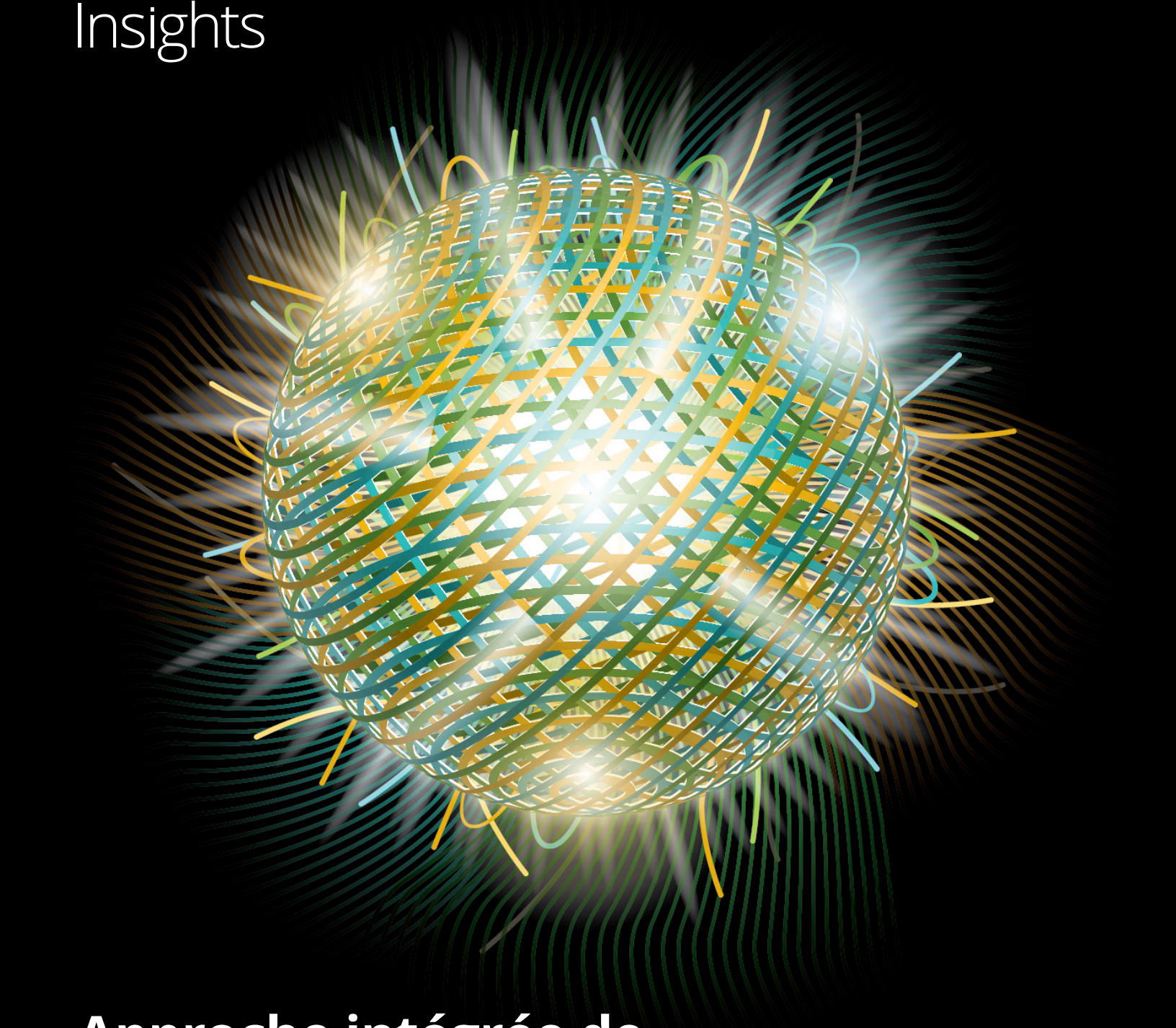
Deloitte. Insights

Rapport du
Centre de recherche intégrée de Deloitte



# Approche intégrée de cybersécurité pour votre stratégie de migration infonuagique

Pourquoi les programmes de migration infonuagique devraient inclure une stratégie infonuagique axée sur la cybertechnologie

# Au sujet du Centre de recherche intégrée de Deloitte

Le Centre de recherche intégrée de Deloitte propose de nouvelles perspectives sur des enjeux commerciaux critiques qui touchent plusieurs secteurs et fonctions, de l'évolution rapide des technologies émergentes au facteur constant du comportement humain. Nous traitons de sujets transformateurs de façon inédite, en offrant de nouvelles façons de penser dans une variété de formats, comme des articles sur des recherches, de courtes vidéos, des ateliers en personne et des cours en ligne.

## Communiquez avec nous

Pour en savoir plus sur la vision du Centre de recherche intégrée, ses solutions, son leadership éclairé et les événements organisés, veuillez visiter www.deloitte.com/us/cir.

# Contenu


| | |
|---|---|
| Introduction | 2 |
| Un nouveau modèle opérationnel de modernisation infonuagique pour une sécurité dès la conception | 5 |
| Cadre de contrôle de la sécurité infonuagique | 9 |
| Considérations relatives à la gestion des risques du programme de cybersécurité et d'infonuagique | 11 |
| Scénarios de mise en œuvre d'un programme infonuagique | 15 |
| Conclusion : pour commencer | 16 |
| Annexes | 17 |
| Notes de fin | 18 |

# Introduction

DE PLUS EN PLUS, LES ORGANISATIONS DU monde désireuses d'acquérir l'agilité et la résilience qu'exige une approche moderne des TI abandonnent leur infrastructure existante sur site au profit du nuage. Trop souvent cependant, cette migration et la cybersécurité sont planifiées séparément et confiées à différentes équipes qui se concentrent chacune de leur côté sur les différentes étapes de ce qui devrait pourtant être un seul et même processus. Selon certaines estimations, la cybercriminalité coûtera 6 000 milliards de dollars américains par an d'ici la fin de l'année[1]. La migration infonuagique s'accompagne donc d'importants enjeux de cybersécurité. Par ailleurs, malgré les avantages inhérents de l'infonuagique et même si « la sécurité et la protection des données » constituent une des deux principales raisons avancées pour justifier cette migration[2], de manière générale, les organisations semblent ne pas investir suffisamment dans une stratégie intégrée de cybersécurité et d'infonuagique. Selon une enquête sur l'avenir de la cybersécurité effectuée en 2019 par Deloitte et Touche S.E.N.C.R.L./s.r.l., 90 % des organisations répondantes consacreraient 10 % ou moins de leur budget de cybersécurité à la migration infonuagique, aux logiciels-services (SaaS), à l'analytique et à l'apprentissage machine[3].

En fait, de nombreuses organisations s'engagent précipitamment dans leur migration infonuagique sans accorder l'attention requise aux questions de sécurité.

Il s'agit d'une occasion pour une modernisation infonuagique afin de rendre les entreprises et les technologies plus résilientes. Dans ce scénario, la cybersécurité est *l'élément différenciateur* qui donne confiance au consommateur. À l'ère du numérique, une approche intégrée de cybersécurité procure aux organisations les outils nécessaires pour faire de la sécurité l'élément de leur transformation qui suscitera la confiance accrue des consommateurs.

Cette approche exige souvent de réunir au sein d'une même équipe des spécialistes de l'infonuagique et des spécialistes de la sécurité, de leur donner des objectifs communs et d'adopter un programme de modernisation ouvrant la porte à un dosage équilibré d'agilité, de sécurité et de confiance des consommateurs.

Pour les organisations à la recherche de résilience commerciale et technologique qui souhaitent resserrer la sécurité et procéder à une migration infonuagique qui inspire confiance, l'adoption réfléchie du concept de « sécurité dès la conception » peut être essentielle. Le principe de la sécurité dès la conception procure aux organisations les avantages suivants :

- intégration de méthodes novatrices et avant-gardistes comme la détection intelligente des menaces;
- atteinte de l'équilibre requis entre le besoin de rapidité et la nécessité de réduire les risques liés à la technologie, aux menaces internes et à la chaîne d'approvisionnement;
- soutien aux développeurs et aux ingénieurs tout en procurant à l'entreprise une fonction de développement, de sécurité et d'exploitation (DevSecOps);
- établissement d'une cyberapproche prospective qui renforce les objectifs de l'entreprise en matière de sécurité et de confiance.

Le présent article confirme l'importance de l'approche de « sécurité dès la conception » (concentrée sur les applications d'affaires essentielles à la mission de l'organisation), car celle-ci favorise une plus grande collaboration entre les équipes d'infonuagique et de cybersécurité et accroît l'agilité, la sécurité et la confiance.

En nous appuyant sur nos études, qui combinent une analyse des données brutes, des recherches secondaires et des entretiens à l'interne avec neuf dirigeants de Deloitte particulièrement versés dans les questions liées aux stratégies d'infonuagique et de cybersécurité, nous avons dressé à l'intention des organisations qui se lancent dans une migration infonuagique une liste détaillée de facteurs à prendre en considération.

