d'obtenir la liste des applications protégées par son CASB.
Imperva	• Imperva est une entreprise de sécurité fondée en 2002. Elle offre un CASB depuis 2013 grâce à l'acquisition de Skyfence qui était spécialisé dans le domaine. • Le CASB offre des fonctionnalités liées à tous les objectifs de sécurité, sauf pour la sécurité des données puisqu'il n'offre pas le chiffrement.
Microsoft Cloud App	• Autrefois appelé Adallom avant l'achat de la compagnie du même nom par Microsoft en 2015. • Le CASB offre des fonctionnalités de visibilité, de gouvernance et de protection contre les menaces, mais pas de chiffrement.

[b] Références : voir la section spécifique de la bibliographie.

Tableau 4.3 Sommaire des fournisseurs de CASB et de leurs principales caractéristiques (suite et fin)

Fournisseur	Description et caractéristiques
Netskope	• Entreprise fondée en Californie en 2012. • Les fonctionnalités de son CASB remplissent les quatre objectifs de sécurité. Le chiffrement des données n'est pas offert dans le logiciel de base et doit faire l'objet d'un achat séparé.
Palerra	• Entreprise américaine fondée en 2013. • Son produit CASB s'appelle *Loric* et offre des fonctionnalités de visibilité, de gouvernance et de protection contre les menaces.
Palo Alto Networks	• Entreprise fondée en 2005 et qui offre plusieurs produits de sécurité dont un CASB. • Son CASB offre des fonctionnalités limitées pour les objectifs de visibilité, de gouvernance et de protection contre les menaces. Il n'offre pas la possibilité de chiffrer les données.
Skyhigh Networks	• Entreprise américaine fondée en 2013 qui offre un CASB depuis 2013. • Les fonctionnalités offertes par son CASB couvrent tous les objectifs de sécurité, sauf la sécurité des données puisqu'il ne permet pas le chiffrement.

Tableau 4.4 : Fonctionnalités offertes par les CASB actuellement sur le marché[c]

Objectifs de sécurité	Objectifs des CASB	Fonctionnalités	Bitglass	BlueCoat (Elastica)	CensorNet	CipherCloud	CloudLock	FireLayers	Imperva	Microsoft Cloud App	Netskope	Palerra	Palo Alto Networks	Skyhigh Networks
a. Confidentialité	a.1 Visibilité	a.1.1 Identification d'applications infonuagiques.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		a.1.2 Évaluation des risques associés aux applications infonuagiques utilisées (échelle de risque pour chaque application selon des critères prédéfinis).	✓	✓	×	✓	✓	×	✓	✓	✓	✓	×	✓
b. Confidentialité et intégrité	b.1 Sécurité des données	b.1.1 Analyse des données pour en identifier le type.	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓
		b.1.2 Chiffrement basé sur la classification des données.	✓	×	×	✓	✓	×	×	×	✓ (optionnel)	×	×	×
		b.1.3 Chiffrement permettant des actions à haut niveau sur les données (tri, recherche, etc.).	✓	×	×	✓	×	×	×	×	×	×	×	×
		b.1.4 Gestion des clés de chiffrement.	✓	×	×	✓	×	×	×	×	✓ (optionnel)	×	×	×

[c] Références : voir la section spécifique de la bibliographie.

Tableau 4.4 : Fonctionnalités offertes par les CASB actuellement sur le marché (suite et fin)

Objectifs de sécurité	Objectifs des CASB	Fonctionnalités	Bitglass	BlueCoat (Elastica)	CensorNet	CipherCloud	CloudLock	FireLayers	Imperva	Microsoft Cloud App	Netskope	Palerra	Palo Alto Networks	Skyhigh Networks
c. Disponibilité	c.1 Protection contre les menaces	c.1.1 Analyse du comportement des utilisateurs.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		c.1.2 Identification des activités anormales et alertes.	✓	✓	✓	✓	✓	✓	✓ (optionnel)	✓	✓	✓	✓ (optionnel)	✓
		c.1.3 Refus d'accès automatique aux applications ou appareils non autorisés.	✓	✓	✓	✓	×	×	✓	✓	✓	×	✓	✓
d. Gouvernance	d.1 Conformité et gouvernance	d.1.1 Conformité aux lois comme CIPA, HIPAA, PCI, etc. grâce à des gabarits intégrés.	✓	✓	×	✓	✓	✓	✓	✓	×	✓	×	✓
		d.1.2 Conformité aux lois canadiennes grâce à des gabarits intégrés.	×	×	×	×	×	×	×	–	×	×	×	×
		d.1.3 Possibilité d'implanter les politiques de gouvernance personnalisées (plutôt qu'un gabarit).	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		d.1.4 Création de journaux sur l'utilisation des applications infonuagiques.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Légende du tableau 4.4 :

✓ : la solution possède la fonctionnalité.
× : la solution ne possède pas la fonctionnalité.
– : l'information sur cette fonctionnalité n'est pas disponible.
(optionnel) : la fonctionnalité n'est pas disponible pour le logiciel de base, mais peut être acquise moyennant des frais supplémentaires.

Tableau 4.5 : Caractéristiques des CASB actuellement sur le marché[d]

Caractéristiques	Caractéristiques spécifiques	Bitglass	BlueCoat (Elastica)	CensorNet	CipherCloud	CloudLock	FireLayers	Imperva	Microsoft Cloud App	Netskope	Palerra	Palo Alto Networks	Skyhigh Networks
a. Logiciels spécifiques protégés (modules disponibles)	a.1 Box	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓
	a.2 Dropbox	✓	✓	×	×	✓	✓	✓	✓	✓	×	✓	✓
	a.3 Google Apps	✓	✓	×	×	✓	✓	✓	✓	✓	✓	✓	✓
	a.4 Microsoft Office 365	✓	✓	×	×	✓	✓	✓	✓	✓	✓	✓	✓
	a.5 Okta	✓	×	×	×	✓	✓	✓	✓	×	×	×	×
	a.6 Salesforce	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓
	a.7 ServiceNow	×	×	×	✓	✓	✓	×	✓	×	✓	×	✓
	a.8 Slack	×	×	×	×	✓	×	×	×	×	×	×	×
	a.9 Workday	×	×	×	×	×	×	✓	×	×	×	×	×
b. Compatibilité avec les logiciels de l'organisation[30]	b.1 Logiciel de protection contre la perte des données (DLP).	✓	✓	×	✓	✓	✓	✓	×	✓	×	×	✓
	b.2 Gestionnaire d'appareils mobiles (MDM).	×	✓	×	×	✓	–	✓	×	×	×	×	✓
	b.3 Service d'annuaire (*Active Directory*).	✓	✓	✓	✓	✓	–	✓	✓	✓	✓	×	✓
	b.4 Gestionnaire d'information et d'événements de sécurité (SIEM).	×	✓	×	✓	✓	–	✓	✓	✓	✓	×	✓
	b.5 Logiciel d'authentification unique (SSO).	✓	✓	✓	✓	✓	–	✓	✓	✓	✓	×	✓

[d] Références : voir la section spécifique de la bibliographie.

[30] Il a été difficile d'obtenir de l'information sur les logiciels exacts qui sont compatibles avec le CASB, malgré les rencontres et les courriels envoyés aux fournisseurs. Un crochet indique que le CASB est compatible avec au moins un logiciel du type mentionné, sans distinction pour le concepteur du logiciel.

Tableau 4.5 : Fonctionnalités des CASB actuellement sur le marché (suite et fin)

Caractéristiques	Caractéristiques spécifiques	Bitglass	BlueCoat (Elastica)	CensorNet	CipherCloud	CloudLock	FireLayers	Imperva	Microsoft Cloud App	Netskope	Palerra	Palo Alto Networks	Skyhigh Networks
c. Modes de déploiement	c.1 Via l'interface de programmation (API)	✓	✓	✖	✓	✓	✓	✓	✓	✓	✓	✓	✓
	c.2 Par *proxy*	✓	✓	✓	✓	✖	✓	✓	✖	✓	✖	✖	✓

Légende du tableau 4.5 :

✓ : la solution possède la fonctionnalité.
✖ : la solution ne possède pas la fonctionnalité.
– : l'information sur cette fonctionnalité n'est pas disponible.
(optionnel) : la fonctionnalité n'est pas disponible pour le logiciel de base, mais peut être acquise moyennant des frais supplémentaires.

Les tableaux précédents donnent un aperçu de l'état actuel du marché des CASB en répertoriant les fonctionnalités et les caractéristiques des produits d'une douzaine de fournisseurs. Afin de mieux analyser cette offre, il convient à présent de se pencher sur chacune des sections de ce tableau.

4.3.1 Visibilité

D'abord, la section 4.2.2 présentant les requis de sécurité de l'organisation à l'étude montre bien le besoin de l'organisation de cerner le problème des appareils et des applications non autorisés afin d'établir des politiques cohérentes en termes de gouvernance de la sécurité. Ce besoin est loin d'être unique à l'organisation étudiée. En effet, un rapport paru l'an dernier estime qu'une entreprise du domaine de la finance utilise en moyenne un millier d'applications infonuagiques[31] (Skyhigh Networks, 2015). De ce nombre, seulement une soixantaine d'applications seraient connues du département TI de l'organisation. Ce besoin de connaître les applications SaaS utilisées par les employés peut être comblé par les CASB. D'ailleurs, les fournisseurs de ces outils font de leurs fonctionnalités de visibilité un de leurs arguments de vente les plus importants. Tous les produits considérés dans le cadre de ce mémoire offrent un module d'identification des applications infonuagiques, généralement vendu séparément des autres modules de protection offerts par le même fournisseur (fonctionnalité a.1.1 du tableau 4.4). Pour faire cette identification, ils récupèrent les journaux de connexion et d'activités produits par les pare-feu et les *proxys* de l'organisation et en font ensuite une agrégation puis une analyse (Microsoft, 2016c). Le tout est présenté dans un tableau de bord avec des statistiques sur le nombre d'applications utilisées, l'identité des utilisateurs et les dates d'accès.

Certains CASB offrent aussi la possibilité d'évaluer le niveau de risque associé à chacune des applications infonuagiques qui est utilisée en établissant un score sur cent (fonctionnalité a.1.2 du Tableau 4.4). Ce niveau de risque est basé sur des critères prédéterminés par le fournisseur (ex : réputation du concepteur, nombre de brèches décelées dans une période donnée, etc.) ou bien, dans certains cas, par des critères personnalisables par le client. Ainsi, une entreprise qui met en place un CASB peut rapidement voir quelles sont les applications utilisées par ses

[31] Ces applications ne sont pas nécessairement toutes autorisées par l'organisation et incluent celles utilisées par les employés de leur propre initiative.

employés et, par la suite, prendre la décision de les autoriser ou non selon le niveau de risque qu'elle est prête à tolérer. Cette fonctionnalité permet aussi de voir quels appareils les employés utilisent pour accéder aux applications infonuagiques et donc de repérer facilement ceux qui sont non autorisés. L'utilisation d'appareils non autorisés crée un grand risque d'introduire des programmes malveillants ou d'autres menaces dans le réseau local de l'organisation. Pour cette raison, les entreprises souhaitent généralement bloquer l'accès à ces appareils, ce qui peut être accompli automatiquement par la majorité des CASB (section c.1 du Tableau 4.4). D'autre part, pour protéger les données, certains CASB peuvent plutôt bloquer l'accès à certains documents ou types de données qui sont accédés par des appareils non autorisés, limitant ainsi les risques associés à la confidentialité des données. À titre d'exemple, le CASB pourrait empêcher les accès aux dossiers financiers des clients pour les utilisateurs qui se connectent à l'application Salesforce à partir d'un appareil mobile personnel non autorisé. Les fonctionnalités de visibilité des CASB permettent donc de non seulement savoir quelles applications et quels appareils sont utilisés par les employés d'une entreprise, mais aussi de l'aider à mettre en place un cadre de gouvernance pour l'utilisation de ces applications et de ces appareils.

4.3.2 Sécurité des données

La seconde catégorie de fonctionnalités est la protection des données, ce qui comprend principalement le chiffrement (fonctionnalités b.1.2 à b.1.4 du Tableau 4.4). Ce ne sont pas tous les CASB qui offrent des fonctionnalités de chiffrement et la minorité qui l'offre ne le fait que pour certaines applications pour lesquelles un module spécifique existe (voir la section a. Logiciels spécifiques protégés du Tableau 4.5). Tel que mentionné précédemment, le chiffrement des données au repos dans les applications est possible, mais encore en développement puisqu'il ne permet pas de faire des calculs, des tris ou des recherches sans devoir déchiffrer les données au préalable. Une des solutions à ce problème et qui permet de conserver un niveau de sécurité acceptable est le chiffrement homomorphique (Yi *et al.*, 2014). Par contre, cette approche n'a pas encore d'application pratique parce que la puissance de calcul requise pour la mettre en place est beaucoup trop grande et exigerait des délais très grands (Naone, 2011). Les limites dans la capacité de chiffrement freinent donc le développement des CASB actuellement sur le marché. Malgré tout, certains fournisseurs annoncent qu'ils possèdent une technologie de chiffrement permettant de traiter les données chiffrées. Toutefois, lorsqu'on s'y penche, on se rend compte

que c'est très généralement au détriment de la sécurité qu'ils le font. En effet, ils utilisent le stratagème qui est décrit ci-après.

Ainsi, une des façons dont les fournisseurs de CASB s'y prennent pour contourner le problème des opérations sur les données chiffrées est de ne chiffrer qu'une partie des données, conservant le reste en texte brut. C'est ce que fait un des fournisseurs de CASB, CipherCloud, qui ne chiffre qu'une partie des données afin de conserver la possibilité de faire des recherches sur les données (CipherCloud, 2015). Ainsi, supposons qu'on souhaite chiffrer des numéros de téléphone dans une application quelconque, le CASB de CipherCloud pourrait ne chiffrer que les sept derniers chiffres et laisser l'indicatif régional en texte brut. Il serait alors possible de rechercher facilement parmi les numéros de clients qui habitent une certaine région, grâce à l'indicatif régional. Évidemment, cette technique de chiffrement partiel est moins sécuritaire que le chiffrement intégral des données.

Il existe une piste de solution au problème de recherche et de tri parmi les données chiffrées chez un fournisseur qui n'implique pas le chiffrement homomorphique. En effet, un autre fournisseur de CASB, Bitglass, a mis au point et a fait breveter une nouvelle technologie de chiffrement qu'il a ensuite intégré à son CASB. Cette technologie fait en sorte que, lorsque les données sont chiffrées avant d'être envoyées dans la base de données du fournisseur, un index avec des mots-clés est créé pour chacune des données. Pour reprendre l'exemple des numéros de téléphone, supposons que le numéro de téléphone saisi dans le champ de l'application possède l'indicatif régional « 514 ». Lors de la sauvegarde du numéro de téléphone, le CASB crée un index avec les mots clés « numéro de téléphone » et « Montréal ». L'index de mots-clés est stocké par le CASB, du côté de l'organisation cliente et non pas chez le fournisseur. Cet index n'est pas chiffré, mais il ne contient pas les vraies données de l'organisation, seulement des mots-clés et il n'est pas non plus accessible au fournisseur. Les données chiffrées, accompagnées d'un « pointeur », sont ensuite stockées chez le fournisseur de services infonuagiques. Ce pointeur permet de retrouver la ou les données associées à un mot-clé spécifique. Donc, lorsqu'un utilisateur fait une recherche parmi les données chiffrées d'une application, le CASB balaie l'index de mots-clés afin de trouver ceux qui correspondent aux termes de recherche qu'a entrés l'utilisateur. Lorsqu'un mot-clé est rencontré pendant l'analyse du CASB, celui-ci cherche le pointeur associé à la donnée en question et déchiffre la donnée (Kahol, Bhattacharjya et Kausik, 2013). Dans notre exemple, si l'utilisateur

souhaite chercher les numéros de téléphones de la région de Montréal, le CASB n'aurait qu'à chercher parmi les index les mots-clés référant aux termes de recherche de l'utilisateur. Les pointeurs associés à ces mots-clés permettraient ensuite de récupérer le numéro de téléphone en question dans la base de données du fournisseur, le déchiffrer puis l'afficher l'application. Ainsi, le numéro de téléphone au repos dans la base de données du fournisseur de services infonuagiques est resté chiffré en tout temps.

Il est difficile de savoir si cette façon de faire est efficace en pratique puisqu'il n'a pas été possible d'avoir une démonstration de cette méthode de chiffrement ou de trouver de l'information de la part d'une organisation qui l'utilise. On peut supposer cependant que cette technique cause de la latence parce que le CASB doit faire quelques opérations supplémentaires pour rechercher dans l'index et ensuite dans les données chez le fournisseur avant d'afficher un résultat de recherche. Il agit donc comme un intermédiaire additionnel entre l'utilisateur et le fournisseur, ce qui a généralement tendance à causer des délais supplémentaires pour le traitement des données. Pour l'instant, Bitglass est la seule solution de CASB qui permet de faire des recherches parmi des données chiffrées grâce à cette technologie puisqu'elle en détient le brevet. Les autres fournisseurs, n'ayant donc pas accès au chiffrement avec un index, doivent se contenter d'utiliser soit un chiffrement édulcoré ou bien tout simplement de ne pas offrir la recherche parmi les données chiffrées.

4.3.3 Protection contre les menaces

La troisième catégorie, la protection contre les menaces, est possible grâce à l'analyse du comportement des utilisateurs afin de déceler des comportements anormaux. Le CASB apprend des habitudes d'utilisation et des comportements des utilisateurs grâce à l'analyse des journaux d'activités des différentes applications infonuagiques (fonctionnalité c.1.1 du Tableau 4.4). Si un utilisateur qui n'en a pas l'habitude tente de télécharger une grande quantité de données de l'application vers une autre application ou un compte personnel ou s'il fait une tentative de connexion hors des heures normales de travail ou à partir d'un lieu inhabituel, le CASB pourrait bloquer l'action ou l'accès, puis émettre une alerte dans le tableau de bord. En plus de ce type de protection, certains fournisseurs intègrent des mécanismes de protection déjà offerts par

d'autres produits comme la détection de logiciels malveillants ou de virus, mais qui s'appliquent spécifiquement au contexte d'utilisation des SaaS.

