Deloitte.

Renforcer la résilience

Perspectives réglementaires pour les institutions financières canadiennes en 2019

CENTRE *de*
STRATÉGIE EN RÉGLEMENTATION
AMÉRIQUES

Table des matières

Avant-propos

Introduction

Près de dix ans après la crise financière, les traces profondes qu'elle a laissées commencent à s'estomper. À l'exception d'un dernier élément de Bâle III, la plupart des politiques prudentielles ultérieures à la crise ont été déterminées, et les banques en particulier ont désormais plus de capitaux permanents et de liquidités qu'avant la crise. Avec la variété d'échéanciers et d'approches pour la mise en œuvre nationale des réformes prudentielles convenues, toute l'attention est maintenant concentrée sur la culture et la gouvernance, les exigences des nouvelles technologies ainsi que les nouveaux risques relatifs à l'économie, à l'exploitation et au marché. Les entreprises doivent être prêtes à s'adapter à ce changement et aux nouvelles exigences qui en découleront.

Levée de la politique d'accompagnement monétaire

À l'échelle mondiale, l'assouplissement monétaire et la baisse des taux d'intérêt cèdent lentement la place à la normalisation des taux d'intérêt, bien qu'on s'attende à ce que ceux-ci soient nettement moins élevés que la norme historique. Les États-Unis ont donné le ton avec une série de hausses de taux, et le bilan de la Réserve fédérale a commencé à diminuer. La Banque d'Angleterre a quant à elle commencé provisoirement à élever ses taux, et la Banque centrale européenne met fin à l'expansion de son bilan. En Australie, les taux d'intérêt demeurent inchangés, mais ils devraient commencer à augmenter. Le Japon représente la grande exception, puisque ses taux devraient demeurer bas à court terme. Compte tenu du nombre de turbulences auxquelles est soumise l'économie mondiale (p. ex., niveau d'endettement considérable, risques géopolitiques élevés et protectionnisme commercial), les taux d'intérêt augmenteront probablement lentement.

La hausse des taux d'intérêt pourrait être avantageuse pour certaines entreprises du point de vue de la valeur nette : les banques pourraient bénéficier d'une augmentation de la marge nette sur les intérêts, et les assureurs pourraient quant à eux voir augmenter le rendement de leurs actifs. Cependant, la normalisation des taux d'intérêt pourrait également entraîner, dans certains cas, une diminution de la valeur des actifs et une hausse des défaillances de crédit en plus de dévoiler des faiblesses structurelles de l'économie mondiale et des finances d'entreprises individuelles. On ne sait pas quelles seront les conséquences globales de ces facteurs opposés, surtout pour les entreprises et secteurs individuels.

Un environnement économique incertain

Entre-temps, la période de la politique d'accompagnement monétaire a contribué à l'augmentation de l'endettement, la dette mondiale s'élevant maintenant à 247 billions de dollars[1], ce qui est beaucoup plus élevé que le sommet atteint avant la crise. Aux yeux de nombreux commentateurs, cela représente une importante vulnérabilité systémique[2]. En outre, la baisse des taux a contribué à la recherche constante de rendement, ce qui a peut être amené bon nombre de prêteurs et d'investisseurs à assouplir leurs critères liés à la qualité du crédit. De plus, les exigences comparativement plus grandes des banques à l'égard des fonds propres ont mené à l'augmentation des prêts non bancaires, ce qui signifie que l'exposition aux marchés du crédit touche dorénavant un plus vaste éventail d'entreprises. Le marché des prêts à effet de levier et celui de l'immobilier risquent tous deux d'être vulnérables aux hausses de taux d'intérêt. Par ailleurs, l'accroissement du crédit à la consommation et l'endettement personnel qui en résulte pourraient avoir rendu de nombreux consommateurs vulnérables aux hausses de taux d'intérêt, surtout après une longue période où les taux étaient peu élevés.

Si l'on aborde la situation économique mondiale dans son ensemble, on constate que les perspectives varient. La croissance économique continue d'être très forte dans des régions de l'Asie, même si elle a ralenti en Chine, mais les perspectives pour les économies émergentes ou en développement sont inégales. La reprise économique au Royaume-Uni et aux États-Unis est en cours depuis près de dix ans, tandis que l'expansion de la zone euro, même si elle se fait lentement, est également bien amorcée. Par le passé, il y a eu des ralentissements économiques

Avant-propos

ou des récessions au moins tous les dix ans, ce qui laisse supposer que l'un ou l'autre pourrait bientôt se produire[3].

Il y a des commentateurs[4] qui croient que l'économie mondiale a atteint la fin de son cycle, d'après les évaluations des actifs dont la valeur semble surévaluée et donc sur le point de devoir être corrigée. Dans l'Union européenne, près de 731 milliards d'euros [5] en prêts improductifs constituent toujours un risque important du point de vue de la résilience et de la rentabilité d'un certain nombre de banques, tandis qu'à l'échelle mondiale, le protectionnisme commercial et l'incertitude politique grandissants préoccupent beaucoup le secteur. Le Brexit continue de susciter beaucoup d'incertitude sur les plans géopolitique et réglementaire, et tant les organismes de réglementation que les politiciens s'emploieront à atténuer ses risques et ses effets en 2019. Quoi qu'il en soit, si le Brexit se fait de façon désordonnée et donne lieu à de nouvelles stratégies et approches politiques, les effets sur un certain nombre de prévisions réglementaires pourraient être très prononcés au Royaume-Uni.

Dans ce contexte, on peut s'attendre à ce que les organismes de réglementation de tous les secteurs demeurent très à l'affût des risques de ralentissement économique et de bouleversement des marchés. Ils voudront probablement faire de nombreuses simulations de crise pour évaluer la vulnérabilité et la résilience des entreprises en tenant compte du fait que, pendant une période sans précédent de faibles taux d'intérêt, certains modèles d'affaires ont évolué dans des conditions plutôt favorables et doivent encore être mis à l'essai dans un contexte de ralentissement soutenu.

Abandon de la coordination mondiale

L'approche réglementaire mondiale évolue. La crise financière a donné lieu à des interventions concertées à l'échelle mondiale visant à établir un ensemble de nouveaux règlements destinés à soutenir un système financier plus robuste et plus stable. Cependant, on commence à délaisser l'élaboration de politiques mondiales et la collaboration transfrontalière en matière de réglementation. En conséquence, il y a de plus en plus de signes de divergence réglementaire, notamment en ce qui concerne la protection géographique et la protection des activités, alors que divers pays et régions cherchent à adapter les règlements à leurs propres besoins. Les entreprises mondiales doivent donc se conformer à ces règles divergentes dans les différents territoires où elles exercent leurs activités, en plus d'optimiser leurs structures de gouvernance, leurs modèles d'exploitation, la structure de leurs entités juridiques et leurs modèles de prestation de services de négociation de valeurs des clients (ou booking models) à l'échelle locale.

Transition à la supervision

On ne s'attend pas à ce que les organismes de réglementation démantèlent ou annulent les réformes mises en œuvre depuis la crise de 2008. Il semble toutefois que, à moins d'un événement d'envergure imprévu, il est peu probable que de nouveaux règlements importants soient adoptés, surtout en ce qui concerne les banques et les capitaux d'assurance. Les grandes priorités des organismes de réglementation consistent à consolider, à protéger et, dans certains cas, à améliorer les réformes de la dernière décennie. On s'attend toutefois à ce que la période de refonte de la réglementation et d'innovation soit suivie d'une autre caractérisée par la mise en œuvre et l'intégration du système de supervision révisé.

En conséquence, dans de nombreux pays, les attentes en matière de surveillance à l'égard des entreprises sont plus grandes, ce qui reflète l'augmentation des approches de supervision fondées sur des principes qui font ressortir l'importance des approches des entreprises en matière de gouvernance, de culture et de gestion et leurs résultats sur les plans prudentiel et des règles de conduite. La conduite de l'entreprise et la façon dont elle traite ses clients font aussi l'objet d'une attention accrue dans bien des pays en raison de préoccupations d'ordre politique ou réglementaire concernant la mauvaise conduite apparente des entreprises dans l'ensemble des secteurs financiers [6].

Avant-propos

En outre, les superviseurs adoptent des pratiques plus intrusives, comme l'utilisation accrue de visites sur place. Cela illustre la pratique mondiale dominante et montre que les superviseurs doivent de plus en plus communiquer directement avec les entreprises pour comprendre leurs stratégies et leurs modèles d'affaires, leur profil de risque et leur tolérance au risque ainsi que leurs cadres et méthodes de gestion des risques et tenir le conseil d'administration et la haute direction responsables des résultats qu'ils produisent.

Nouvelles technologies

Les entreprises, les organismes de réglementation et leurs clients s'emploient à examiner les possibilités et les risques associés aux nouvelles technologies. Par exemple, en raison de l'évolution rapide de l'intelligence artificielle, de l'apprentissage machine et des solutions liées aux technologies financières, les nouvelles technologies deviennent vite la norme. Il ne faut pas sous-estimer l'incidence considérable qu'auront ces technologies non seulement sur les clients, mais également sur la réglementation et la supervision. C'est donc dire que le rythme des changements technologiques exige une profonde réflexion quant à la bonne façon de réglementer les processus, les produits et les institutions pour éviter les lacunes réglementaires et assurer la stabilité financière et la protection des clients.

Ces innovations et perturbations technologiques ont déclenché un débat sur le périmètre de la réglementation des services financiers. De nombreuses entreprises traditionnelles craignent que les nouveaux venus centrés sur les technologies offrent des services qui dépassent les limites de la réglementation actuelle régissant les services financiers que les entreprises traditionnelles trouvent plus coûteux à offrir en raison des risques de perte de profits puisqu'elles doivent se soumettre à la réglementation alors que les nouveaux venus ne sont pas assujettis aux mêmes règles. On ne s'attend pas à ce que les organismes de réglementation viennent à la rescousse des entreprises traditionnelles, qui devront mettre à profit leurs propres ressources pour se mesurer à la concurrence. On s'attend toutefois à ce que les préoccupations relatives à l'équité des règles et les inquiétudes concernant le rôle des technologies dans la société en général rehaussent l'intérêt porté à la façon dont les entreprises de technologies financières et les actifs cryptographiques sont réglementés ou plutôt à l'absence de réglementation dans ce domaine à l'heure actuelle. Des précisions devraient être apportées au sujet du traitement réglementaire des actifs cryptographiques, en particulier dans les domaines des investissements des acheteurs au détail, du blanchiment d'argent et du capital prudentiel pour les banques.

Comment réagir à l'incertitude

Même si l'environnement réglementaire actuel semble s'être stabilisé comparativement à ce qu'il était tout récemment, les organismes de réglementation du monde entier continuent de fixer des attentes élevées pour faire en sorte que le secteur financier demeure vigoureux et robuste grâce à la solide résilience financière et opérationnelle des entreprises, soutenue par de bonnes capacités de gestion des risques et de conformité. À notre avis, cela pourrait fournir aux grandes entreprises de services financiers l'occasion de passer de l'établissement de cadres en fonction des nombreux nouveaux règlements à l'utilisation de nouveaux modèles d'exploitation et technologies.

Le monde change et la réglementation aussi

Les débats concernant le périmètre réglementaire et la fragmentation possible du système financier montrent que la résilience opérationnelle des entreprises ainsi que leur vulnérabilité à la cybercriminalité et à la criminalité financière posent de plus en plus de problèmes aux organismes de réglementation. À cet égard, on s'attend à ce que la supervision soit davantage centrée sur la façon dont les conseils d'administration et les équipes de la haute direction contrôlent les risques découlant du recours à des fournisseurs externes et d'autres tiers.

Avant-propos

La dernière décennie a été marquée par des changements profonds et durables dans la structure de l'économie, l'emploi et la société. Les fournisseurs, les clients et les organismes de réglementation du secteur des services financiers sont en train de changer. Les populations vieillissantes et les nouveaux consommateurs de la génération du millénaire exigent des types de services et de produits financiers différents qui sont offerts de manières différentes. Compte tenu de ce contexte difficile en constante évolution, il est essentiel d'examiner l'avenir de la réglementation de façon globale plutôt que fragmentaire.

L'ensemble des secteurs et des parties prenantes ont un rôle important à jouer, et nous espérons que les perspectives de cette année de nos centres de stratégie en réglementation influenceront et susciteront le débat.

Kevin Nixon
Centre de stratégie en réglementation de Deloitte
APAC

Christopher Spoth
Centre de stratégie en réglementation de Deloitte
Amériques

David Strachan
Centre de stratégie en réglementation de Deloitte
EMEA

Introduction canadienne

Dans un contexte économique mondial où l'assouplissement monétaire et la baisse des taux d'intérêt cèdent lentement la place à la normalisation des taux d'intérêt, on peut dire que la situation économique du Canada se situe à la croisée des chemins. Selon les plus récentes **Perspectives économiques** de Deloitte, « soit la solide croissance économique se poursuivra, provoquant une surchauffe de l'économie et créant des tensions inflationnistes, soit elle affichera un rythme d'expansion plus modéré et viable[7] ». L'analyse de Deloitte privilégie le second scénario.

Dans ce contexte, le secteur des services financiers devrait poursuivre sur deux fronts : l'innovation axée sur la technologie pour stimuler la croissance grâce à une expérience client améliorée, et l'innovation de produits qui met l'accent sur la productivité, le levier d'exploitation et la diminution des coûts structurels. Ces deux facteurs d'innovation et d'optimisation fourniront l'environnement créatif dans lequel la plupart des institutions financières devront prendre des décisions pour soutenir la croissance et renforcer la gestion des risques.

En même temps, les organismes de réglementation indiquent que la priorité est accordée à la protection des consommateurs. En 2018, un régime de protection des consommateurs en matière financière a été instauré dans le plus récent projet de loi d'exécution du budget du gouvernement canadien, ce qui montre que l'on souhaite un resserrement des attentes en matière de dénonciations, de plaintes et de surveillance des questions liées à la protection des consommateurs par la direction et le conseil d'administration des institutions réglementées. En outre, la décision de la Cour suprême de novembre 2018 dans laquelle elle se prononçait en faveur d'une loi visant à créer un organisme de réglementation unifié pancanadien des valeurs mobilières a eu des répercussions considérables sur le contexte réglementaire canadien. Même si l'on ne sait pas encore ce qui en résultera, cette décision marque un tournant potentiel pour la législation canadienne sur les valeurs mobilières. L'établissement d'un organisme de réglementation national aura pour avantage d'uniformiser les règles au pays, d'aider les organismes de réglementation à gérer les risques systémiques et d'améliorer l'application de la loi.

Dans cette optique, nous avons déterminé pour l'année qui vient que les domaines figurant ci-dessous sont ceux qui auront le plus d'incidence sur les institutions financières canadiennes.

- **Transformation des modèles d'affaires :** en 2019, il faudra réaliser de véritables progrès concernant l'abandon du taux interbancaire offert à Londres (LIBOR) et la préparation à la revue fondamentale du portefeuille de négociation (RFPN). Alors que la date limite pour la mise en œuvre se rapproche, ceux qui seront les mieux préparés détiendront un clair avantage.
- **Cybersécurité :** à une époque où le piratage informatique et les atteintes à la protection des données sont devenus monnaie courante au point où l'on s'y attend presque, la cybersécurité continue de faire les manchettes et de dominer le programme de réglementation. Les superviseurs élargissent leur surveillance au-delà des rouages des programmes de gestion des risques; la déclaration des atteintes à la protection des données et les répercussions de l'infonuagique sur les risques et la réglementation sont les principaux nouveaux thèmes.
- **Conformité numérique :** à mesure que les banques avancent avec des programmes d'innovation, il est primordial qu'elles établissent et suivent un programme de conformité progressif pour assurer la sécurité des clients et de la banque tout en favorisant la transformation opérationnelle. En fait, la conformité numérique est en train de devenir un véritable impératif d'affaires.
- **Crimes financiers :** au moyen des technologies numériques, les criminels commettent des crimes financiers de plus en plus complexes dans l'ensemble des canaux, des régions et des secteurs. Pourtant, les institutions financières n'en continuent pas moins de s'en remettre à des modèles opérationnels qui sont cloisonnés, inefficaces et rigides et font double emploi

Introduction canadienne

pour détecter et prévenir les crimes financiers. Elles devront élaborer une approche globale et intégrée qui tienne compte des nouvelles réalités des crimes financiers, c'est à-dire le fait qu'ils sont interreliés et qu'ils touchent plusieurs produits et canaux.