**POURQUOI EST-CE IMPORTANT : UNE CYBERAPPROCHE INTÉGRÉE DE L'INFONUAGIQUE PEUT DONNER DE LA RÉSILIENCE À L'ENTREPRISE ET À LA TECHNOLOGIE**

Selon le quatrième rapport annuel de Deloitte mondial sur l'état de préparation, qui s'appuie sur la participation de 2 260 hauts dirigeants d'entreprise et de hauts fonctionnaires[4], les organisations dont les stratégies d'infonuagique et de cybersécurité sont plus matures ont tendance à être plus résilientes que la moyenne et plus résilientes aussi que les organisations qui appliquent une stratégie d'infonuagique avancée ou une stratégie de cybersécurité avancée. Les organisations qui ont mis en œuvre des stratégies de cybersécurité ou d'infonuagique avancées sont celles qui ont répondu le plus favorablement à la question suivante : « Dans quelle mesure votre organisation utilise-t-elle des technologies de pointe pour accroître sa résilience et son agilité (75 % par rapport à 53 % pour l'ensemble des répondants), et pour prévoir les tendances, les risques et les menaces à venir (70 % par rapport à 49 % pour l'ensemble des répondants)? » Si l'application d'une stratégie d'infonuagique ou d'une stratégie de cybersécurité augmente bien la résilience dans des proportions plus ou moins équivalentes, la combinaison des deux stratégies a un effet multiplicateur qui génère deux fois plus de résilience et d'agilité comparativement à celles acquises par les organisations qui n'ont pas adopté de stratégie en infonuagique ou de stratégie en cybersécurité (voir la note 5 pour les détails de la méthodologie d'analyse[5]).

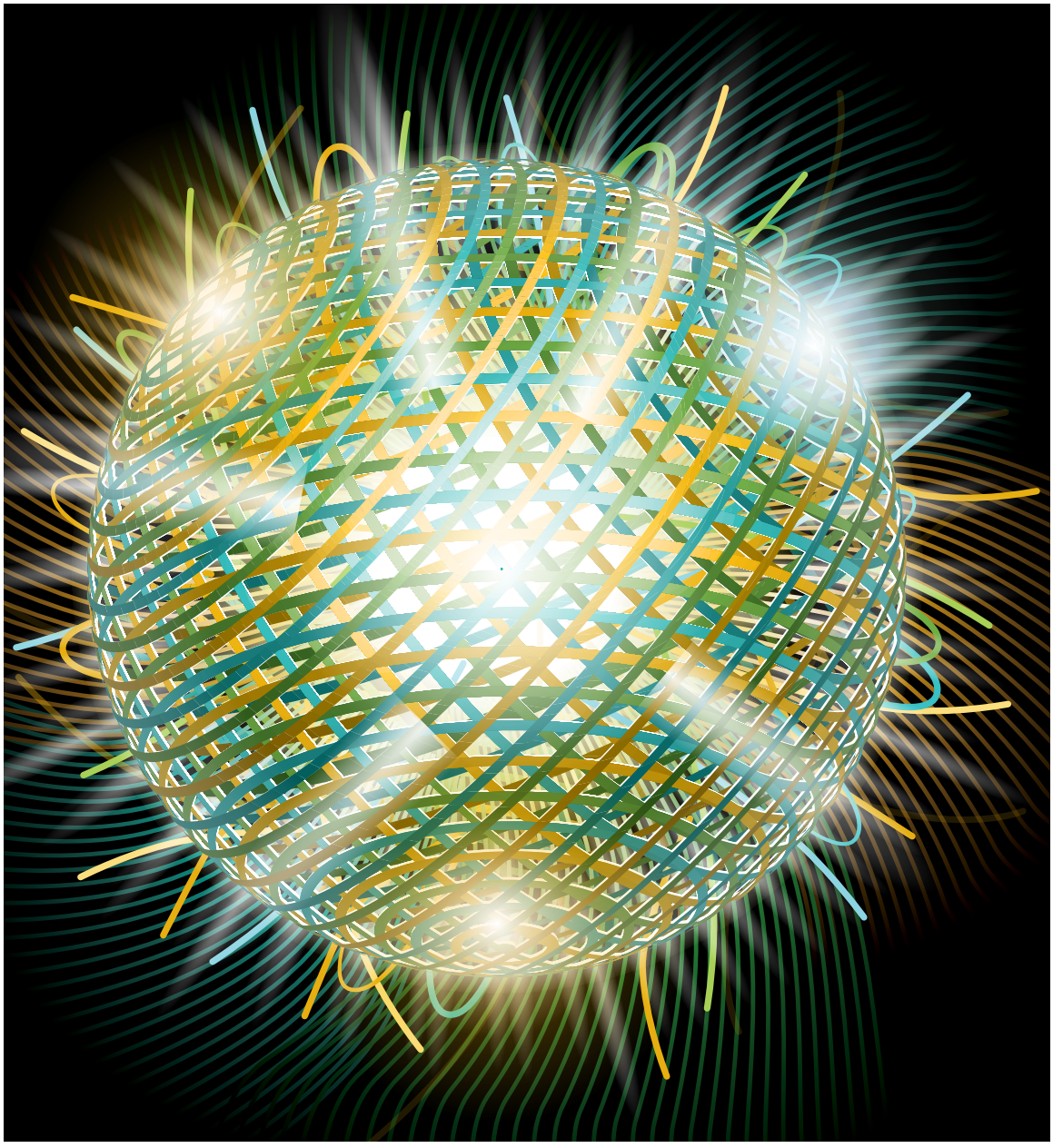
## Sécurité dès la conception : considérations particulières

En fin de compte, les équipes d'infonuagique et de cybersécurité devraient être fusionnées et avoir à leur tête le leader d'un centre d'excellence en modernisation et en migration (souvent le leader de la transformation numérique), appliquer les principes du soutien réciproque et de la polyvalence et adopter un modèle opérationnel commun. Une fois en place, ce modèle opérationnel peut servir à encourager la collaboration, la coordination et la mise en œuvre de pratiques de contrôle, de gestion du risque et de conformité de manière à ce que la sécurité soit intégrée à une des couches de l'infrastructure de TI tout en faisant la promotion de l'entreprise et (en définitive) de l'expérience client.

Cette équipe intégrée pourrait mener en collaboration les tâches suivantes :

- **Lancement du programme de modernisation et de migration.** Cette tâche ne peut être menée d'une manière compartimentée, car elle exige en préalable une bonne compréhension des objectifs d'affaires plus larges et comprend une évaluation des enjeux liés à la continuité des activités, à l'amélioration du niveau de service et aux éventuelles retombées pour les clients. Cette tâche exige aussi de bien comprendre quels sont les actifs importants de l'organisation afin de mieux les protéger au moyen d'une stratégie axée sur la cybersécurité. Dans le cas d'un grand détaillant, par exemple, on songera à protéger les données sur les ventes de produits et les préférences des clients.
- **Compréhension des nouvelles technologies et approches de cybersécurité et d'infonuagique.** Les leaders devraient adopter un nouveau modèle opérationnel dans lequel les équipes de cybersécurité et d'infonuagique fusionneraient tout en tenant compte des différents aspects de la modernisation : modèle d'utilisation des talents; développement, sécurité et exploitation; microservices; etc. Le modèle opérationnel peut englober de nouvelles offres, des mises en œuvre et l'acquisition de capacités auprès de fournisseurs de solutions (comme des points d'accès natifs en nuage) et des pratiques de cybersécurité prépondérantes (comme le cadre de cybersécurité du National Institute of Standards and Technology).
- **Détermination initiale des besoins de sécurité de l'entreprise.** Il est parfois fondamental de s'assurer que les besoins ne créent aucun irritant et que leur analyse est entièrement intégrée au processus de développement plutôt que de s'y greffer après coup. La plateforme sélectionnée doit comporter un certain nombre de couches de sécurité qui correspondent aux besoins de l'entreprise, notamment en matière de gestion des risques et de réglementation. Par exemple, un fournisseur de services infonuagiques peut proposer des solutions plus évoluées et mieux adaptées au secteur d'activité de l'organisation conformément à la *Health Insurance Portability and Accountability Act* (HIPAA), dont l'objectif est de moderniser les flux de données sur les soins de santé, d'offrir une conformité supérieure à celle d'une autre solution ou d'en venir éventuellement à un partage trimestriel plutôt que mensuel des données ayant une incidence sur les rapports de conformité.

- **Identification des exécutants probables du travail dans un modèle de services partagés et une structure d'équipe unifiée d'infonuagique et de cybersécurité.** La sécurité infonuagique développée doit l'être avec soin et englober la gestion de l'accès ainsi que la sécurité au chapitre des applications, du réseau, de la plateforme, de l'infrastructure et même du code. Idéalement, ce processus devrait dénoter une compréhension des accords de niveau de service avec les fournisseurs d'infonuagique et s'appuyer sur des pratiques pertinentes en matière de contrôle, de gestion stratégique du risque et de conformité à la réglementation. Certaines organisations peuvent, par exemple, créer un centre d'excellence regroupant des membres des équipes internes d'infonuagique et de cybersécurité ainsi que des fournisseurs externes de services gérés et de services d'infonuagique.



# Un nouveau modèle opérationnel de modernisation infonuagique pour une sécurité dès la conception

DANS DE NOMBREUSES organisations, les cyberentités sont isolées du reste de l'organisation et affichent souvent une transparence minimale ou incomplète, d'où une possible perte de confiance. Au fil de la migration infonuagique, cet enjeu gagnera vraisemblablement en importance et viendra compliquer la situation.

Ce facteur fait de la prise en compte de la sécurité dès la conception par une équipe intégrée un enjeu plus crucial. En fait, selon des données probantes, ce processus est déjà en cours. Nos entretiens révèlent que le plus important virage des organisations en sécurité infonuagique a été la décision de ne plus attribuer les tâches de sécurité aux développeurs et d'adopter plutôt un modèle axé sur la collaboration entre les hauts dirigeants du secteur technologique. Il y a cinq ans à peine, le chef de l'information d'une entreprise supervisait et finançait les projets de migration infonuagique et le groupe de la sécurité n'entrait en piste qu'à la toute fin du processus. De nos jours, les actions du chef de la sécurité, du chef de la sécurité de l'information et du chef de l'information sont mieux coordonnées et cet esprit de collaboration[6] devrait se transmettre au centre d'excellence en modernisation et en migration et s'accompagner d'un transfert clair des responsabilités de la phase précontractuelle et de développement vers le modèle opérationnel et le modèle de responsabilisation partagés.