4.3.4 Conformité et gouvernance

Pour ce qui est des fonctionnalités liées à la gouvernance, elles varient selon le produit, mais il y a trois principales possibilités : 1) utiliser des gabarits qui respectent certaines lois de protection des données personnelles, 2) implanter des politiques de gouvernance propres à l'entreprise ou bien 3) faire les deux à la fois (fonctionnalités d.1.1 à d.1.3 du Tableau 4.4). Les gabarits disponibles varient en fonction du fournisseur, mais ils couvrent un certain nombre de lois, principalement américaines, concernant la protection des données des consommateurs ou des citoyens. Ces lois obligent les entreprises à protéger les données confidentielles. Les CASB permettent soit d'identifier la catégorie d'une donnée (publique, privée ou confidentielle) qui lui a été assignée au préalable par un humain ou bien d'analyser les données afin d'en déterminer lui-même le type dans certains cas spécifiques (ex : les CASB peuvent reconnaître les numéros de cartes de crédit ou les dates de naissance). Selon le type de données, ils peuvent ensuite mettre en place les mesures nécessaires (ex : chiffrer, masquer, bloquer, mettre en quarantaine, etc.) pour les protéger selon ce que dicte la loi en question. L'entreprise n'a qu'à sélectionner le gabarit de la loi à laquelle elle souhaite se conformer, par exemple PCI DSS, et le CASB se chargera d'identifier ou de déterminer, d'analyser et de protéger les données qui doivent s'y conformer. Pour les données au repos, cette option n'est disponible que pour certaines applications couvertes par le CASB qui agit en tant qu'intermédiaire vers l'API alors que pour les données en transit, elle est disponible que pour les CASB offerts en mode *proxy*. Il est aussi possible de personnaliser les politiques de protection des données dans les cas où les gabarits ne conviennent pas à l'organisation cliente, c'est-à-dire le cas où l'organisation choisit elle-même les paramètres et les données à protéger.

Une autre fonctionnalité de gouvernance qui est offerte par les CASB étudiés est la création de journaux liés à l'utilisation des applications, ce qui est nécessaire pour certaines entreprises qui doivent se soumettre à des audits de conformité ou qui auraient à fournir des preuves en cas de litige (fonctionnalité d.1.4 du Tableau 4.4). Ces journaux permettent de garder une trace des activités liées aux applications infonuagiques, permettant ainsi d'assurer une certaine

imputabilité. En somme, lorsqu'on analyse les fonctionnalités de gouvernance offertes par les CASB, on se rend compte qu'elles se rapprochent beaucoup de ce que permet un logiciel contre la perte de données (*Data Loss Prevention* ou DLP), mais avec la différence qu'elles sont spécifiques aux SaaS. En effet, les DLP permettent aussi de gérer et de faire le suivi des données afin de prévenir leur fuite hors des frontières de l'organisation (Elastica, 2014).

4.3.5 Autres observations

Il faut noter que l'élaboration des requis a été influencée par la définition et les caractéristiques actuelles des CASB. À la suite de l'identification des fonctionnalités des CASB présentement sur le marché, on se rend compte que, pour l'instant, les CASB ne protègent que les SaaS et laissent de côté les PaaS et les IaaS. Il va sans dire que l'organisation à l'étude a des contrats avec des fournisseurs de PaaS et de IaaS et qu'elle a des besoins en termes de sécurité et de protection pour ces services comme le montre le Tableau 4.2.

Il est important aussi de rappeler que l'analyse effectuée ici est à haut niveau et que les résultats présentés sont agrégés. Plusieurs CASB se vendent par module, ce qui a une incidence sur le nombre et la nature des fonctionnalités offertes. Dans la plupart des cas, il faut acheter un module différent pour l'identification d'applications infonuagiques (visibilité), puis des modules séparés pour protéger chacune des applications spécifiques comme Office 365 ou Salesforce. Malheureusement, le nombre d'applications ainsi couvertes par les CASB est plutôt limité pour l'instant.

Plusieurs fournisseurs de CASB ont aussi des versions de base de leur logiciel avec des fonctionnalités limitées et une version supérieure qui contient plus de fonctionnalités. Cette façon de faire a évidemment un impact sur les coûts, mais aussi sur la perception des consommateurs. En effet, les fournisseurs commercialisent les CASB comme des outils complets qui possèdent plusieurs fonctionnalités permettant non seulement de rehausser la sécurité de l'information, mais aussi d'en centraliser et d'en faciliter la gestion. Toutefois, lorsqu'on se penche sur l'offre du marché, on réalise que les fonctionnalités varient beaucoup d'un produit à l'autre et que pour un même fournisseur, il existe plusieurs configurations possibles qui n'offrent pas toutes le même niveau de protection. On constate donc, à la lecture des résultats, que les CASB correspondent

bien à la définition de produits complexes proposée par Novak et Eppinger (2001) et que le choix d'une solution s'avère lui aussi très complexe puisque plusieurs éléments sont à prendre en considération.

Pour conclure, ce chapitre a permis, grâce à l'application de la méthodologie de *recherche action design*, d'aller plus loin que ce que propose la littérature et de répondre aux deux premières questions de recherche présentées en introduction du mémoire. Dans un premier temps, l'intervention en entreprise a permis l'élaboration d'une grille des requis fonctionnels et technologiques pour un CASB utilisé dans une organisation de la finance et de l'assurance au Canada. Dans un deuxième temps, l'analyse de l'offre actuelle a permis de dresser un inventaire des fonctionnalités et des caractéristiques des CASB sur le marché. Le chapitre suivant propose une discussion sur la façon de réconcilier les requis des organisations du domaine de la finance et de l'assurance avec l'offre actuelle afin d'évaluer le potentiel des CASB en tant qu'outil qui permet d'aider à assurer la sécurité des services infonuagiques.

Chapitre 5: Discussion

Le cinquième chapitre du mémoire est en quelque sorte le résultat de la troisième étape de la méthodologie de *recherche action design*, soit celle de « Réflexion et apprentissage ». À la suite de l'intervention en entreprise et de la présentation des résultats colligés au chapitre précédent, il convient de se pencher sur ces résultats et de les analyser afin d'en tirer des apprentissages. Ce chapitre propose, en premier lieu, une analyse des écarts entre les requis en sécurité de l'organisation à l'étude et des fonctionnalités des CASB sur le marché. En second lieu, une discussion sur l'influence de l'industrie et du contexte organisationnel amorce la réflexion sur le potentiel et les limites des CASB.

5.1 Analyse des écarts entre les requis fonctionnels et technologiques de l'entreprise à l'étude et l'offre actuelle des CASB

L'intervention a permis d'identifier les requis fonctionnels et technologiques pour un CASB (artefact #1), ce qui correspond à la réponse à la première question de recherche. Ensuite, l'inventaire des fonctionnalités et des caractéristiques de l'offre actuelle des CASB (artefact #2) a permis de répondre à la seconde question de recherche. La troisième et dernière question concerne la façon dont les produits actuels sont en mesure de combler les requis identifiés, ce qui permettra de réaliser le troisième et dernier artefact. Pour ce faire, il a fallu analyser une à une chacune des fonctionnalités offertes par les douze fournisseurs de CASB choisis et évaluer si la fonctionnalité comblait entièrement, en partie ou pas du tout le besoin inventorié. Ce travail a requis une analyse en profondeur et exhaustive des fonctionnalités offertes afin de différencier entre la réalité et les affirmations marketing trop souvent nébuleuses. La présente section vise ainsi à analyser les écarts entre ces requis et l'offre, d'abord en présentant un tableau récapitulatif montrant les écarts constatés, suivi d'une analyse de ce tableau et, finalement, en formulant des pistes de réflexion.

Le tableau qui suit permet de réconcilier les requis de l'organisation avec l'offre de chacun des fournisseurs de CASB. Les trois premières colonnes reprennent celles du Tableau 4.2 qui portent sur les objectifs et les requis globaux et spécifiques de sécurité de l'entreprise. À la droite de ces

colonnes, chacun des douze fournisseurs présentés précédemment apparaissent, en ordre alphabétique. Pour chacun des requis, il est indiqué si le produit offert par le fournisseur le comble complètement, partiellement ou pas du tout. Dans de rares cas, il n'a pas été possible de trouver l'information liée à un requis spécifique. Les références qui ont servi à l'élaboration de ce tableau sont les mêmes que celles des tableaux des fournisseurs du Chapitre 4 et elles peuvent être consultées dans une section à part à la fin de la bibliographie.

Tableau 5.1 : Analyse des écarts entre les requis de l'organisation et l'offre actuelle des fournisseurs de CASB[e]

Objectifs de sécurité	Requis globaux	Requis spécifiques	Bitglass	BlueCoat (Elastica)	CensorNet	CipherCloud	CloudLock	FireLayers	Imperva	Microsoft Cloud App	Netskope	Palerra	Palo Alto Networks	Skyhigh Networks
Requis fonctionnels														
a. Confidentialité	a.1 Gestion de l'identité et des accès pour s'assurer que seules les personnes autorisées aient accès.	a.1.1 Fédération des identités.	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	×	✓
		a.1.2 Intégration des politiques de gestion des accès et des privilèges de l'entreprise.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
		a.1.3 Authentification multi-facteur pour les comptes à hauts privilèges (comptes bénéficiant de privilèges d'administrateur ou à haut risque de sécurité pour l'organisation).	✓	✓	✓	-	✓	✓	✓	-	✓	-	-	✓
		a.1.4 Contrôle des accès basé sur le rôle (*Role-based Access Control* ou RBAC).	✓	×	-	✓	-	-	✓	✓	✓	×	-	✓
	a.2 Empêcher l'accès aux données confidentielles des clients par le fournisseur ou par les autres clients du même service infonuagique.	a.2.1 Chiffrement des données confidentielles au repos.	✓	×	×	✓	✓	×	×	×	✓	×	×	×
		a.2.2 Chiffrement de toutes les données en transit, incluant celles échangées entre les machines virtuelles.	✓	×	×	✓	✓	×	×	×	✓	×	×	×
		a.2.3 Le chiffrement ne doit pas affecter la performance des fonctions de recherche ou de tri des données utilisées par l'application.	✓	×	×	✓	×	×	×	×	×	×	×	×
		a.2.4 Utilisation d'algorithmes standards, éprouvés et à jour pour le chiffrement.	✓	×	×	✓	✓	×	×	×	✓	×	×	×
		a.2.5 Identification des appareils autorisés ou non qui utilisent des services infonuagiques.	✓	×	×	×	✓	✓	✓	✓	✓	-	-	✓
		a.2.6 Identification des applications infonuagiques qui sont utilisées dans l'organisation.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

[e] Références : voir la section spécifique de la bibliographie.

Tableau 5.1 : Analyse des écarts entre les requis de l'organisation et l'offre actuelle des fournisseurs de CASB (suite)

Objectifs de sécurité	Requis globaux	Requis spécifiques	Bitglass	BlueCoat (Elastica)	CensorNet	CipherCloud	CloudLock	FireLayers	Imperva	Microsoft Cloud App	Netskope	Palerra	Palo Alto Networks	Skyhigh Networks
b. Intégrité	b.1 Altération des données.	b.1.1 Chiffrement des données.	✓	×	×	✓	✓	×	×	×	✓	×	×	×
c. Disponibilité	c.1 Gestion des incidents et des attaques.	c.1.1 Automatisation de la surveillance (journaux des accès et surveillance des incidents ou des anomalies) pour les couches sous le contrôle de l'organisation.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		c.1.2 Centralisation des informations liées aux services infonuagiques (nom du fournisseur, nature du service, responsabilités, systèmes reliés, etc.) dans un répertoire afin de pouvoir répondre rapidement aux incidents.	×	×	×	×	×	×	×	×	×	×	×	×
d. Gouvernance	d.1 Surveillance et imputabilité.	d.1.1 Suivi et journalisation de la création, de la modification et de la suppression de données utilisées par les applications infonuagiques.	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓
		d.1.2 Journalisation des connexions, des autorisations et détection de comportements anormaux.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	d.2 Conformité.	d.2.1 Conformité avec la réglementation et les normes de sécurité de l'information en vigueur au Canada (ex : Loi de la protection des renseignements personnels, Loi sur les banques, etc.).	×	×	×	×	×	×	×	-	×	×	×	×

Tableau 5.1 : Analyse des écarts entre les requis identifiés et l'offre actuelle des fournisseurs de CASB (suite et fin)

Objectifs de sécurité	Requis globaux	Requis spécifiques	Bitglass	BlueCoat (Elastica)	CensorNet	CipherCloud	CloudLock	FireLayers	Imperva	Microsoft Cloud App	Netskope	Palerra	Palo Alto Networks	Skyhigh Networks
Requis technologiques														
e. Disponibilité	e.1 Gestion des incidents et des attaques.	e.1.1 Alertes en temps réel en cas d'attaque ou d'anomalie et intégration avec les outils du centre de surveillance de la sécurité de l'organisation.	±	±	±	±	±	±	±	±	±	±	±	±
f. Autres	f.1 Intégration.	f.1.1 Compatibilité avec les composantes de l'architecture d'entreprise actuelle.	±	±	±	±	±	±	±	±	±	±	±	±
		f.1.2 Intégration avec les mécanismes de sécurité (ex : logiciel de gestion des événements en sécurité de l'information, logiciel d'authentification unique, logiciel de gestion des appareils mobiles, pare-feu, etc.) déjà en place dans l'organisation, sans les compromettre.	✖	✓	✖	✖	✓	-	✓	✖	✖	✖	✖	✓
		f.1.3 Déploiement local (et non pas en mode infonuagique).	✓	✖	✓	✓	✖	✓	✓	✓	✓	✖	✖	✓

Légende du tableau 5.1 :

✓ : le CASB du fournisseur répond au requis.
✖ : le CASB du fournisseur ne répond pas au requis.
– : l'information sur ce requis n'est pas disponible.
± : le CASB du fournisseur répond partiellement au requis.

Suite à la lecture du tableau précédent, il convient d'apporter quelques précisions afin de remettre les requis en contexte. La première ligne du tableau (a.1.1) mentionne la fédération des identités, un concept qui signifie que l'identité d'un utilisateur est la même pour tous les systèmes de l'organisation. Comme les CASB ne sont pas des logiciels spécialisés en gestion des identités, ce ne sont pas eux qui permettent la fédération des identités, mais plutôt le service d'annuaire jumelé au logiciel d'authentification unique (*Single Sign-on* ou SSO). Le CASB ne remplace pas ces logiciels. Néanmoins, lorsqu'il est compatible avec ceux-ci, il fait en sorte que les politiques de gestion des identités configurées dans ces logiciels, incluant la fédération des identités, soient appliquées aux applications infonuagiques. Ce n'est donc pas le CASB lui-même qui permet la fédération des identités, mais plutôt les logiciels de gestion des identités, pour peu que le CASB soit compatible avec ces derniers.

Une autre ligne du tableau qui nécessite quelques précisions est celle concernant la centralisation des informations associées aux applications infonuagiques utilisées dans l'organisation (requis c.1.2). Ce requis découle d'un besoin d'avoir rapidement accès à l'information concernant le contrat avec le fournisseur, les responsabilités, le canal de communication et le protocole en cas d'un incident de sécurité impliquant le service infonuagique. Ces informations, à condition d'être disponibles aux bonnes personnes dans les différentes équipes, permettraient de répondre plus rapidement aux incidents de sécurité liés à des services infonuagiques. Malheureusement, les CASB ne stockent qu'une information très limitée sur les services infonuagiques comme par exemple, le nom du service et le nombre d'utilisateurs. Ils sont donc, dans leur état actuel, insuffisants pour remplir le requis de l'organisation.

Dans la section sur les requis technologiques dans le tableau précédent, deux ne sont que partiellement remplis, soit la compatibilité avec l'infrastructure de l'organisation (requis f.1.1) et l'intégration avec les outils du centre de surveillance (requis f.1.2). Ces deux requis dépendent des outils et des logiciels en place dans l'organisation. Les fournisseurs de CASB ne sont pas très transparents lorsqu'il est question de la compatibilité avec d'autres logiciels. Ils mentionnent généralement la classe de logiciels avec lesquels ils sont compatibles (par exemple, les gestionnaires d'information et d'événements de sécurité (SIEM) ou le service d'annuaire), mais ils ne précisent pas les logiciels spécifiques parmi tous ceux offerts sur le marché. Des demandes

auprès de certains fournisseurs n'ont pas permis d'obtenir des réponses claires. Ce manque de transparence laisse supposer que la compatibilité des CASB avec d'autres outils est encore très limitée. D'ailleurs, dans un rapport paru cette année, des analystes de Gartner mentionnent que l'intégration des CASB avec les autres composantes de l'infrastructure est une question épineuse à cause de la grande variabilité dans les différentes solutions CASB offertes et dans les outils de sécurité utilisés par les organisations (Reed et Lowans, 2016).

La lecture du tableau précédent permet de conclure qu'aucun produit ne remplit à lui seul tous les requis technologiques et fonctionnels de l'organisation à l'étude. Toutefois, lorsqu'on fait un amalgame de toutes les solutions disponibles sur le marché, on se rend compte que la grande classe d'outils des CASB offre tout de même une bonne couverture en remplissant une majorité de requis. Seuls deux requis ne sont pas comblés par les CASB actuels. Le premier, soit la centralisation des informations liées aux services infonuagiques dans un répertoire, a été discuté plus haut. Le second requis est celui de la conformité avec la réglementation et les normes de sécurité de l'information en vigueur au Canada. Les CASB ont le potentiel d'aider les organisations à se conformer aux lois canadiennes et québécoises de protection des renseignements personnels en imposant le chiffrement, la segmentation en unités ou le masquage[32] des données confidentielles. Certains CASB proposent d'ailleurs des gabarits de politiques de protection des données qui facilitent le respect de certaines lois. Le seul inconvénient est que les lois couvertes sont souvent spécifiques aux États-Unis et les CASB ne proposent pas de gabarits collés aux lois canadiennes, ce qui est peu pratique pour les entreprises d'ici. Heureusement, la plupart des CASB qui offrent ces gabarits permettent aussi de les modifier afin de les personnaliser selon les besoins d'une organisation qui évolue dans un contexte légal différent. Donc, une entreprise canadienne peut tout de même bénéficier de ces fonctionnalités avec quelques efforts de configuration. Toutefois, la configuration personnalisée augmente les coûts et demande des efforts de maintenance supplémentaires. Il serait donc intéressant que les fournisseurs de CASB proposent des gabarits adaptés à leurs clients canadiens s'ils souhaitent percer ce marché.

Cette section avait comme objectif d'analyser les écarts entre les requis spécifiques de l'entreprise à l'étude et des CASB actuellement offerts. Cette analyse dresse un portrait restreint

[32] Le masquage des données consiste à limiter l'exposition de la donnée (Microsoft, 2016e). On la cache des utilisateurs non autorisés en la remplaçant par des étoiles ou des points.

des limites et du potentiel des CASB puisqu'elle est ancrée dans le contexte organisationnel dans lequel a eu lieu l'intervention. La section suivante approfondit la réflexion entamée en se penchant sur l'influence de l'industrie et du contexte organisationnel sur les requis nécessaires pour un CASB.