- **Technologies financières :** le marché des technologies financières (*Fintech*) arrive à maturité, et les banques traditionnelles et les entreprises de technologies fintech créent des partenariats afin d'offrir des services innovateurs. Le contexte réglementaire des technologies fintech évolue simultanément avec l'annonce du Global Financial Innovation Network (GFIN), qui repose sur la proposition qu'a faite la Financial Conduct Authority du Royaume-Uni au début de l'année de créer un bac à sable mondial. Parmi les organismes de réglementation participants figure la Commission des valeurs mobilières de l'Ontario (CVMO), qui a été le premier organisme de réglementation canadien à créer son propre bac à sable : la Rampe de lancement de la CVMO. La récente création par le gouvernement canadien du Comité consultatif sur un système bancaire ouvert et les efforts soutenus du secteur des services financiers pour la modernisation des paiements montrent que le Canada continuera d'évoluer.
- **Intégration des données :** la qualité des données et l'accès aux données sont des préoccupations grandissantes pour tous les aspects de la gestion des risques et de la conformité réglementaire. Pour l'assurer, il faut que toute l'entreprise voie à la gestion et à la qualité des données et que les responsabilités et l'imputabilité soient réparties entre les trois lignes de défense.
- **Modernisation des paiements :** la modernisation des paiements est porteuse d'avantages importants pour l'économie canadienne. Ces avantages s'accompagnent de nouveaux risques, plus particulièrement le risque accru de fraude et les fortes pressions exercées sur les opérations de trésorerie. Les institutions financières doivent maintenant s'employer à déterminer les conséquences de la modernisation des paiements pour leurs profils de risques et à établir une liste de mesures prioritaires pour y réagir.
- **Transformation du modèle opérationnel de gestion des risques :** les institutions financières repensent leurs activités liées aux risques et à la conformité pour accroître leur efficacité et cherchent des moyens de tirer parti des investissements et d'éliminer le double emploi découlant de la complexité excessive. Les entreprises veulent quant à elles optimiser leur méthode de gestion des risques et exploiter les innovations technologiques et commerciales tant internes qu'externes tout en assurant la sécurité et l'intégrité.

C'est dans cette optique que j'ai le plaisir de présenter *Renforcer la résilience, perspectives réglementaires pour les institutions financières canadiennes en 2019.* Cette vue d'ensemble propose des observations clés sur l'importance accrue du double parcours de l'innovation et de l'optimisation pour la gestion des priorités en matière de réglementation et des exigences opérationnelles.

Jay F. McMahan
Leader canadien, Centre de stratégie en réglementation
Canada

Transformation des modèles d'affaires

Revue fondamentale du portefeuille de négociation (RFPN)

Mise en œuvre et échéancier

Instaurée en janvier 2016 par le Comité de Bâle sur le contrôle bancaire (CBCB), la RFPN est une norme mondiale qui sert à mesurer le risque du marché dans les portefeuilles de négociation. Elle a donné lieu à une période de vastes consultations auprès du secteur. Sa version définitive a été finalisée en janvier 2019 et son entrée en vigueur est prévue pour 2022. Les décideurs de l'Union européenne (UE) ont récemment signalé que les banques pourraient être tenues de mettre en œuvre la RFPN initialement à titre d'exigence en matière de rapport uniquement dès janvier 2021.

La RFPN dans le contexte de l'Union européenne

Les données que l'Autorité bancaire européenne (ABE) a publiées à l'automne 2018 concernant les répercussions potentielles des réformes de Bâle III sur les banques de l'Union européenne (UE) ont fait ressortir l'importance de la mise en œuvre prochaine dans l'UE des normes réglementaires mondiales relatives aux fonds propres que doivent détenir les banques pour des activités en particulier. Selon l'UE, les exigences de fonds propres en regard du risque de marché constituent l'une des questions les plus pressantes dont il faut s'occuper en mettant en œuvre la RFPN. Compte tenu de l'ampleur de la hausse des fonds propres prévue, les décideurs de l'UE ont choisi une approche de mise en œuvre en plusieurs étapes qui pourrait être plus complexe que ce que prévoyaient les normes internationales.

Pour les banques qui sont actives dans l'UE, cela a de sérieuses répercussions sur les démarches liées à la RFPN, mais pourrait également représenter une excellente occasion de procéder à la mise en œuvre de la RFPN de manière à bien soutenir leurs objectifs stratégiques et opérationnels.

Faits récents concernant la mise en œuvre de la RFPN

Dans l'UE, la RFPN a d'abord été proposée dans le cadre du deuxième règlement sur les exigences de fonds propres (CRR2) en 2016. En décembre 2017, le CBCB a accepté de repousser à janvier 2022 la date cible pour la mise en œuvre de la RFPN à l'échelle internationale. Le CBCB a ensuite rouvert le cadre de la RFPN en mars en tenant une consultation sur certains de ses éléments de sorte que les répercussions sur les activités de négociation des banques soient réparties de façon proportionnée. C'est en partie en raison de ces faits nouveaux touchant le CBCB que les négociateurs de l'UE ont décidé de modifier l'élément du CRR2 portant sur le risque de marché pour initialement mettre en œuvre la RFPN à titre d'exigence en matière de rapport uniquement.

Même si la version définitive du CRR2 n'a pas encore été établie, le cautionnement le 4 décembre 2018 par les ministres des Finances de l'UE des progrès réalisés à ce jour avec le Parlement européen montre que l'adoption par l'UE de l'exigence en matière de rapport de la RFPN est le résultat le plus probable.

Si cette approche est ratifiée par le Conseil européen et le Parlement européen l'an prochain, la mise en œuvre complète de la RFPN se fera au moyen d'une nouvelle loi, que la Commission européenne ne proposera pas avant le milieu de 2020, selon nous.

Fonctionnement de l'exigence en matière de rapport de la RFPN

Pour mettre en œuvre l'exigence en matière de rapport et tenir compte de toute modification apportée à la suite de la consultation menée par le CBCB, la Commission européenne adoptera, d'ici la fin de 2019, un Acte délégué (Delegated Act) modifiant le cadre de la RFPN dans le CRR2. Dans les faits, cela signifie que la Commission aura recours à une législation secondaire pour achever la mise en œuvre de la RFPN dans la législation de l'UE à titre d'exigence de fonds propres entièrement fonctionnelle qui ne servira qu'à la production de rapports jusqu'à ce que la nouvelle loi la rende obligatoire.

Revue fondamentale du portefeuille de négociation (RFPN)

En vertu du CRR2, les banques devront commencer à faire rapport en fonction des pondérations révisées du risque de marché découlant des changements apportés par la RFPN entièrement fondées sur la nouvelle approche normalisée un an après l'adoption de l'Acte délégué (probablement dès janvier 2021, soit une année complète avant la date cible de mise en œuvre du CBCB). Les banques qui souhaitent faire approuver leur approche des modèles internes (AMI) selon le nouveau régime de production de rapports pour des pupitres de négociation en particulier pourront encore le faire et commencer à utiliser ces modèles trois ans après l'adoption de l'Acte délégué (c.-à-d. en 2023). Pendant cette période, les exigences de fonds propres obligatoires pour le risque de marché continueront d'être fondées sur les règles existantes du CRR. Par conséquent, toute réduction des pondérations du risque découlant des modèles de l'AMI nouvellement approuvés en vertu du CRR2 ne procurerait aucun bénéfice au chapitre des fonds propres pendant la durée d'application de l'exigence en matière de rapport.

Les banques admissibles à la dérogation concernant les petits portefeuilles de négociation pourraient se faire exempter de l'exigence en matière de rapport jusqu'à ce qu'un cadre obligatoire soit instauré. Cependant, les grandes banques doivent déjà planifier la mise en œuvre de la RFPN en deux étapes, car bon nombre des exigences opérationnelles pourraient devoir être mises en œuvre d'ici 2021 au lieu de 2022.

Pour assurer la mise en œuvre complète de la RFPN à titre d'exigence obligatoire pour des fonds propres, la Commission devra présenter une nouvelle proposition législative à cette fin. Selon nous, cela devrait se faire d'ici juin 2020 dans le cadre de la proposition législative concernant le CRR3.

En conséquence, compte tenu du temps qu'il faudra pour négocier le CRR3 (au moins d'ici le milieu de 2022) et, par la suite, le délai vraisemblable pour mettre en œuvre la RFPN, il est pratiquement impossible que l'UE puisse mettre en vigueur la norme obligatoire relative à la RFPN d'ici la date cible fixée par le CBCB, soit janvier 2022. Il faudra probablement au moins deux ans de plus pour y arriver.

Ce que cela signifie pour les banques

Comme il est de plus en plus probable que la RFPN sera instaurée en deux étapes dans l'UE, les banques doivent maintenant examiner l'incidence que cela aura sur la planification de sa mise en œuvre. Ce ne sera pas chose facile, puisque les banques qui exercent des activités dans l'UE pourraient devoir se conformer à l'exigence en matière de rapport fondée sur la RFPN dès 2021, même s'il subsistera beaucoup d'incertitude quant à la forme définitive et aux caractéristiques économiques du cadre.

Les banques qui utilisent actuellement l'AMI risquent d'avoir des pondérations du risque de marché beaucoup plus importantes au cours des deux premières années de la mise en œuvre dans l'UE, puisque l'approche normalisée sera la seule façon pour elles de produire des rapports. Les différents calendriers et approches de mise en œuvre utilisés dans l'UE et le reste du monde poseront un problème de taille aux banques internationales.

Une décision particulièrement importante sera de savoir si les banques demanderont ou non une approbation réglementaire pour utiliser les modèles de l'AMI en vertu du nouveau régime prévu par le CRR2 pendant la période d'application des exigences relatives à la production de rapport. Pour celles qui ne le font pas, il pourrait être difficile de le faire dans les délais si elles ne commencent leurs démarches qu'après que la version définitive de la législation relative au CRR3 sera établie ou elles risquent d'attendre longtemps pour qu'un superviseur approuve leur modèle. De nombreux superviseurs bancaires ont indiqué que le processus d'approbation de modèles pour la RFPN s'échelonnera probablement sur plusieurs années.

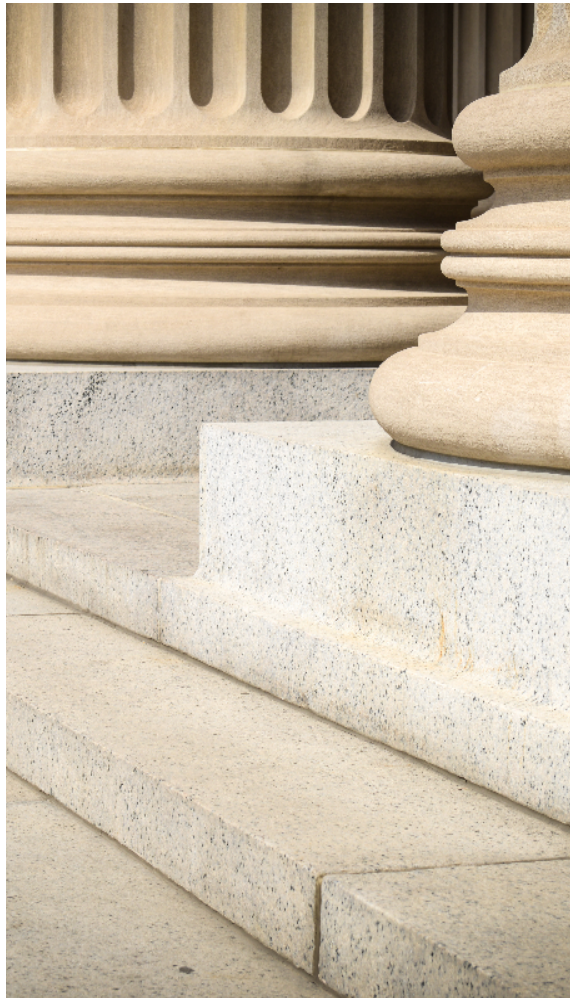
Revue fondamentale du portefeuille de négociation (RFPN)

Comment les banques canadiennes seront-elles touchées?

Les institutions de dépôt canadiennes qui sont présentes sur les marchés financiers de l'UE doivent s'attendre à devoir déclarer les fonds propres selon l'approche normalisée pour leurs filiales de l'UE d'ici janvier 2021. Comme le Bureau du surintendant des institutions financières (BSIF) a déjà indiqué que le premier rapport réglementaire selon les règles de la RFPN ne sera pas exigé avant le premier trimestre de 2021, les récents événements dans l'UE ne doivent pas faire dévier les banques canadiennes de leur programme de mise en œuvre. Cependant, il y a des répercussions qui doivent être examinées par la haute direction, notamment :

- La nécessité de maintenir deux modèles d'exploitation parallèles – AN selon la RFPN et Bâle 2.5 – ainsi que des cadres de gestion distincts pour les hiérarchies et les limites du portefeuille de négociation et du portefeuille d'intermédiation bancaire.
- L'incapacité de faire approuver l'AMI pour les pupitres de négociation situés dans l'UE, et ce, potentiellement jusqu'en 2023.
- Pour les banques qui n'ont pas encore amorcé l'élaboration de leur programme, la nouvelle de l'UE leur laisse seulement un an pour se préparer à la nouvelle approche normalisée si leur objectif est une année complète de mise à l'essai.

- **La RFPN n'est pas qu'une question de modèles; elle a une incidence sur l'ensemble de la stratégie de la banque.** La RFPN influe sur les pratiques d'affaires liées à la salle des marchés plus que tout autre règlement prudentiel antérieur. Les approbations du pupitre de négociation signifient que l'entreprise aura un intérêt direct et quotidien dans la performance des modèles de gestion des risques, tandis que l'incidence sur les actifs pondérés en fonction des risques sera largement redistribuée entre les pupitres.
- **Une approche stratégique suprême pour l'analyse des fonds propres.** Notre expérience de l'analyse des répercussions des fonds propres nous a amenés à dissuader les clients d'effectuer des analyses portant exclusivement sur le pupitre de négociation des produits, car cela peut s'avérer trompeur lorsque les effets de la diversification du portefeuille sont pris en compte.



Revue fondamentale du portefeuille de négociation (RFPN)

Difficultés

- Le changement de méthode pour le calcul des charges de capital peut faire augmenter celles-ci et rendre certains produits économiquement non viables, ce qui pourrait inciter les banques à abandonner des activités. Il peut même y avoir des répercussions politiques, par exemple pour des marchés émergents.
- Une interprétation prudente des exigences, par exemple catégoriser chaque facteur de risque non observable à titre de facteur de risque individuel non modélisable, mène rapidement à des niveaux de fonds propres extrêmement élevés. Des mesures d'atténuation, comme trouver une source de données fiables sur les marchés, risquent d'accroître considérablement le délai et les dépenses nécessaires à la mise en œuvre.
- Les calculs effectués selon les règles de la RFPN, si on suppose une réévaluation complète de l'AMI, nécessitent beaucoup de données très détaillées et exigent une augmentation notable de la capacité de traitement.