Cette approche délibérément intégrée peut servir de cadre à l'analyse fondamentale et fixer les exigences de sécurité aux étapes *de l'exploration et de la sélection du fournisseur de services infonuagiques*; de l'établissement *du modèle de responsabilité partagée* au sein de l'équipe intégrée du centre d'excellence et du fournisseur de services d'infonuagique; de la fixation *de balises dans l'infrastructure de TI* comme telle; et de la gestion *des processus de développement, de sécurité et d'exploitation* au moyen de la combinaison applicable de talents et de technologies en place.

## Exploration et sélection du fournisseur de services infonuagiques

Avant la conclusion d'un contrat, de nombreux fournisseurs de services infonuagiques s'attendent à ce qu'un minimum d'analyses et de configurations de sécurité de base aient été effectuées par le client. Ces attentes diffèrent d'un fournisseur à l'autre. Les équipes d'infonuagique peuvent tirer parti du point de vue de leurs collègues de la cybersécurité afin de régler les problèmes pertinents pendant le processus de négociation du contrat. Lorsque le contrat est conclu et pendant la mise en œuvre, une approche s'appuyant sur une équipe conjointe d'infonuagique et de cybersécurité peut accélérer la compréhension, l'évaluation et la reconfiguration par l'équipe de l'environnement infonuagique. Cette approche peut aussi placer le chef de l'information ou le chef de la sécurité de l'information en meilleure position pour évaluer comme il se doit les risques que ferait courir un fournisseur tiers de services d'infonuagique à la viabilité des affaires. Il peut même être stipulé dans le contrat que cette évaluation doit être annuelle pour assurer la continuité des affaires et éviter de se retrouver dans une situation « d'enfermement propriétaire ».

De plus, dans un univers où les menaces de cybersécurité ne cessent d'évoluer, les fournisseurs de services d'infonuagique sont susceptibles d'avoir une connaissance plus pointue des nouveaux produits de sécurité et des considérations relatives à leur mise en œuvre ainsi que des innovations à intégrer dans le modèle opérationnel. Voici quelques exemples survenus en 2020 :

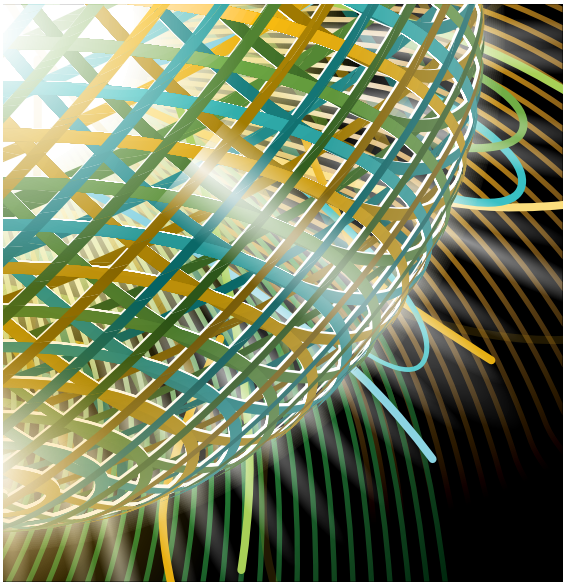
- L'armée de l'air américaine a créé le premier point d'accès natif en nuage accrédité qui permet à l'organisation de se brancher directement au nuage sans passer par un point d'accès partagé[7].
- Un spécialiste de l'hyperéchelle a lancé l'informatique confidentielle, un système qui permet aux organisations de stocker des données dans leur mémoire à l'état chiffré[8].
- Des organisations ont eu recours à « des processus d'affaires en tant que service » pour épurer des données confidentielles ou des données permettant d'identifier une personne.

Par ailleurs, une plus grande sensibilisation aux **exigences de communication de l'information sur la conformité lorsqu'on négocie des contrats avec un fournisseur de services d'infonuagique** peut aider à déterminer si les données partagées le seront à la fréquence requise pour produire les rapports. À cette fin, un organisme public envisageait de communiquer de l'information sur les mesures correctives prises et ainsi démontrer sa conformité continue, mais l'entente sur les niveaux de service (ENS) ne prévoyait pas la communication de données à la fréquence requise. Pour résoudre ce problème, les responsables ont été en mesure d'extraire les données du code source et de les intégrer à un processus manuel de communication de l'information. Toutefois, ce processus aurait pu être plus fluide s'il avait été mis au point à l'étape de la conclusion du contrat[9]. Pour éviter les problèmes de cette nature, il importe d'évaluer les besoins de communication de l'information et d'adapter les ENS en conséquence ou de trouver des solutions de communication de l'information de rechange.

## Modèle de responsabilité partagée

Dans une étude du secteur, 66 % des dirigeants interrogés ont déclaré utiliser des fournisseurs de services d'infonuagique pour assurer la sécurité de base, 73 % ont dit estimer qu'il incombe surtout aux fournisseurs publics de services d'infonuagique de sécuriser les solutions SaaS et 42 % ont affirmé qu'il incombe aussi à ces derniers de sécuriser les solutions d'infrastructure-service (IaaS)[10]. Pourtant, malgré ce penchant des organisations à s'en remettre au fournisseur de services d'infonuagique pour sécuriser les centres de données et l'infrastructure, ce modèle de responsabilité partagée comporte des limites inhérentes. Il incombe notamment malgré tout à l'organisation de sécuriser ses propres données et applications dans le nuage. Une équipe intégrée d'infonuagique et de cybersécurité permet de plus facilement tracer la ligne là où se termine la responsabilité de l'organisation et où commence celle du fournisseur (et vice versa) et d'orienter l'approche retenue pour la surveillance continue.

Contrairement à ce qui se produit dans un environnement de services sur site, dans le nuage, l'infrastructure physique est louée et les modèles opérationnels partagés peuvent varier en fonction de plusieurs facteurs. Par exemple, dans 40 % des États américains, on a adopté un modèle fédéré en vertu duquel le chef de la sécurité de l'information supervise les politiques de l'entreprise et les organismes dirigent les services partagés; 10 % des États américains ont plutôt adopté un modèle décentralisé en vertu duquel le chef de l'information informe les organismes d'État individuels des politiques[11]. Ce fut notamment le cas dans le cadre de l'initiative de cybercommande de la ville de New York, où le chef adjoint de la sécurité de l'information du projet et le responsable de la gestion des menaces de l'agence ont adopté la technologie infonuagique pour accéder aux données de sécurité d'un dispositif gouvernemental branché au réseau de la ville[12].



### SÉCURITÉ INFONUAGIQUE : ASSISTE-T-ON À UNE MONTÉE DE L'INNOVATION?

Les menaces ne cessent d'évoluer et les parties malveillantes de recourir à de nouvelles tactiques s'inspirant du « minage pirate » et des rançongiciels malveillants[13] ou à des stratégies de cyberintelligence artificielle qui propagent la contamination des données, à des attaques par réseau antagoniste génératif et à la manipulation de robots[14]. Pour maintenir notre avantage sur les parties malveillantes à l'origine de ces attaques, il faudra constamment mettre à jour les plus récentes innovations en infonuagique et en cybersécurité. Notre analyse des demandes de brevet déposées et des brevets accordés aux États-Unis de 2018 à 2020 démontre ce qui suit :

- plus de la moitié des demandes de brevet portaient sur des technologies de sécurité infonuagique de base mettant l'accent sur le chiffrement des données, les authentifications, les jetons, les modules de contrôle et de stockage et autres;
- les organisations s'intéressent de plus en plus à différentes technologies de pointe comme l'intelligence artificielle (IA), l'apprentissage-machine, les mégadonnées et les chaînes de blocs pour améliorer la sécurité infonuagique;
- outre les brevets technologiques, les organisations se concentrent aussi sur la conception de processus liés au déploiement, à la surveillance, à la programmation et aux approvisionnements.

Si environ 1 500 brevets ont été accordés dans le domaine de la sécurité infonuagique en 2018 et en 2019, ce nombre a chuté à 500 l'année dernière, probablement à cause de la pandémie[15]. Il s'ensuit que la création d'équipes intégrées dotées d'une structure solide (modèle opérationnel, processus et contrôles) pourrait être aujourd'hui plus cruciale que jamais.

*« Tous les renseignements sur les brevets de sécurité infonuagique sont extraits du site de l'indice Derwent World Patents par l'entremise de Quid (https://quid.com). Le but de cette analyse est de définir les thèmes généraux qui s'imposent dans le domaine de la sécurité infonuagique. L'analyse de Deloitte ne portait pas sur la nature des brevets pris individuellement. ».*

## Fixation de balises dans l'infrastructure de TI

Comme la sécurité est au cœur du processus de sélection du fournisseur et de création du modèle de responsabilisation, l'équipe de la sécurité se trouve dans une position avantageuse pour intégrer la sécurité au processus de migration infonuagique en fixant les balises de départ et en imposant les configurations minimales nécessaires pour protéger le déploiement avant même que la migration comme telle ne s'engage. Par exemple, la protection des charges de travail et la sécurisation des zones d'accueil peuvent créer un modèle de configuration standard adaptable et viable qui pourra ensuite être déployé rapidement pour la mise en œuvre de futures applications sans exiger de réingénierie. Comme la méthodologie infonuagique est conçue pour les méthodes Agile et DevOps, une organisation qui n'aurait pas sécurisé le développement de ses opérations (DevOps) pourrait assumer des risques importants en plus de ceux liés à la gestion du développement pendant le processus de migration.