5.2 L'industrie ou le contexte organisationnel : un déterminant des requis fonctionnels et technologiques pour un CASB ?

De par sa nature, la méthodologie choisie pour ce mémoire ne permet d'étudier qu'une seule entreprise. À ce stade-ci, il est toutefois pertinent de se questionner sur la généralisation possible des résultats à d'autres entreprises et à d'autres industries. En effet, on peut croire que les entreprises œuvrant dans l'industrie de la finance et de l'assurance partagent certaines caractéristiques qui se traduisent par des requis similaires pour un CASB. On pense notamment à l'utilisation de gabarits qui permettent la conformité à des lois spécifiques ou le chiffrement de certaines données. Néanmoins, au-delà de l'appartenance à une industrie, le fruit des discussions tenues et la réflexion faite pointent vers l'identification d'autres facteurs spécifiques à une organisation qui pourraient avoir une grande influence sur les requis technologiques et fonctionnels pour un CASB. L'analyse permet d'en pointer trois, soit la complexité de son infrastructure, son niveau de maturité en termes de sécurité et sa taille.

D'abord, la complexité de l'infrastructure pourrait avoir un impact considérable sur les efforts d'intégration du CASB avec les autres composantes et sur la capacité de cet outil à évoluer avec le reste de l'infrastructure au fil des ajouts de composantes et des mises à jour. La section précédente fait d'ailleurs état de l'importance du requis de compatibilité pour un CASB. Pour une entreprise qui possède une faible complexité technologique, par exemple une entreprise en démarrage, l'implantation d'un CASB semble avantageuse puisque le nombre de composantes avec lesquelles il doit s'intégrer est restreint. Le CASB implanté dans une telle entreprise aurait le potentiel de devenir la pierre angulaire des processus de gestion des services infonuagiques puisque toutes les composantes ajoutées subséquemment à l'infrastructure viendraient s'y intégrer. Dans ces cas, le CASB a réellement la capacité d'assurer la centralisation de la sécurité infonuagique d'une organisation. Dans le cas contraire où l'entreprise possède une infrastructure

beaucoup plus développée, le nombre de composantes impliquées dans l'implantation du CASB risque de causer plusieurs problèmes de compatibilité. Cette lourdeur supplémentaire pourrait venir contrecarrer les économies d'échelle associées à l'utilisation de l'infonuagique. Toujours dans le cas où l'infrastructure est complexe, il est aussi fort possible que les fonctionnalités offertes par les CASB soient déjà disponibles grâce aux outils en place, ce qui amènerait une duplication économiquement difficile à justifier.

En plus de la nature de l'infrastructure en place, le niveau de maturité en sécurité de l'information pourrait avoir une incidence sur la décision d'acquérir un CASB. En effet, une organisation dont les processus de sécurité de l'information sont peu développés est plus vulnérable aux incidents ou aux attaques. Dans ces cas, l'acquisition d'un outil de protection comme un CASB pourrait l'aider en automatisant et en simplifiant une partie de sa gestion de la sécurité. De plus, il est possible que l'implantation d'un CASB dans une organisation qui a un faible niveau de maturité en sécurité requerrait moins de modifications aux processus déjà en place et serait ainsi plus facile et plus économique que dans le cas d'une organisation ayant un plus haut niveau de maturité.

Finalement, au-delà des requis, il est impossible d'ignorer l'aspect économique pur et simple lié à l'implantation d'un CASB et celui-ci est directement dépendant de la taille de l'organisation. En effet, comme les CASB sont généralement facturés en fonction du nombre d'utilisateurs, le coût de possession d'un CASB sera directement proportionnel à la taille de l'organisation. Ce mode de facturation pourrait convenir dans le cas de plus petites entreprises avec un nombre restreint d'employés, mais peut devenir vite prohibitif dans le cas d'une organisation de grande taille. En effet, dans un mode d'utilisation sous licence plus traditionnel (par exemple, pour l'acquisition d'un pare-feu ou d'un logiciel de gestion d'information et d'événements de sécurité (SIEM)), plus le nombre d'employés dans l'organisation est élevé, moins grand est le coût par employé pour le logiciel, ce qui avantage l'organisation de grande taille. De l'autre côté, la facture mensuelle pour l'utilisation d'un CASB demeure constante et est directement proportionnelle au nombre d'utilisateurs. Dans un tel contexte, le mode de facturation d'un CASB par utilisateur (plutôt que fixe ou par paliers) est économiquement plus difficile à justifier pour une entreprise de grande taille, dont le modèle de licence traditionnelle lui permet de bénéficier d'économies d'échelle. Si on multiplie le nombre de CASB par le nombre de services infonuagiques utilisés et le fait qu'un

seul employé peut utiliser plusieurs applications infonuagiques, cela peut faire monter drastiquement la facture.

Cette analyse nous mène à penser que les CASB, tels qu'ils sont actuellement, sont peut-être une option plus adaptée à certains types d'organisations que d'autres. Une entreprise de petite taille, avec une infrastructure technologique rudimentaire ou dont le niveau de maturité des processus de sécurité est faible risque de tirer plus de bénéfices de la mise en place d'un CASB qu'une organisation qui ne possède pas ces caractéristiques. Actuellement, le potentiel des CASB pour combler les besoins d'une entreprise semble être dépendant, du moins en partie, du contexte organisationnel dans lequel il est implanté. Cette situation pourrait s'avérer un frein au développement et à l'adoption massive de cette classe d'outils.

Ainsi, les requis identifiés ici pour les CASB, en plus des avantages économiques qu'il est possible d'en tirer, peuvent s'avérer plus ou moins importants selon le contexte organisationnel. On peut assumer qu'une entreprise de grande taille du domaine de la finance et de l'assurance aura des requis fonctionnels et technologiques ainsi que des impératifs économiques semblables. Même s'il est possible de croire qu'ils demeureront tous présents, cette réflexion nous porte à croire que l'importance accordée à chacun des requis identifiés pourrait varier selon les caractéristiques de l'organisation et de son contexte.

Certaines pistes d'amélioration sont proposées dans la section suivante afin que les CASB puissent devenir un outil de sécurité largement adopté dans les organisations.

5.3 Le potentiel et les limites des CASB

Même si l'analyse a été faite pour un contexte organisationnel spécifique, les résultats sont suffisamment généraux pour qu'il nous soit permis d'identifier trois avenues qui permettraient aux CASB de mieux exploiter leur potentiel afin d'assurer la sécurité des services infonuagiques. Ces trois avenues sont l'étendue de la protection offerte, l'étendue des fonctionnalités de cette classe d'outils et, en dernier lieu, la technologie et les modes d'implantation des CASB.

5.3.1 L'étendue de la protection

Chacun des services infonuagiques utilisé dans l'organisation devrait bénéficier des mécanismes de protection requis pour assurer la sécurité de l'information qu'il traite. Or, la multiplication du nombre de services, tous les types confondus, rend cette tâche particulièrement difficile. Les CASB, bien qu'ils représentent un pas dans la bonne direction, n'incarnent pas une solution de protection complète pour deux principales raisons : 1) le nombre limité de SaaS qui sont protégés par les modules des CASB présents sur le marché et 2) les CASB ne sont actuellement disponibles que pour des services de type SaaS. Ces deux points sont discutés à tour de rôle.

Le nombre limité de SaaS couverts par les CASB sur le marché

Malgré le grand nombre d'applications infonuagiques disponibles et utilisées, tel que mentionné dans la revue de la littérature (Chapitre 2) et dans les résultats (Chapitre 4), il y a seulement une poignée d'applications pour lesquelles un module de CASB est proposé. En plus des neuf applications les plus populaires répertoriées dans le Tableau 4.5 sur les caractéristiques des CASB actuels, onze autres applications (ex : SAP Successfactors ou Yammer) ont pu être identifiées sur les sites des fournisseurs (Bitglass, 2016b; CloudLock, 2016; Elastica, 2016; FireLayers, 2016; Microsoft, 2016b; Netskope, 2016; Palerra, 2016; Palo Alto Networks, 2016; Skyhigh Networks, 2016). La couverture totale des CASB actuels s'étend donc à vingt applications, ce qui est très peu si on compare ce chiffre au nombre d'applications que les organisations utilisent. Il y a ainsi une grande proportion des applications utilisées au sein des organisations qui bénéficient d'une moins grande protection. Les fournisseurs de produits de type CASB se doivent de développer des solutions qui couvrent un éventail plus large d'applications afin de répondre aux besoins de leurs clients. Autrement, la protection offerte par ces produits est si limitée par rapport au nombre d'applications utilisées dans l'entreprise qu'il devient difficile d'en justifier l'acquisition.

Mis à part la couverture limitée offerte par les CASB, le format modulaire de ces produits est une autre limite à leur adoption. En effet, l'achat de plusieurs modules pour simplifier la gestion de la sécurité infonuagique est contre-productif puisqu'au lieu d'avoir un logiciel unique qui couvre toutes les applications, il faut en acquérir et en gérer plusieurs. Le gain associé à l'achat d'un CASB est alors marginal puisque l'effort associé à la gestion du CASB et de ses divers modules devient trop grand. Une entreprise pourrait questionner l'intérêt de se procurer un tel produit et préférer assurer sa gestion de la sécurité manuellement plutôt que d'y avoir recours.

Les limites dans les types de services protégés par les CASB

Le second point à considérer est le type de services couverts par les fonctionnalités des CASB actuels. Les entreprises utilisent une combinaison des différents types de services infonuagiques. En effet, selon un rapport publié par Cisco, 45 % des services utilisés par les organisations sont des SaaS, 42 % sont des IaaS alors que 13 % sont des PaaS (Cisco, 2015). Malgré cette diversité dans les services utilisés, l'étendue de la protection offerte par les CASB n'est présentement limitée qu'aux SaaS. Les statistiques démontrent donc que les fournisseurs de CASB se privent d'un marché important en ne se concentrant que sur un seul des trois types de services. Ce manque de couverture pour les différents services risque de causer des inefficiences liées à la duplication des efforts, des processus et des outils de protection pour chacun des trois services.

L'inclusion des PaaS et des IaaS dans l'offre des CASB serait très bénéfique pour les organisations qui n'auraient pas à acquérir un logiciel de sécurité différent pour chacun des trois types de services puisqu'elles auraient accès à toutes les fonctionnalités de gestion de leurs services infonuagiques au cœur d'un seul produit. Un CASB qui ciblerait les PaaS et les IaaS permettrait d'accomplir les objectifs de gouvernance, de protection des données et de protection contre les menaces externes. Pour accomplir ces objectifs, certaines fonctionnalités pourraient être similaires à celles déjà offertes (ex : imposer les politiques de sécurité de l'organisation, chiffrer les données au repos et celles en transit, offrir des mécanismes de surveillance, etc.), alors que d'autres pourraient être adaptées aux caractéristiques spécifiques des PaaS et IaaS (ex : la protection des plateformes de développement pour les PaaS ou la ségrégation et l'intégrité des différentes machines virtuelles du client pour les IaaS). L'inconvénient de se tourner vers ces deux autres types de services pour les fournisseurs est évidemment les investissements dans le développement de fonctionnalités qui leur sont spécifiques. Toutefois, la carence dans l'offre de produits CASB pouvant protéger tous les types de services infonuagiques, tout comme le manque de modules disponibles, représentent un casse-tête pour l'organisation. En effet, l'organisation cliente doit alors se procurer plusieurs produits pour assurer la sécurité des différents services (SaaS, IaaS et PaaS), ce qui cause une lourdeur administrative et une plus grande difficulté à justifier les investissements requis.

5.3.2 L'étendue des fonctionnalités

Ensuite, tout au long du mémoire, il fut beaucoup question de compatibilité entre les CASB et les logiciels de sécurité existants. La plupart des entreprises ont déjà mis en place des mécanismes de sécurité comme des pare-feu, des gestionnaires d'information et d'événements de sécurité (*Security Information and Event Management* ou SIEM) ou des gestionnaires d'appareils mobiles (*Mobile Device Management* ou MDM). Bien que ceux-ci n'ont pas été conçus spécifiquement à cet effet, ils sont tout de même en mesure de protéger les différents services infonuagiques, peu importe leur type. Les CASB entrent donc dans un marché plutôt mature de logiciels de sécurité et certains questionnent leur pertinence puisque plusieurs des fonctions qu'ils offrent sont disponibles grâce aux logiciels déjà présents dans les organisations.

Pour l'instant, les CASB offrent une protection verticale, c'est-à-dire qu'ils possèdent beaucoup de fonctionnalités, mais que chacune de ces fonctionnalités n'offre qu'une protection limitée comparée à un logiciel spécialisé. Par exemple, les CASB offrent le chiffrement des données, mais souvent avec plusieurs bémols et limité à quelques applications pour lesquelles un module spécifique existe. Il devient donc impératif que les CASB, s'ils veulent survivre comme classe d'outils, trouvent un moyen de se démarquer des logiciels de sécurité actuellement offerts. Une solution serait que les fournisseurs choisissent de diminuer le nombre de fonctionnalités offertes par leur CASB, mais qu'ils développent davantage la puissance de chacune des fonctionnalités conservées. Un tel CASB plus spécialisé éliminerait ainsi la concurrence de certains autres logiciels de sécurité tels les SIEM ou les MDM et pourrait les remplacer. Il serait donc beaucoup plus facile de justifier l'achat d'un CASB puisqu'il permettrait de rationaliser les dépenses en licences pour d'autres logiciels. Considérant que la plupart des CASB se vendent à un coût mensuel par utilisateur, il devient important d'être en mesure de justifier cette dépense auprès de la direction de l'entreprise. De plus, le fait de développer davantage certaines fonctions permettrait de centraliser les processus de sécurité de l'organisation, simplifiant ainsi toute la gestion de la sécurité.

Des CASB plus spécialisés avec moins de fonctionnalités viendraient néanmoins avec quelques inconvénients. Ils seraient possiblement plus coûteux à développer parce qu'ils requerraient davantage d'efforts en recherche et en développement de la part des fournisseurs. En effet, la technologie actuelle utilisée par les fournisseurs est loin d'être révolutionnaire et les CASB

fonctionnent selon des mécanismes (ex : utilisation des API ou des *proxy*, utilisation de technologies de chiffrement) qui ont fait leurs preuves. Ainsi, pour développer davantage les fonctionnalités de cette classe d'outils, les fournisseurs devront vraisemblablement investir dans le développement de nouvelles façons de faire. L'autre inconvénient attaché à des CASB plus spécialisés est qu'en adoptant cette voie, les fournisseurs risquent d'attirer moins de clients et de se cantonner dans un marché de niche pour des clients avec des besoins de sécurité très pointus. L'intérêt actuel pour les CASB s'explique entre autres par le fait qu'ils peuvent accomplir des objectifs de sécurité communs à toutes les organisations, peu importe l'industrie. S'ils prennent le virage de la spécialisation, même en offrant un outil de sécurité plus puissant, les fournisseurs de CASB risquent de s'aliéner une certaine clientèle qui a des besoins de sécurité de base. On risque de se retrouver dans un cercle vicieux où les revenus générés par les ventes ne sont pas suffisants pour justifier les investissements en recherche.

5.3.3 La technologie sous-jacente

Un autre point soulevé par l'étude est la technologie utilisée pour protéger les données. L'implantation d'un CASB par *proxy* présuppose que tout le trafic sur le réseau de l'organisation passe par un seul centre de données et qu'il y a un point unique d'entrée. Le CASB est alors utilisé comme une barrière qui intercepte ce trafic, l'analyse et y applique les politiques de protection des données de l'entreprise. Or, cette configuration avec une seule entrée est souvent impossible dans le cas d'une grande entreprise qui a des milliers d'utilisateurs dans différents bureaux et points de services. En effet, dans ce genre d'organisation, il existe plusieurs portes d'entrée qui permettent de gérer et d'équilibrer le trafic pour minimiser la latence. Donc, l'implantation d'un CASB par *proxy*, telle qu'elle se fait aujourd'hui, n'est pas viable pour une entreprise avec plusieurs points d'accès à son réseau et de hautes exigences en sécurité. Pour ce qui est des multiples points d'entrée, l'alternative est un CASB en tant qu'intermédiaire vers l'API, mais la revue de la littérature (Chapitre 2) explique les limites de cette approche et c'est pourquoi un CASB hybride est souvent préconisé. Une solution alternative doit être proposée par les fournisseurs de CASB, sinon ce type d'outil risque de ne pouvoir représenter une solution que pour les entreprises de taille modeste.

Toujours en lien avec le point précédent, dans un mode par *proxy*, le trafic chiffré qui passe par le CASB doit être déchiffré par celui-ci pour l'analyse, puis chiffré de nouveau avant d'être envoyé vers l'application ou l'utilisateur final. Si le CASB est implanté en mode infonuagique, cette façon de faire implique alors que le fournisseur de CASB ait accès à toutes les données de l'entreprise en texte brut, ce qui va à l'encontre de toutes les bonnes pratiques de sécurité mentionnées dans la revue de la littérature. Le fournisseur de CASB ne devrait pas avoir accès aux données en texte brut, ni aux clés de chiffrement. Cette méthode d'implantation en mode infonuagique, la seule offerte par certains fournisseurs, a de quoi rendre les responsables de la sécurité d'une organisation très nerveux. La solution est d'implanter le CASB localement plutôt qu'en mode infonuagique. C'est d'ailleurs pour cette raison que l'implantation du CASB en mode local est un des requis de l'organisation à l'étude. Le contrecoup est que le CASB implanté de cette façon ne bénéficie pas des avantages de l'infonuagique comme l'ajustement selon la demande, l'utilisation en libre-service ou le paiement par utilisateur. Pour un logiciel qui promet de protéger les applications infonuagiques, cela semble plutôt ironique. De plus, l'implantation locale requiert plus de temps, des efforts de maintenance et exige des coûts initiaux plus grands.

En bref, pour développer leur potentiel et devenir un produit de sécurité essentiel, les CASB doivent capitaliser sur leur capacité à centraliser et à standardiser la gestion de la sécurité des services infonuagiques, tous types confondus. En plus de bonifier leur offre d'applications couvertes, ils doivent aussi cibler davantage leurs efforts de protection afin de justifier leur pertinence pour une organisation. Pour le moment, ils représentent un autre logiciel de sécurité parmi tant d'autres et ne se démarquent pas suffisamment du lot pour justifier l'investissement. De plus, leur mode de fonctionnement qui oblige le déchiffrement des données par le CASB risque de créer un certain malaise au sein de plusieurs entreprises, surtout celles de l'industrie de la finance et l'assurance, de la santé ou de la défense, qui ont toutes des données confidentielles à protéger. Ces entreprises ne souhaitent pas laisser une tierce partie avoir accès à toutes leurs données. Les fournisseurs doivent continuer d'être à la recherche de moyens d'implanter cet outil sans compromettre la sécurité des données et du réseau de l'entreprise cliente.