Principaux points à retenir

- Même si l'approche complexe de l'UE accroît l'incertitude à l'égard de la mise en œuvre de la RFPN, les banques doivent saisir l'occasion de faire une utilisation stratégique du délai supplémentaire qu'elles auront probablement avant l'entrée en vigueur des exigences obligatoires.
- L'alignement de bon nombre des améliorations devant être apportées à l'infrastructure de gestion des risques et des données exigées par la RFPN en fonction d'une bonne connaissance des étapes de mise en œuvre permettra aux banques de réaliser la mise en œuvre de manière à soutenir leurs objectifs stratégiques, réglementaires et commerciaux généraux.
- Le manque de précisions techniques pourrait donner lieu à des interprétations et à des niveaux d'APR très divergents dans le secteur, ce qui est exactement ce que la RFPN cherche à éviter.

Transformer les perspectives en action

- La mise en œuvre de la RFPN est une démarche d'envergure très coûteuse et elle doit servir à rationaliser et à améliorer les processus et les capacités technologiques d'une institution à long terme. Les possibilités à cet égard doivent être explorées et incluses dans le plan de mise en œuvre.
- Il est fortement recommandé de participer à la stratégie d'investissement quantitatif (SIA) du secteur; ce processus est un moyen efficace pour déterminer si une banque est prête à la mise en œuvre et donne accès aux résultats des pairs.
- Compte tenu de l'incidence des règles de la RFPN sur la structure des pupitres de négociation et la viabilité économique de certains types de produits, il faut mettre les parties prenantes de l'entreprise à contribution dès le début du processus et leur fournir les renseignements et les outils nécessaires pour évaluer les répercussions des fonds propres et prendre des décisions quant aux modifications à apporter à la stratégie d'affaires.
- Les améliorations à l'infrastructure de gestion des risques et des données exigées par la RFPN doivent être alignées sur les étapes de la mise en œuvre pour permettre aux banques de réaliser la mise en œuvre de manière à soutenir leurs objectifs stratégiques, réglementaires et commerciaux généraux.
- Il faut tirer parti de la mise en œuvre de la RFPN pour aligner davantage la fonction de gestion des risques et la fonction des finances, améliorer la surveillance quotidienne et intrajournalière des risques de marché et accroître l'efficacité opérationnelle dans l'ensemble du processus appliqué aux risques de perte de profits liés à la négociation.

Abandon du taux interbancaire offert (IBOR)

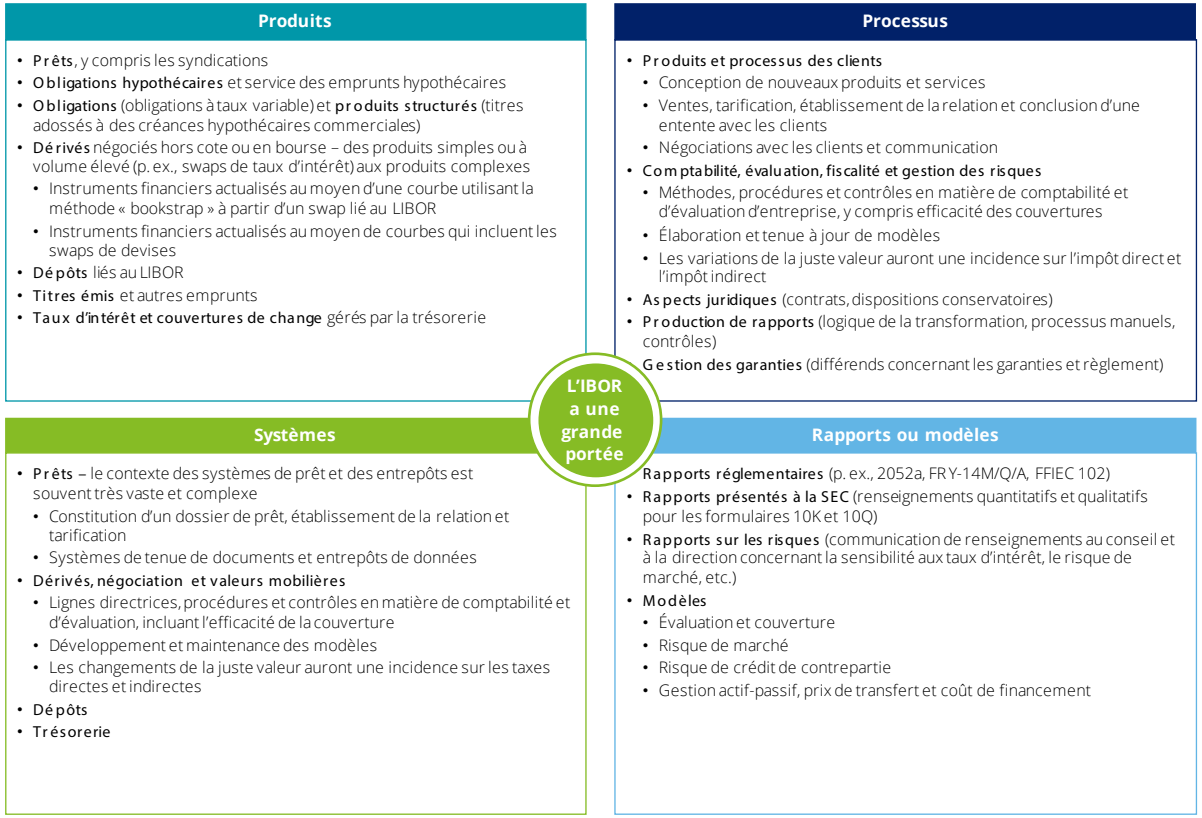
Abandon du taux interbancaire offert (IBOR)

Le taux interbancaire offert à Londres ou LIBOR est une référence clé en matière de taux d'intérêt qui sert à calculer les flux de trésorerie flottants ou variables pour les prêts, les obligations, les dérivés et d'autres instruments financiers. Il existe également des taux interbancaires offerts ou IBOR à l'extérieur des pays du G5.

En 2017, Andrew Bailey, chef de la direction de la Financial Conduct Authority (FCA) du Royaume-Uni, a annoncé que d'ici la fin de 2021, la FCA ne chercherait plus à inciter ou à obliger les banques du panel à contribuer au LIBOR. En juillet 2018, M. Bailey a ajouté ce qui suit [traduction] : « [...] Les entreprises doivent voir cela [l'abandon du LIBOR] comme un événement à venir auquel elles doivent se préparer[8]. » En outre, les organismes de réglementation à l'échelle mondiale ont clairement indiqué que les entreprises doivent délaisser l'IBOR au profit d'autres taux sans risque (TSR) à un jour.

Difficultés

L'IBOR est largement utilisé par les banques, les gestionnaires d'actifs, les assureurs et les entreprises. Ce taux est bien ancré dans les activités opérationnelles des institutions ayant recours aux produits financiers concernés, ce qui fait de la transition une tâche très complexe. Il s'agira probablement de l'une des plus importantes transformations que les entreprises n'auront jamais à réaliser, puisqu'elle influera sur la plupart des unités fonctionnelles et aura d'importantes répercussions financières et opérationnelles.



Abandon du taux interbancaire offert (IBOR)

Données clés

Nous prévoyons qu'en 2019, il y aura une hausse du niveau d'activité à mesure que les entreprises se rendront compte qu'il y a beaucoup à faire. La surveillance réglementaire et la supervision exercée augmenteront probablement dans les différents pays, et il y aura des interventions ciblées là où aucun progrès concret ne semblera avoir été réalisé, et ce, malgré l'absence d'un mandat réglementaire ou juridique officiel à l'égard de ce changement. Malgré ce climat d'incertitude et même si les entreprises trouvent peut-être que 2021 est encore loin, il ne faut pas sous-estimer la tâche.

Répercussions de l'IBOR

La figure à la page précédente indique de façon générale les répercussions que l'abandon de l'IBOR aura sur une institution financière. Il faut tenir compte de tous les secteurs d'activité, puisque l'IBOR est mentionné dans le profil de tarification ou de gain d'un vaste éventail de produits financiers. Les produits utilisés pour la gestion des risques internes, comme les couvertures, doivent également être pris en considération.

Où sont les marchés?

Le processus visant à remplacer les taux sans risque (TSR) a véritablement commencé. Le taux des prêts garantis à un jour (ou SONIA, qui est le TSR du LIBOR pour la livre sterling), même s'il existe depuis un certain temps, a été mis à jour en 2018; le taux des prêts garantis à un jour (SOFR) pour le dollar américain est négocié activement, tandis qu'en Europe, le taux à court terme pour les opérations d'emprunt libellées en euro (ESTER) sera lancé à la fin de 2019. En Suisse et au Japon, le taux moyen à un jour de la Suisse (SARON) et le taux moyen à un jour de Tokyo (TONA) remplaceront le LIBOR pour le franc suisse (CHF) et le yen japonais (JPY) respectivement. Le Groupe de travail sur le taux de référence complémentaire pour le marché canadien (TARCOM) s'est réuni tous les trimestres depuis l'annonce de la FCA et est en train d'élaborer des plans pour remplacer le taux des opérations de pension à un jour (taux CORRA).

Perspectives d'avenir

De véritables progrès doivent être réalisés en 2019. Les conseils doivent créer un comité directeur supérieur coordonné qui sera chargé de gérer et de superviser la transition et de mettre en place les activités et contrôles clés nécessaires au programme. Les entreprises doivent s'attendre à ce que les organismes de réglementation leur posent des questions sur leurs risques financiers, leur état de préparation en vue de la transition et sur la gestion des risques liés à la conduite. Les entreprises les plus importantes feront probablement l'objet d'examens réglementaires très rigoureux, mais l'ensemble des entreprises, y compris les investisseurs institutionnels, doivent examiner et comprendre le contenu de la lettre de la FCA adressée aux chefs de la direction et veiller à se positionner de manière à pouvoir surmonter les difficultés. Une stratégie de communication claire destinée à la clientèle, étayée par des contrôles rigoureux pour le programme, de la documentation et la gestion des conflits d'intérêts, sera primordiale.

Par ailleurs, les entreprises devront gérer un certain nombre d'incertitudes, notamment la configuration différente de l'IBOR et des TSR, l'absence de structure par échéances des TSR et le coût d'un programme d'une telle envergure.

Pour comprendre les répercussions financières, les entreprises doivent évaluer les risques pour l'ensemble des IBOR, en déterminant les contrats qui doivent être renégociés et la façon de gérer les risques et les vulnérabilités, et les réduire avec le temps. Elles devront décider à quel moment émettre les produits liés aux TSR pour « établir le prix sur le marché » (c'est déjà fait pour certaines) et cesser d'émettre des produits liés à l'IBOR. En outre, il faudra apporter des changements opérationnels et modifier les systèmes.

Abandon du taux interbancaire offert (IBOR)

Le passage des anciens produits basés sur l'IBOR aux TSR pourrait faire des gagnants et des perdants, c'est-à-dire que le montant que paiera ou recevra l'une des parties sera plus élevé ou moins élevé, parce que les méthodes servant à calculer les TSR sont différentes. La gestion des risques liés à la conduite est cruciale dans les transitions de cette nature, et les entreprises devront montrer qu'elles gèrent bien les interactions avec les clients. Celles qui continueront de conclure des contrats basés sur l'IBOR arrivant à maturité après 2021 ou même d'ici 2021 verront augmenter leur exposition à l'IBOR et, en conséquence, les risques connexes. Les entreprises ont besoin d'une stratégie claire pour déterminer à quel moment elles doivent cesser de conclure ces contrats et pour assurer une surveillance et une supervision régulières de leur exposition.

Transformer les perspectives en action

Pour faire progresser le programme d'abandon de l'IBOR, les institutions financières doivent prendre les mesures actives ci-dessous :

- Établir un programme de transition regroupant diverses unités fonctionnelles et régions avec l'appui des hauts dirigeants.
- Créer une feuille de route de transition fondée sur une stratégie de transition et planifier les activités qui ne dépendent pas de ressources externes.
- Cerner les risques et mettre en œuvre des mesures d'atténuation à un stade peu avancé du processus.

Principaux points à retenir

Le programme de transformation lié à l'abandon de l'IBOR sera sans pareil. Les conseils d'administration doivent veiller à établir leur programme. En outre, ils doivent avoir un plan de transition clair et le gérer activement.

Répercussions de la réforme de l'IBOR sur la modélisation des risques selon la RFPN

Des entreprises craignent que le manque de liquidités et de transactions observables, que ce soit avec les nouveaux TSR ou l'ancien IBOR de référence, pendant la transition initiale rende certains facteurs de risque non modélisables. Si ces craintes se concrétisent, les entreprises visées pourraient voir augmenter considérablement les exigences de fonds propres. Certaines se sont adressées aux organismes de réglementation pour demander une dispense à la règle de la RFPN afin que les transactions touchées par l'abandon de l'IBOR soient exemptées.

Cybersécurité

La cybersécurité est une question cruciale qui retient beaucoup l'attention sur le plan réglementaire.

À une époque où le piratage informatique et les atteintes à la protection des données sont devenus monnaie courante au point où l'on s'y attend presque, la cybersécurité continue de faire les manchettes et de dominer le programme de réglementation, qu'il s'agisse de la production de rapports sur les coûts des cybercrimes (et sur les investissements que font les organisations pour améliorer leur programme de gestion des cyberrisques) ou de l'importance accrue accordée à la réglementation de la cybersécurité et à la conformité.

Avec la reconnaissance accrue de l'importance de la gestion des cyberrisques, les superviseurs élargissent leur champ de surveillance au-delà des programmes de gestion des risques de base; la déclaration des atteintes à la protection des données et les répercussions de l'infonuagique sur les risques et la réglementation sont les principaux nouveaux thèmes.

Divulgation : déclaration des atteintes à la protection des données

Le Canada s'est doté d'une loi sur la déclaration obligatoire des atteintes à la protection des données au palier fédéral. En effet, depuis le 1er novembre 2018, les entreprises assujetties à la loi canadienne en matière de protection de la vie privée, la *Loi sur la protection des renseignements personnels et les documents électroniques*, devront consigner et déclarer les atteintes aux mesures de sécurité.

À mesure qu'évoluent les cybermenaces et la législation visant à les éliminer, les organisations doivent adapter leur stratégie d'intervention en cas d'atteinte à la sécurité. Pour atténuer efficacement les cyberrisques complexes d'aujourd'hui, les organisations doivent adopter une approche proactive qui est organisée et exécutée de façon harmonieuse, soit une approche qui transforme un processus à volets multiples en une intervention cohésive.

Pour élaborer ce genre de stratégie d'intervention, les organisations doivent coordonner les mesures prises par leurs diverses fonctions, c.-à-d. services juridiques, protection de la vie privée, assurance, cybersécurité et juricomptabilité. En travaillant ensemble, les équipes devraient être en mesure de gérer l'éventail complet de cyberrisques auxquels leur organisation pourrait être exposée et de s'occuper de la gestion des cyber incidents, de la conservation des preuves et des interventions en cas d'atteinte à la sécurité.

Coût de la non-conformité

- Une intervention inadéquate à une atteinte à la sécurité peut donner lieu à une surveillance réglementaire accrue (p. ex., enquête, audit, examen de tout le programme de protection de la vie privée et sanctions), à des pénalités financières (p. ex., amendes, perte de valeur pour les actionnaires ou poursuites) et entacher la réputation (diminution de la confiance des clients, de la valeur de la marque et des revenus).
- Les cas de non-conformité ne seront pas ignorés, et les atteintes causant un préjudice grave – p. ex., humiliation, tort à la réputation ou à des relations et vol d'identité – ne peuvent être dissimulées. Même s'il appartient aux entreprises de déterminer le moment de déclarer une atteinte à la sécurité, elles sont tenues de le faire rapidement. Elles doivent également être en mesure de fournir au commissaire à la protection de la vie privée, à sa demande, un dossier de toutes les atteintes à la sécurité.
- Le commissaire à la protection de la vie privée est autorisé à publier les atteintes à la sécurité, ce qui accroît le risque de recours collectif.