## Gestion des processus DevSecOps avec la combinaison appropriée

La méthodologie DevSecOps permet aux organisations d'intégrer la sécurité à leurs flux de travail plutôt que d'en faire un élément qui se greffe au résultat des efforts de développement[16]. Les développeurs et professionnels de la sécurité ont ainsi la possibilité de travailler ensemble dans l'objectif commun de mettre au point des configurations sûres qui sont constamment surveillées, corrigées et gérées afin d'assurer une cybersécurité propice à la création de solutions agiles et résilientes. Prenons l'exemple d'une compagnie d'assurance ayant fait migrer des centaines d'applications dans le nuage. Grâce à la méthodologie DevSecOps, l'équipe d'ingénierie infonuagique a mieux planifié l'architecture de l'environnement et a créé une infrastructure infonuagique capable d'assurer la sécurité de la migration. Des outils d'automatisation et d'orchestration de la sécurité pourront ensuite être

greffés à ces processus afin de mettre en œuvre des flux de travail structurés, d'automatiser les tâches de sécurité et de détecter et de contrer les menaces.

- **Compétences/talents.** Les technologies existantes s'appuient sur des dispositifs virtuels comme ceux proposés par les fournisseurs de pare-feux pour sécuriser les systèmes, tandis que pour les technologies infonuagiques, il est essentiel de comprendre les configurations de sécurité. La migration infonuagique exige donc un nouveau modèle d'utilisation des talents qui s'éloigne du cadre habituel « développement, mise en œuvre, déploiement et mise en place de la sécurité ». Pour améliorer la sécurité en amont, il faut qu'elle soit envisagée dès le départ afin de disposer des bases et des configurations requises et créer l'architecture avant la mise en service, ce qui réduit les interventions subséquentes. Cet aménagement des tâches force l'adoption d'un modèle très différent d'utilisation et d'intégration des talents.

- **Microservices.** À mesure que les organisations modernisent leurs applications existantes pour créer des services point à point plus agiles, les modèles opérationnels s'appuyant sur les microservices infonuagiques devraient prendre en compte les limites des fournisseurs et les enjeux liés à la portabilité et à l'interopérabilité d'un fournisseur à l'autre. Les organisations peuvent envisager la mise en place d'une couche d'intergiciel agnostique ou d'un modèle de déploiement de microservices qui aidera le client à régler certains problèmes multinuages et autres enjeux liés aux systèmes de l'entreprise.

## Grâce à la méthodologie DevSecOps, l'équipe d'ingénierie infonuagique a mieux planifié l'architecture de l'environnement et a créé une infrastructure infonuagique capable d'assurer la sécurité de la migration.

# Cadre de contrôle de la sécurité infonuagique

AU SEIN DE la haute direction, le passage de l'infrastructure sur site à l'infonuagique exige habituellement l'adoption d'une mentalité plus axée sur la sécurité. Il faut passer de la gestion d'une infrastructure physique à la surveillance de l'accès à « un environnement apatride à traitement réparti ». Plus important encore, le cadre de contrôle devrait régler les points suivants : *réseau, plateforme et infrastructure; sécurité des utilisateurs et des données; et sécurité des applications fondamentales*.

## Réseau/plateforme/ infrastructure

La « sécurité dès la conception » permet aux développeurs et aux équipes de sécurité des systèmes infonuagiques d'installer dans l'infrastructure comme telle des balises qui facilitent la mise en place de processus agiles et sûrs. Par conséquent, avant même que les développeurs aient accès à l'environnement infonuagique, le chef de l'information et son équipe devraient réfléchir à l'approche dominante qui servira à sécuriser le réseau. Elle peut consister à intégrer des balises dans la plateforme infonuagique comme telle au moyen d'une infrastructure informatique intégrant la « sécurité dès la conception » ou à mettre en place des processus informatiques restrictifs intégrant la « sécurité dès la conception » (p. ex. donner à des utilisateurs autorisés la responsabilité d'examiner l'infrastructure et le code source avant la mise en production). Les pratiques prépondérantes au sein de l'industrie s'écartent de plus en plus des dispositifs de sécurité axés sur le périmètre pour plutôt favoriser des architectures de sécurité réseau à confiance zéro[17] qui permettent la mise en place d'environnements modulaires pour les développeurs et la microsegmentation, soit la création de différents niveaux d'accès à l'infrastructure et aux contrôles sur le réseau, aux identités et aux accès, et aux applications.

À titre d'exemple d'approche axée sur l'infrastructure, une organisation de gestion d'actifs passant d'une plateforme infonuagique privée à une plateforme publique a intégré des centaines de contrôles dans sa plateforme d'infonuagique au niveau du code avant même de donner un accès administratif aux développeurs. Ces contrôles ont servi de balises et permis la création d'un environnement de développement sûr et conforme[18].

Adoptant plutôt une approche axée sur les processus, une autre organisation de services financiers a supprimé ou fortement restreint l'utilisation des clés utilisées par les développeurs afin de changer les accès et les processus de déploiement du code. Cette décision a provoqué un virage culturel majeur pour les développeurs qui avaient auparavant plus d'autonomie dans la mise en ligne des changements aux applications. Ce privilège est maintenant réservé à un petit groupe de développeurs. Pour renforcer ce nouveau protocole, l'organisation a exercé une surveillance pour détecter les comportements qui s'écartaient du nouveau processus de contrôle. On s'intéressait plus particulièrement à un scénario courant en vertu duquel des développeurs qui n'en avaient plus l'autorisation tentaient de mettre en service des mises à jour au moyen d'une machine virtuelle pour contourner la gestion des accès et des privilèges et se trouvaient à ouvrir ce faisant un port et à créer une vulnérabilité potentielle. Pour contrer ce risque, l'organisation a mis en œuvre une solution d'orchestration et d'automatisation de la sécurité et des interventions, ce qui lui a permis de collecter des données opérationnelles sur la sécurité, de créer un dossier d'analyse pour détecter les changements apportés à la configuration de sécurité et d'orchestrer des flux de travail personnalisés pour les passer en revue. L'organisation a ainsi obtenu la visibilité requise pour procéder à une surveillance réseau proactive et la capacité de fermer les ports ouverts.

## Sécurité des utilisateurs et des données

La migration infonuagique exige souvent une nouvelle approche de gestion des identités. Si, auparavant, les pièces d'identité physiques (p. ex. les cartes d'accès à un immeuble) constituaient des autorisations acceptables, dans un système à traitement réparti accessible d'à peu près n'importe où, des identifiants de connexion particuliers à chaque utilisateur et dirigeant principal peuvent être nécessaires. Les protocoles de gestion des identités et des accès peuvent être intégrés à une plateforme modulaire d'identification contenant toutes les exigences d'accès de chaque utilisateur[19].
En mettant l'accent sur la protection des données et des renseignements personnels, et sur la résilience et la réglementation, on peut encadrer la gestion des droits d'accès aux données et des privilèges des utilisateurs. Les dirigeants devraient rechercher dans leur plan l'atteinte d'un équilibre entre les exigences minimales légales de chiffrement et un chiffrement trop poussé qui ralentirait les applications[20].

## Sécurité des applications de base

Avant de transférer les données ou les charges de travail dans le nuage, les équipes de cybersécurité et d'infonuagique devraient s'assurer que les contrôles minimaux ci-dessous ont été mis en place.

- **Protection des charges de travail** — mettre en place les balises de base et les configurations minimales nécessaires pour protéger le déploiement. Par exemple, une organisation peut recourir à des modèles préétablis pour les applications fondées sur la fonction ou sur des conteneurs.
- **Zone d'accueil sécurisée** — établir un environnement sécurisé pour protéger les structures des comptes, les règles de sécurité et les autres services fondamentaux du modèle opérationnel. Par exemple, de nombreuses organisations se dotent d'un sous-réseau public et d'un sous-réseau privé afin de créer, d'une part, une zone d'accueil destinée au public et, d'autre part, un réseau privé virtuel à l'intention des utilisateurs de l'entreprise.
- **Sécurité dès la conception/DevSecOps** — fsuivre les principes de la sécurité dès la conception et les méthodes DevSecOps mentionnées dans nos recommandations sur le modèle opérationnel.
- **Segmentation et confiance zéro** — s'appuyer sur des protocoles de segmentation du réseau et le principe de confiance zéro. Par exemple, l'organisation peut réserver le privilège d'administration des applications aux seuls développeurs se situant au sommet de la structure hiérarchique qui répondent à des normes de sécurité plus strictes et qui possèdent une formation plus poussée, en utilisant des conteneurs pour segmenter l'accès aux applications.
- **Gestion de la surface d'attaque** — gérer la vulnérabilité par le recours à des services personnalisés qui rehaussent la qualité des programmes de gestion de la vulnérabilité et des surfaces d'attaque. Les organisations se concentrent sur l'identification et l'évaluation des biens sur le nuage tout au long de leur cycle de vie et aux différentes couches de l'architecture. Par exemple, les usines intelligentes peuvent concevoir leur flux de données sur le nuage et aux différents paliers afin de déterminer la sécurité mise en place dans l'ensemble de l'écosystème.

# Considérations relatives à la gestion des risques du programme de cybersécurité et d'infonuagique

LA MIGRATION INFONUAGIQUE peut atténuer certains risques de sécurité liés à une infrastructure gérée sur place grâce au chiffrement, au système d'ouverture de session, au réseau privé, à la surveillance, à la protection contre les attaques par déni de service distribué, à l'automatisation des correctifs et à d'autres éléments intégrés dans l'environnement infonuagique. Toutefois, de nombreux systèmes et applications implantés dans ce nouvel environnement n'ont pas été initialement conçus pour fonctionner en ligne. Pour éviter des déceptions sur ce plan, avant que la migration infonuagique ne commence, les organisations devraient procéder à une évaluation de la maturité des risques de cybersécurité[21] pour bien comprendre l**es risques précis liés aux différentes technologies et à la réglementation, les risques internes, les risques liés à la chaîne d'approvisionnement** et les correctifs recommandés[22].