Chapitre 6: Conclusion

Ce mémoire porte sur un sujet peu exploré jusqu'à maintenant en TI, soit la sécurité de l'information dans un environnement infonuagique. Devant le peu de ressources disponibles, les entreprises sont nombreuses à se questionner sur la meilleure façon d'adopter ce mode d'approvisionnement sans mettre en péril leur sécurité. L'étude présentée dans ces pages tente de comprendre les requis en sécurité des entreprises d'une industrie particulière, celle de la finance et de l'assurance au Canada. Ces besoins en sécurité sont nombreux et une nouvelle classe d'outils, les *Cloud Access Security Brokers* ou CASB, a vu le jour afin d'en faciliter leur gestion. Le présent chapitre offre un récapitulatif des apprentissages réalisés en plus de décrire comment ceux-ci contribuent à la recherche et à la pratique. Une présentation des limites de l'étude conclut ensuite le mémoire.

6.1 Rappel de l'objectif et des questions de recherche

L'émergence de l'infonuagique en tant que mode d'approvisionnement informatique force les entreprises à se questionner sur leurs besoins en sécurité de l'information et sur leur tolérance au risque. Bien que l'infonuagique offre certains avantages indéniables, elle comporte aussi certains risques en sécurité de l'information qui diffèrent de ceux présents dans une infrastructure traditionnelle. Parmi les défis spécifiques liés à ce mode d'approvisionnement, il faut noter la difficulté d'assurer la confidentialité, l'intégrité et la disponibilité des données qui sont traitées ou qui logent chez le fournisseur. De plus, il faut ajouter à cela la division des responsabilités entre le client et le fournisseur qui varie selon le type de services infonuagiques et qui peut s'avérer parfois floue. Les obligations légales auxquelles sont soumises les entreprises viennent également complexifier davantage le choix d'une solution ou d'un fournisseur infonuagique. Les CASB ont été proposés comme une classe d'outils qui permettrait justement de simplifier la gestion de la sécurité infonuagique. Bien qu'ils aient un potentiel intéressant, leur nouveauté et la complexité de leurs interactions avec les autres composantes de l'infrastructure technologique de l'entreprise en font des produits complexes.

Le mémoire cherchait donc à comprendre, dans un premier temps, quels seraient les requis fonctionnels et technologiques d'un CASB mis en place dans le domaine de la finance et de

l'assurance au Canada. Pour ce faire, une revue exhaustive de la littérature a été réalisée afin de jeter les bases conceptuelles nécessaires à une intervention en entreprise. Cette intervention s'est déroulée selon une approche de *recherche action design* qui a permis d'identifier les requis fonctionnels et technologiques qui ont ensuite été présentés dans une grille (artefact #1) au chapitre des résultats du mémoire.

La seconde question de recherche visait à dresser un inventaire des fonctionnalités et des caractéristiques des outils de type CASB actuellement sur le marché. Plusieurs sources dont la documentation des fournisseurs, les rapports de firmes de recherche Gartner et Forrester et d'autres revues professionnelles ont été consultées. De plus, des rencontres virtuelles avec deux fournisseurs ont été organisées afin d'obtenir une démonstration de leur produit et des clarifications quant à leurs fonctionnalités. De cet exercice, il est ressorti une grille qui inventorie les fonctionnalités et les caractéristiques de douze CASB (artefact #2).

Dans un troisième temps, l'étude avait comme objectif de répondre à la question suivante : comment les solutions de type CASB actuellement offertes sur le marché répondent-elles aux requis identifiés ? Pour élaborer une réponse à cette question, une comparaison entre la grille des requis de l'organisation et de l'analyse détaillée des différents produits sur le marché a mené à l'identification et à une discussion des écarts entre les requis de l'entreprise et l'offre actuelle et sur le potentiel des CASB pour mieux combler ces requis (artefact #3).

En plus de répondre aux trois questions de recherche énoncées dans l'introduction du mémoire, l'étude a permis de remplir les deux objectifs de la méthodologie de *recherche action design.* Ces objectifs étaient de résoudre un problème organisationnel spécifique grâce à l'intervention ainsi que de réaliser des artefacts qui formulent des réponses au problème rencontré dans le contexte particulier de l'organisation.

6.2 Synthèse des résultats

Les requis en sécurité infonuagique de l'organisation participante sont nombreux et variés. Les facteurs influençant l'identification de ces requis varient selon l'industrie, mais aussi possiblement selon le contexte organisationnel. On peut cependant croire qu'une partie les requis identifiés

dans le mémoire sont quelques peu universels, du moins dans les organisations de l'industrie de la finance et de l'assurance. À part pour quelques aspects, on a toutes les raisons de croire que toutes les organisations de ce secteur ayant recours à l'infonuagique et qui possèdent des caractéristiques les amenant à contempler les CASB souhaiteraient des fonctionnalités semblables. Certains de ces requis sont couverts par l'offre actuelle des fournisseurs de solutions CASB alors que d'autres ne le sont que partiellement ou pas du tout.

Pour ce qui est des requis qui sont comblés par les CASB, on note ceux associés à la gestion des accès et des identités. L'augmentation du nombre de services infonuagiques utilisés dans l'entreprise signifie aussi une augmentation du nombre de comptes d'utilisateur à gérer pour chaque employé. Des outils comme les CASB doivent donc être en mesure d'intégrer les politiques de gestion des identités et des accès, de permettre la fédération des identités et le contrôle des accès basé sur le rôle (*Role-based Access Control* ou RBAC), le tout dans le but de faciliter l'adoption et l'accès aux services infonuagiques. Généralement, les CASB utilise le RBAC pour permettre ou pour interdire l'accès à certaines données confidentielles dont l'utilisation est requise par les applications infonuagiques.

Parmi les autres requis qui sont remplis par les CASB, il y a ceux de visibilité et de l'identification des applications et des appareils utilisés par les employés. On reconnaît avant tout l'importance d'établir un inventaire des applications infonuagiques utilisées au sein de l'entreprise afin de contrer les risques associés au *shadow IT*. Cet inventaire permet de faire des choix plus éclairés en matière de gouvernance et de cibler davantage les processus de surveillance vers les applications les plus à risque. Les CASB étudiés proposent tous des fonctionnalités d'identification d'applications infonuagiques qui permettent même, dans certains cas, d'obtenir une évaluation du niveau de risque associé à chacune.

Du côté des requis qui sont partiellement ou pas du tout comblés par les CASB, il y a les fonctionnalités de surveillance des différents services et la collaboration entre le client et le fournisseur. Ces dernières sont essentielles pour répondre rapidement aux incidents de sécurité de l'information. Bien que cela ne soit pas typique à l'infonuagique, la surveillance dans ce contexte comporte certains défis particuliers à cause de la division des responsabilités. Un outil qui permettrait non seulement de journaliser toutes les activités et les événements de sécurité

des services infonuagiques, mais aussi de centraliser les informations provenant de ces différents services est nécessaire. Cet outil de centralisation permettrait aux différentes équipes d'une cellule de crise d'avoir accès rapidement à toutes les informations nécessaires lors d'un événement compromettant la sécurité d'un service infonuagique. Les CASB actuels offrent certains mécanismes de journalisation ou de surveillance des activités anormales en lien avec l'utilisation des services infonuagiques. Toutefois, ils sont bien loin d'offrir le niveau de surveillance requis dans une institution du domaine de la finance ou de l'assurance et présentent quelques lacunes. Ces lacunes sont comblées par les logiciels de gestion d'information et d'événements de sécurité (*Security Information Event Management* ou SIEM) qui offrent une meilleure protection dans ce domaine. Malheureusement, les CASB, tels qu'ils sont aujourd'hui, à cause des limites de leurs fonctionnalités, ne sont pas en mesure de concurrencer les SIEM.

Ensuite, toujours parmi les requis partiellement comblés, il y a le chiffrement. Le chiffrement des données utilisées dans un environnement infonuagique est une solution proposée par plusieurs experts et organismes pour protéger les données confidentielles des organisations. Les besoins en chiffrement augmenteront proportionnellement avec l'adoption de services infonuagiques, d'où l'importance de se doter d'outils dès maintenant. Peu de CASB offrent des mécanismes de chiffrement et ceux qui en possèdent n'offrent pas des technologies toujours acceptables du point de vue de leur robustesse.

Dans la définition des produits complexes, on retrouve le degré de complexité des interactions entre les composantes du produit (Novak et Eppinger, 2001). Les CASB, étant composés de plusieurs modules, n'y échappent pas. Non seulement, les différents modules, qu'ils proviennent du même fournisseur ou pas, doivent être compatibles entre eux, mais ils doivent aussi être compatibles avec les autres composantes de l'infrastructure technologique de l'entreprise. Comme aucun des CASB étudié n'est en mesure de remplir tous les requis de l'entreprise, on peut imaginer qu'une organisation choisisse de se tourner vers plusieurs fournisseurs pour combler ses requis. La compatibilité est un besoin essentiel afin de ne pas causer de latence dans l'utilisation des services infonuagiques, de réduire la lourdeur associée à l'exécution manuelle des processus, d'assurer une protection optimale et de faciliter l'échange des données avec les autres composantes. Considérant la technologie sous-jacente aux CASB, il est possible que ce requis soit difficile à satisfaire, du moins pour l'instant parce que les résultats montrent une grande

variabilité dans les logiciels de l'infrastructure avec lesquels ils sont compatibles. Un manque de transparence de la part des fournisseurs face à cette question a aussi été grandement remarqué.

Les CASB permettent donc de combler plusieurs des besoins identifiés en sécurité de l'information des applications infonuagiques, mais sont encore limités. Il ne faut pas oublier que la collecte de données de cette étude a été influencée par la définition et les fonctionnalités actuelles des CASB. Dans un monde idéal, cette classe d'outils permettrait une automatisation complète de la gestion des services infonuagiques, tous les types et les modes confondus, mais en réalité, on est loin de cet objectif. Le fait que le nombre de modules disponibles soit limité et que les CASB ne protègent que les SaaS, par exemple, limite grandement leur attrait pour les organisations. De plus, les CASB sont de bons outils généralistes grâce à leurs multiples fonctionnalités réparties sous quatre objectifs de sécurité, mais n'offrent pas beaucoup de profondeur pour chacune. Le marché des outils et logiciels de sécurité est mature, contrairement à celui des CASB. Il est donc difficile de voir comment les CASB, dans leur format actuel, pourront être compétitifs puisque la plupart de leurs fonctionnalités se retrouvent dans des produits déjà en vente sur le marché.

À la lumière des résultats du mémoire, on comprend que les CASB sont loin de représenter l'outil qui viendra résoudre tous les problèmes de sécurité infonuagique auxquels sont confrontées les entreprises. Ils sont encore émergents et ont donc un grand potentiel, pour peu que les fournisseurs les développent en unisson avec les besoins de leurs clients potentiels. La prochaine section est consacrée aux contributions que ce mémoire apporte et des pistes de recherches futures qui pourraient contribuer à rendre ces outils encore plus pertinents pour les organisations qui souhaitent les adopter.

6.3 Contributions et pistes de recherches futures

Les contributions faites dans ce mémoire sont de deux ordres, soit celles pour la pratique et celles pour la recherche appliquée.

6.3.1 Contributions à la pratique

Considérant la nature de la méthodologie choisie pour ce mémoire, les contributions pratiques de la recherche sont nombreuses. Selon la méthodologie RAD, le livrable issu de la recherche tient

compte des spécificités de l'organisation à l'étude et il s'intègre dans son contexte (Sein *et al.*, 2011). La grille des requis présentée au Chapitre 4 correspond spécifiquement aux besoins de l'entreprise à l'étude, mais la plupart de ces besoins sont généralisables à l'ensemble des entreprises canadiennes de la finance et de l'assurance. Inévitablement, les entreprises de cette industrie ont beaucoup en commun et utilisent plusieurs forums d'échange sur la sécurité de l'information afin d'apprendre les unes des autres. Les institutions du domaine n'ont pas avantage à ce qu'un compétiteur soit la cible d'attaques informatiques (parce que cela affecte toutes les entreprises de l'industrie) et elles misent donc sur la coopération, du moins en sécurité de l'information. Ainsi, toutes ces discussions permettent aux membres de l'organisation d'affirmer que la plupart des grandes organisations de ce secteur en sont sensiblement au même point dans leur réflexion sur l'impartition infonuagique et que les résultats de ce mémoire peuvent les aider, de la même façon qu'ils aident l'entreprise participante. Toutefois, malgré des besoins en sécurité semblables au sein de l'industrie, la discussion (Chapitre 5) a jeté la lumière sur l'influence des caractéristiques propres à l'organisation lorsqu'on souhaite traduire les besoins en requis pour un CASB. En effet, d'autres facteurs comme la complexité de l'infrastructure TI de l'organisation, sa maturité en sécurité et sa taille ont un impact sur les fonctionnalités et les caractéristiques requises pour un CASB.

En second lieu, les entreprises dans le domaine de la finance et de l'assurance sont hautement réglementées au Canada et elles traitent des données financières, personnelles et confidentielles de leurs clients, de leurs employés et même de certains partenaires d'affaires. Le niveau de protection qu'elles se doivent d'avoir pour ces données est très élevé puisque l'impact et le préjudice en cas de bris de la confidentialité ou de l'intégrité des données risquent d'être importants. Peu d'industries ont des normes de confidentialité aussi élevées, sauf peut-être les domaines médical et militaire pour lesquels des brèches de sécurité peuvent avoir des conséquences directes sur la vie de gens. Ces trois industries (médicale, militaire et financière) représentent de ce fait trois des cas « extrêmes » en termes de requis en sécurité de l'information. Les autres organisations qui ne sont pas dans ces industries ont des requis moindres qui sont des sous-groupes des requis pour les cas « extrêmes ». Ces organisations, peuvent s'inspirer de ces cas pour encadrer leur utilisation de l'infonuagique et en apprendre sur le potentiel des CASB. L'entreprise participante, tout comme d'autres entreprises dans différents secteurs d'activités,

avait un intérêt réel d'en apprendre davantage sur cette classe d'outils afin de comprendre comment elle pourrait l'aider à soutenir ses processus de sécurité infonuagique.

Il revient à l'entreprise sous étude de décider de se procurer ou non un CASB à court ou à moyen terme suite aux résultats de cette étude. Le mémoire a été l'occasion de l'informer sur cette nouvelle classe d'outils et de cerner ses besoins en sécurité de l'information dans un contexte d'impartition infonuagique. Cet inventaire permettra de l'aider à mettre en place des règles de gouvernance appropriées aux besoins en plus de faciliter l'acquisition de nouveaux services infonuagiques dans le futur. L'étude a aussi permis aux membres de l'entreprise et de la direction d'en apprendre davantage sur cette nouvelle classe d'outils qui est en vogue et d'amorcer leur réflexion quant à la nécessité de se doter ou non d'un CASB. Elle a permis de répondre à plusieurs de leurs questions sur le sujet, d'entamer la discussion avec certains fournisseurs de solutions et de voir certains produits en action grâce à des démonstrations. Toutefois, les limites des outils présentement offerts ont, du moins dans l'immédiat, conduit l'organisation participante à ne pas poursuivre son exploration des CASB comme outils pour combler ses besoins de gestion de ses services infonuagiques.

6.3.2 Contributions à la recherche appliquée et pistes de recherches futures

D'un point de vue de la recherche, la principale contribution de l'étude est d'établir un meilleur cadre définissant la classe d'outils des CASB en faisant l'inventaire des fonctionnalités. Le mémoire a permis de différencier les affirmations marketing des différents fournisseurs de la réalité, ce qui contribuait à créer de la confusion autour de la définition des CASB. En effet, le mémoire a permis de constater que, parmi la vingtaine de fournisseurs clamant que leur produit est un CASB, seulement douze remplissent les critères d'au moins deux des quatre objectifs que sont supposés accomplir les CASB.

En plus du cadre de définition des CASB, l'étude est un pas vers ce que pourrait être le futur de ces outils afin qu'ils puissent mieux répondre aux besoins des organisations. Le présent mémoire a exposé les besoins d'un cas « extrême » en termes de sécurité infonuagique. Il a aussi examiné la possible influence des caractéristiques et du contexte organisationnels lors de l'identification

des requis fonctionnels et technologiques pour un CASB. Quelques pistes pour mieux répondre aux besoins ont ensuite été proposées dans la discussion du Chapitre 5. Les points soulevés permettraient de rendre les CASB encore plus pertinents pour les entreprises qui cherchent à centraliser et à automatiser leurs processus de sécurité des services infonuagiques. Force est de constater que les fournisseurs ont simplement repris des fonctionnalités, généralement les plus accessibles et faciles à intégrer, qui existaient déjà et les ont proposées dans un nouvel emballage. De ce fait, plusieurs requis fonctionnels représentent aujourd'hui de grands défis technologiques qui doivent alimenter les chercheurs en informatique, en cryptographie et en génie logiciel.

Parmi ces défis, le chiffrement représente une limite importante pour les CASB à cause de sa complexité technique et des coûts qui y sont rattachés. Le mémoire a mis en lumière une limite importante des façons de faire actuelles qui ne permettent pas de faire des recherches ou de trier des données chiffrées. Le chiffrement homomorphique représente une avenue intéressante pour le développement d'outils de protection des données. Bien qu'actuellement le chiffrement permette de protéger les données utilisées dans un environnement infonuagique, il est encore coûteux et parfois complexe à mettre en place, ce qui a pour résultat que les fournisseurs et les organisations sont confrontés à des choix difficiles lorsque vient le temps de décider quelles méthodes de chiffrement doivent être utilisées et quelles données doivent être protégées. Il est certain que la pratique pourrait grandement bénéficier de la recherche en cryptographie qui contribuerait aussi à rendre les services infonuagiques plus sécuritaires et attrayant pour les entreprises.

Un autre aspect technique qui pourrait profiter de la recherche est la façon dont les outils de type CASB sont implantés dans les organisations. La revue de la littérature et le chapitre de discussion ont permis de soulever les limites associées à chacun des deux modes de déploiement, soit le CASB en tant qu'intermédiaire vers l'API et le CASB en mode *proxy.* Les recherches futures pourraient se pencher sur ces problèmes qui permettraient de grandes avancées dans le développement d'outils de protection et ferait en sorte que ces outils puissent répondre de façon plus adéquate aux besoins des organisations.