Cyberrisques

Côté positif

Même si la non-conformité peut avoir de graves répercussions, il est avantageux pour une organisation d'établir un plan d'intervention en cas d'atteinte à la sécurité et un programme général de protection de la vie privée ou d'améliorer ceux existants. Elle peut ainsi :

- Accroître son avantage concurrentiel en renforçant la confiance et la fidélité des clients, en sensibilisant davantage l'ensemble de l'entreprise à la protection de la vie privée et en augmentant l'efficacité des fonctions liées à la protection de la vie privée, à la sécurité, aux technologies de l'information et à la gouvernance des données.
- Réduire les risques grâce à une gestion efficace des cyberrisques.

Répercussions de l'infonuagique

L'infonuagique évolue rapidement. Elle permet d'héberger des données et des applications en ligne auxquelles les utilisateurs peuvent accéder au moyen d'un appareil connecté à internet et qui font partie intégrante de l'entreprise élargie. Comme le nuage crée une séparation entre les personnes et leurs données, il existe des préoccupations inhérentes à la protection des renseignements personnels et à la surveillance réglementaire.

Les organismes de réglementation ont établi des attentes dans ces domaines : protection des données, gestion de l'identité et de l'accès, gestion des fournisseurs, audit, journalisation et surveillance, gouvernance et gestion des risques.

Difficultés

À mesure que d'autres composantes de l'entreprise adoptent l'infonuagique, il devient plus difficile de veiller à ce que les risques déjà identifiés et gérés à l'intérieur de l'organisation soient toujours pertinents et bien gérés dans le nuage. L'utilisation accrue des services infonuagiques a fait augmenter la demande d'assurance concernant les contrôles pour les systèmes à la base de ces services.

Cadre réglementaire

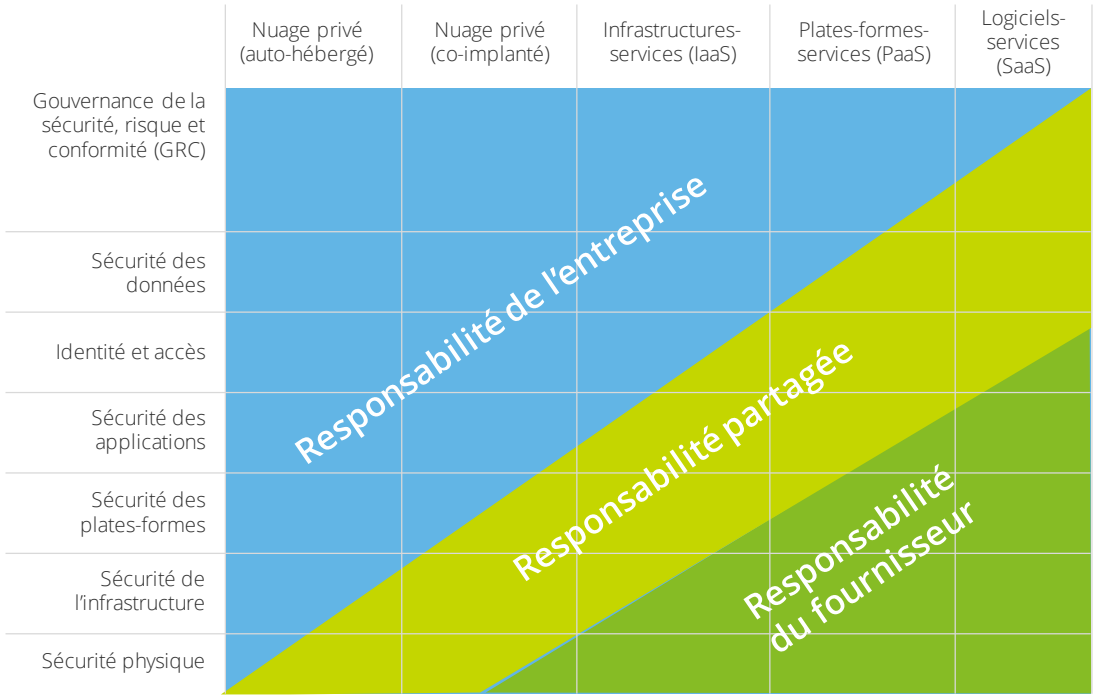
L'élaboration de directives réglementaires se poursuit à l'échelle mondiale. Aucun organisme de réglementation en Amérique du Nord n'a interdit l'utilisation de l'infonuagique. Au Canada, le BSIF n'a pas encore communiqué de position concernant l'infonuagique; entre-temps, les organisations s'en remettent à la ligne directrice B10 du BSIF concernant l'impartition et utilisent les exigences et lignes directrices établies dans d'autres territoires.

Même si les exigences réglementaires sont encore au stade de l'élaboration, les entreprises doivent être au courant des directives ainsi que des préoccupations et risques actuels.

Exigences réglementaires	La plupart des organismes de réglementation ont publié des directives indiquant les exigences précises que doivent respecter les entreprises pour atténuer les risques liés à l'adoption de l'infonuagique.
Risques et préoccupations	Les principaux aspects qui préoccupent les organismes de réglementation sont les suivants : la protection des données; la gestion des identités et des accès; la gestion des fournisseurs; les droits d'audit; la journalisation et la surveillance; la gestion de la gouvernance et des risques; l'emplacement des données; le nettoyage des données.
Participation au programme réglementaire	En attendant que des exigences normalisées précises concernant l'infonuagique soient établies (p. ex., FedRamp), les organisations devront collaborer avec les acteurs du secteur, les agences, les fournisseurs de services infonuagiques et les organismes de réglementation afin de respecter les exigences réglementaire générales.

Cyberrisques

Tandis que les institutions financières font la transition à l'infonuagique pour leurs opérations et applications d'affaires, qui est gérée par des fournisseurs de services infonuagiques, la gestion des cyberrisques et de la conformité devient une responsabilité partagée par l'institution financière et son fournisseur de services infonuagiques.



Transformer les perspectives en action

Cyberrisques

- Les organisations doivent améliorer le programme actuel de gestion des risques afin d'y inclure un processus de contrôle diligent ou un tableau d'analyse des risques ainsi que des politiques et procédures servant à gérer les risques associés aux services infonuagiques.
- On doit adopter un cadre d'infonuagique pour définir une stratégie de prestation des services infonuagiques, une architecture et un modèle opérationnel durable.
- Il faut envisager d'inclure une clause sur le « droit d'audit » ou d'autres clauses concernant le respect des exigences de sécurité dans le contrat conclu avec le fournisseur de services infonuagiques pour obtenir une assurance.
- Une stratégie officielle pour les communications avec les organismes de réglementation doit être élaborée pour démontrer la compatibilité avec la directive de réglementation concernant l'infonuagique.

Fusion de la cybersécurité

Compte tenu des nombreuses menaces en constante évolution, le service des fraudes et celui de la cybersécurité doivent collaborer afin de réduire les cybermenaces. Les attaques antérieures ont révélé l'existence de liens étroits entre les deux et ont fait ressortir que de nombreuses fraudes découlaient de problèmes de cybersécurité.

Un concept émergent consiste à créer un **centre de fusion de la cybersécurité** qui intègre des équipes fonctionnelles de différentes parties de l'organisation. Ces équipes possèdent des capacités fonctionnelles très diversifiées, notamment en matière de renseignements, de juricomptabilité, d'opérations, de sécurité matérielle, de fraude, de science des données et d'autres domaines connexes. Elles sont conçues pour assurer une connaissance de la situation en tout temps, communiquer rapidement des renseignements dans l'ensemble de l'organisation et éliminer les obstacles qui empêchent l'organisation d'agir en plus de faire office de point central en cas de crise. Les équipes des centres de fusion peuvent également travailler à l'échelle de l'écosystème (partenaires, fournisseurs, clients, etc.) pour bien faire connaître la situation. Par conséquent, les entreprises prennent connaissance des menaces plus rapidement et de façon plus efficace, ce qui permet de réduire les coûts et de prendre des mesures d'atténuation avant, pendant et après une cyberattaque.

Fusion de la cybersécurité

Principaux points à retenir

L'adoption des meilleures pratiques de gestion avisée des risques, jumelée à la collaboration entre le service des fraudes et celui de la cybersécurité, sera essentielle pour promouvoir la sécurité, la protection de la vie privée et la résilience afin de renforcer la confiance dans l'infonuagique.

Transformer les perspectives en action

Centre de fusion de la cybersécurité

- La convergence des gens, des processus, des technologies et des données de différents domaines tels que la cybersécurité, la fraude et la lutte contre le blanchiment d'argent assurera une visibilité accrue pour prédire, prévenir et détecter les attaques dans l'ensemble des canaux.

Gouvernance

- Chaque fonction (cybersécurité, fraude, lutte contre le blanchiment d'argent, sécurité de l'entreprise, etc.) doit continuer d'assumer la responsabilité de son mandat existant et d'en assurer l'exécution. Cependant, il doit y avoir un représentant de chaque fonction au centre de fusion (rotation des ressources entre la fonction et le centre de fusion).
- La meilleure pratique consiste à établir un comité directeur des crimes financiers (composé d'un représentant de chaque fonction) dont fait partie le directeur du centre de fusion (nouveau rôle) pour assurer la réussite de cette démarche de collaboration interfonctionnelle.

Processus et compétences

- Les processus et les compétences propres à chaque fonction (gestion de cas, résolution d'identité, enquêtes, etc.) doivent continuer d'être appliqués en vue de l'intégration, de l'alignement ou de la convergence des processus pour permettre de détecter plus activement les menaces interfonctionnelles.

Données, technologie et installations

- Il faut identifier des éléments de données en particulier provenant de chaque fonction qui peuvent faciliter l'élaboration de scénarios pour le centre de fusion.
- Il faut mettre en œuvre une solution permettant de transmettre des champs de données choisis à la pile technologique du centre de fusion.

Technologie et installations

- Le centre de fusion doit comporter une salle de crise commune pour favoriser la collaboration et l'innovation.

Conformité numérique

Un concept émergent

Avec la révolution numérique, la société a assisté à l'évolution des outils analogiques, électriques et mécaniques, qui utilisent la technologie numérique accessible de nos jours. Avec les innovations technologiques, et notamment la numérisation, qui ont engendré une croissance sans précédent dans le secteur des institutions financières, la conformité numérique ne représente toujours qu'un objectif inspirant pour la plupart des institutions financières. Dans cette perspective, elle se veut un terme général désignant l'utilisation de la technologie au service des pratiques de conformité. Les incidences pourraient se faire ressentir sur les talents, les processus et mécanismes de contrôle, les données et l'infrastructure. Pour le moment, les organisations en sont encore à des stades préliminaires d'application durable de la numérisation des pratiques de conformité.

Les entreprises vont de l'avant, mais les pratiques de conformité peuvent-elles suivre la cadence?

Les institutions financières adoptent de plus en plus l'intelligence artificielle (IA) et l'apprentissage machine (AM) pour faire des affaires et prendre des décisions. En 2018, les institutions financières ont collaboré avec les instituts d'IA, elles ont investi dans la recherche sur l'IA et elles ont acheté des entreprises d'IA ou y ont fait des investissements. Les capacités que l'IA apporte aux banques sont intimement reliées à la création d'autres innovations technologiques. En août 2018, le Forum économique mondial et Deloitte mondial ont publié **The New Physics of Financial Services** (en anglais seulement), un rapport conjoint sur leur étude des répercussions stratégiques, opérationnelles, réglementaires et sociétales de l'IA sur le secteur des services financiers. Le rapport démontre que l'IA change la physique des services financiers, affaiblissant les liens qui unissaient les éléments constitutifs des institutions financières actuelles, et ouvre la porte à des modèles d'exploitation entièrement nouveaux.

À mesure que les banques procèdent à l'innovation, il est impératif pour elles de se doter d'un programme de conformité progressif pour assurer la sécurité des consommateurs et de la banque tout en facilitant la réalisation des activités. Même si la numérisation des pratiques est un impératif d'affaires de plus en plus important, les investissements affectés spécifiquement à ce type de stratégies se font rares. Cette inertie est un symptôme de l'absence généralisée d'innovation dans la gestion des risques liés à la conformité. Même si les services bancaires se numérisent de plus en plus, le rythme des progrès semble entravé par l'incapacité de la deuxième ligne de défense de la banque à s'adapter à l'évolution de l'environnement.

Les pionniers

Un nombre restreint mais croissant d'organisations expérimentent l'utilisation des technologies de numérisation pour leurs processus quotidiens de conformité. Leur expérience sert de point de référence pour les autres entreprises qui souhaitent aussi numériser leurs pratiques de conformité. D'après les études de cas réunies par Deloitte pour les besoins d'une analyse, on constate que la numérisation dans le domaine de la conformité est particulièrement prometteuse pour les applications suivantes :

- les décisions d'affaires et la gestion des processus dans le but d'intégrer les mécanismes de contrôle de la conformité aux systèmes d'opérations pour permettre la prise de décisions en temps réel.
- l'automatisation, la robotique et l'analytique avancée pour la surveillance et la mise à l'essai de pratiques.
- l'examen amélioré de la documentation, notamment à l'aide de Deloitte Intelligent Contract Execution (D-ICE), qui combine un logiciel de reconnaissance optique de caractères à l'AM et au traitement du langage naturel pour examiner les documents de marketing et d'information en fonction des attentes réglementaires. Cela peut permettre d'améliorer l'efficacité et la qualité pour tout un éventail de cas d'utilisation.

Conformité numérique

Le chef de la conformité peut décider d'investir dans l'une ou l'ensemble de ces initiatives. La collaboration entre le chef de la conformité, le chef de l'exploitation et d'autres membres de l'équipe de direction sera importante pour déterminer les pratiques de conformité pour lesquelles la numérisation serait le plus avantageuse. Il serait préférable d'envisager de numériser entièrement la fonction de conformité pour les première et deuxième lignes de défense. La décision dépendra en grande partie des stratégies, des capacités et des besoins actuels de la banque ainsi que des technologies et compétences existantes.

Avantages

Pour les entreprises qui ont procédé à l'adoption à un stade précoce et qui ont intégré les exigences de conformité (aux processus numériques de première ligne, aux systèmes d'opérations, etc.), les avantages ont été considérables :

- Facilitation de la prise de décisions en temps réel.
- Identification instantanée des cas de non-conformité et prévention des problèmes de conformité potentiels.
- Réduction des coûts grâce à l'automatisation des tâches manuelles répétitives (p. ex., accès à des produits multiples et aux systèmes sources de connaissance du client à l'aide de la robotique).
- Intégration harmonieuse de la conformité à l'expérience client.
- Amélioration de l'efficacité de la surveillance et de la mise à l'essai des processus grâce à l'automatisation, à la robotique et à l'analytique avancée.

Contexte réglementaire

La gestion des risques liés à l'innovation est une priorité tant pour les institutions financières que pour les organismes de réglementation. Comme les applications d'IA et d'AM sont relativement nouvelles, il n'existe pas de normes internationales connues propres à ce domaine. Les organismes de réglementation novateurs adoptent les technologies de pointe et s'attendent à ce que les institutions financières évoluent et s'adaptent. Par exemple, les autorités monétaires de Singapour ont annoncé une feuille de route progressive visant à réduire le dédoublement des données et à automatiser la présentation des données par les institutions financières.

Messages clés

- Les entreprises et les responsables de la conformité doivent collaborer, de manière à intégrer les exigences liées à la conformité réglementaire aux processus numériques de première ligne et à surveiller automatiquement la conformité continue. Ceux qui collaboreront, tout en soutenant leur mandat en parallèle, auront de meilleures chances de réussite.
- Il est important de disposer des talents nécessaires pour faciliter le changement. Cela peut exiger une transformation des talents afin que le profil des talents affectés à la conformité soutienne les capacités numériques. On devra notamment engager des professionnels de la conformité qui sont au fait des nouvelles technologies et former des partenariats avec des experts en conformité pour permettre le jumelage et l'échange des connaissances.
- La numérisation des pratiques de conformité ne se limite pas à l'automatisation des processus et à l'acquisition des plus récentes technologies nécessaires à cette fin. Les organisations qui s'y prennent de la bonne manière mettront également l'accent sur les capacités de leurs ressources et veilleront à les améliorer pour les aligner sur la numérisation. Il pourrait s'agir notamment de fournir du meilleur matériel ou de meilleurs logiciels aux employés (p. ex., tablettes ou outils d'analytique) pour favoriser la collaboration et instaurer une mentalité d'amélioration continue.