## Risques technologiques

Même si certains de ces risques peuvent représenter une nouveauté pour une équipe de migration infonuagique, les organisations sont toujours aux prises avec un certain nombre de risques technologiques qu'elles doivent atténuer dans le cadre de leurs programmes de cybersécurité infonuagique et c'est à ce point que l'intégration des équipes de cybersécurité et d'infonuagique peut contribuer à l'obtention d'un résultat plus sûr, plus agile et plus fiable (figure 1).

La compréhension des risques technologiques peut jouer un rôle crucial et bien des organisations convaincues que leurs systèmes sont bien protégés pourraient être surprises. Ainsi, une institution financière ayant décidé de procéder à une vérification de routine a constaté que globalement, ses systèmes comportaient plus de 100 000 vulnérabilités intégrées, ce qui représentait une très grave menace sur le plan de la sécurité et exigeait la mise en place immédiate de correctifs au chapitre des applications, des bases de données, des intergiciels et du code. Ce risque explique en partie la décision de

FIGURE 1

## Quatre types de risques technologiques à prendre en compte et méthode d'atténuation

| Risque technologique | Manifestation du risque | Méthode d'atténuation |
|---|---|---|
| Plateformes et applications existantes sur site | Peuvent *sembler sûres* en raison du haut niveau de contrôle et de la proximité physique, mais il peut être difficile de les rendre conformes aux normes de sécurité modernes ou elles peuvent comporter des vulnérabilités connues. | Analyser le système d'exploitation, les centres de données, les applications, les intergiciels et autres afin de détecter les vulnérabilités. |
| Lacune sur le plan des talents technologiques | Le savoir des talents technologiques en place va de la connaissance de langages de codage périmés, comme COBOL par opposition à Python, à la connaissance de fonctions comme la gestion des serveurs qui ne peuvent « migrer » vers une équipe de sécurité infonuagique. | Réaffecter le talent actuel dans de nouvelles fonctions parallèles; recycler les membres de l'effectif afin qu'ils acquièrent de l'expérience de codage pertinente (Python, Java) et qu'ils acquièrent les attestations requises pour la plateforme infonuagique du fournisseur, y compris ses fonctions de sécurité afin de gérer le risque lié au talent. |
| Continuité des activités et reprise après sinistre | Les systèmes existants n'ont pas été conçus dans la perspective de plans modernes de continuité des activités et de reprise après sinistre. | Voir la migration infonuagique comme une occasion de mettre à jour le plan de continuité des activités et de reprise après sinistre et se procurer une capacité infonuagique additionnelle afin de pouvoir basculer vers une copie de sûreté en cas de catastrophe conformément aux principes des plans modernes de reprise après sinistre. |
| Risque d'erreur de configuration | Peut ouvrir un point d'accès à des agents malveillants[23]. Selon une étude de l'industrie sur les atteintes aux données signalées à l'échelle mondiale de janvier 2018 à décembre 2019, les erreurs de configuration infonuagiques ont causé 196 atteintes aux données et l'exposition de plus de 33 milliards de dossiers, ce qui a coûté une somme estimée à près de 5 000 milliards de dollars américains[24]. Ce risque d'erreur de configuration touche indifféremment les services de stockage, de base de données et autres s'appuyant sur l'infonuagique[25]. | Mettre en œuvre des solutions de surveillance de la conformité pour détecter les nouvelles configurations et notamment l'ouverture non autorisée d'un port qui pourrait exposer le réseau à certaines menaces. |

Source : Analyse de Deloitte

cette institution d'effectuer une migration infonuagique et est un bon exemple des risques liés aux plateformes et applications existantes sur site mentionnés à la figure 1[26]. Si l'équipe de la migration infonuagique avait choisi de simplement déplacer l'infrastructure sans d'abord chercher à comprendre ses vulnérabilités, l'organisation aurait pu simplement transférer sur le nuage les risques déjà existants.

Autre exemple : dans une organisation du secteur des produits de consommation qui utilisait un système d'exploitation périmé, un centre de traitement de données a été visé par un rançongiciel au moment même où un correctif logiciel était mis en service dans un environnement de développement. Les vulnérabilités de sécurité existantes qui auraient pu être en quelque sorte couvertes par les pare-feux et le périmètre sont devenues actives au moment du passage à l'infonuagique, car elles n'avaient pas été corrigées. Si l'organisation avait mieux

orchestré les travaux des équipes de cybersécurité et d'infonuagique et avait mis en place les contrôles appropriés, cet incident (qui peut avoir des conséquences désastreuses sur la confiance des consommateurs) aurait peut-être pu être évité.

La gestion des risques technologiques exige d'en venir à un équilibre approprié entre la compréhension fondamentale de la technologie actuelle et à venir (une des forces de l'équipe de migration infonuagique) et la formulation de conseils sur la manière souhaitable d'atténuer les vulnérabilités par une démarche de sécurité inspirée des pratiques dominantes dans les quatre catégories de risques avant la migration, voire avant le choix du fournisseur de services infonuagiques.

## Risques liés à la réglementation

Au moment d'évaluer les fournisseurs de services infonuagiques et avant de procéder à la migration des données ou des charges de travail, l'organisation devrait réunir ses équipes de cybersécurité et d'infonuagique afin qu'elles prennent en compte quatre exigences de conformité réglementaire essentielles qui auront vraisemblablement des retombées sur les flux de données en aval et sur la configuration du système, soit la réglementation mondiale et régionale de la gouvernance des données, les cadres fixés par l'industrie, les normes technologiques plus générales ainsi que la réglementation particulière de l'administration américaine (figure 2).

Les grandes organisations multinationales présentes dans de nombreux pays et actives dans les secteurs public et privé sont souvent appelées à composer avec un grand nombre de règlements sur les données et la technologie tandis que les organisations plus petites peuvent malgré tout devoir prendre en compte certaines combinaisons de règlements régissant les données dans un secteur ou une région donnée et concevoir leur propre stratégie de stockage de données sur le nuage et les contrôles connexes afin de contrôler les risques.
Toutefois, avec la mondialisation des données, même « les plus petites organisations » peuvent être assujetties à la réglementation transfrontalière.

Un examen des exigences liées au risque de réglementation effectué par une équipe combinée de cybersécurité et d'infonuagique peut améliorer la compréhension des cadres existants de gestion des données, des risques pertinents et des caractéristiques que doivent posséder les solutions technologiques pour améliorer le processus de sélection des fournisseurs, la négociation des ententes de niveau de service et la passation des marchés.

## Risques internes et risques liés à la chaîne d'approvisionnement

Finalement, un programme de gestion des risques de cybersécurité et d'infonuagique devrait prendre en compte les menaces internes et la *chaîne d'approvisionnement* de l'organisation comme des vecteurs de risques afin d'en arriver à un juste équilibre entre sécurité et confiance à l'extérieur et à l'intérieur de l'organisation, de manière à éviter d'éventuelles fuites de données. La migration infonuagique peut permettre à un risque interne de se concrétiser lorsque des identifiants d'accès sont partagés ou lorsqu'un point d'accès au réseau est ouvert. Les courtiers de sécurité d'accès au nuage qui exercent une surveillance sur les pertes de données et appliquent les contrôles dans les environnements multinuages sont en plein essor. Ces courtiers ont les outils pour aider les organisations à mieux gérer les menaces internes[33] et à prévenir les éventuelles fuites de données, des problèmes qui sont perçus par environ 75 % des organisations comme des éléments importants de la sécurité infonuagique[34].

La gestion des cyberrisques exige des organisations qu'elles aient une capacité d'analyse de leur environnement interne et externe afin de détecter les risques et les vulnérabilités possibles de leurs chaînes d'approvisionnement. Elles peuvent confier cette tâche à une équipe intégrée de cybersécurité et d'infonuagique possédant la visibilité et la transparence voulues ainsi que la capacité de communication, de collaboration et d'exécution voulue pour appliquer un programme de conformité intégré (de même que l'outillage pertinent nécessaire) de l'ensemble de la chaîne d'approvisionnement. Pour en savoir davantage sur cette question, nous vous invitons à consulter le document (en anglais seulement) de Deloitte Consulting LLP intitulé *Looking beyond the horizon: Preparing today's supply chains to thrive in uncertainty*.

FIGURE 2

## Quatre exemples de risques de réglementation à prendre en compte dans la mise sur pied d'un programme de cybersécurité et d'infonuagique