Finalement, en termes de gestion, le mémoire met en lumière les défis de gouvernance et de gestion des services infonuagiques ainsi que la difficulté d'évaluer les solutions existantes. Il met

en évidence le manque de modes d'évaluation des coûts concernant la gestion des services infonuagiques et l'évaluation de la contribution potentielle des CASB à les minimiser. Les entreprises sont aujourd'hui en carence d'outils méthodologiques qui pourraient les aider à compléter un dossier de justification pour un tel outil.

6.4 Limites de l'étude

Finalement, le mémoire a certaines limites qu'il convient de mettre en lumière afin que le lecteur ait toutes les informations nécessaires pour avoir un regard critique sur le contenu du document. Malgré la rigueur de la méthodologie RAD proposée par Sein *et al*., sa principale limite est qu'elle ne permet d'étudier qu'une seule entreprise. Les requis présentés dans le chapitre de résultats sont ceux d'une unique entreprise du milieu de la finance et de l'assurance. Bien que certaines généralisations puissent être faites quant à ces résultats, il convient de conserver une certaine retenue lors de leur généralisation. D'ailleurs, la discussion met en exergue certains facteurs, tels que la complexité de l'infrastructure, la maturité des processus de sécurité et la taille de l'entreprise, qui pourraient aussi avoir une influence sur les requis de sécurité. La validation des résultats dans d'autres entreprises de l'industrie et ensuite dans d'autres organisations au-delà de ce domaine est à encourager afin de mieux explorer la protection et le potentiel des CASB dans une variété de contextes organisationnels.

Le sujet des CASB est intéressant pour les organisations et pour les chercheurs puisqu'il s'agit d'une classe d'outils en pleine émergence. Toutefois, comme les CASB sont des produits très nouveaux sur le marché, l'information à leur sujet est limitée et difficile d'accès. La plupart des sources utilisées pour rédiger la section sur les CASB dans la revue de la littérature au Chapitre 2 et dans les résultats du Chapitre 4 proviennent des fournisseurs eux-mêmes. Il faut donc utiliser ces informations avec prudence et faire la distinction entre les allégations marketing et l'information objective. Malgré les précautions prises lors de la rédaction de ce mémoire pour ne pas offrir de jugement biaisé envers l'un ou l'autre des fournisseurs, il convient d'avertir le lecteur de la nature des sources consultées.

En lien avec le point précédent, la nouveauté relative du sujet du mémoire et l'évolution rapide du marché des CASB font aussi en sorte que l'information contenue dans ce mémoire peut devenir

rapidement désuète. Les informations sur les fonctionnalités des différents CASB présentés dans ce mémoire sont exactes en date d'août 2016. Elles sont néanmoins sujettes à changement à tout moment de la part des fournisseurs.

En conclusion, après avoir complété ce mémoire, on comprend bien l'intérêt des entreprises pour cette classe d'outils que sont les CASB. Il convenait ainsi d'en explorer le potentiel. La popularité grandissante de l'infonuagique dans la dernière décennie a aussi mis en évidence l'importance de développer des mécanismes et des outils permettant d'assurer la sécurité de ces services. Considérant que l'infonuagique apporte son lot de défis particuliers, les CASB ont souvent été décrits comme une classe d'outils qui révolutionnera la gestion de la sécurité. À la lecture de ce mémoire, on se rend compte que cette perception a été grandement influencée par le discours des fournisseurs de CASB et que, même s'ils permettent d'accomplir certains objectifs de sécurité, ils sont encore loin de représenter une solution tous azimuts pour assurer la sécurité des services infonuagiques. Leur potentiel est cependant intéressant, pour peu que les fournisseurs investissent davantage dans la recherche et le développement de fonctionnalités originales répondant aux besoins actuels et futurs de sécurité des organisations. Avec la popularité croissante de l'infonuagique, les besoins en gestion de la sécurité de ces applications grandiront aussi. Étant donné le marché actuel, il est impossible aujourd'hui de prévoir le futur de cette classe d'outils.

Bibliographie

Références générales

Ab Rahman, N.H. et K.-K.R. Choo (2015). « A survey of information security incident handling in the cloud », *Computers & Security*, vol. 49, p. 45-69.

Aceto, G., A. Botta, W. Donato et A. Pescapè (2013). « Cloud monitoring: A survey », *Computer Networks*, vol. 57, no 9, p. 2093-2115.

Adams, C. (2011). « Trusted Third Party », dans H.C.A. van Tilborg et S. Jajodia (dir.), *Encyclopedia of Cryptography and Security*, New York, Springer, p. 1416.

Aguiar, E., Y. Zhang et M. Blanton (2013). « An Overview of Issues and Recent Developments in Cloud Computing and Storage Security », dans J.H. Keesook, C. Baek-Young et S. Sejun (dir.), *High Performance Cloud Auditing and Applications*, New York, Springer, p. 3-33.

Al Morsy, M., J. Grundy et I. Müller (2010). « An Analysis of the Cloud Computing Security Problem », *Proceedings of 17th Asia-Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop*.

Ali, M., S. U. Khan et A. V. Vasilakos (2015). « Security in Cloud Computing: Opportunities and Challenges », *Information Sciences*, vol. 305, p. 357-383.

Ardagna, C.A., R. Asal, E. Damiani et Q.H. Vu (2015). « From Security to Assurance in the Cloud: A Survey », *ACM Computing Surveys*, vol. 48, no 1, p. 2-50.

Armbrust, M., A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica et M. Zaharia (2009). *Above the Clouds: A Berkeley View of Cloud Computing*, Berkeley, University of California, Berkeley, 23 p.

Armbrust, M., A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica et M. Zaharia (2010). « A View of Cloud Computing », *Communications of the ACM*, vol. 53, no 4, p. 50-58.

Asghar, M.R., M. Ion, G. Russello et B. Crispo (2013). « ESPOONerbac : Enforcing Security Policies in Outsourced Environments », *Computers & Security*, vol. 35, p. 2-24.

Avram, M. G. (2014). « Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective », *Procedia Technology*, vol. 12, p. 529-534.

Badger, L., D. Bernstein, R. Bohn, F. de Vaulx, M. Hogan, M. Iorga, J. Messina, K. Mills, E. Simmon, A. Sokol, J. Tong, F. Whiteside et D. Leaf (2014). *Special Publication 500-293: US Government Cloud Computing Technology Roadmap, Volume 1 & Volume 2*, Gaithersburg, National Institute of Standards and Technology (NIST), 140 p. Récupéré de http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf

Badger, L., T. Grance, R. Patt-Corner et J. Voas (2012). *Special Publication 800-146: Cloud Computing Synopsis and Recommendations*, Gaithersburg, National Institute of Standards and Technology (NIST), 81 p. Récupéré de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

Baker, L.B. (2016). *Symantec to Buy Blue Coat for $4.7 Billion to Boost Enterprise Unit*, Reuters. Consulté le 19 juillet 2016 de http://www.reuters.com/article/us-bluecoat-m-a-symantec-idUSKCN0YZ0BM

Ball, M.O., C.J. Colbourn et J.S. Provan (1995). « Chapter 11: Network reliability », dans *Handbooks in Operations Research and Management Science, vol. 7*, Amsterdam, Elsevier, p. 673-762.

Baskerville, R. et M.D. Myers (2004). « Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice - Foreword », *MIS Quarterly*, vol. 28, no 3, p. 329.

Benbasat, I. et R.W. Zmud (1999). « Empirical Research in Information Systems: The Practice of Relevance », *MIS Quarterly*, vol. 23, no 1, p. 3-16.

Benbasat, I. et R.W. Zmud (2003). « The Identity Crisis Within the IS Discipline: Defining and Communicating the Discipline's Core Properties », *MIS Quarterly*, vol. 27, no 2, p. 183-194.

Bitglass (2015). *Bitglass Standard Edition: Datasheet*, Campbell, Bitglass Inc., 4 p. Récupéré de https://pages.bitglass.com/Cloud-Security-Solutions-Brief.html

Bitglass (2016a). *The Definitive Guide to Cloud Access Security Brokers (whitepaper)*, Campbell, Bitglass Inc., 17 p. Récupéré de http://www.ciosummits.com/Online_Asset_Bitglass_White_Paper__The_Definitive_Guide_to_Cloud_Access_Security_Brokers.pdf

Bitglass (2016b). *Discover Risks on Your Network*, Bitglass Inc. Consulté le 9 juin 2016 de http://www.bitglass.com/shadow-it-and-breach-discovery

Bitglass (2016c). *Securely Enable Cloud Storage Across Your Org.*, Bitglass Inc. Consulté le 9 juin 2016 de http://www.bitglass.com/cloud-security

Bittman, T.J. (2016). *When Private Cloud Infrastructure Isn't Cloud, and Why That's Okay*, no G00302342, Stamford, Gartner, 8 p.

Borenstein, N. et J. Blake (2011). « Cloud Computing Standards: Where's the Beef? », *IEEE Internet Computing*, vol. 15, no 3, p. 74-78.

Bradbury, D. (2014). « Does Canada Need NIST? », *Secure Computing Magazine*, no Mai 2014, p. C1-C3.

Brun, E., A. Steinar Saetre et M. Gjelsvik (2009). « Classification of Ambiguity in New Product Development Projects », *European Journal of Innovation Management*, vol. 12, no 1, p. 62-85.

Buyya, R., C.S. Yeo, S. Venugopal, J. Broberg et I. Brandic (2009). « Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility », *Future Generation Computer Systems*, vol. 25, no 6, p. 599-616.

Cavusoglu, H., H. Cavusoglu, J.-Y. Son et I. Benbasat (2015). « Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources », *Information & Management*, vol. 52, no 4, p. 385-400.

CensorNet (2016a). *CensorNet Unified Security Solution Datasheet*, Basingstoke, CensorNet Ltd, 2 p. Récupéré de https://cdn.censornet.com/wp-content/uploads/2015/02/censornet_productsheet_2016_02_USS_commercial.pdf

CensorNet (2016b). *Unified Security Solution*, CensorNet Ltd. Consulté le 10 juin 2016 de https://www.censornet.com/products/unified-security-service/

CensorNet (2016c). *Unified Security Solution: Web [Datasheet]*, Basingstoke, CensorNet Ltd, 3 p. Récupéré de https://cdn.censornet.com/wp-content/uploads/2016/03/censornet_productsheet_2015_01_USS_webmodule.pdf

Chen, H., M.A. Violetta et C.J. Yang (2013). « Contract RBAC in Cloud Computing », *Journal of Supercomputing*, vol. 66, no 2, p. 1111-1131.

CipherCloud (2015a). *CipherCloud for Cloud Discovery [Datasheet]*, San Jose, CipherCloud Inc., 2 p. Récupéré de http://pages.ciphercloud.com/rs/ciphercloud/images/CipherCloud-for-cloud-discover-data-sheet.pdf

CipherCloud (2015b). *Guide to Cloud Data Protection: Whitepaper*, San Jose, CipherCloud Inc., 32 p. Récupéré de http://pages.ciphercloud.com/Guide-to-Cloud-Data-Protection.html

CipherCloud (2016). *CipherCloud for ServiceNow [Datasheet]*, San Jose, CipherCloud Inc., 2 p. Récupéré de http://pages.ciphercloud.com/rs/ciphercloud/images/DS-CC-SN.pdf

Cisco (2015). *Cisco Global Cloud Index: Forecast and Methodology, 2014–2019 (Whitepaper)*, San Jose, Cisco, 44 p. Récupéré de http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf

Clark, D. et B. Laryea (2015). *Cisco to Buy Cloud-Security Provider CloudLock $293 Million.*, Wall Street Journal. Consulté le 21 septembre 2016 de http://www.wsj.com/articles/cisco-to-buy-cloud-security-provider-cloudlock-293-million-1467124386

Cloud Security Alliance (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing, v3*, Seattle, Cloud Security Alliance, 176 p. Récupéré de https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf

Cloud Security Alliance (2014). *Cloud Controls Matrix*, Cloud Security Alliance. Consulté le 21 mai 2016 de https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

Cloud Security Alliance (2016a). *Cloud Security Alliance: About*, Cloud Security Alliance. Consulté le 21 mai 2016 de https://cloudsecurityalliance.org/about/

Cloud Security Alliance (2016b). *Corporate Members*, Cloud Security Alliance. Consulté le 4 septembre 2016 de https://cloudsecurityalliance.org/membership/corporate/

Cloud Special Interest Group et PCI Security Standards Council (2013). *Information Supplement: PCI DSS Cloud Computing Guidelines*, Wakefield, PCI Security Standards Council, 44 p. Récupéré de https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

CloudLock (2015b). *Data Encryption in the Cloud: A Handy Guide [Whitepaper]*, Waltham, CloudLock Inc., 12 p. Récupéré de http://www.cloudlock.com/wp-content/uploads/2014/10/CL_Data-Encryption-In-The-Cloud.pdf

CloudLock (2016a). *The CloudLock Cybersecurity Platform*, CloudLock Inc. Consulté le 16 juin 2016 de https://www.cloudlock.com/platform/

Coles, C. (2016a). *How CASB is Different from Web Proxy / Firewall*, Skyhigh Networks. Consulté le 2 juillet 2016 de https://www.skyhighnetworks.com/cloud-security-blog/how-casb-is-different-from-web-proxy-firewall/

Coles, C. (2016c). *The Top Cloud Security Vendors*, Skyhigh Networks. Consulté le 4 septembre 2016 de https://www.skyhighnetworks.com/cloud-security-blog/top-cloud-security-vendors/

Columbus, L. (2015). *Roundup of Cloud Computing Forecasts and Market Estimates Q3 Update, 2015*, Forbes. Consulté le 5 juin 2016 de http://www.forbes.com/sites/louiscolumbus/2015/09/27/roundup-of-cloud-computing-forecasts-and-market-estimates-q3-update-2015/ - a3c68256c7ad

Cross, T. (2016). « The Future of Computing: After Moore's law », *The Economist*, vol. 418, no 8980, p. 11.

Cser, A., S.S. Balaouras et P. Dostie (2015a). *Vendor Landscape: Cloud Access Security Intelligence (CASI) Solutions*, Cambridge, Forrester Research, 21 p.

Cser, A., R. Holland, S.S. Balaouras et P. Dostie (2015b). *Brief: The Emergence of the Cloud Security Gateway*, Cambridge, Forrester Research, 6 p.

Damiani, E., S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi et P. Samarati (2007). « Selective Data Encryption in Outsourced Dynamic Environments », *Electronic Notes in Theoretical Computer Science*, vol. 168, p. 127-142.

Dorey, P.G. et A. Leite (2011). « Commentary: Cloud computing – A Security Problem or Solution? », *Information Security Technical Report*, vol. 16, no 3 & 4, p. 89-96.

Dwivedi, Y.K. et N. Mustafee (2010). « It's Unwritten in the Cloud: the Technology Enablers for Realising the Promise of Cloud Computing », *Journal of Enterprise Information Management*, vol. 23, no 6, p. 673-679.

Elastica (2014). *The 7 Deadly Sins of Traditional Data Loss Prevention in the New World of Shadow IT (whitepaper)*, San Jose, Elastica, Inc., 4 p. Récupéré de https://www.bluecoat.com/documents/download/4d97ec18-939a-4dbe-b033-d82deaa9cc72/44fbce36-f5a4-4fc3-a84e-089bf94cedd7

Elastica (2016a). *The CloudSOC Platform*, Blue Coat Systems Inc. Consulté le 9 juin 2016 de https://www.elastica.net/cloudsoc/

Elastica (2016b). *Enabling Dropbox for Business [Whitepaper]*, San Jose, BlueCoat Systems Inc., 13 p. Récupéré de http://dc.bluecoat.com/wp-dropbox/

Emison, J.M. (2013). *Cloud Standards: Bottom Up, Not Top Down*, InformationWeek. Consulté le 20 juillet 2016 de http://www.informationweek.com/cloud/infrastructure-as-a-service/cloud-standards-bottom-up-not-top-down/d/d-id/1108220?

Erl, T., Z. Mahmood et R. Puttini (2013). *Cloud Computing: Concepts, Technology & Architecture*, Upper Saddle River, Prentice Hall/Pearson, 528 p.

European Telecommunication Standards Institute (2013). *Cloud Standards Coordination: Final Report v1.0*, Sophia Antipolis, European Telecommunication Standards Institute, 59 p. Récupéré de http://www.etsi.org/images/files/events/2013/2013_csc_delivery_Ws/csc-Final_report-013-csc_Final_report_v1_0_pdF_format-.pdF

FireLayers (2016b). *Platform*, FireLayers Inc. Consulté le 15 juin 2016 de https://www.firelayers.com/product/platform/

Gartner (2016). *IT Glossary: Tokenization [site web]*, Gartner. Consulté le 26 octobre 2016 de http://www.gartner.com/it-glossary/tokenization

Goettelmann, E., N. Mayer et C. Godart (2013). « A General Approach for a Trusted Deployment of a Business Process in Clouds », *Proceedings of the Fifth International Conference on Management of Emergent Digital EcoSystems*, p. 92-99.

Gordon, A. (2016). *The Official (ISC)² Guide to the CCSP CBK*, 2e éd., Indianapolis, Wiley, 544 p.

Green, T. (2016). *The President Wants to Spend $3.1 Billion to Just Upgrade Legacy Systems*, CSO. Consulté le 12 février 2016 de http://www.csoonline.com/article/3031666/security/obama-s-new-cybersecurity-agenda-what-you-need-to-know.html

Gregor, S. et A. Hevner (2013). « Positioning and Presenting Design Science Research for Maximum Impact », *MIS Quarterly*, vol. 37, no 2, p. 337-355.

Hashizume, K., D. G. Rosado, E. Fernández-Medina et E.B. Fernandez (2013). « An Analysis of Security Issues for Cloud Computing », *Journal of Internet Services and Applications*, vol. 4, no 1, p. 1-13.

Hassan, Q.F. (2011). « Demystifying Cloud Computing », *CrossTalk - The Journal of Defense Software Engineering*, no Jan-Fev, p. 16-21.

Heiser, J. (2015). *Developing Your SaaS Governance Framework*, no G00274895, Stamford, Gartner, 12 p.

Hevner, A. et S. Chatterjee (2010). *Design Research in Information Systems - Theory and Practice*, vol. 22, New York, Springer US, coll. Integrated Series in Information Systems, 335 p.