Conformité numérique

- Les responsables de la conformité doivent faire en sorte d'avoir les capacités voulues pour exercer leur mandat de surveillance dans un contexte d'adoption des technologies émergentes. Par exemple, les capacités requises pour surveiller la conformité de façon indépendante de processus majoritairement manuels pourraient être bien différentes de celles requises pour surveiller la conformité de façon indépendante de solutions reposant sur l'IA.
- Les pratiques de conformité doivent, dans la mesure du possible, permettre de faire le suivi des avantages pour montrer la valeur ou le rendement du capital investi. Dans le cas contraire, elles doivent faire en sorte qu'un autre groupe puisse faire le suivi de ces données et les communiquer.

Principaux points à retenir

Le recours à la technologie pour gérer la conformité réglementaire accroît l'efficacité de la gestion des risques liés à la conformité et l'efficacité opérationnelle. Cela devrait permettre de faire des économies opérationnelles à long terme et de prévenir les problèmes de conformité.

Transformer les perspectives en action

- Une feuille de route stratégique peut aider à concrétiser la conformité numérique. Il faut déterminer l'objectif à cet égard.
- La priorité est d'améliorer les procédures qui utilisent des processus structurés fondés sur des règles où la technologie peut permettre d'automatiser des tâches courantes, permettant ainsi aux professionnels de la conformité de se concentrer sur des problèmes plus complexes et la gestion des exceptions.
- Tandis que les institutions financières amorcent un nouveau parcours menant à la conformité numérique, avec l'aide de données massives ou d'applications d'IA, elles devront connaître l'incidence que l'utilisation de ces technologies a sur leur profil de risque global.
- Un effort concerté est nécessaire pour faire avancer les choses au chapitre de la numérisation; si cela fait partie du travail accessoire des employés les plus performants, la vision ne se concrétisera pas.
- Il faut travailler activement avec le personnel de première ligne pour apporter une solution aux processus numérisés de conformité; les progrès technologiques signifient que les processus et contrôles des première et deuxième lignes peuvent être harmonisés.
- Pour assurer la conformité, il faudra avoir accès à des données de bonne qualité. Il sera crucial de pouvoir extraire des données de nombreuses sources et de les regrouper pour obtenir une vue d'ensemble complète. L'IA ne pourra être utile que si les données sur lesquelles reposent ses algorithmes le sont aussi.

Crimes financiers

Les pressions pour s'attaquer aux crimes financiers sont plus importantes que jamais. Au moyen des technologies numériques, les criminels commettent des crimes financiers de plus en plus complexes dans l'ensemble des canaux, des régions et des secteurs. Pourtant, les institutions financières n'en continuent pas moins de s'en remettre à des modèles d'exploitation qui sont cloisonnés, inefficaces et rigides et font double emploi pour détecter et prévenir les crimes financiers, ce qui donne lieu à un rendement sous-optimal et, dans certains cas, à des pénalités et à des amendes. Bien souvent, les institutions financières n'ont pas de perspective globale du client pour l'ensemble des produits, des canaux et des régions. Il devient de plus en plus complexe de gérer les risques liés aux crimes financiers, puisque les méthodes criminelles évoluent, les nouvelles technologies rehaussent les attentes des clients et la nouvelle réglementation fait augmenter les coûts liés à la conformité. Pour éviter de se faire distancer, les institutions financières doivent reconnaître le risque d'atteinte à la réputation auquel elles sont constamment exposées et revoir leur approche pour atténuer les crimes financiers.

Risques découlant de l'augmentation de la numérisation

Malgré les avantages de la numérisation, les nouvelles technologies représentent pour les institutions financières de nouvelles formes de risque. En plus de rehausser les attentes en temps réel des clients et d'accroître la concurrence parmi les institutions financières, la numérisation exige la gestion et la surveillance d'une quantité imposante et grandissante de données. En outre, les technologies de numérisation fournissent aux criminels de plus en plus de points d'entrée aux services bancaires, ce qui crée davantage d'occasions de perpétrer des crimes financiers. Les institutions sont également exposées au risque que des initiés donnent la capacité d'agir à des parties représentant des menaces externes, que ce soit consciemment ou non.

Difficultés

Malgré le contexte en constante évolution, la plupart des institutions financières continuent de s'en remettre à des mécanismes désuets de gestion des risques. Les modèles d'exploitation cloisonnés qu'elles utilisent à l'heure actuelle découlent souvent de changements apportés après coup afin de suivre le rythme des nouvelles exigences réglementaires. En conséquence, les institutions financières gèrent les crimes financiers avec plusieurs équipes, chacune utilisant un éventail d'outils et de technologies et ayant des structures hiérarchiques différentes, ce qui complique la communication optimale de l'information dans l'ensemble de l'organisation.

Comment les institutions financières réagiront-elles?

Compte tenu de ces importantes difficultés, de nombreuses institutions financières se demandent à quel point elles veulent être considérées comme des leaders du marché au chapitre de la protection des clients contre les crimes financiers tout en cherchant la façon optimale d'obtenir les résultats souhaités dans leur environnement d'exploitation actuel. Beaucoup d'entre elles cherchent le moyen le plus rentable de réinitialiser leur modèle d'affaires et leur organisation afin de réduire au minimum leur vulnérabilité en matière de protection des clients tout en gérant leurs bénéfices.

La voie de l'avenir

Il est vrai que la voie de l'avenir est simple : élaborer une approche globale et intégrée qui reconnaisse que les crime financiers sont interreliés et qu'ils touchent plusieurs produits et canaux. Cependant, la création d'une infrastructure pour les crimes financiers est en réalité beaucoup plus complexe. Cela nécessite la transition à un cadre intégré offrant une capacité opérationnelle unique et unifiée qui soit à la fois souple et adaptable. Ce cadre exige l'intégration des données et des systèmes pour procurer une vision à l'échelle de l'entreprise de l'identité et du risque, l'élaboration d'un langage standard servant à définir les crimes financiers pour l'ensemble de la banque et les diverses typologies de risques auxquelles elle est exposée, ce qui permettra une identification, un classement et une évaluation efficaces. Le cadre doit également prévoir une plate-forme technologique commune et l'analytique avancée pour permettre la prise de décisions en temps réel et la détection proactive des menaces.

Crimes financiers

Occasions

L'adoption d'une approche intégrée axée sur les services partagés peut procurer des avantages à toute l'entreprise, notamment :

- La capacité de protéger le client et la banque contre les risques liés aux crimes financiers compte tenu des nouvelles réalités.
- L'alignement des objectifs et des mandats dans l'ensemble des canaux où sont perpétrés des crimes financiers avec des rôles et des responsabilités bien définis.
- Des économies d'échelle et la réduction générale des coûts opérationnels grâce à l'automatisation et à la réduction du double emploi.
- Une perspective globale du client et une expérience client améliorée.
- L'amélioration de l'échange de l'information dans l'organisation grâce à un seul entrepôt de données.
- De meilleures perspectives sur les crimes financiers et des mesures d'atténuation claires.
- L'efficacité accrue grâce à l'adoption et à l'utilisation de l'analytique avancée des données et des technologies numériques.
- La détection proactive des menaces dans une plate-forme unifiée, ce qui permet aux institutions financières de mieux se protéger elles-mêmes ainsi que leur réputation.
- Le contrôle amélioré des pertes et la réduction des fraudes.

Principaux points à retenir

D'après les tendances actuelles, les menaces liées aux crimes financiers et leurs conséquences ne feront qu'augmenter, ce qui fera de la résilience par rapport aux crimes financiers un impératif crucial pour le succès à long terme des institutions. Il faut élaborer une nouvelle approche intégrée pour gérer ces risques et protéger la réputation des banques et des clients.

Transformer les perspectives en action

Afin de prévenir et d'atténuer les menaces internes et externes pour les banques tout en offrant une expérience client de premier plan, les institutions financières doivent mettre en œuvre une approche globale pour la gestion des crimes financiers qui s'aligne sur les rôles et les responsabilités selon un modèle de services partagés centralisés, qui comprend :

- L'intégration des fonctions liées à la cybersécurité, aux fraudes internes et externes et au blanchiment d'argent.
- La capacité d'examiner les crimes financiers du point de vue numérique, en temps réel, ce qui met efficacement, et proactivement, à profit les technologies et l'analytique avancée.

Ces initiatives sont les premières étapes menant à la création d'une unité des crimes financiers capable de gérer les menaces à l'encontre des institutions financières et de leurs clients.

Technologies financières

Comment s'y retrouver dans le contexte réglementaire en évolution tandis que le marché des technologies financières arrive à maturité

Les nouveaux investissements dans les entreprises de technologies financières (*Fintech*) demeurent importants, et le nombre d'acquisitions et de partenariats en matière de services financiers est en hausse. C'est le signe d'un marché des technologies fintech arrivant à maturité où les banques traditionnelles et les entreprises de technologies fintech unissent leurs efforts pour offrir des services innovateurs. Les banques traditionnelles reconnaissent les avantages des technologies innovatrices et concurrentielles pour répondre à la demande des clients, tandis que les entreprises de technologies financières voient les avantages associés à l'infrastructure et aux fonds propres qu'apportent ces partenariats.

Deux événements importants se sont produits dans l'environnement réglementaire des fintechs aux États-Unis à la fin de juillet 2018 lorsque le Département du Trésor a publié un rapport intitulé *A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*. Ce document présentait les principes de base d'un cadre réglementaire pour le secteur des technologies financières ainsi que des recommandations. Une des principales recommandations était que l'Office of the Comptroller of the Currency (OCC) aille de l'avant avec la charte nationale sur les technologies financières. Le même jour, l'OCC a annoncé qu'il commencerait à accepter les demandes de charte de banque à vocation particulière pour les fintechs qui offrent des produits et services bancaires.

Plus tard durant l'été, de plus en plus soucieux de trouver un moyen plus efficace pour les fintechs d'interagir avec eux, 12 organismes de réglementation des quatre coins du monde ont annoncé la création du Global Financial Innovation Network (GFIN), qui repose sur la proposition qu'a faite la Financial Conduct Authority du Royaume-Uni au début de l'année de créer un bac à sable mondial. Parmi les organismes de réglementation participants figure la Commission des valeurs mobilières de l'Ontario (CVMO), qui a été le premier organisme de réglementation canadien à créer son propre bac à sable en 2016 : la Rampe de lancement de la CVMO.

Dans un rapport de 2018, Deloitte décrit le changement du secteur des fintechs aux États-Unis [9]. Le rapport révèle que le nombre de nouvelles entreprises de technologies financières en démarrage a augmenté, passant de 177 en 2008 à 668 en 2014. Cependant, en 2015, le taux de création d'entreprises dans le secteur des fintechs a commencé à baisser, et il n'y a eu que 41 entreprises en démarrage au cours des 9 premiers mois de 2017. Dans la catégorie des entreprises de technologies financières spécialisées dans les services bancaires et les marchés financiers, le nombre d'entreprises en démarrage a atteint un sommet, soit 281 en 2012, puis a diminué de façon constante pour s'établir à seulement 10 durant les 9 premiers mois de 2017. Le secteur semble arriver à maturité et, compte tenu de la concurrence qui existe parmi les entreprises de technologies financières elles-mêmes, certaines quittent le secteur, ce qui donne matière à réflexion à d'autres qui envisagent d'y faire leur entrée.

Malgré la diminution du nombre d'entreprises en démarrage, le financement des nouvelles entreprises fintechs demeure solide aux États-Unis, où un virage vers les investissements dans des entreprises ayant atteint un stade plus avancé s'opère dans un marché arrivant à maturité. Au moment du rapport, on comptait plus de 2 000 entreprises dans les domaines des opérations bancaires, de la mobilisation de fonds, de la gestion financière, des dépôts et prêts ainsi que des paiements. Les acquisitions sont en hausse, puisqu'il y a eu environ 50 acquisitions dans la catégorie des entreprises spécialisées dans les services bancaires et les marchés financiers au cours des 9 premiers mois de 2017.

Technologies financières

Pour les banques traditionnelles, les entreprises fintechs peuvent représenter une menace sur le plan de la concurrence ou une occasion d'améliorer les services et les processus grâce à des partenariats stratégiques. Bon nombre de banques ont opté pour les partenariats et ont même acquis des entreprises de technologies financières afin de moderniser leurs propres activités et services.

Même si l'OCC a annoncé qu'il était prêt à commencer à accepter les demandes de charte de banque à vocation particulière provenant des entreprises de technologies financières aux États-Unis, celles-ci ne sont aucunement obligées de demander une charte nationale. Pourtant, il pourrait être utile d'envisager de demander une charte semblable à l'OCC, surtout pour les entreprises de technologies financières qui exercent des activités dans plusieurs États. Cependant, la promesse d'une réglementation plus uniforme pourrait présenter des inconvénients, selon le modèle d'affaires des entreprises de technologies financières. Parmi ces inconvénients, mentionnons l'alourdissement des exigences réglementaires et, au début, une contestation judiciaire de la part des États, dont un grand nombre s'opposent à la charte sur les technologies financières de l'OCC.

Pour l'OCC, une banque nationale à vocation particulière (BNVP) s'entend d'une banque nationale qui exerce un éventail restreint d'activités bancaires ou fiduciaires, qui a une clientèle cible limitée, qui intègre des éléments non traditionnels ou qui a un plan d'affaires bien ciblé. La charte de l'OCC sur les technologies financières est un sous-ensemble de tout cela. Les entreprises de technologies financières à charte peuvent exercer des activités bancaires de base comme offrir l'encaissement des chèques et accorder des prêts, mais elles ne peuvent pas accepter des dépôts et ne seront pas assurées par la Federal Deposit Insurance Corporation (FDIC).

Cependant, pour d'autres entreprises fintechs, il pourrait être très avantageux de former des partenariats avec des banques afin de tirer parti des avantages et capacités uniques de chaque entité. Le fait d'unir les forces pourrait créer plus de valeur qu'une seule entreprise pourrait le faire à elle seule.

Les banques et les entreprises fintechs doivent chercher à connaître les capacités et les besoins les unes des autres en participant à des tables rondes et des forums sectoriels qui réunissent des banques traditionnelles et des entreprises fintechs. En outre, elles doivent se tenir au courant des nouveautés en matière de réglementation qui concernent les entreprises de technologies financières et les ententes de partenariat, en cherchant sans cesse des moyens d'améliorer leurs services grâce aux partenariats ou même aux fusions.

Le secteur des fintechs au Canada est différent de celui de son voisin du Sud. S'il est vrai que le Canada est propice à l'évolution du secteur, des obstacles peuvent empêcher les entreprises fintechs d'arriver à maturité et de réaliser leur plein potentiel. La croissance de celles-ci ne s'est pas faite au même rythme que leurs homologues américaines, et le retard dans l'adoption des technologies financières est principalement attribuable à quatre facteurs :

- La crise financière a eu une incidence relativement faible, ce qui a évité le bouleversement des modèles d'affaires qui a permis aux entreprises fintechs de prospérer dans d'autres pays.
- Le haut degré de confiance dans le secteur financier est attribuable à la qualité, la diversité et la complexité de ses institutions financières.
- Le secteur canadien des services financiers est à la fois relativement petit et très concurrentiel, ce qui diminue son importance en tant que marché stratégique pour les entreprises fintechs qui envisagent de prendre de l'expansion.