| Catégorie de risques de réglementation | Description | Exemple |
|---|---|---|
| Réglementation mondiale et régionale sur la gouvernance des données | La réglementation sur la protection des données et des renseignements personnels exige la mise en place d'un cadre de gouvernance des données qui établit clairement à qui les données appartiennent, comment elles seront conservées, les interventions et la coordination requises en cas d'atteinte aux données et la nécessité d'une stratégie internationale en matière d'infonuagique[27], etc.<br>De nombreuses régions et de nombreux pays possèdent leurs propres lois de protection des données, ce qui rend nécessaire une harmonisation de la réglementation, particulièrement pour les entreprises qui ont des clients dans plusieurs États ou régions. | Le Règlement général sur la protection des données (RGPD) de l'Union européenne a des retombées mondiales, car il exige une compréhension des données mondiales de l'entreprise[28].<br>Amérique du Nord et Amérique latine : la *Consumer Privacy Act* de Californie, les lois canadiennes sur la protection des renseignements personnels et les lois brésiliennes, pour n'en nommer que quelques-unes.<br>Asie : la loi thaïlandaise sur la protection des renseignements personnels ainsi que d'autres lois similaires en Australie, au Japon, à Hong Kong, en Malaisie, à Singapour et dans un certain nombre d'autres pays de la région. |
| Exemples de codes fondés sur le secteur | Dans certains secteurs d'activité, notamment les soins de santé et l'assurance, les services bancaires et financiers, l'éducation et les communications, des lois et des cadres précis régissent les politiques de gouvernance des données et complexifient le processus. | Aux États-Unis :<br>· **Soins de santé et assurance :** HIPAA;<br>· **Services bancaires et financiers :** la loi Sarbanes-Oxley, la loi Gramm Leach-Bliley, la Payment Card Industry Data Security Standard (PCI DSS);<br>· **Éducation :** la *Family Educational Rights and Privacy Act* (FERPA);<br>· **Télécommunications, médias et divertissement :** la *Video Privacy Protection Act*, Motion Picture Association of America (MPAA) |
| Normes technologiques plus larges | Les normes de cybersécurité protègent le cyberenvironnement et, par conséquent, ses utilisateurs, les réseaux, les dispositifs, les logiciels, les processus, les applications, les services, les systèmes, etc. | **Le cadre de sécurité du National Institute of Standards and Technology** est un instrument prépondérant en matière de normes technologiques qui régit les activités des organisations commerciales aux États-Unis. Ses cinq éléments fonctionnels sont l'identification, la protection, la détection, l'intervention et la récupération[29]. Même s'ils ont été conçus dans une perspective conforme aux infrastructures traditionnelles, les principes de base peuvent être étendus au déploiement de solutions infonuagiques.<br>**Les points de comparaison du CIS** qui fournissent des lignes directrices sur la configuration des produits pour les solutions proposées par les différents fournisseurs. |
| Administration américaine – cadres particuliers | Les organismes publics désireux d'utiliser les technologies modernes d'infonuagique sont assujettis à des exigences additionnelles de sécurité et de protection des renseignements fédéraux[30]. Les fournisseurs de solutions infonuagiques doivent s'assurer que leurs solutions sont conformes à ces exigences avant d'offrir leurs services à des organismes fédéraux[31]. Certains cadres imposent des restrictions additionnelles, notamment sur les données exportées à l'extérieur des États-Unis qui doivent faire l'objet d'une segmentation additionnelle et de contrôles de sécurité. | ***Attestation du modèle de cybersécurité* (CMMC)**<br>**La *Federal Information Security Management Act* et la *Federal Information Security Modernization Act* des États-Unis** se concentrent sur les normes et les lignes directrices destinées à moderniser les pratiques fédérales de sécurité et de gestion du risque de cybersécurité des chaînes d'approvisionnement.<br>**Le programme américain de gestion des risques fédéraux et d'autorisation** permet aux organismes gouvernementaux d'utiliser les technologies modernes d'infonuagique tout en s'assurant que l'information fédérale est en sécurité et protégée[32].<br>**L'*International Traffic in Arms Regulations* (ITAR)**<br>**Le *Defense Federal Acquisition Regulation Supplement* (DFARS)** qui est lié au traitement, au stockage et à la transmission de renseignements protégés de la défense et autres. |

Source : Analyse de Deloitte

# Scénarios de mise en œuvre d'un programme infonuagique

FINALEMENT, LE TYPE de programme d'infonuagique aura une incidence sur le modèle opérationnel et sur le programme qui suivra. Le graphique ci-dessous décrit en détail quatre scénarios courants de mise en œuvre de programmes d'infonuagique et certaines considérations de complexité élevée, moyenne ou faible dont doit tenir compte l'équipe intégrée de cybersécurité et d'infonuagique (figure 3).

FIGURE 3

**Scénarios de mise en œuvre d'un programme d'infonuagique : considérations relatives aux risques, aux contrôles et à la conformité**

| | Risques | Contrôles | Conformité |
|---|---|---|---|
| Migration du centre de données – déplacement | **Complexité faible** Spécialistes de l'hyperéchelle accrédités possédant les attestations conformes essentielles en matière de données, de normes, d'industrie, de région, etc. | **Complexité faible** Investissement sans équivalent venant de fournisseurs de services de sécurité pour centres de données infonuagiques. | **Complexité faible** Les fournisseurs appliquent la réglementation avec une rigueur considérable. |
| Migration des applications – déplacement | **Complexité élevée** Les erreurs de configuration potentielles représentent une menace grave qui compromet la sécurité et créent un risque organisationnel et réglementaire qui exige une planification du traitement des données et de la gouvernance. | **Complexité modérée** Une dépendance excessive aux caractéristiques technologiques de sécurité intégrées exige une plus grande coordination des contrôles et des exigences plus larges en matière de sécurité. | **Complexité faible** Le marché de l'automatisation de la conformité et de la surveillance du marché est arrivé à maturité, mais il y a encore des innovations possibles dans l'orchestration de la sécurité multinuage. |
| Développement natif au nuage – virage et adoption | **Complexité faible** Réusinage/redéploiement des applications. | **Complexité modérée** L'intégration de la cybersécurité aux nouveaux produits, services et canaux est une source de préoccupation[35] même si les organisations y gagnent une interopérabilité au niveau du code des systèmes Java. | **Complexité modérée** Les organisations devraient adopter les principes de la sécurité dès la conception pour les développements propres à l'infonuagique. |
| Combinaison sur site/migration infonuagique/ solution native en nuage | **Complexité élevée** Importante superficie de la zone de menace dans une infrastructure complexe et hétérogène exigeant une coordination suivie entre les équipes de cybersécurité et d'infonuagique. | **Complexité élevée** Multitude de mécanismes de contrôle nécessaires sur site et aux différentes couches de l'infrastructure multinuage, du modèle de propriété au flux d'information au sein de l'entreprise. | **Complexité modérée** Éventail plus large d'exigences de conformité applicables exigeant une plus grande automatisation à des fins d'autocorrection et de détection des activités anormales. |

Source : Analyse de Deloitte

# Conclusion : pour commencer

ON NE PEUT s'attendre à ce que les développeurs de nuages deviennent du jour au lendemain des spécialistes de la sécurité ni à ce qu'ils soient constamment au fait de l'évolution de toutes les menaces. En revanche, ils peuvent travailler au sein d'équipes intégrées de cybersécurité et d'infonuagique qui mettront à profit les modèles opérationnels cibles et qui privilégieront la prévention, les microservices, la gestion des risques ainsi que les contrôles et qui assureront la conformité aux points cruciaux du cycle de la migration infonuagique tout en adhérant aux principes de la sécurité dès la conception. Voici, en terminant, quelques réflexions susceptibles de guider ces équipes dans leur périple de modernisation de l'infonuagique et dans leur migration, d'accroître la résilience organisationnelle et technologique, de rehausser la sécurité et de renforcer la confiance des clients :

- **Développement d'un modèle opérationnel de modernisation qui réunira les nouvelles approches et technologies novatrices.** Ce modèle doit inclure de nouveaux modèles de gestion des talents; des activités de développement, de sécurité et d'exploitation (DevSecOps); et des microservices. Il doit aussi tenir compte des responsabilités précontractuelles et prévoir la répartition des rôles et des responsabilités à l'intérieur d'un modèle de responsabilité partagée. L'investissement dans la sécurité du fournisseur de services d'infonuagique peut vous donner accès à une sécurité supérieure à celle dont vous bénéficiez à l'heure actuelle.

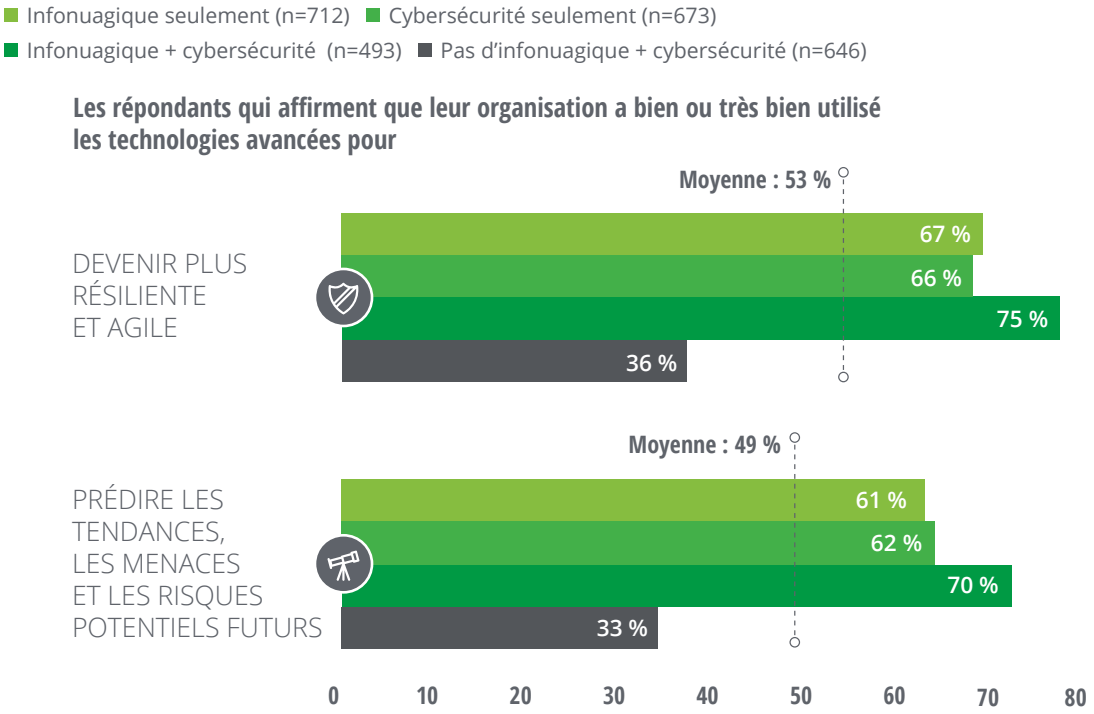
- **Développement d'un cadre de contrôle qui vous permettra de passer à l'étape suivante grâce à une approche mieux intégrée de la cybersécurité et de l'infonuagique.** La migration vous offre une occasion de repenser vos modèles, vos outils et vos capacités en matière de sécurité. La mise en place d'un cadre de contrôle infonuagique commence par une bonne compréhension des besoins de données et englobe l'adoption de contrôles sur l'accès des utilisateurs et les identités; sur le réseau, l'infrastructure et les applications; et sur les applications de base. Les organisations peuvent procéder à une évaluation globale des risques présents dans leur environnement technologique, réglementaire et de cybersécurité; mettre en œuvre les contrôles nécessaires pour combler les lacunes et atténuer les risques; et procéder à la migration des charges de travail pour sécuriser les zones d'accueil infonuagiques.