Hevner, A., S.T. March, J. Park et S. Ram (2004). « Design Science in Information Systems Research », *MIS Quarterly*, vol. 28, no 1, p. 75-105.

Iivari, J. (2007). « A Paradigmatic Analysis of Information Systems as a Design Science », *Scandinavian Journal of Information Systems*, vol. 19, no 2, p. 39-64.

Imperva (2016a). *Imperva Skyfence Cloud Gateway*, Imperva Inc. Consulté le 15 juin 2016 de http://www.imperva.com/Products/Skyfence

ISO (2016a). *Membres de l'ISO*, Organisation internationale de normalisation. Consulté le 20 juillet 2016 de http://www.iso.org/iso/fr/home/about/iso_members.htm?membertype=membertype_MB

ISO (2016b). *Normes*, Organisation internationale de normalisation. Consulté le 20 juillet 2016 de http://www.iso.org/iso/fr/home/standards.htm

ISO (2016c). *Qui élabore les normes ISO?*, Organisation internationale de normalisation. Consulté le 20 juillet 2016 de http://www.iso.org/iso/fr/home/standards_development/who-develops-iso-standards.htm

ISO (2016d). *Structure et gouvernance*, Organisation internationale de normalisation. Consulté le 20 juillet 2016 de http://www.iso.org/iso/fr/home/about/about_governance.htm

ISO/CEI 27001 (2013). *Technologies de l'information - Techniques de sécurité: Systèmes de management de la sécurité de l'information - Exigences*, Genève, Organisation internationale de normalisation/Commission électrotechnique internationale, 23 p.

ISO/CEI 27002 (2013). *Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information*, Genève, Organisation internationale de normalisation/Commission électrotechnique internationale, 80 p.

ISO/CEI 27017 (2015). *Information technology - Security techniques - Code of practice based on ISO/IEC 27002 for cloud services*, Genève, Organisation internationale de normalisation/Commission électrotechnique internationale, 30 p.

ISO/CEI 27018 (2014). *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*, Genève, Organisation internationale de normalisation/Commission électrotechnique internationale, 23 p.

ISO/CEI (2016). *Directives ISO/IEC, Partie 1: Supplément ISO consolidé — Procédures spécifiques à l'ISO*, Genève, Organisation internationale de normalisation/Commission électrotechnique internationale, 180 p. Récupéré de http://www.iso.org/iso/fr/extrait_de_l_annexe_sl_2016_-7eme_edition_-hls_and_guidance

Jensen, W. et T. Grance (2011). *Special Publication 800-144 : Guidelines on Security and Privacy in Public Cloud Computing*, Gaithersburg, National Institute of Standards and Technology (NIST), 80 p. Récupéré de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Johnson, A.M. (2009). « Business and Security Executives Views of Information Security Investment Drivers: Results from a Delphi Study », *Journal of Information Privacy and Security*, vol. 5, no 1, p. 3-27.

Juels, A. et A. Oprea (2013). « New Approaches to Security and Availability for Cloud Data », *Communications of the ACM*, vol. 56, no 2, p. 64-73.

Kahol, A. (2015). *CASBs: A Better Approach to Cloud Encryption*, Bitglass, Inc. Consulté le 8 juin 2016 de http://www.bitglass.com/blog/casbs_better_encryption

Kahol, A., A.K. Bhattacharjya et B.N. Kausik (2013). *Patent 9047480: Secure Application Access System [Brevet]*, États-Unis, Cessionnaire: Bitglass, Inc. Récupéré de http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=/netahtml/PTO/srchnum.html&r=1&f=G&l=50&s1=20150039886.PGNR.

Kanwal, A., R. Masood, M.A. Shibli et R. Mumtaz (2015). « Taxonomy for Trust Models in Cloud Computing », *The Computer Journal*, vol. 58, no 4, p. 601-626.

Kapsalis, V., L. Hadellis, D. Karelis et S. Koubias (2006). « A Dynamic Context-aware Access Control Architecture for e-Services », *Computers & Security*, vol. 25, no 7, p. 507-521.

Kepes, B. (2014). *Big News Day on the Cloud Application Security Front*, Forbes. Consulté le 11 juin 2016 de http://www.forbes.com/sites/benkepes/2014/01/28/big-news-day-on-the-cloud-application-security-front/ - 73d7775512d6

Kepes, B. (2016). *Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS*, Rackspace Inc. Consulté le 16 juillet 2016 de https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/

Khansa, L. et C.W. Zobel (2014). « Assessing Innovation in Cloud Security », *Journal of Computer Information Systems*, vol. 54, no 3, p. 45-56.

Kirti, G. (2016). *Why APIs Beat Proxies for Cloud Security*, InfoWorld. Consulté le 1 juillet 2016 de http://www.infoworld.com/article/3087361/security/why-apis-beat-proxies-for-cloud-security.html

Kohgadai, A. (2016). *17 Salesforce Data Security Best Practices*, Skyhigh Networks. Consulté le 5 septembre 2016 de https://www.skyhighnetworks.com/cloud-security-blog/17-must-enable-salesforce-security-capabilities-and-other-best-practices/

Kshetri, N. (2013). « Privacy and security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution », *Telecommunications Policy*, vol. 37, no 4 & 5, p. 372-386.

Laan, S. (2013). *IT Infrastructure Architecture - Infrastructure Building Blocks and Concepts*, 2e éd., Raleigh, Lulu Press Inc., 436 p.

Lawson, C., N. MacDonald et S. Deshpande (2015a). *Select the Right CASB Deployment for Your SaaS Security Strategy*, no G00270559, Stamford, Gartner, 16 p.

Lawson, C., N. MacDonald et J. Heiser (2015b). *Technology Overview for Cloud Access Security Broker*, no G00269985, Stamford, Gartner, 18 p.

Lawson, C., N. MacDonald et B. Lowans (2015c). *Market Guide for Cloud Access Security Broker*, no G00274053, Stamford, Gartner, 19 p.

Leong, L., D. Toombs et R. Gill (2015). *Magic Quadrant for Cloud Infrastructure as a Service, Worldwide*, no G00278620, Stamford, Gartner, 48 p.

Leong, N. (2016). *Cloud Access Security Brokers and Mobile Device Management: A Yin and Yang of Cloud Security*, Imperva Inc. Consulté le 4 septembre 2016 de https://www.skyfence.com/blog/cloud-access-security-brokers-and-mobile-device-management-a-yin-and-yang-of-cloud-security/

Lowans, B. (2016). *Choosing Between Cloud SaaS and CASB Encryption Is Problematic*, no G00314973, Stamford, Gartner, 9 p.

Lowans, B., J. Heiser et S. Buchanan (2016). *Unsanctioned Business Unit IT Cloud Adoption Will Increase Financial Liabilities*, no G00293279, Stamford, Gartner, 9 p.

MacDonald, N. et P. Firstbrook (2012). *The Growing Importance of Cloud Access Security Brokers*, no G00233292, Stamford, Gartner, 15 p.

MacDonald, N. et C. Lawson (2015). *How to Evaluate and Operate a Cloud Access Security Broker*, no G00292468, Stamford, Gartner, 20 p.

Malinverno, P. (2014). *Basic API Management Will Grow into Application Services Governance*, no G00271064, Stamford, Gartner, 7 p.

Marston, S., Z. Li, S. Bandyopadhyay, J. Zhang et A. Ghalsasi (2011). « Cloud computing: The Business Perspective », *Decision Support Systems*, vol. 51, no 1, p. 176-189.

Mas, S. (2015). *Steven Blaney Announces New Funding for Cyber Security*, Canadian Broadcasting Corporation. Consulté le 12 février 2016 de http://www.cbc.ca/news/politics/steven-blaney-announces-new-funding-for-cyber-security-1.3163391

Mell, P. et T. Grance (2011). *Special Publication 800-145: The NIST Definition of Cloud Computing: Recommandations of the National Institute of Standards and Technology*, Gaithersburg, National Institute of Standards and Technology (NIST), 3 p. Récupéré de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Messmer, E. (2009). *Cloud Security Alliance Formed to Promote Best Practices*, Reuters. Consulté le 22 mai 2016 de http://www.computerworld.com/article/2523598/security0/cloud-security-alliance-formed-to-promote-best-practices.html

Microsoft (2016a). *Cloud App Security Datasheet*, Redmond, Microsoft Corporation, 4 p. Récupéré de http://download.microsoft.com/download/C/E/3/CE357CE2-3A98-4493-BAEB-CEB13F333302/Cloud_App_Security_datasheet.pdf

Microsoft (2016b). *Enable instant visibility, protection and governance actions for your apps*, Microsoft Corporation. Consulté le 8 juin 2016 de https://technet.microsoft.com/en-us/library/mt657563.aspx

Microsoft (2016c). *Enterprise-grade Security for Your Cloud Apps*, Microsoft Corporation. Consulté le 4 juin 2016 de https://www.microsoft.com/en-us/cloud-platform/cloud-app-security

Microsoft (2016d). *How Cloud Discovery Works*, Microsoft Corporation. Consulté le 2 août 2016 de https://technet.microsoft.com/en-us/library/mt725301.aspx

Microsoft (2016e). *Prise en main du masquage de données dynamiques de base de données SQL (portail Azure)*, Microsoft Corporation. Consulté le 26 octobre 2016 de https://azure.microsoft.com/fr-fr/documentation/articles/sql-database-dynamic-data-masking-get-started/

Microsoft (2016f). *What Is a Proxy Server?*, Microsoft Corporation. Consulté le 17 mai 2016 de http://windows.microsoft.com/en-gb/windows-vista/what-is-a-proxy-server

Mitnick, K.D. et W.L. Simon (2002). *The Art of Deception: Controlling the Human Element of Security*, Indianapolis, Wiley, 368 p.

Mouratidis, H., S. Islam, C. Kalloniatis et S. Gritzalis (2013). « A Framework to Support Selection of Cloud Providers Based on Security and Privacy Requirements », *Journal of Systems and Software*, vol. 86, no 9, p. 2276-2293.

Munteanu, V.I., A. Edmonds, T.M. Bohnert et T-F. Fortis (2014). « Cloud Incident Management, Challenges, Research Directions, and Architectural Approach », *Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, p. 786-791.

Naone, E. (2011). *Homomorphic Encryption*, MIT Technology Review. Consulté le 19 juillet 2016 de http://www2.technologyreview.com/news/423683/homomorphic-encryption/

Netskope (2016). *How Netskope Secures Your Apps*, Netskope Inc. Consulté le 11 juin 2016 de https://www.netskope.com/product/how-netskope-works/

NIST (2016). *NIST General Information*, National Institute of Standards and Technology. Consulté le 17 avril 2016 de http://www.nist.gov/public_affairs/general_information.cfm

NIST Cloud Computing Standards Roadmap Working Group (2013). *Special Publication 500-291, Version 2 : NIST Cloud Computing Standards Roadmap*, Gaithersburg, National Institute of Standards and Technology (NIST), 113 p. Récupéré de https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

NIST Joint Task Force (2013). *Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4*, Gaithersburg, National Institute of Standards and Technology (NIST), 462 p. Récupéré de http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Novak, S. et S.D. Eppinger (2001). « Sourcing by Design: Product Complexity and the Supply Chain », *Management Science*, vol. 47, no 1, p. 189-204.

Orman, H. (2016). « Both Sides Now: Thinking about Cloud Security », *Internet Computing*, vol. 20, no 1, p. 83-87.

Ouedraogo, M. et H. Mouratidis (2013). « Selecting a Cloud Service Provider in the Age of Cybercrime », *Computers & Security*, vol. 38, p. 3-13.

Overby, S. (2016). « Managing the Multivendor Cloud », *CIO*, no Janvier 2016, p. 27-29.

Paar, C. et J. Pelzl (2009). *Understanding Cryptography: A Textbook for Students and Practitioners*, Berlin, Springer, 372 p.

Palerra (2015a). *LORIC for Office 365: Solution Brief*, Santa Clara, Palerra Inc., 2 p. Récupéré de http://info.palerra.com/rs/palerra/images/solution-brief-loric-for-office-365.pdf

Palerra (2015b). *LORIC: The Cloud Security Automation Platform [Datasheet]*, Santa Clara, Palerra Inc., 2 p. Récupéré de http://info.palerra.com/rs/palerra/images/DS_LORICOverview.pdf

Palerra (2016). *LORIC*, Palerra Inc. Consulté le 10 juin 2016 de http://palerra.com/platform/

Palo Alto Networks (2016a). *Aperture*, Palo Alto Networks. Consulté le 10 juin 2016 de https://www.paloaltonetworks.com/products/secure-the-cloud/aperture

Palo Alto Networks (2016c). *Aperture Solution Brief*, Santa Clara, Palo Alto Networks, 5 p. Récupéré de https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/aperture-at-glance

Patiniotakis, I., Y. Verginadis et G. Mentzas (2015). « PuLSaR: Preference-based Cloud Service Selection for Cloud Service Brokers », *Journal of Internet Services and Applications*, vol. 6, no 26, p. 1-14.

PCI Security Standards Council (2013). *Norme de scurité des données de l'Industrie des cartes de paiement (PCI), v3.0*, Wakefield, PCI Security Standards Council, 135 p. Récupéré de https://fr.pcisecuritystandards.org/_onelink_/pcisecurity/en2frfr/minisite/en/docs/PCI_DSS_v3.pdf

Ponemon Institute (2015). *2015 Cost of Data Breach Study: Global Analysis*, Traverse City, Ponemon Institute, 30 p. Récupéré de https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

PricewaterhouseCoopers (2014). *Why You Should Adopt the NIST Cybersecurity Framework*, London, PricewaterhouseCoopers, 10 p. Récupéré de http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

PricewaterhouseCoopers (2015). *Turnaround and Transformation: Key Findings from The Global State of Information Security Survey 2016*, London, PricewaterhouseCoopers, 32 p. Récupéré de http://www.pwc.com/ca/en/consulting/publications/pwc-2016-01-20-turnaround-and-transformation-in-cybersecurity.pdf

Proctor, P.E., K. Thielemann, E. Perkins et K. Pratap (2016). *Best Practices in Implementing the NIST Cybersecurity Framework*, no G00296149, Stamford, Gartner, 12 p.

Proffitt, B. (2013). *What APIs Are and Why They're Important*, ReadWrite. Consulté le 2 juillet 2016 de http://readwrite.com/2013/09/19/api-defined/

Rebollo, O., D. Mellado, E. Fernández-Medina et H. Mouratidis (2015). « Empirical Evaluation of a Cloud Computing Information Security Governance Framework », *Information and Software Technology*, vol. 58, p. 44-57.

Reed, B. et B. Lowans (2016). *CASBs Must Not Be Data Security Islands*, no G00281086, Stamford, Gartner, 9 p.

RightScale (2015). *State of the Cloud Report*, Santa Barbara, RightScale Inc., 31 p. Récupéré de http://assets.rightscale.com/uploads/pdfs/RightScale-2015-State-of-the-Cloud-Report.pdf

Riley, S. (2016). *Staying Secure in the Cloud Is a Shared Responsibility*, no G00296799, Stamford, Gartner, 12 p.

Rizvi, S., K. Cover et C. Gates (2014). « A Trusted Third-party (TTP) based Encryption Scheme for Ensuring Data Confidentiality in Cloud Environment », *Procedia Computer Science*, vol. 36, p. 381-386.

Rojas, V. (2014). *The Importance of Framing the Cloud*, Organisation internationale de normalisation (ISO). Consulté le 20 juillet 2016 de http://www.iso.org/iso/news.htm?refid=Ref1897

Rong, C., S.T. Nguyen et M.G. Jaatun (2013). « Beyond Lightning: A Survey on Security Challenges in Cloud Computing », *Computers & Electrical Engineering*, vol. 39, no 1, p. 47-54.

Rountree, D. (2013). *Federated Identity Primer*, Waltham, Elsevier/Syngress, 96 p.

Ryan, M.D. (2013). « Cloud Computing Security: The Scientific Challenge, and a Survey of Solutions », *Journal of Systems and Software*, vol. 86, no 9, p. 2263-2268.

Salesforce (2016). *Salesforce Help: What's the Difference Between Classic Encryption and Shield Platform Encryption?* Consulté le 5 septembre 2016 de https://help.salesforce.com/HTViewHelpDoc?id=security_pe_comparison_table.htm&language=en_US

Scarfone, K., M. Souppaya et P. Hoffman (2011). *Special Publication 800-125 : Guide to Security for Full Virtualization Technologies*, Gaithersburg, National Institute of Standards and Technology (NIST), 35 p. Récupéré de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf

Schuricht, M. et S. Hafid (2016). *Beyond the Firewall: Securing the Cloud with a CASB*, [Vidéo], BrightTalk. Consulté le 19 juillet 2016 de https://www.brighttalk.com/webcast/10415/197745/beyond-the-firewall-securing-the-cloud-with-a-casb

Sein, M., O. Henfridsson, S. Purao, M. Rossi et R. Lindgren (2011). « Action Design Research », *MIS Quarterly*, vol. 35, no 1, p. 37-56.

Silic, M. et A. Back (2014a). « Information Security: Critical Review and Future Directions for Research », *Information Management & Computer Security*, vol. 22, no 3, p. 279-304.

Silic, M. et A. Back (2014b). « Shadow IT – A View from Behind the Curtain », *Computers & Security*, vol. 45, p. 274-283.

Siponen, M. et R. Willison (2009). « Information Security Management Standards: Problems and Solutions », *Information & Management*, vol. 46, no 5, p. 267-270.

Skyhigh Networks (2015a). *Cloud Adoption and Risk in Financial Services Report*, Campbell, Skyhigh Networks, 15 p. Récupéré de http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP_Skyhigh_Cloud_Adoption_Risk_Report_Q4_2015.pdf

Skyhigh Networks (2015b). *Skyhigh Data Security [Whitepaper]*, Campbell, Skyhigh Networks, 4 p. Récupéré de http://info.skyhighnetworks.com/rs/274-AUP-214/images/SB Skyhigh Data Security 0116.pdf

Skyhigh Networks (2015c). *Skyhigh for Shadow IT [Whitepaper]*, Campbell, Skyhigh Networks, 4 p. Récupéré de http://info.skyhighnetworks.com/rs/274-AUP-214/images/DS-Skyhigh-for-Shadow-IT.pdf

Skyhigh Networks (2016a). *Cloud Access Security Broker*, Skyhigh Networks. Consulté le 10 juin 2016 de https://www.skyhighnetworks.com/cloud-access-security-broker/

Sookasa (2016). *The Next Vision for CASB: API*, Sookasa. Consulté le 2 juillet 2016 de https://www.sookasa.com/blog/next-vision-casb-api

Stanton, B., M. Theofanos et K.P. Joshi (2015). *Special Publication 500-316: Framework for Cloud Usability*, Gaithersburg, National Institute of Standards and Technology (NIST), 18 p. Récupéré de http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-316.pdf

Takabi, H., J.B.D. Joshi et G. Ahn (2010). « Security and Privacy Challenges in Cloud Computing Environments », *IEEE Security & Privacy*, vol. 8, no 6, p. 24-31.