Technologies financières

- Jusqu'ici, les organismes de réglementation canadiens n'ont rien fait pour encourager l'innovation, et le cadre de réglementation canadien est considéré comme un obstacle à l'adoption des technologies financières au pays. Par exemple, les entreprises américaines ont instauré les modèles de prêts entre pairs qui ont eu du succès, mais une offre similaire au Canada n'a pas permis d'assurer un fonctionnement efficace à l'intérieur du cadre réglementaire de la CVMO.

Quoi qu'il en soit, le secteur canadien des fintechs continue d'évoluer, surtout dans le domaine de l'IA, en fait le Canada est considéré comme un chef de file mondial pour ses innovations. En 2018, des institutions financières ont collaboré avec des organisations d'IA, investissant dans la recherche en IA et acquérant ou finançant des entreprises d'IA.

Principaux points à retenir

À mesure que la réglementation sur les services financiers continue d'évoluer, mentionnons notamment la création par le gouvernement canadien du Comité consultatif sur un système bancaire ouvert jumelée à la priorité que le secteur des services financiers continue d'accorder à la modernisation des paiements, la tendance à la hausse des activités dans le secteur des technologies financières va probablement se poursuivre.

Transformer les perspectives en action

- Dans le cas des institutions financières traditionnelles, les entreprises de technologies financières continueront probablement de se concentrer sur les segments de la chaîne de valeur, qui représente la plus grande source de désagréments pour les clients tout en offrant les occasions de profit les plus importantes.
- Les entreprises de technologies financières qui ont le plus de chance de réussir seront celles qui sont le plus aptes à tirer parti des données sur les clients provenant des différentes plates-formes et qui n'ont pas besoin d'un montant excessif de fonds propres réglementaires.
- La coexistence de l'analytique avancée, des exigences en matière de protection des clients, de la tendance concernant le système bancaire ouvert et l'intelligence artificielle pourrait créer des conditions contribuant à accélérer la transformation des modèles d'affaires et à procurer de nouvelles sources de revenus.
- Les institutions financières doivent tenir compte de ces facteurs et élaborer leur propre vision de la valeur stratégique qu'elles procurent à leurs clients pour saisir les occasions que créera la combinaison de ces forces.

Intégration des données

Cadre visant à améliorer la qualité, l'intégrité et la disponibilité des données.

La qualité et la disponibilité des données sont des facteurs de plus en plus importants pour tous les aspects de la gestion des risques et de l'observation de la réglementation. Pour pouvoir les assurer, la gestion et la qualité des données ne peuvent plus relever uniquement de la haute direction ou de hauts dirigeants précis comme le chef des finances, le chef de la gestion des risques ou le chef des données. Il doit plutôt s'agir d'une fonction de l'entreprise entière avec des responsabilités partagées et des obligations de rendre compte sur les trois lignes de défense.

Les propriétaires de données dans le secteur des institutions financières doivent se poser les questions suivantes : la qualité des données est-elle suffisante pour l'usage prévu? Les origines des données sont-elles claires et dûment consignées? Les définitions et les normes relatives aux données sont-elles définies et sont-elles les mêmes dans toute l'entreprise?

Dernièrement, les exigences relatives à la présentation de l'information ont été réduites grâce à la diminution du fardeau imposé par les organismes de réglementation, des lois d'allègement de la réglementation et l'adaptation des exigences en matière de données. Ces réductions ne changent cependant rien aux attentes des organismes de réglementation pour la gestion de données. Une partie des réductions ont été contrebalancées par de nouvelles exigences en matière de données, en particulier pour les grandes entreprises complexes, et la nouvelle tendance générale consiste à demander des données détaillées pour chaque produit à une plus grande fréquence. Voilà qui fait ressortir à quel point de bonnes pratiques de gestion des données d'entreprise et de responsabilisation sont importantes.

Les attentes réglementaires par rapport aux données d'entreprise portent avant tout sur trois aspects :

- Renforcer la gouvernance et de la surveillance.
- Acquérir des compétences en matière de données dans toute l'entreprise.
- Etablir une approche intégrée de gestion des données.

Le cadre est applicable non seulement à la présentation d'information pour les besoins de la réglementation, mais à toutes les activités relatives aux données, comme la divulgation de l'information publique, la gestion des liquidités, la gestion des risques et les rapports de gestion.

Renforcer la gouvernance et la surveillance

L'industrie bancaire évolue et est en train de mettre au point son approche de gouvernance et de surveillance des données. À mesure que les pratiques deviennent mieux établies, les grandes institutions financières évaluent comment leurs processus de gestion des données s'alignent sur le modèle d'exploitation de l'organisation. L'objectif d'un cadre de gouvernance et de surveillance est d'élaborer, de communiquer et de surveiller des normes et politiques efficaces en matière de données. Les normes et politiques sont les bases mêmes de l'implantation d'un bon environnement de gestion des données, et l'un des impératifs est d'avoir des définitions uniformes pour les données et des normes relatives à la qualité des données. Un autre impératif consiste à se doter d'une méthode permettant de déterminer les éléments de données critiques. L'entreprise doit, pour ce faire, connaître l'origine des données, les utilisations des données en aval et les effets sur tous les utilisateurs des données (y compris ceux en dehors de l'entreprise).

Bien souvent, la plus grande difficulté pour les institutions financières à cet égard est de réaliser un changement de culture. Pour avoir des programmes efficaces de gestion des données à l'échelle de l'entreprise, il faut le soutien de la haute direction et du conseil d'administration.

Intégration des données

Sans un changement de culture et le soutien de la haute direction, les principaux volets du processus de gouvernance, soit la responsabilisation des principales parties prenantes, notamment les gammes de services, ne pourront vraisemblablement pas être réalisés.

Pour assurer une bonne supervision et une responsabilisation efficaces, on doit procéder à des mesures et à des contrôles fondés sur des critères quantitatifs d'évaluation de la qualité des données. Ces mesures servent à rationaliser et à appliquer la responsabilisation au niveau du propriétaire de données ou de la gamme de services. Les responsables de la surveillance doivent aussi être chargés de recueillir de l'information sur les problèmes relatifs aux données et d'en assurer le suivi, idéalement en utilisant un seul système central. Pour analyser les problèmes relatifs aux données, il faut adopter une perspective globale par rapport à l'entreprise, de manière à identifier tout problème systémique et à s'en remettre à des niveaux hiérarchiques supérieurs lorsque les risques le justifient.

Contrôles de la qualité des données

Pour qu'une structure de gouvernance des données puisse être efficace, il faut notamment adopter des mécanismes de contrôle servant à assurer l'intégrité des données. Les programmes d'assurance de la qualité des données ne peuvent reposer sur une seule personne ou une seule action. En effet, pour qu'un programme soit efficace, il faut se doter d'un service d'assurance de la qualité indépendant qui procède à des tests détaillés complets basés sur un calendrier de planification pluriannuel tenant compte des incidences des éléments de données critiques qui sont complétés par une évaluation des risques. Des programmes efficaces d'assurance de la qualité des données comprennent aussi des rapprochements entre des ensembles de données. Ces rapprochements constituent un outil indispensable pour déceler les problèmes systémiques relatifs aux données et assurer l'exhaustivité des données.

Acquérir les compétences liées aux données dans toute l'entreprise

Avec l'importance accrue accordée à la qualité des données et le besoin de plus en plus grand d'obtenir des données détaillées par produit, les responsabilités des propriétaires de données (qui appartiennent le plus souvent à une gamme de services en particulier) en ce qui concerne la qualité des données ont augmenté. Afin de répondre aux attentes réglementaires, les gammes de services, le service des finances et les autres services participant à la compilation de données doivent avoir une expertise en gestion et en analytique des données.

Bien souvent, les propriétaires de données connaissent bien leurs données dans le contexte de leurs propres activités, mais ils ont une connaissance limitée des effets de leurs données sur les autres utilisateurs de l'ensemble de l'entreprise. Voilà pourquoi la première étape pour les gammes de services consiste à se renseigner sur les normes et programmes relatifs aux données qui existent déjà dans l'entreprise. Une formation de sensibilisation en bonne et due forme est importante pour la haute direction et pour tout le personnel participant à la diffusion de données dans le reste de l'entreprise. La formation de sensibilisation, qui varie selon le rôle, aide les propriétaires de données à savoir comment leurs données sont utilisées par le reste du personnel de l'entreprise.

À mesure que les exigences liées aux données deviennent de plus en plus complexes, il sera encore plus nécessaire d'avoir des spécialistes sachant bien interpréter comment les exigences réglementaires s'appliquent aux produits et aux opérations de l'entreprise. Pour ce faire, les propriétaires de données et les responsables des rapports (soit les services chargés d'établir les rapports) devront avoir accès à un bassin de gens de talent qui sont au courant des exigences de fonds propres, de la gestion des liquidités et des définitions générales associées à la réglementation.

Établir une approche intégrée de gestion des données

Traditionnellement, les gammes de services ont souvent utilisé des architectures distinctes pour les données et les TI. Cependant, le cloisonnement ne permet plus de remplir les exigences liées à la réglementation ni les besoins en matière de

Intégration des données

données des entreprises d'aujourd'hui. Pour avoir un programme de gestion des données très efficace, il faut établir une approche intégrée incluant les données sur les finances, la réglementation, les risques et les fonds propres.

À mesure que les données exigées deviennent de plus en plus détaillées et complexes, il sera aussi plus important de se doter d'outils permettant d'analyser et de valider les données. Par ailleurs, l'intégration permettra d'améliorer l'accès aux données dans l'ensemble de l'entreprise. Il est également plus facile d'appliquer l'analytique des données et les technologies d'IA à des ensembles de données, de manière à améliorer les capacités de l'entreprise en matière de données et l'efficacité des processus. C'est quelque chose de particulièrement important pour les données relatives aux produits et opérations comportant un grand nombre d'attributs de données.

Principaux points à retenir

L'évolution des pratiques relatives aux données dans le secteur bancaire continuera d'être influencée par le besoin de plus en plus grand d'accéder à des données détaillées sur chaque produit. Pour la planification ou la correction de données, les institutions financières devraient envisager la transition à des pratiques mieux établies permettant d'améliorer la qualité, l'intégrité et l'accessibilité des données.

Transformer les perspectives en action

- Les institutions financières doivent éliminer les obstacles à la gestion intégrée des données qui découlent des pratiques traditionnelles. La transition à un environnement intégré pour les données devrait être soutenue par un programme de gérance des données à l'échelle de l'entreprise englobant ce qui suit :
  - Les clients
  - Les gammes de services
  - Les produits
  - Les entités juridiques
- Le programme nécessite une expertise en pratiques et structures de gestion des données et de culture organisationnelle permettant d'aborder les données et d'exercer les activités en allant au-delà de la stricte hiérarchie.
- Les institutions financières doivent se concentrer sur les stratégies d'innovation encourageant une culture d'échec rapide et d'apprentissage accéléré pour tirer parti du plein potentiel à l'aide de l'expérimentation.
- Les institutions financières doivent comprendre les obstacles à l'élaboration de produits et services personnalisés permettant d'améliorer l'engagement, la rétention et la confiance des clients.

Modernisation des paiements

Contexte

Ces dernières années, de nombreux pays se sont lancés dans la mise à niveau de leurs systèmes classiques vieillissants pour accélérer le traitement des paiements, les règlements en temps réel et les opérations riches en données. En 2016, le Canada s'est lancé dans cette quête en vue de mettre au point un nouveau système de compensation et de règlement de base, de créer une fonctionnalité de paiement en temps réel, de perfectionner les transferts de fonds automatisés, de se conformer aux normes de réglementation mondiales et de moderniser les règles-cadres. La vision qui sous-tend ce projet consiste à créer un système de paiements moderne à la fois rapide, souple et sécuritaire afin de promouvoir l'innovation et de raffermir la compétitivité du Canada.

Risques et gains du traitement en temps réel

S'il est vrai que cette initiative comporte des avantages considérables pour les clients, les entreprises et les organismes gouvernementaux, elle est également avantageuse pour les institutions financières. Après tout, une plate-forme de paiements moderne ne fera pas que simplifier et accélérer les paiements. Elle procurera également une base d'analytique plus solide, ce qui fournira aux institutions financières un meilleur éclairage sur les habitudes de dépenses des particuliers et des organisations, rehaussera leur capacité d'améliorer la gestion des capitaux et des liquidités et leur permettra de commercialiser des produits et des services mieux adaptés aux besoins.

La modernisation des paiements n'est toutefois pas dépourvue de risques. Les craintes que le secteur, Paiements Canada et les organismes de réglementation ne soient pas aptes à exécuter collectivement le plan de modernisation des paiements – en raison de son envergure, de sa portée et de sa rapidité – mettent en lumière certains risques liés à son exécution. Par exemple, il se peut que des priorités concurrentes, des pénuries de compétences et des contraintes de capacité empêchent le secteur d'atteindre l'état cible à temps, ce qui pourrait alourdir les coûts et les risques. La dépendance grandissante à l'égard des nouvelles technologies pourrait compliquer l'exécution, en particulier si celles-ci sont incompatibles avec les systèmes qui traitent actuellement les paiements cruciaux. Outre le risque lié à l'exécution, cela pourrait semer la confusion dans l'esprit des clients, perturber le service, causer des pannes de système et aggraver les lacunes dans la surveillance de la gestion des risques.

Les efforts du secteur pour atteindre l'état cible de l'initiative s'accompagnent de nouveaux risques qui se multiplient, soit l'incapacité potentielle des banques à mesurer proactivement l'importance des risques additionnels qu'elles créeront en raison de la menace de l'augmentation possible des activités frauduleuses, de leur exposition accrue aux cybermenaces et des exigences plus rigoureuses relatives aux garanties. Collectivement, ces risques créent des défis pour les institutions financières, qui doivent assurer la sécurité et la solidité du système financier, en particulier aux étapes précoces de sa mise en œuvre, c'est-à-dire au moment où les risques de perturbation de systèmes et d'une éventuelle perte de données sont vraisemblablement les plus élevés.

Répercussions de la modernisation des paiements

Outre les nombreux avantages qu'elle comporte, la modernisation des paiements aura des répercussions importantes sur les institutions financières. Les deux plus importantes sont le risque de fraude et les pressions sur les opérations de trésorerie.

1. Risque de fraude

Lorsque le Royaume-Uni a lancé le système Faster Payments en 2008, les pertes attribuables à la fraude liée aux opérations bancaires en ligne ont grimpé de près de 300 %, passant de 22,6 M£ en 2007 à 59,7 M£ en 2009 [10]. Si une banque n'est pas bien préparée dès le début, les activités frauduleuses risquent de se multiplier et seront plus difficiles à prévenir une fois commencées. Il est évident que les principaux avantages du traitement des paiements en temps réel sont également, en partie, ses principales faiblesses, notamment ce qui suit :

Modernisation des paiements

- **Rapidité :** les paiements en temps réel sont si rapides que les banques ont très peu de temps pour exercer une surveillance complète de la fraude.
- **Irrévocabilité :** avec le système Lynx, qui remplacera le Système de transfert de paiements de grande valeur (STPGV) et le système de paiements en temps réel, les transferts de paiements entre les institutions financières canadiennes deviennent irrévocables une fois qu'ils ont été autorisés.
- **Identifiants de substitution :** pour répondre aux besoins en évolution des clients, la nouvelle infrastructure de paiement au Canada propose le recours à des substituts supplémentaires – identifiants sur appareils mobiles, adresses courriel et numéros de téléphone – afin de permettre l'identification des clients et d'habiliter ces derniers à effectuer des paiements. Il en résultera certes une souplesse de paiement sans précédent, mais également une augmentation des préoccupations liées à la sécurité et du risque de fraude.
- **Limites d'opération plus élevées :** les limites de transfert électronique Interac s'établissent actuellement à 3 000 $ par jour, mais leur plafonnement est appelé à changer. Avec la modernisation des paiements, les limites d'opération quotidiennes s'établiront à 10 000 $ pour potentiellement atteindre 100 000 $, voire davantage. Le relèvement des limites d'opération, qui présente pour les cybercriminels des occasions de fraude plus lucratives, risque de causer des pertes plus lourdes.
- **Opérations riches en données :** Paiements Canada propose la mise en application d'une norme mondiale pour les messages sur les paiements, assortie d'une syntaxe étendue. Ces opérations riches en données feront croître le risque d'exposition à des logiciels malveillants qui pourraient être intégrés dans des pièces jointes aux paiements ou aux hyperliens.