- **Approches novatrices de gestion de la conformité.** De nouvelles approches et de nouveaux processus novateurs d'automatisation et d'allégement du fardeau de la surveillance moderne de la conformité émergent constamment. Tenez-vous au courant des plus récents outils et processus.

En réunissant toutes ces composantes à l'intérieur d'un centre d'excellence en migration infonuagique doté d'une équipe intégrée de professionnels possédant des compétences en cybersécurité et en infonuagique, les organisations seront mieux placées pour répondre au besoin d'étendre le « cycle de vie » et pour hiérarchiser les risques de sécurité et les atténuer au moyen des outils de gouvernance, de gestion du risque et de conformité requis. Au bout du compte, la migration infonuagique est l'occasion idéale non seulement de renforcer la résilience de l'entreprise et de sa technologie, mais aussi d'accroître la sécurité, voire la confiance des consommateurs.

# Annexe : Des stratégies de cybersécurité et d'infonuagique intégrées favorisent une plus grande résilience organisationnelle et technologique

## Des stratégies de cybersécurité et d'infonuagique intégrées favorisent une plus grande résilience organisationnelle et technologique.




Remarques : Des stratégies matures axées uniquement sur l'infonuagique ont été déterminées en fonction de ceux qui ont répondu « Bien » ou « Très bien » à la question *Dans quelle mesure croyez-vous que votre organisation a bien fait la transition de ses systèmes d'affaires vers l'infonuagique pour soutenir le télétravail (p. ex. outils de collaboration, RPV, centres de données, serveurs, etc.) de juillet à septembre 2020?*

Des stratégies matures axées uniquement sur la cybersécurité ont été déterminées en fonction de ceux qui ont répondu « Bien » ou « Très bien » à la question *Dans quelle mesure croyez-vous que votre organisation a bien géré l'évolution de la détection des menaces liées à la cybersécurité, des mesures correctives et de la prévention de juillet à septembre 2020?*

Et l'infonuagique + la cybersécurité ont été déterminés en combinant ceux qui ont répondu « Bien » ou « Très bien » à ces deux questions.

Source : Analyse par Deloitte des données de l'étude sur la résilience de 2021

# Notes de fin

1. Steve Morgan. *« Cybercrime To Cost The World $10.5 Trillion Annually By 2025 »*, *Cybercrime Magazine*, 13 novembre 2020.
2. Karthik Ramachandran et David Linthicum. *Why organizations are moving to the cloud*, Deloitte Insights, 5 mars 2020.
3. Deloitte. *The future of cyber survey 2019*, 2019.
4. Analyse des données d'une enquête menée auprès de 2 260 hauts dirigeants et hauts fonctionnaires de 21 pays par KS&R Inc. en juillet, août et septembre 2020 aux fins d'une étude sur la résilience publiée par Deloitte Mondial en 2021 et intitulée *Bâtir une organisation résiliente : rapport de Deloitte Mondial sur la résilience en 2021*, https://www2.deloitte.com/global/en/insights/topics/strategy/characteristics-resilient-organizations.html.
5. Les organisations ayant déjà un programme d'infonuagique arrivé à maturité ont en général répondu « bien » ou « très bien » à la question à savoir comment leur organisation avait fait ou était en train de faire « la transition de ses systèmes d'exploitation vers le nuage pour appuyer le télétravail (p. ex. outils de collaboration, RPV, centres de données, serveurs, etc.) » et celles qui sont reconnues comme ayant un programme de cybersécurité arrivé à maturité sont celles ayant répondu « bien » ou « très bien » à la question à savoir dans quelle mesure leur organisation était arrivée à « gérer la détection, la correction et la prévention des cybermenaces en constante évolution » pendant la période de juillet à septembre 2020.
6. Expérience de Deloitte.
7. Jason Miller. *Air Force's game-changing approach to cloud accreditation*, *Federal News Network*, 30 juillet 2020.
8. Sunil Potti. *Expanding Google Cloud's Confidential Computing portfolio*, *Google Cloud Blog*, 8 septembre 2020.
9. Expérience de Deloitte.
10. Help Net Security. *Top security risks for companies to address as cloud migration accelerates*, 11 juin 2020.
11. NASCIO et Deloitte. *States at risk: The cybersecurity imperative in uncertain times*, Deloitte Insights, 14 octobre 2020.
12. Ryan Johnston. *Remote work marked 'culmination' of NYC Cyber Command's cloud initiatives, agency heads said*, State Scoop, 7 octobre 2020.
13. Alicia Hope. *« Almost All Cyber Attacks on Cloud Servers Involve Cryptocurrency Mining, a New Study Found »*, *CPO Magazine*, 25 septembre 2020.
14. Veronica Combs. *3 ways criminals use artificial intelligence in cybersecurity attacks, Tech Republic*, 7 octobre 2020.
15. Analyse par Deloitte des données sur les brevets de 2018 à 2020 visant à trouver les mots-cibles centrés sur l'infonuagique et la cybersécurité.
16. Vikram Kunchala et coll. *DevSecOps and the cyber imperative, Deloitte Insights*, 16 janvier 2019.
17. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2021/zero-trust-security-framework.html/
18. Expérience de Deloitte.
19. David Linthicum et coll. *The future of cloud-enabled work infrastructure*, Deloitte Insights, 23 septembre 2020.
20. David Linthicum. *Three cloud security problems that you can solve today*, Deloitte On Cloud Blog, 20 septembre 2018.

21. Paul Klein et Roland Labuhn. *Deloitte Tech Trends – Trend 7: Modernizing core technologies*, Deloitte Insights, 3 février 2020.

22. Aaron Brown et coll. *Achieving cyber governance risk & compliance in the cloud*, Deloitte, 2019.

23. Accurics. *State of DevSecOps Report for Summer 2020*, 4 août 2020.

24. DivvyCloud. *2020 Cloud Misconfiguration Report*, février 2020.

25. *Ibid.*

26. Expérience de Deloitte.

27. Alex Tolsma. *GDPR and the impact on cloud computing*, Deloitte, consulté le 7 janvier 2021.

28. Deloitte. *GDPR and the impact on cloud computing*, cybersécurité, confidentialité, Deloitte Pays-Bas.

29. NIST. *Cybersecurity Framework*, consulté le 7 janvier 2021.

30. U.S. General Services Administration. *FedRAMP*, consulté le 7 janvier 2021.

31. Josh Fruhlinger. *What is FedRAMP? How cloud providers get authorized to work with the U.S. government*, CSO, 3 avril 2018.

32. U.S. General Services Administration. *FedRAMP*.

33. Itir Clarke. *What Is CASB (Cloud Access Security Broker)?*, ProofPoint, 20 juin 2019.

34. Cloud Security Alliance. *The Cloud Balancing Act for IT: Between Promise and Peril*, janvier 2016.

35. Julie Bernard et Mark Nicholson. *Reshaping the cybersecurity landscape*, Deloitte Insights, 24 juillet 2020.

# Remerciements

Les auteurs tiennent à remercier **Douglas Bourgeois**, **Aaron Brown**, **Mark Campbell**, **Mike Kavis**, **Timothy Li**, **Ryan Lindeman**, **Lauren Nalu** et **Tony Witherspoon** pour leurs idées. Nous remercions spécialement **David Linthicum**, **Natasha Buckley**, **Monika Mahto**, **Lisa Beauchamp**, **Purnima Roy**, **Jayee Hegde**, **Bhadra Gordon**, **Kavita Saini**, **Aparna Prusty** et **Kimberly Donohue** pour leur perspective et leur soutien.

# Au sujet des auteurs

**Deborah Golden | debgolden@deloitte.com**

Deborah Golden est associée chez Deloitte & Touche LLP et responsable des cyberrisques et des risques stratégiques aux États-Unis pour Conseils en gestion des risques et Conseils financiers de Deloitte. Comptant 25 ans d'expérience dans divers secteurs, elle dirige actuellement l'une des plus importantes initiatives de croissance de Deloitte, qui consiste à positionner l'informatique pour une différenciation stratégique en combinant les affaires, la technologie et le cyberespace afin de fournir des solutions au-delà de l'organisation technologique, à mesure que les entreprises continuent à exercer leurs activités dans un monde caractérisé par la cyberculture. Elle aide principalement les entreprises et les agences gouvernementales à régler des problèmes informatiques complexes et à transformer leur entreprise, les stratégies liées à leur mission et leurs activités. Elle est titulaire d'un baccalauréat en finance de l'Université Virginia Tech et d'une maîtrise en technologies de l'information de l'Université George Washington.

**Vikram Kunchala | vkunchala@deloitte.com**

Vikram Kunchala, un associé chez Deloitte & Touche LLP, est responsable des secteurs de consommation de la pratique des cyberrisques et des risques stratégiques pour Conseils en gestion des risques et Conseils financiers de Deloitte. Il est aussi responsable de l'infonuagique pour la pratique des services de cyberrisques pour Conseils en gestion des risques et Conseils financiers de Deloitte. Il possède plus de 20 ans d'expérience en conception et en mise en place de solutions de cybersécurité et de programmes de gestion des cyberrisques. Ses spécialités comprennent la sécurité des applications, la sécurité de l'infonuagique, la gestion des identités et des accès ainsi que la gestion des cybermenaces et des vulnérabilités. Il possède une vaste expérience dans le soutien des organisations techniques et commerciales en vue d'atteindre des objectifs stratégiques et tactiques.