Tang, C. et J. Liu (2015). « Selecting a Trusted Cloud Service Provider for Your SaaS Program », *Computers & Security*, vol. 50, p. 60-73.

Tebaa, M., S. El Hajji et A. El Ghazi (2012). « Homomorphic Encryption Method Applied to Cloud Computing », *Proceedings of the 2012 National Days of Network Security and Systems*, p. 86-89.

Thomas, A. et K.R. Moyer (2016). *Articulating the Business Value of APIs*, no G00291965, Stamford, Gartner, 11 p.

von Solms, R. et J. van Niekerk (2013). « From Information Security to Cyber Security », *Computers & Security*, vol. 38, p. 97-102.

von Solms, S.H. et R. von Solms (2009). *Information Security Governance*, New York, Springer, 138 p.

Waldrop, M.M. (2016). *The Chips Are Down for Moore's Law*, Nature Publising. Consulté le 17 avril 2016 de http://www.nature.com/news/the-chips-are-down-for-moore-s-law-1.19338

Wang, H., X. Yi, E. Bertino et L. Sun (2016). « Protecting Outsourced Data in Cloud Computing through Access Management », *Concurrency and Computation: Practice and Experience*, vol. 28, no 3, p. 600-615.

Waters, B. (2005). « Software as a Service: A Look at the Customer Benefits », *Journal of Digital Asset Management*, vol. 1, no 1, p. 32-39.

Wright, R. (2015). *Blue Coat Merges CASBs with Web Gateway Security*, TechTarget. Consulté le 19 juillet 2016 de http://searchcloudsecurity.techtarget.com/news/4500258069/Blue-Coat-merges-CASBs-with-Web-gateway-security

Yi, X., R. Paulet et E. Bertino (2014). *Homomorphic Encryption and Applications*, Cham, Springer, 126 p.

Zissis, D. et D. Lekkas (2012). « Addressing cloud computing security issues », *Future Generation Computer Systems*, vol. 28, no 3, p. 583-592.

Références des tableaux 4.2, 4.3, 4.4 et 5.1

Bitglass (2015). *Bitglass Standard Edition: Datasheet*, Campbell, Bitglass Inc., 4 p. Récupéré de https://pages.bitglass.com/Cloud-Security-Solutions-Brief.html

Bitglass (2016b). *Discover Risks on Your Network*, Bitglass Inc. Consulté le 9 juin 2016 de http://www.bitglass.com/shadow-it-and-breach-discovery

Bitglass (2016c). *Securely Enable Cloud Storage Across Your Org.*, Bitglass Inc. Consulté le 9 juin 2016 de http://www.bitglass.com/cloud-security

CensorNet (2016a). *CensorNet Unified Security Solution Datasheet*, Basingstoke, CensorNet Ltd, 2 p. Récupéré de https://cdn.censornet.com/wp-content/uploads/2015/02/censornet_productsheet_2016_02_USS_commercial.pdf

CensorNet (2016b). *Unified Security Solution*, CensorNet Ltd. Consulté le 10 juin 2016 de https://www.censornet.com/products/unified-security-service/

CensorNet (2016c). *Unified Security Solution: Web [Datasheet]*, Basingstoke, CensorNet Ltd, 3 p. Récupéré de https://cdn.censornet.com/wp-content/uploads/2016/03/censornet_productsheet_2015_01_USS_webmodule.pdf

Centrify (2015). *Centrify Partners with Leading Cloud Access Security Brokers to Enhance Cloud Security for SaaS Applications [Press Release]*, Centrify. Consulté le 4 novembre 2016 de https://www.centrify.com/about-us/news/press-releases/2015/centrify-partners-with-leading-cloud-access-security-brokers/

Chopra, R. (2014a). *Protecting Data in the Cloud with Encryption*, Netskope Inc. Consulté le 2 août 2016 de https://www.netskope.com/blog/protecting-data-cloud-encryption/

Chopra, R. (2014b). *Safe Cloud Enablement in EMEA*, Netskope Inc. Consulté le 2 août 2016 de https://www.netskope.com/blog/safe-cloud-enablement-emea/

CipherCloud (2015a). *CipherCloud for Cloud Discovery [Datasheet]*, San Jose, CipherCloud Inc., 2 p. Récupéré de http://pages.ciphercloud.com/rs/ciphercloud/images/CipherCloud-for-cloud-discover-data-sheet.pdf

CipherCloud (2015b). *Guide to Cloud Data Protection: Whitepaper*, San Jose, CipherCloud Inc., 32 p. Récupéré de http://pages.ciphercloud.com/Guide-to-Cloud-Data-Protection.html

CipherCloud (2016). *CipherCloud for ServiceNow [Datasheet]*, San Jose, CipherCloud Inc., 2 p. Récupéré de http://pages.ciphercloud.com/rs/ciphercloud/images/DS-CC-SN.pdf

CloudLock (2015a). *The CASB & Cloud Cybersecurity Platform [Datasheet]*, Waltham, CloudLock Inc., 5 p. Récupéré de https://www.cloudlock.com/wp-content/uploads/2015/01/CloudLock-Security-Fabric-Product-Sheet.pdf

CloudLock (2015b). *Data Encryption in the Cloud: A Handy Guide [Whitepaper]*, Waltham, CloudLock Inc., 12 p. Récupéré de http://www.cloudlock.com/wp-content/uploads/2014/10/CL_Data-Encryption-In-The-Cloud.pdf

CloudLock (2016a). *The CloudLock Cybersecurity Platform*, CloudLock Inc. Consulté le 16 juin 2016 de https://www.cloudlock.com/platform/

CloudLock (2016b). *Comprehensive Salesforce Security [Solution Brief]*, Waltham, CloudLock Inc., 2 p. Récupéré de https://www.cloudlock.com/wp-content/uploads/2016/05/Comprehensive-Salesforce-Security-DataSheet.pdf

CloudLock (2016c). *Platform: How It Works*, CloudLock Inc. Consulté le 23 octobre 2016 de https://www.cloudlock.com/platform/how-it-works/

Coles, C. (2016b). *New eBook: Which CASB Deployment Architecture is Right for Me?*, Skyhigh Networks. Consulté le 20 novembre 2016 de https://www.skyhighnetworks.com/cloud-security-blog/new-ebook-which-casb-deployment-architecture-is-right-for-me/

Cser, A., S.S. Balaouras et P. Dostie (2015a). *Vendor Landscape: Cloud Access Security Intelligence (CASI) Solutions*, Cambridge, Forrester Research, 21 p.

Elastica (2015a). *Adaptive Security for Google Drive [Solution Brief]*, San Jose, Elastica Inc., 3 p. Récupéré de https://www.elastica.net/wp-content/uploads/2015/08/Elastica-SolutionBrief-GOOGLEDRIVE.pdf

Elastica (2015b). *Adaptive Security for Office 365 [Solution Brief]*, San Jose, Elastica Inc., 3 p. Récupéré de https://www.elastica.net/wp-content/uploads/2015/08/Elastica-SolutionBrief-OFFICE365.pdf

Elastica (2015c). *Shadow IT Assessment & Monitoring with Elastica CloudSOC & Audit [Solution Brief]*, San Jose, Elastica Inc., 8 p. Récupéré de https://www.elastica.net/wp-content/uploads/2015/07/Elastica_SolutionBrief_ShadowIT.pdf

Elastica (2016a). *The CloudSOC Platform*, Blue Coat Systems Inc. Consulté le 9 juin 2016 de https://www.elastica.net/cloudsoc/

Elastica (2016b). *Enabling Dropbox for Business [Whitepaper]*, San Jose, BlueCoat Systems Inc., 13 p. Récupéré de http://dc.bluecoat.com/wp-dropbox/

Elastica (2016c). *Securely Enabling Cloud Apps with Elastica CloudSOC & Gateway [Solution Brief]*, San Jose, Elastica Inc., 8 p. Récupéré de https://www.elastica.net/wp-content/uploads/2016/03/Elastica_SolutionBrief_Gateway.pdf

FireLayers (2016a). *FireLayers: Platform Review [Solution Brief]*, Redwood City, FireLayers Inc., 4 p. Récupéré de https://www.firelayers.com/wp-content/uploads/2016/04/FireLayers-Overview-1-1-1.pdf

FireLayers (2016b). *Platform*, FireLayers Inc. Consulté le 15 juin 2016 de https://www.firelayers.com/product/platform/

Imperva (2016a). *Imperva Skyfence Cloud Gateway*, Imperva Inc. Consulté le 15 juin 2016 de http://www.imperva.com/Products/Skyfence

Imperva (2016b). *Imperva Skyfence Cloud Gateway [Datasheet]*, Redwood Shores, Imperva, 4 p. Récupéré de https://www.skyfence.com/wp-content/uploads/2015/06/DS-Imperva-Skyfence-Cloud-Gateway.pdf

Lawson, C., N. MacDonald et B. Lowans (2015c). *Market Guide for Cloud Access Security Broker*, no G00274053, Stamford, Gartner, 19 p.

Lawson, C., N. MacDonald, B. Lowans et B. Reed (2016). *Market Guide for Cloud Access Security Brokers*, no G00293664, Stamford, Gartner, 23 p.

Microsoft (2016a). *Cloud App Security Datasheet*, Redmond, Microsoft Corporation, 4 p. Récupéré de http://download.microsoft.com/download/C/E/3/CE357CE2-3A98-4493-BAEB-CEB13F333302/Cloud_App_Security_datasheet.pdf

Microsoft (2016b). *Enable instant visibility, protection and governance actions for your apps*, Microsoft Corporation. Consulté le 8 juin 2016 de https://technet.microsoft.com/en-us/library/mt657563.aspx

Microsoft (2016c). *Enterprise-grade Security for Your Cloud Apps*, Microsoft Corporation. Consulté le 4 juin 2016 de https://www.microsoft.com/en-us/cloud-platform/cloud-app-security

Microsoft (2016d). *How Cloud Discovery Works*, Microsoft Corporation. Consulté le 2 août 2016 de https://technet.microsoft.com/en-us/library/mt725301.aspx

Netskope (2015a). *The Netskope Active Platform: Enabling Safe Migration to the Cloud [Solution Brief]*, Los Altos, Netskope Inc., 6 p. Récupéré de http://go.netskope.com/rs/665-KFP-612/images/NS-Netskope-Platform-DS-00.pdf

Netskope (2015b). *Netskope Cloud Confidence Index [Solution Brief]*, Los Altos, Netskope Inc., 4 p. Récupéré de https://resources.netskope.com/h/i/40484891-netskope-cloud-confidence-index

Netskope (2016). *How Netskope Secures Your Apps*, Netskope Inc. Consulté le 11 juin 2016 de https://www.netskope.com/product/how-netskope-works/

Palerra (2015a). *LORIC for Office 365: Solution Brief*, Santa Clara, Palerra Inc., 2 p. Récupéré de http://info.palerra.com/rs/palerra/images/solution-brief-loric-for-office-365.pdf

Palerra (2015b). *LORIC: The Cloud Security Automation Platform [Datasheet]*, Santa Clara, Palerra Inc., 2 p. Récupéré de http://info.palerra.com/rs/palerra/images/DS_LORICOverview.pdf

Palerra (2016). *LORIC*, Palerra Inc. Consulté le 10 juin 2016 de http://palerra.com/platform/

Palo Alto Networks (2016a). *Aperture*, Palo Alto Networks. Consulté le 10 juin 2016 de https://www.paloaltonetworks.com/products/secure-the-cloud/aperture

Palo Alto Networks (2016b). *Aperture Administrator's Guide*, Santa Clara, Palo Alto Networks, 78 p. Récupéré de https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/aperture/aperture/Aperture_guide.pdf

Palo Alto Networks (2016c). *Aperture Solution Brief*, Santa Clara, Palo Alto Networks, 5 p. Récupéré de https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/aperture-at-glance

Skyhigh Networks (2015b). *Skyhigh Data Security [Whitepaper]*, Campbell, Skyhigh Networks, 4 p. Récupéré de http://info.skyhighnetworks.com/rs/274-AUP-214/images/SB Skyhigh Data Security 0116.pdf

Skyhigh Networks (2015c). *Skyhigh for Shadow IT [Whitepaper]*, Campbell, Skyhigh Networks, 4 p. Récupéré de http://info.skyhighnetworks.com/rs/274-AUP-214/images/DS-Skyhigh-for-Shadow-IT.pdf

Skyhigh Networks (2016a). *Cloud Access Security Broker*, Skyhigh Networks. Consulté le 10 juin 2016 de https://www.skyhighnetworks.com/cloud-access-security-broker/

Skyhigh Networks (2016b). *Cloud Access Security Broker [Datasheet]*, Campbell, Skyhigh Networks, 4 p. Récupéré de http://info.skyhighnetworks.com/rs/274-AUP-214/images/DS-Skyhigh-Cloud-Security-Platform.pdf

Skyhigh Networks (2016c). *Skyhigh Compliance [Solution Brief]*, Campbell, Skyhigh Networks, 4 p. Récupéré de http://info.skyhighnetworks.com/rs/274-AUP-214/images/SB Skyhigh Compliance 0116.pdf

Tollefson, R. (2015). *Firewall Vendor Palo Alto Networks Enters Crowded Field*, Third Certainty. Consulté le 30 août 2016 de http://thirdcertainty.com/featured-story/firewall-vendor-palo-alto-networks-enters-crowded-field/

Annexe A : Mots-clés utilisés pour la recherche

Tableau A1 : Mots-clés utilisés lors des recherches dans les bases de données

Catégories	Mots-clés
Sécurité de l'information	Cybersecurity Infosec Information confidentiality Information privacy Information security Information security standards Security framework Security breach
Infonuagique	Cloud benefits Cloud computing Cloud compliance Cloud framework Cloud review Cloud risks / issues Cloud security Cloud trust IaaS ISO 27001 / ISO 27002 / ISO 27017 / ISO 27018 NIST PaaS SLA SaaS
CASB	CASB Cloud access security Cloud security requirements Cloud security intelligence Emerging software requirements Emerging technology requirements Product ambiguity* Product complexity* Product innovation*

*Ces mots-clés ont été utilisés en combinaison avec les termes *cloud computing* et *information security*.

Annexe B : Lignes directrices de la Cloud Security Alliance

Tableau B1 : Les lignes directrices de la Cloud Security Alliance, version 3

Section	Description	Exemple de recommandations
1. Architecture sous-jacente à l'infonuagique	Définition de l'infonuagique, des types de services et des modes d'implantation.	• Aucune ; cette section est informative.
2. Gouvernance et gestion des risques	Gestion des risques associés à l'infonuagique. Mise en place de politiques internes et de cadres de gouvernance pour assurer la sécurité.	• Impliquer le département de sécurité d'une entreprise dans le développement des ententes de niveau de service (SLA). • Mise en place de normes et de mesures pour évaluer le niveau de sécurité du service. • Faire une évaluation des risques avant de sélectionner un produit ou un fournisseur.
3. Questions juridiques : contrats et investigation électronique	Problèmes légaux liés à l'infonuagique. Inclut aussi les requis légaux et de confidentialité auxquels doivent se soumettre les entreprises (cette section couvre surtout les lois américaines).	• Aucune ; les entreprises doivent se plier aux lois en vigueur.
4. Gestion de la conformité et des audits	Mécanismes de conformité, de surveillance et de contrôle dans un contexte infonuagique.	• Les fournisseurs de services infonuagiques ont souvent des contrats standards qui s'appliquent sans distinction à tous les clients. Les entreprises qui sont tenues de se conformer à plusieurs lois et règlements doivent tenter de négocier ces contrats. • Mobiliser les services d'auditeurs externes qui ont une connaissance de l'infonuagique.

[f] Traduction libre de Cloud Security Alliance (2011)

Tableau B1 : Les lignes directrices de la Cloud Security Alliance, version 3 (suite)

Section	Description	Exemple de recommandations
5. Gestion de l'information et sécurité des données	Gestion des données infonuagiques, incluant la responsabilité et l'imputabilité.	• Comprendre l'architecture sous-jacente au stockage de données dans l'environnement infonuagique afin de déterminer les risques inhérents en sécurité. • Utiliser des mécanismes de protection contre la perte des données. • Chiffrer toutes les données sensibles qui sont stockées ou utilisées dans un environnement infonuagique. • Choisir un fournisseur qui est transparent dans ses pratiques de sécurité. • Retirer les données stockées chez un fournisseur de services dès que le contrat vient à échéance.
6. Interopérabilité et portabilité	La capacité de transférer les données d'un fournisseur à un autre ou bien de les rapatrier à l'interne. Les questions de compatibilité entre les différents fournisseurs sont abordées.	• Utiliser la virtualisation pour faciliter l'intégration entre les différentes composantes de l'infrastructure. • Utiliser autant que possible des interfaces de programmation d'applications libres (*open-source*). • Stocker les données dans un format fiable et standard. • S'assurer que les mécanismes d'authentification fonctionnent pour toutes les plateformes et les applications infonuagiques afin d'éviter les multiples connexions ou les problèmes de compatibilité. • S'assurer que le fournisseur fasse fréquemment des copies de sauvegarde des données.
7. Sécurité traditionnelle, continuité des affaires et reprise après sinistre	Les impacts de l'infonuagique sur les processus actuels en gestion de la sécurité de l'organisation.	• Créer et maintenir à jour la documentation liée à l'analyse des risques et des vulnérabilités ainsi que celle liée aux plans de continuité, aux plans de reprise après sinistre et de contingence, aux plans de formation en sécurité, etc. • Choisir un fournisseur qui est fiable et transparent dans ses pratiques de sécurité. • Diversifier les fournisseurs de services infonuagiques afin de ne pas dépendre d'un seul fournisseur, surtout en cas de panne de service.