Réagir de façon stratégique

Les banques ont besoin d'un délai d'un an à 18 mois pour bien se préparer à l'accroissement du risque de fraude. Les institutions financières devront veiller à ce que les pratiques et les processus permettent de contourner ce risque en faisant ce qui suit :

- Mettre en place des capacités de détection et de prévention de la fraude en temps réel en ayant recours à une analytique avancée pour détecter les stratagèmes frauduleux dès leur apparition.
- Renforcer les procédures d'authentification.
- Protéger tous les canaux et types de paiements dans la même mesure.
- Exercer une surveillance sur les paiements tant sortants qu'entrants.
- Renforcer les systèmes de cybersécurité pour empêcher que les cybercriminels utilisent des outils de pointe afin d'attaquer des systèmes ou d'insérer des codes malveillants dans le champ du message riche en données des opérations.

2. Pressions sur les opérations de trésorerie

Il est évident que l'initiative de modernisation de Paiements Canada permettra d'accélérer les transferts de fonds et d'accroître l'efficacité du règlement des paiements. Cependant, les nouvelles plateformes et règles liées à ces activités auront des conséquences néfastes sur les opérations de trésorerie des institutions financières. Voici ce dont les banques auront besoin :

- De renforcer sensiblement les exigences relatives aux garanties.
- D'une nouvelle approche de la gestion des liquidités intrajournalières.
- De mises à niveau des données et de la technologie.

Réagir de façon stratégique

Tandis que l'initiative de modernisation progressera, les institutions financières devront prendre des mesures pour atténuer ces risques émergents. Il n'existe aucune solution universelle, mais les banques pourront faire ce qui suit :

Modernisation des paiements

- Renforcer la gestion des garanties pour améliorer leur surveillance, réduire les risques financiers et rationaliser leurs systèmes de manière à optimiser la conformité aux règles de garanties de Lynx, du Moteur d'optimisation du règlement et des systèmes de PTR.
- Evaluer et remanier les modèles de liquidités intrajournalières pour acquérir une visibilité dynamique sur les réserves de liquidités, améliorer leurs projections en la matière et adopter des mécanismes adéquats d'épargne des liquidités.
- Examiner les fonctionnalités des systèmes technologiques pour cerner les lacunes possibles et déterminer les mises à niveau qui s'imposent pour répondre aux exigences additionnelles de surveillance et de production de rapports découlant de la modernisation des paiements.
- Analyser en quoi les nouveaux processus relatifs aux garanties et aux liquidités peuvent influer sur la conformité à la réglementation en modifiant les ratios financiers et adopter des indicateurs d'alerte rapide pour éviter de dévier.

Principaux points à retenir

- La modernisation des paiements est porteuse d'atouts importants pour l'économie canadienne. Ces avantages s'accompagnent néanmoins de nouveaux risques allant du renforcement des exigences relatives aux garanties, aux pressions plus fortes sur les modèles de liquidités et à la nécessité de mettre à niveau la technologie pour réagir à l'augmentation des risques de fraude et de cyberattaques.
- Le moment est maintenant venu pour les institutions financières de déterminer les conséquences de la modernisation des paiements pour leurs profils de risques et d'établir une liste de mesures prioritaires pour y réagir. L'essentiel sera d'aborder la modernisation des paiements non seulement comme un exercice de mise en conformité, mais aussi comme une occasion de renforcer les modèles de gestion des risques, d'optimiser les processus de gestion des liquidités et des paiements et d'accroître la satisfaction de la clientèle par la mise en place de systèmes et de technologies plus solides et plus sécuritaires.

Transformer les perspectives en action

- Il est essentiel que les institutions financières prennent le temps de planifier dès maintenant pour décourager les criminels dès le jour du lancement des paiements en temps réel.
- Les institutions financières doivent se doter de bonnes capacités d'authentification pour l'ensemble des canaux.
- Elles doivent se préparer aux changements touchant les liquidités intrajournalières et les garanties qu'entraînera la modernisation des paiements. Plus précisément, les institutions financières devront faire ce qui suit :
  - Renforcer les exigences relatives aux garanties
  - Adopter une nouvelle approche pour la gestion des liquidités intrajournalières
  - Mettre à niveau les données et la technologie
- Les institutions financières doivent réagir de façon stratégique aux répercussions importantes de la modernisation des paiements. En agissant rapidement, elles pourraient vraisemblablement bénéficier d'économies de coûts qu'il leur sera plus difficile de réaliser à l'approche des dates limites de mise en œuvre.

Transformation du modèle opérationnel de gestion des risques

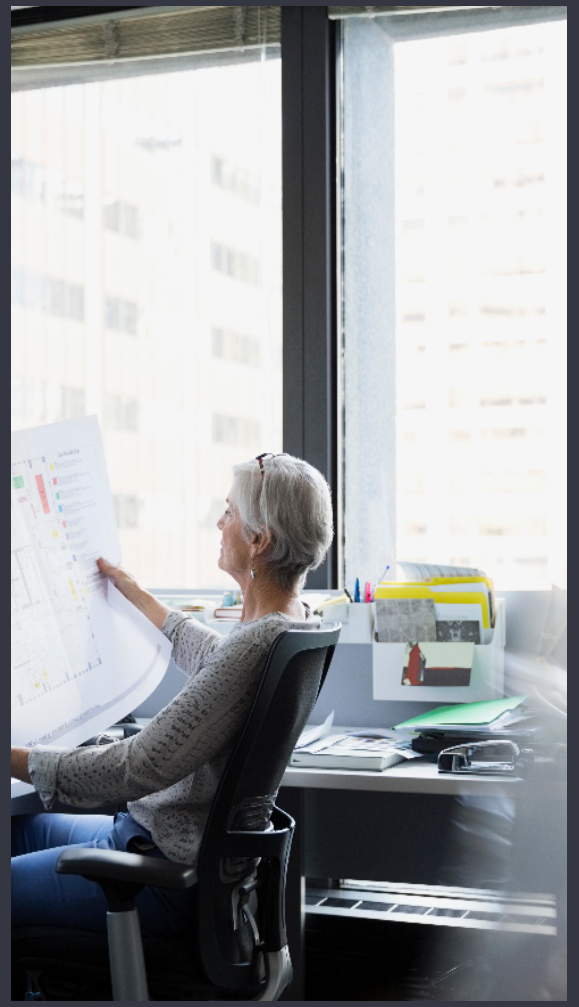
Tirer parti des plus récentes innovations en technologies et processus afin d'améliorer l'efficacité des systèmes de gestion des risques tout en assurant leur sécurité et leur intégrité.

Survol

La gestion des risques se situe à un tournant où les pressions de la concurrence et les innovations technologiques remettent en question les idées reçues conventionnelles.

- La réglementation est devenue à la fois un catalyseur et une contrainte pour la stratégie d'affaires, les fonds propres, les liquidités, le comportement attendu des entreprises, les besoins en infrastructure de gestion des risques ainsi que les coûts.
- Malgré des dépenses colossales pour satisfaire ces besoins, il arrive souvent que la gestion des risques ne réponde pas entièrement aux attentes des parties prenantes.
- En même temps, le marché a créé de nouveaux modèles de prestation de services et de nouvelles capacités qui offrent la possibilité de transformer l'environnement de risque.

Ces événements sont l'occasion pour les institutions financières de redéfinir leur modèle opérationnel de gestion des risques. Celles-ci veulent que les activités liées aux risques et à la conformité soient plus efficaces et elles cherchent à éliminer le double emploi découlant de la complexité excessive, en particulier pour ce qui est du modèle des trois lignes de défense. Cependant, tandis que les entreprises s'emploient à optimiser leur méthode de gestion des risques en exploitant les innovations technologiques et commerciales, la protection des clients et la gestion des risques liés à l'éthique ont simultanément grimpé sur la liste des priorités des organismes de réglementation et des législateurs.



Trois lignes de défense

Dix ans après la crise financière et huit ans après l'adoption de la loi intitulée *Dodd-Frank Wall Street Reform and Consumer Protection Act*, de nombreuses entreprises ont terminé ou presque terminé l'élaboration de nouveaux systèmes de gestion des risques et sont maintenant vraiment prêtes à reprendre leurs activités normales. Cependant, même si le travail intensif est terminé, les clients, le marché, les technologies et le contexte réglementaire ont beaucoup changé depuis la conception du plan de ces systèmes.

Avant la crise financière, les systèmes liés aux risques et à la conformité étaient très cloisonnés, et l'environnement d'exploitation était caractérisé par des processus hautement manuels, des contrôles fragmentés et une mentalité de cocher la case. Par la suite, compte tenu de plus grandes attentes découlant de la réforme de Dodd-Frank et de la faible tolérance des organismes de réglementation au non-respect des dates limites et des mauvaises solutions, des systèmes ont été élaborés rapidement en mettant l'accent sur la robustesse plutôt que sur l'efficacité. Les institutions financières s'efforcent maintenant d'exploiter les innovations technologiques et commerciales tant internes qu'externes pour maximiser leurs méthodes et systèmes de gestion de risques de manière à en accroître l'automatisation et à les rendre plus souples, capables de produire des rapports sur les risques en temps quasi réel et plus conformes à la stratégie et à la tolérance au risque de l'entreprise.

Pour ce faire, les institutions financières doivent examiner globalement les trois lignes de défense afin de comprendre le fonctionnement actuel du modèle et la relation qui existe entre les trois lignes. L'intégration d'une culture de sensibilisation et de soutien réciproque permettra d'optimiser le modèle. Cette culture ne peut être instaurée que si la direction donne le ton.

Les institutions financières qui effectuent un examen approfondi des processus complets sont de plus en plus nombreuses à reconnaître qu'il y a des redondances improductives pour certains aspects et que les contrôles ne sont pas toujours au bon endroit pour être efficaces. Par exemple, certaines entreprises sont en train de transférer des activités choisies de mise à l'essai et de surveillance à la première ligne de défense dans le but d'améliorer la détection, la prévention et la responsabilisation. Cette démarche permet aux deuxième et troisième lignes de défense d'effectuer un examen plus stratégique, en plus de libérer des ressources pour l'analytique avancée des données, le regroupement des risques et les essais ciblés visant à bien évaluer les risques.

Remettre en question le modèle d'exploitation actuel

Les entreprises évaluent aussi leur modèle d'exploitation actuel au niveau du détail en fonction de plusieurs aspects importants.

Structure

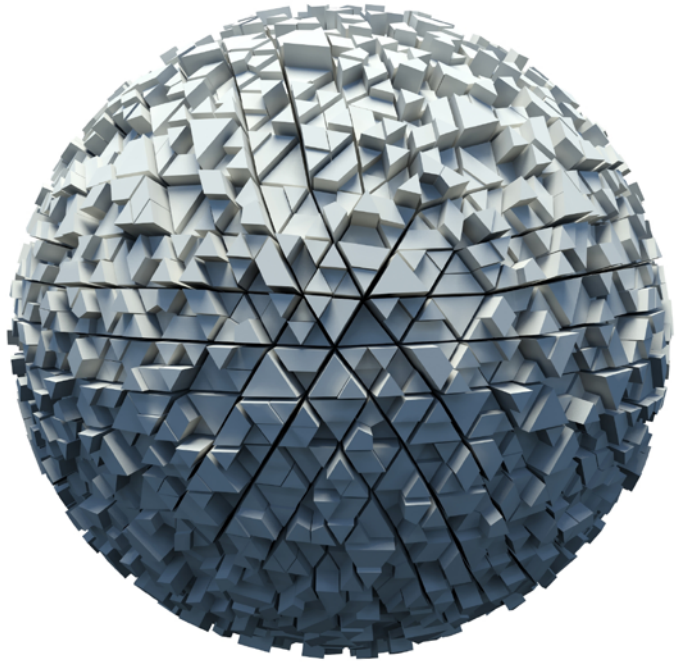
- **Emplacement des ressources :** les rôles et les responsabilités de chaque ligne sont-ils appropriés ou y aurait-il lieu de déplacer des rôles de sorte qu'ils soient plus près de l'origine du risque et puissent ainsi le détecter et l'atténuer de façon rapide et efficace?
- **Répartition des ressources :** les ressources sont-elles réparties – en particulier entre la première et la deuxième lignes de défense – de manière à favoriser la responsabilisation et à répondre aux besoins fondamentaux à l'origine du risque?

Modes de prestation de services alternatifs

- **Centralisation des principaux processus d'affaires :** comment centraliser les principaux processus d'affaires dans l'entreprise pour les rendre plus efficaces, adaptables et normalisés? Comment peut-on contrôler les processus internes en vue d'accroître la qualité pour l'ensemble des opérations d'affaires, p. ex., grâce à la centralisation de la mise à l'essai et de la surveillance des contrôles?

Trois lignes de défense

- Mise à profit des experts en la matière (centres d'excellence mondiaux) : comment mieux tirer parti des experts des domaines clés, comme la planification des fonds propres et des mesures de résolution, la gestion des fournisseurs et la cybersécurité, pour orienter les démarches de la première et de la deuxième lignes de manière à assurer l'uniformité et la qualité?
- Co-impartition d'une partie des rôles relatifs au risque (services liés aux risques gérés) : comment le recours à des tiers ou à la délocalisation permet-il de bien gérer les risques à moindres coûts, en particulier dans les domaines où il est difficile de recruter des talents spécialisés ou encore où des tâches répétitives pourraient permettre à un fournisseur externe de réaliser de plus grandes économies d'échelle?
- Coentreprises (avec des fournisseurs) : comment les coentreprises avec d'autres institutions bancaires pourraient elles permettre de partager les coûts avec le secteur pour des activités courantes telles que le contrôle diligent annuel pour les tiers fournisseurs auxquels ont recours plusieurs banques?