**Amod Bavare | abavare@deloitte.com**

Amod Bavare est associé de la division de génie infonuagique chez Deloitte Consulting LLP, et il dirige les efforts de Deloitte dans la migration et la modernisation de l'infonuagique à l'échelle mondiale dans tous les secteurs et les sous-secteurs. Il possède plus de 25 ans d'expérience dans le secteur des TI. Il se spécialise dans la rénovation de l'architecture et la migration d'applications d'entreprise complexes vers l'infonuagique, contribuant essentiellement à créer de la valeur en modernisant les systèmes existants des clients. Il siège au conseil d'administration de la chambre de commerce indo-américaine de la région métropolitaine de Houston et dirige la campagne annuelle de collecte de dons de Centraide pour Deloitte Consulting LLP.

**Bhavin Barot | bbarot@deloitte.com**

Bhavin Barot est un associé de la pratique de conseils en cybertechnologie de Deloitte. Depuis plus de 20 ans, il aide ses clients à améliorer leurs cyberprogrammes, à répondre aux normes de sécurité et à maintenir une conformité continue. Il se concentre sur la sécurité des applications, les contrôles des processus d'entreprise et la conception et la mise en œuvre de mesures de contrôle des technologies de l'information. Il a dirigé de nombreuses initiatives stratégiques englobant la stratégie de sécurité informatique et de gestion des risques, la gouvernance, la cybersécurité, la gestion des identités, la résilience technologique et organisationnelle et la gestion des services, en plus d'un certain nombre d'importants projets mondiaux de gestion des risques et de transformation de la sécurité.

**Ritesh Bagayat | rbagayat@deloitte.com**

Ritesh Bagayat est directeur principal au sein de la pratique des Services liés aux cyberrisques de Deloitte & Touche. Il possède plus de 14 ans d'expérience en conception et en mise en place de solutions de cybersécurité et de conformité réglementaire. Ses compétences pointues comprennent la modernisation des applications, la sécurité de l'infonuagique, la gestion des identités, la sécurité des applications, les mesures de contrôle des processus et la conformité réglementaire. Il possède une vaste expérience en architecture, en conception et en mise en œuvre de solutions de sécurité pour les transformations numériques des entreprises à grande échelle.

**Diana Kearns-Manolatos | dkearnsmanolatos@deloitte.com**

Diana Kearns-Manolatos est directrice principale du Centre de recherche intégrée de Deloitte. Elle y analyse l'évolution du marché et les nouvelles tendances dans tous les secteurs. Ses recherches portent sur les stratégies technologiques intégrées et l'infonuagique. Elle soutient également l'initiative de recherche « Big Ideas : Future of the Workforce » (grandes idées sur l'avenir de la main-d'œuvre) de Deloitte et de MIT Sloan Management Review, et possède plus de 15 ans d'expérience reconnue dans le domaine de la communication et du marketing, permettant d'harmoniser les idées et la stratégie commerciale. Elle donne des conférences sur la technologie et les femmes leaders, et est titulaire d'un baccalauréat et d'une maîtrise de l'Université Fordham.

**Jay Parekh | jparekh@deloitte.com**

Jay Parekh est un analyste principal au sein du Centre de recherche intégrée de Deloitte. Il possède plus de six ans d'expérience dans la recherche et l'analyse axées sur les nouvelles technologies et les innovations numériques liées à l'infonuagique, à la réalité augmentée et virtuelle, à l'Internet des objets et à d'autres technologies avancées. Il se consacre également au développement des perspectives de Deloitte sur de sujets intersectoriels, comme les changements climatiques et la durabilité. Il se spécialise dans l'application de techniques de recherche quantitative et qualitative afin d'obtenir des renseignements fondés sur des données.

# Communiquez avec nous

*Nos perspectives peuvent vous aider à tirer parti du changement. Si vous êtes à la recherche de nouvelles idées pour relever vos défis, nous devrions en discuter.*

## Leadership sectoriel

**Robert Masse**
Associé | Conseils en gestion des risques | Leader national de la sécurité de l'infonuagique | Deloitte Canada
+1 514 393 7003 | rmasse@deloitte.ca

M. Masse est associé et leader national de la Sécurité de l'infonuagique au sein des Conseils en gestion des risques de Deloitte Canada.

**Jean-François Allard**
Associé | Conseils en gestion des risques | Leader national, Crises et résilience | Deloitte Canada
+1 514 393 7147 | jeallard@deloitte.ca

M. Allard est associé et leader national du groupe Crises et résilience des Conseils en gestion des risques de Deloitte Canada.

**Aaron Fleming**
Directeur de service | Sécurité de l'infonuagique | Conseils en gestion des risques | Deloitte Canada
+1 416 521 4632 | aafleming@deloitte.ca

M. Flemming est directeur de service de la Sécurité de l'infonuagique au sein des Conseils en gestion des risques de Deloitte Canada.

**Naresh Kurada**
Directeur de service | Sécurité de l'infonuagique | Conseils en gestion des risques | Deloitte Canada
+1 416 956 9194 | nkurada@deloitte.ca

M. Karuda est directeur de service de la Sécurité de l'infonuagique au sein des Conseils en gestion des risques de Deloitte Canada.

**Vikram Kunchala**
Associé | Responsable de l'infonuagique | Responsable de la cybertechnologie et des risques stratégiques pour les secteurs de consommation | Deloitte & Touche LLP
+1 713 982 2807 | vkunchala@deloitte.com

M. Kunchala est responsable de l'infonuagique pour la pratique des services de cyberrisques pour Conseil en gestion des risques et Conseils financiers de Deloitte.

**Bhavin Barot**
Associé | Conseils en cybertechnologie | Deloitte Consulting LLP
+1 313 396 3472 | bbarot@deloitte.com

M. Barot est un associé de la pratique de conseils en cybertechnologie de Deloitte. Depuis plus de 20 ans, il aide ses clients à améliorer leurs cyberprogrammes, à répondre aux normes de sécurité et à maintenir une conformité continue.

**Amod Bavare**
Associé | Responsable de la migration à l'infonuagique à l'échelle mondiale | Deloitte Consulting LLP
+1 713 982 3040 | abavare@deloitte.com

M. Bavare est associé du génie infonuagique chez Deloitte Consulting LLP, et il dirige les efforts de Deloitte dans la migration et la modernisation de l'infonuagique à l'échelle mondiale dans tous les secteurs et les sous-secteurs.

## Centre de recherche intégrée de Deloitte

**Diana M. Kearns-Manolatos**
Directrice principale | Spécialiste | Deloitte Services LLP
+1 212 436 3301 | dkearnsmanolatos@deloitte.com

Diana M. Kearns-Manolatos est directrice principale du Centre de recherche intégrée de Deloitte, et elle se concentre sur la transformation technologique intégrée et l'infonuagique.

Deloitte.
Insights

Inscrivez-vous pour recevoir les mises à jour de Deloitte Insights, à l'adresse www.deloitte.com/insights.

Suivez @DeloitteInsight


**Collaborateurs de Deloitte Insights**
**Rédaction :** Kavita Saini, Aparna Prusty et Nairita Gangopadhyay
**Création :** Nagaraju Mangala, Sanaa Saifi et Victoria Lee
**Promotion :** Alexandra Kawecki
**Illustration de la page de couverture :** Daniel Hertzberg


**À propos de Deloitte Insights**

Deloitte Insights publie des articles, des rapports et des périodiques originaux qui fournissent des perspectives à l'intention des entreprises, du secteur public et des ONG. Notre objectif est de puiser dans les recherches et l'expérience de l'ensemble de notre organisation de services professionnels, et de coauteurs du milieu universitaire et de celui des affaires, pour faire avancer le dialogue sur un large spectre de sujets d'intérêt à l'intention des dirigeants d'entreprise et des leaders gouvernementaux.

Deloitte Insights est une marque d'éditeur de Deloitte Development LLC.

**À propos de cette publication**

Les renseignements contenus dans la présente publication sont d'ordre général. Deloitte Touche Tohmatsu Limited, ses cabinets membres et leurs sociétés affiliées ne fournissent aucun conseil ou service dans les domaines de la comptabilité, des affaires, des finances, du placement, du droit, de la fiscalité, ni aucun autre conseil ou service professionnel au moyen de la présente publication. Ce document ne remplace pas les services ou conseils professionnels et ne devrait pas être utilisé pour prendre des décisions ou mettre en œuvre des mesures susceptibles d'avoir une incidence sur vos finances ou votre entreprise. Avant de prendre des décisions ou des mesures qui peuvent avoir une incidence sur votre entreprise ou vos finances, vous devriez consulter un conseiller professionnel reconnu.

Ni Deloitte Touche Tohmatsu ni aucun de ses cabinets membres ou leurs sociétés affiliées respectives ne pourront être tenus responsables à l'égard de toute perte que pourrait subir une personne qui se fie à cette publication.

**Au sujet de Deloitte**

Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni (DTTL), ainsi que son réseau de cabinets membres et leurs entités liées. DTTL et chaque cabinet membre de DTTL sont des entités juridiques distinctes et indépendantes. DTTL (appelé également « Deloitte mondial ») n'offre aucun service aux clients. Aux États-Unis, Deloitte désigne un ou plusieurs cabinets membres américains de DTTL ainsi que leurs entités liées qui exercent leurs activités sous le nom de « Deloitte » aux États-Unis et leurs entités affiliées respectives. Certains services peuvent ne pas être offerts aux clients d'attestation en vertu des règles et règlements qui s'appliquent aux services d'experts-comptables. Pour obtenir une description détaillée de Deloitte Touche Tohmatsu Limited et de ses cabinets membres, voir www.deloitte.ca/apropos.