Tableau B1 : Les lignes directrices de la Cloud Security Alliance, version 3 (suite)

Section	Description	Exemple de recommandations
8. Exploitation des centres de données	Évaluation de l'architecture, des activités d'exploitation et des centres de données des fournisseurs de services afin d'identifier les caractéristiques essentielles de sécurité.	• S'assurer des bonnes pratiques du fournisseur. • Faire attention à la localisation géographique du centre de données. • Bien établir les responsabilités entre le fournisseur qui gère le centre de données et le client.
9. Gestion des incidents	Processus de détection, de gestion et de prévention des incidents dans un contexte infonuagique. Inclut la division des responsabilités entre le client et le fournisseur dans ces situations.	• Créer et maintenir des canaux de communication avec le fournisseur. • Comprendre le service offert par le fournisseur en cas d'incident. • Préparer des stratégies de gestion des incidents. • Obtenir l'historique de réponses aux incidents du fournisseur.
10. Sécurité des applications	Utilisation et développement d'applications de façon sécuritaire dans un environnement infonuagique.	• Faire une évaluation des risques spécifiques au développement et à l'utilisation d'applications infonuagiques. • Prioriser les requis en sécurité et en confidentialité lors du développement. • S'assurer de la traçabilité entre les risques identifiés et les fonctionnalités des applications. • Utiliser ou développer un cadre d'architecture sécuritaire.
11. Chiffrement et gestion des clés de chiffrement	Identification des meilleures pratiques en matière de chiffrement et de gestion des clés.	• Mettre en place les meilleures pratiques lors de l'utilisation de méthodes de chiffrement. • Utiliser une technologie prête à l'emploi plutôt qu'une solution personnalisée. • Gérer soi-même ses clés de chiffrement ou bien se tourner vers un fournisseur de confiance spécialisé dans le domaine.
12. Gestion de l'identité, des droits et des accès	Mécanismes d'authentification pour les services infonuagiques.	• Le principal répertoire des utilisateurs de l'entreprise ne devrait pas être situé dans un environnement infonuagique. • Maintenir des journaux des connexions et des authentifications.

Tableau B1 : Les lignes directrices de la Cloud Security Alliance (suite et fin)

Section	Description	Exemple de recommandations
13. Virtualisation	Risques associés à la virtualisation, une technologie très utilisée en infonuagique.	• Identifier le type de virtualisation utilisé par le fournisseur. • Prendre en considération les limites en termes de performance lors de l'utilisation de la virtualisation. • Choisir un système d'exploitation virtuel qui incorpore des fonctionnalités de sécurité. • Les environnements de production doivent être séparés des environnements de développement et de test.
14. Security-as-a-Service	Utilisation des services d'une tierce partie afin d'assurer la sécurité infonuagique d'une organisation et les risques que cela implique.	• S'assurer de mettre en place des canaux de communication sécuritaires. • L'entreprise devrait exiger des audits faits par une tierce partie.

Annexe C : Normes ISO/CEI 27017 et 27018

Tableau C1 : Les recommandations de la norme ISO/CEI 27017: Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage et de la norme ISO/CEI 27018: 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 [g]

Article	Recommandations
5. Politiques de sécurité de l'information[33]	**ISO/CEI 27017** • Le client doit tenir compte des éléments suivants lors de l'élaboration de ses politiques en sécurité de l'information infonuagique : o Les données stockées chez le fournisseur de services infonuagiques o La gestion des actifs dans un environnement infonuagique o Les impacts de la colocation et de la virtualisation o Les utilisateurs et le contexte d'utilisation des services o Les administrateurs et les comptes à accès privilégié o La localisation géographique où les données sont stockées **ISO/CEI 27018** • Les politiques de sécurité de l'information doivent faire état de l'engagement de l'organisation à se conformer aux lois et aux clauses contractuelles entre celle-ci et le fournisseur infonuagique traitant des données personnelles. • Les clauses contractuelles doivent clairement identifier les responsabilités entre le fournisseur traitant des données confidentielles, ses sous-contractants et le client selon le type de services infonuagiques (IaaS, PaaS ou SaaS).

[g] Traduction libre de ISO/CEI 27017 (2015); ISO/CEI 27018 (2014)

[33] Seuls les articles pertinents pour le client de services infonuagiques sont présentés dans ce tableau.

Tableau C1 : Les recommandations de la norme ISO/CEI 27017: Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage et de la norme ISO/CEI 27018: 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 (suite)

Article	Recommandations
6. Organisation de la sécurité de l'information	**ISO/CEI 27017** • Le client et le fournisseur doivent s'entendre sur les rôles et les responsabilités de chacun. **ISO/CEI 27018** • Aucun nouveau contrôle ne s'applique.
7. La sécurité des ressources humaines	**ISO/CEI 27017** • Des programmes de formation et de sensibilisation sur la sécurité infonuagique doivent être mis en place par le client. • Le client doit ajouter les éléments suivants à ses programmes de formation pour les employés qui utilisent les services infonuagiques : o Normes et procédures pour l'utilisation des services infonuagiques o Les risques de sécurité de l'information liés aux services infonuagiques o Les risques liés aux systèmes et au réseau utilisés en mode infonuagique o Les considérations légales **ISO/CEI 27017** • Des mesures doivent être mises en place pour s'assurer que les employés du client soient sensibilisés aux conséquences d'une brèche de confidentialité des données personnelles traitées par un fournisseur d'infonuagique publique.
8. Gestion des actifs	**ISO/CEI 27017** • Les actifs et l'information stockée dans les services infonuagiques du client doivent être identifiés et répertoriés. De plus, cet inventaire doit mentionner dans quels départements ils sont utilisés. **ISO/CEI 27018** • Aucun nouveau contrôle ne s'applique.

Tableau C1 : Les recommandations de la norme ISO/CEI 27017: Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage et de la norme ISO/CEI 27018: 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 (suite)

Article	Recommandations
9. Contrôle d'accès	**ISO/CEI 27017** • Les politiques de contrôle et d'accès du client au réseau doivent spécifier les requis pour l'accès des utilisateurs pour chacun des services infonuagiques utilisés. • Le client doit avoir des mécanismes d'authentification suffisants (ex : identification multi-facteur) pour l'authentification des gestionnaires de services infonuagiques selon le niveau de risque identifié. • Le client doit vérifier que les procédures d'allocation d'information liées aux identités remplissent les requis de confidentialité du client. • Le client doit s'assurer que l'accès à l'information stockée dans les services infonuagiques est restreint selon ses politiques de gestion des accès. **ISO/CEI 27018** • Selon le type de services infonuagiques, il est possible que le client soit responsable d'une partie ou de toute la gestion des accès des utilisateurs sous son contrôle. Si tel est le cas, le fournisseur traitant des données personnelles doit permettre au client de gérer les accès des utilisateurs sous son contrôle, incluant les privilèges administratifs liés à la gestion et à la suppression des accès. • Les processus de création ou de suppression d'utilisateurs doivent prévoir des dispositions pour les situations dans lesquelles les accès sont compromis.

Tableau C1 : Les recommandations de la norme ISO/CEI 27017: Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage et de la norme ISO/CEI 27018: 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 (suite)

Article	Recommandations
10. Chiffrement	**ISO/CEI 27017** • Le client doit mettre en place le chiffrement pour les services si cela est justifiable suite à une analyse de risque. Le chiffrement doit être suffisant pour mitiger les risques identifiés. • Lorsque le chiffrement est fait par le fournisseur, le client doit réviser toute information transmise par le fournisseur afin de confirmer que le chiffrement : o Rencontre les requis du client o Est compatible avec les autres protections de chiffrement utilisées par le client o S'applique aux données au repos et en transit depuis et vers le service infonuagique • Le client doit identifier les clés de chiffrement pour chaque service infonuagique et mettre en place un processus de gestion des clés. • Lorsque les clés sont gérées par le fournisseur, le client doit exiger l'information suivante : o Le type de clé o Les spécifications liées au système de gestion des clés o Les processus de gestion du cycle de vie des clés • Le client ne doit pas permettre au fournisseur de stocker et de gérer les clés de chiffrement lorsque le client gère lui-même ses clés ou utilise une tierce partie pour la gestion de ses clés. **ISO/CEI 27018** • Aucun nouveau contrôle ne s'applique.
11. Sécurité physique et environnementale	**ISO/CEI 27017** • Le client doit exiger la confirmation que le fournisseur a mis en place les processus et les politiques nécessaires pour disposer ou réutiliser les ressources de façon sécuritaire. **ISO/CEI 27018** • Dans une perspective de recyclage ou de destruction sécurisé, tout équipement susceptible de contenir des données personnelles doit être traité de la même façon qu'un équipement contenant des données personnelles.

Tableau C1 : Les recommandations de la norme ISO/CEI 27017: Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage et de la norme ISO/CEI 27018: 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 (suite)

Article	Recommandations
12. Sécurité liée à l'exploitation	**ISO/CEI 27017** • Les processus de gestion du changement du client doivent tenir compte de l'impact des changements faits du côté du fournisseur. • Le client doit s'assurer que le niveau de service de l'entente est bien respecté par le fournisseur. • Le client doit surveiller l'utilisation des services infonuagiques et planifier ses besoins en termes de capacité afin de s'assurer de la performance des services infonuagique dans le temps. • Le client doit définir les requis pour les journaux d'événements et s'assurer que le fournisseur remplisse ces requis. • Le client doit exiger de l'information du fournisseur concernant sa gestion des vulnérabilités qui peuvent affecter le service fourni. Le client doit identifier les vulnérabilités pour lesquelles le fournisseur est responsable et définir un processus pour les gérer. **ISO/CEI 27018** • Lorsque l'utilisation de données personnelles à des fins de test est inévitable, une analyse de risque doit être effectuée. Des mesures doivent être mises en place pour minimiser les risques identifiés. • Des processus doivent être mis en place pour permettre la restauration des activités de traitement de données personnelles suite à un événement perturbateur. • Un processus de révision des journaux d'événements doit être mis en place à une fréquence régulière afin d'identifier les anomalies et pour proposer des moyens de remédiation. • L'information journalisée à des fins de surveillance et de diagnostic opérationnel pourrait contenir des données personnelles. Des mesures de contrôle doivent être mises en place pour s'assurer que l'information journalisée n'est utilisée qu'aux fins prévues. • Une procédure, préférablement automatisée, doit être mise en place pour s'assurer que l'information journalisée est supprimée dans des délais précis et documentés.

Tableau C1 : Les recommandations de la norme ISO/CEI 27017: Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage et de la norme ISO/CEI 27018: 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 (suite)

Article	Recommandations
13. Sécurité des communications	**ISO/CEI 27017** • Le client doit définir ses requis pour la ségrégation des réseaux afin de s'assurer de l'isolation de l'environnement partagé et il doit s'assurer que le fournisseur remplisse ces requis. **ISO/CEI 27018** • Lorsqu'un support physique est utilisé pour transférer des données personnelles, un système doit être mis en place pour enregistrer l'information concernant ce support. Lorsque possible, le client doit mettre en place des mesures additionnelles en place (tel que le chiffrement) pour s'assurer que les données ne seront accédées qu'à la destination et non en transit.
14. Acquisition, maintenance et développement des systèmes d'information	**ISO/CEI 27017** • Le client doit établir ses requis en sécurité de l'information pour les services infonuagiques et s'assurer que le fournisseur soit en mesure de les remplir. Pour cette évaluation, le client doit s'informer auprès du fournisseur sur ses capacités en sécurité de l'information. • Le client doit demander au fournisseur de l'information sur la sécurité de ses processus de développement. **ISO/CEI 27018** • Aucun nouveau contrôle ne s'applique.
15. Relations avec les fournisseurs	**ISO/CEI 27017** • Le client doit inclure l'infonuagique en tant que type de fournisseur dans sa politique sur les relations avec les fournisseurs. Cela aidera à mitiger les risques associés à la gestion des données et à l'accès qu'ont les employés du fournisseur aux données du client. • Le client doit confirmer avec le fournisseur les rôles et responsabilités en lien avec le service infonuagique. **ISO/CEI 27017** • Aucun nouveau contrôle ne s'applique.

Tableau C1 : Les recommandations de la norme ISO/CEI 27017: Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage et de la norme ISO/CEI 27018: 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 (suite et fin)

Article	Recommandations

16. Gestion des incidents liés à la sécurité de l'information	**ISO/CEI 27017**
	• Le client doit demander de l'information du fournisseur concernant les mécanismes pour :
	  ○ Le signalement d'événements en sécurité de l'information détectés dans les services du fournisseur
	  ○ La transmission de rapports d'événements provenant du fournisseur
	  ○ Le suivi du statut d'un événement déclaré
	• Le client et le fournisseur doivent s'entendre sur la procédure en cas de demande d'investigation numérique (*electronic discovery*) de l'information contenue dans l'environnement infonuagique.
	ISO/CEI 27018
	• Il est possible que le fournisseur traitant des données personnelles ait à collaborer avec le client afin d'implanter les contrôles de son processus de gestion des incidents.

17. Aspect de la sécurité de l'information dans la gestion de la continuité de l'activité	• Aucun nouveau contrôle ne s'applique spécifiquement à l'infonuagique.
18. Conformité	**ISO/CEI 27017** • Le client doit considérer que les lois et les règlements qui s'appliquent peuvent être ceux de la juridiction du fournisseur de services en plus de ceux de la juridiction du client. • Le client doit exiger du fournisseur qu'il se soumette aux lois et règlements auxquels le client est assujetti dans le cadre de ses activités. • L'installation d'un logiciel commercial dans un environnement infonuagique peut causer une violation de la licence d'utilisation. Le client doit avoir des processus pour identifier les spécificités des licences liées aux services infonuagiques avant d'autoriser l'installation d'un logiciel dans un environnement infonuagique. • Le client doit exiger du fournisseur de l'information concernant la protection des données stockées par le fournisseur. • Le client doit s'assurer que l'ensemble des contrôles de chiffrement utilisés sont conformes aux ententes, aux lois et aux règlements pertinents. **ISO/CEI 27018** • Aucun nouveau contrôle ne s'applique.

Annexe D : Recommandations du NIST

Tableau D1 : Publications spéciales du NIST traitant de l'infonuagique[h]

Titre des publications	Description	Recommandations spécifiques à la sécurité infonuagique
SP 500-291 v2 : NIST Cloud Computing Standards Roadmap (2013)	Guide pour aider le gouvernement américain dans l'adoption sécuritaire et efficace de l'infonuagique.	• Protéger les données des clients de l'accès, de la divulgation, de la modification ou de la surveillance non autorisés. • Empêcher l'accès non autorisé à l'infrastructure et aux ressources infonuagiques. Cela inclut la séparation logique (grâce à la virtualisation) entre les ressources et l'utilisation de configurations sécuritaires. • Prendre des mesures pour protéger les logiciels de navigation web utilisés dans l'environnement infonuagique pour mitiger les vulnérabilités en sécurité du côté de l'utilisateur. • Inclure des contrôles d'accès et des solutions de détection et de prévention dans l'environnement infonuagique en plus de mener des évaluations indépendantes pour s'assurer que les solutions sont bien installées et fonctionnelles. • Définir la frontière de confiance entre le client et le fournisseur afin de s'assurer que les responsabilités en termes de contrôles de sécurité sont clairement identifiées.

[h] Traduction libre des publications spéciales du NIST.

Tableau D1 : Publications spéciales du NIST traitant de l'infonuagique (suite)

Titre des publications	Description	Recommandations spécifiques à la sécurité infonuagique
SP 500-293 : US Government Cloud Computing Technology Roadmap (2014)	Recommandations de haut niveau pour faciliter l'adoption de l'infonuagique au sein du gouvernement américain.	• Les applications infonuagiques doivent être intégrées au processus de gestion des identités et des accès de l'organisation. • Une solution d'authentification unique doit être adoptée pour faciliter l'accès aux services infonuagiques et éviter les multiples authentifications. • Pour les applications sensibles, une authentification forte (p.ex. authentification multi-facteur) doit être adoptée. • Une interface standard de gestion des accès doit être mise en place pour faciliter la gestion des services. • Les données au repos qui sont considérées comme sensibles doivent être chiffrées. Les clés doivent être modifiées régulièrement. • Les données en transit qui sont considérées comme sensibles doivent être chiffrées. • Dans un environnement en colocation où les ressources infonuagiques sont partagées, les clés ne doivent pas être accessibles au fournisseur, ni aux autres clients. • Toutes les données liées aux services infonuagiques doivent être transmises au client à la fin du contrat et le fournisseur doit supprimer les données de ses systèmes.
SP 500-316 : Framework for Cloud Usability (2015)	Cadre de référence pour l'expérience utilisateur dans un contexte infonuagique.	• S'assurer que le service infonuagique soit résistant aux attaques d'utilisateurs non autorisés, des autres services infonuagiques, des logiciels malveillants et des attaques sur le matériel et par Internet. • S'assurer que le service infonuagique ne permette pas aux utilisateurs non autorisés d'avoir accès aux données.
SP 800-125 : Guide to Security for Full Virtualization Technologies (2011)	Recommandations pour mitiger les risques de sécurité associés à la virtualisation des serveurs et des postes de travail.	• Rendre tous les éléments de la virtualisation sécuritaires et maintenir leur niveau de sécurité. • Restreindre les privilèges et les accès à la solution de virtualisation seulement aux employés autorisés. • S'assurer de la sécurité de l'hyperviseur. • Créer un plan de sécurité pour la virtualisation avant l'installation, la configuration et le déploiement de la solution.

Tableau D1 : Publications spéciales du NIST traitant de l'infonuagique (suite et fin)

Titre des publications	Description	Recommandations spécifiques à la sécurité infonuagique
SP 800-144 : Guidelines on Security and Privacy in Public Cloud Computing (2011)	Donne une vue d'ensemble de l'infonuagique publique et des risques de sécurité qu'elle implique.	• Planifier avec minutie les aspects de sécurité et de protection de la vie privée associés aux services infonuagiques, avant de les mettre en place. • S'assurer que la solution choisie corresponde aux requis en sécurité de l'organisation. • Mettre en place des mécanismes d'audit pour s'assurer de la conformité des pratiques de sécurité du fournisseur à celles de l'organisation. • Établir clairement la responsabilité et les droits par rapport aux données. • Mettre en place un programme de gestion des risques qui pourra s'adapter à l'évolution de l'environnement infonuagique. • Surveiller constamment l'état et la sécurité du système. • S'assurer qu'un processus de gestion des incidents transparent est en place chez le fournisseur.
SP 800-146 : Cloud Computing Synopsis and Recommendations (2012)	Document récapitulatif sur la définition et les caractéristiques de l'infonuagique et les opportunités et risques associés.	• S'assurer que les mécanismes de protection des données et les technologies associées à la solution remplissent les exigences de sécurité du client. • Mettre en œuvre des mécanismes de protection des appareils utilisés pour accéder aux services infonuagiques. • S'assurer de chiffrer toutes les données qui pourraient être utilisées ou qui pourraient transiter par les services infonuagiques. • S'assurer que le fournisseur ait des mécanismes fiables de suppression des données.