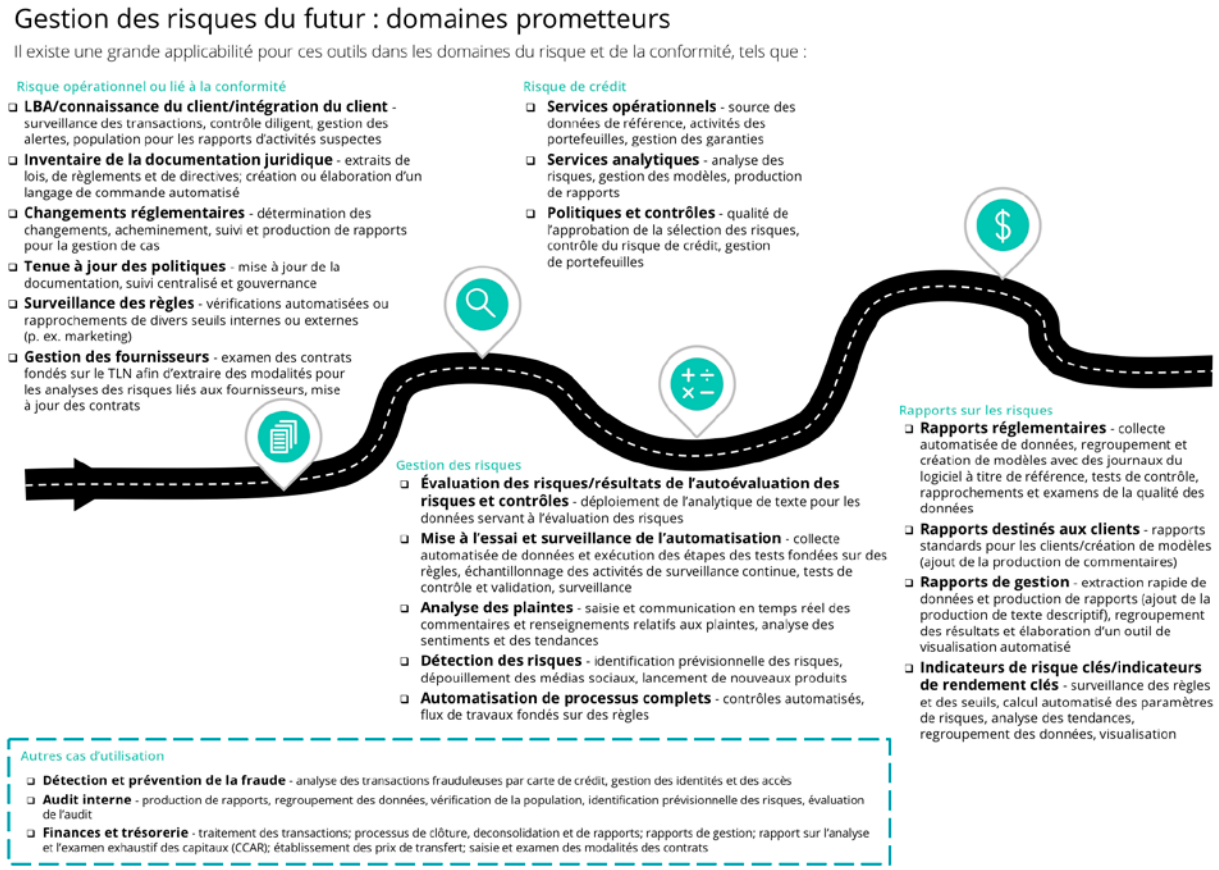


Simplification et amélioration des modèles d'exploitation et des contrôles

Dans le cadre du processus de remaniement, les entreprises doivent déterminer si elles disposent des outils qu'il faut pour soutenir la transformation et permettre aux employés les plus brillants et les plus talentueux d'imaginer et de concrétiser l'art du possible. Les technologies nouvelles ou existantes peuvent faciliter considérablement la transformation en contribuant à automatiser les flux de travaux et les tâches répétitives, à améliorer les plates-formes et à permettre l'analytique avancée des données.

Des outils tels que la robotisation des processus et le traitement du langage naturel peuvent aider les entreprises à éliminer des tâches essentielles, mais répétitives et banales, créant ainsi des économies d'échelle et libérant des ressources pour les analyses procurant davantage de valeur. L'analytique avancée des données et la production de rapports permettent aux utilisateurs de tirer parti des mêmes données pour les trois lignes de défense sans créer de redondances et de personnaliser les rapports en fonction du rôle et des besoins de chaque ligne.

Au moment de déterminer comment progresser, les entreprises doivent se demander si l'investissement en temps, en efforts et en argent nécessaire pour optimiser le modèle et les capacités des trois lignes de défense, malgré la hausse des coûts à court terme, en vaudra la peine pour améliorer la gestion des risques de façon durable et à moindres coûts à long terme. Bien entendu, elles doivent également réfléchir à l'autre option possible, soit apporter sans cesse de petites améliorations aux systèmes inefficaces qui ne permettront pas nécessairement de répondre aux attentes tant internes que réglementaires et qui pourraient aboutir à un remaniement plus perturbant et coûteux à la longue.



Conduite

La promotion d'un programme de conduite et de culture continue de susciter l'intérêt à l'échelle mondiale. Le concept de risque lié à la conduite a un sens plus large depuis la crise financière. Depuis dix ans, les pratiques d'affaires et la conduite sont devenues des sujets d'actualité prioritaires. Il y a cinq ans, les entreprises ont commencé à établir des cadres pour identifier, gérer et surveiller les questions de conduite en tant que nouvelle dimension du risque. Aujourd'hui, de nombreux secteurs acceptent ce qui doit être fait pour prévenir activement l'inconduite des employés et gérer les répercussions culturelles connexes.

Cependant, les progrès nécessaires pour transformer la gouvernance et la culture des services financiers continuent d'être compromis par des cas d'inconduite. Tandis que l'on s'attaque aux causes fondamentales de l'inconduite, on s'attend à ce que les autorités renforcent la supervision de la gouvernance et des contrôles internes des entreprises et accordent de plus en plus d'importance à la diversité en tant que rempart contre la pensée de groupe. Par ailleurs, l'intérêt pour les régimes de responsabilisation renforcés augmente. Au sortir de la crise financière mondiale, les organismes de réglementation ont signalé le risque que les entreprises relâchent leur vigilance quant à la gouvernance et à la culture. On s'attend à ce que les entreprises montrent qu'elles prennent la question de la culture au sérieux et disposent de cadres de gouvernance et de contrôle qui sont résilients, stables et suffisamment robustes pour s'adapter au contexte actuel et permettre d'identifier les risques nouveaux et émergents.

Les entreprises devront s'assurer en particulier que leurs cadres de gouvernance interne et de contrôle permettent de bien gérer les risques, notamment pour leurs clients et leur résilience opérationnelle, qui peuvent découler de l'innovation et de la technologie. Soucieux de préserver la confiance du public, les superviseurs s'attendront à ce que l'utilisation des technologies et des innovations par les entreprises repose sur de solides principes, p. ex., objectifs précis, surveillance appropriée et communication claire avec les clients.

La diversité peut apporter un vaste éventail de compétences et une expérience diversifiée et remettre en question de manière constructive le processus décisionnel. Si les entreprises doivent éviter les incidents liés à la mauvaise utilisation des données personnelles, il peut s'avérer crucial d'avoir un conseil d'administration diversifié et inclusif pour faire en sorte que les répercussions techniques et éthiques des nouveautés, comme l'utilisation accrue de l'IA ou l'utilisation des données sur les clients, soient bien prises en compte et examinées en détail.

En outre, les entreprises doivent se préparer à un changement potentiel d'orientation de la réglementation, qui mettra l'accent sur le renforcement de la responsabilisation. Elles peuvent commencer par clarifier et consigner les rôles et les responsabilités des cadres supérieurs et d'autres personnes clés et communiquer les attentes à l'égard de la responsabilisation et de l'éthique à tous les échelons.

Au Canada, les questions liées à la culture et à la conduite figurent parmi les grandes priorités de l'Agence de la consommation en matière financière du Canada pour la surveillance. En 2018, un régime de protection des consommateurs en matière financière a été instauré dans le plus récent projet de loi d'exécution du budget du gouvernement canadien, ce qui ce qui implique que la direction et le conseil d'administration devront resserrer leurs attentes envers les dénonciations, les plaintes et la surveillance des questions liées à la protection des consommateurs.

L'avenir

Opinion de l'entreprise face aux risques liés à la conduite

On s'attend à ce que les grandes institutions aient un programme de gestion des risques liés à la conduite et une fonction responsable des risques liés à la conduite à l'échelle de l'entreprise. La réglementation met l'accent sur la surveillance continue de la conduite et des améliorations, et les mécanismes de détection et de prévention afin d'influencer la façon dont les objectifs stratégiques sont atteints.

Conduite

L'accent mis sur la conduite des employés comme on le faisait par le passé se concentre dorénavant sur les pratiques du marché, les pratiques d'affaires et l'incidence sur les clients et les marchés. En outre, on accorde beaucoup d'importance à l'élaboration de contrôles internes, ce qui crée un besoin de rationaliser les activités pour gérer efficacement le programme. Cela pourrait entraîner un certain réalignement des activités de supervision ou de surveillance.

Analytique et intelligence prédictive appliquées à la conduite et à la culture

Les entreprises souhaitent produire des données utiles sur la conduite des employés à l'intention du conseil, de la haute direction et des organismes de réglementation. La capacité de prévoir et de prévenir l'inconduite des employés est un impératif d'affaires dans le secteur institutionnel et ceux du commerce de détail et de la gestion du patrimoine. Les entreprises veulent repérer tôt les employés ayant une mauvaise conduite, identifier de façon proactive le prochain groupe d'employés et d'activités présentant des risques, et élaborer des méthodes améliorées de supervision renforcée et de surveillance ciblée.

Difficultés et possibilités que présentent les technologies émergentes

La technologie continue de perturber la façon dont les entreprises créent des relations, fournissent des services, assurent une surveillance et interagissent avec les clients. En tant qu'élément perturbateur, la technologie donne lieu à de nouvelles pratiques d'affaires qui peuvent créer de nouveaux risques et difficultés liés à la conduite ou les accroître (p. ex., services bancaires numériques, robots-conseillers, commerce électronique ou algorithmique et nouveaux produits comme le bitcoin). Par contre, cela crée également des occasions de mettre en œuvre et d'améliorer les contrôles nécessaires à une bonne gestion des risques liés à la conduite (p. ex., tirer parti de l'accès accru aux données pour mieux prévoir – ou détecter plus rapidement – les cas d'inconduite chez les employés).

Accent mis sur la rémunération

Cela demeure un aspect important pour les organismes de réglementation. Le Conseil de stabilité financière prévoit publier des recommandations sur la façon dont les institutions financières peuvent renforcer leur capacité d'examiner et de surveiller l'efficacité des outils de rémunération. En outre, ces recommandations indiqueront des mécanismes permettant de promouvoir une bonne conduite et de remédier aux risques d'inconduite. En Australie, la Banking Royal Commission a examiné un certain nombre d'institutions financières et a déterminé que la rémunération était l'une des causes fondamentales de l'inconduite.

Principaux points à retenir

Tandis que les institutions financières revoient leurs modèles d'exploitation en cette période caractérisée par l'innovation technologique, la réduction des coûts et les changements opérationnels et structurels, elles doivent reconnaître que, pour répondre aux attentes réglementaires concernant la sécurité et l'intégrité, il est impératif d'intégrer la gouvernance, l'éthique et la culture.

Transformer les perspectives en action

- Afin de maintenir une approche solide, souple et viable pour la gestion des risques et de la conformité, les institutions financières doivent réévaluer les possibilités d'innovation et d'amélioration de la productivité dans leur modèle d'exploitation associé aux risques.
- La maximisation des fonctions de gestion des risques et de la conformité peut non seulement aider à réduire les coûts et à améliorer l'efficacité, mais peut aussi servir à **accroître l'évolutivité, l'agilité et la vitesse d'adaptation** aux besoins d'affaires en évolution et à la réglementation et aux politiques futures.
- L'intégration d'une culture de sensibilisation et de soutien mutuel contribuera à la maximisation du modèle des trois lignes de défense. Il n'est possible de créer une culture semblable qu'en donnant le ton à partir de la direction et en veillant à l'adhésion des échelons intermédiaires.

Renforcer la résilience

Nous sommes dans une ère d'innovation technologique qui amène les institutions financières à revoir leurs modèles d'exploitation. À mesure que les services bancaires évoluent, la gestion des risques subira les mêmes pressions pour l'innovation que le reste de l'institution.

La vague d'innovation vient ébranler la convention des pratiques de gestion des risques acceptées et attendues. Les institutions bancaires souhaitent maintenant maximiser leurs approches et leurs systèmes de gestion des risques pour les automatiser et les rendre plus souples et capables de procurer l'information sur les risques quasiment en temps réel, et mieux les aligner sur la stratégie d'entreprise et la tolérance au risque. Même si, par le passé, on croyait que le principe des trois lignes de défense était incontournable, les institutions financières revoient aujourd'hui leurs modèles. La technologie applicable à la réglementation et le mouvement vers la technologie pour la gestion des risques sont en train de devenir des impératifs d'affaires.

Le défi du secteur des services financiers est aujourd'hui d'innover sans affaiblir la gestion des risques. La gestion de l'innovation en matière de risques est donc une des grandes priorités des institutions financières comme des organismes de réglementation. Si les organismes de réglementation ne veulent pas dicter aux institutions financières comment s'y prendre pour gérer l'innovation, ils s'opposeront aux solutions adoptées si elles ont le potentiel de compromettre une bonne gestion des risques.

Perspectives d'avenir

Les modèles d'affaires sont, de toute évidence, en pleine transformation. Des facteurs comme l'accès aux services financiers, le système bancaire ouvert, les technologies financières et l'innovation technologique ainsi que l'environnement de réglementation continueront d'évoluer et d'engendrer le changement. Il ne s'agit plus de se demander si tout cela viendra transformer le secteur, car cela est déjà en cours. Les institutions financières qui prennent l'initiative d'innover, au lieu de se distancer avec scepticisme, et qui favorisent une culture de conduite et de gouvernance rigoureuse renforceront leur résilience aux forces et en retireront un atout concurrentiel manifeste.

Glossaire

ABE – Autorité bancaire européenne
AM – Apprentissage machine
AMI – Approche des modèles internes
AN – Approche normalisée
APR – Actif pondéré en fonction des risques
BSIF – Bureau du surintendant des institutions financières
CBCB – Comité de Bâle sur le contrôle bancaire
CD – Chef des données
CRR2 – Deuxième règlement sur les exigences de fonds propres
CRR3 – Troisième règlement sur les exigences de fonds propres
CSF – Conseil de stabilité financière
EDC – Éléments de données critiques
FCA – Financial Conduct Authority
FRNM – Facteur de risque non modélisable
IA – Intelligence artificielle
IBOR – Taux interbancaire offert
IF – Institutions financières
LBA – Lutte contre le blanchiment d'argent
LIBOR – Taux interbancaire offert à Londres
PTR – Paiement en temps réel
RFPN – Revue fondamentale du portefeuille de négociation
RN – Résultat net
SIQ – Stratégie d'investissement quantitatif
TARCOM – Groupe de travail sur le taux de référence complémentaire pour le marché canadien
Taux CORRA – Taux des opérations de pension à un jour
TI – Technologies de l'information
TLN – Traitement du langage naturel
TSR – Taux sans risque
UE – Union européenne

Notes

1. Institute of International Finance, « *Global Debt Monitor* », juillet 2018.
2. Fonds monétaire international,, « *Bringing Down High Debt* », avril 2018.
3. Alex J Pollock, « *Financial Crises Occur About Once Every Decade* », Financial Times, mars 2015.
4. E*TRADE Capital Management LLC, « *Where are we in the current business cycle?* », juin 2018.
5. Autorité bancaire européenne, « *Risk Dashboard Data* », Q2 2018.
6. Financial Conduct Authority, « *Transforming Culture in Financial Services* », mars 2018.
7. Deloitte, « *Perspectives économiques : le blues de fin de cycle* », https://www2.deloitte.com/ca/fr/pages/finance/articles/perspectives-economiques-blues-fin-cycle.html, consulté le 3 décembre 2018.
8. Financial Conduct Authority, « *The future of LIBOR* », https://www.fca.org.uk/news/speeches/the-future-of-libor, Juillet 2018.
9. Deloitte, « *Fintech by the Numbers: Incumbents, Startups, Investors Adapt to Maturing Ecosystem* », 2017.
10. ACI Worldwide, Universal Payments, « *Immediate Need for Fraud Prevention* », 2016, https://www.pymnts.com/wp-content/uploads/2016/09/Best-practices-for-preventing-fraud-in-a-real-time-world.pdf, consulté le 26 avril 2018.

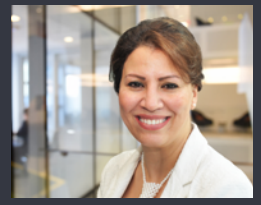
Personnes-ressources

Michael Chau
Associé, Conseils en gestion des risques
416-601-6722
michau@deloitte.ca

Azer Hann
Associé, Conseils en gestion des risques
416-601-5777
ahann@deloitte.ca

Jay F. McMahan
Associé, Conseils en gestion des risques
416-874-3270
jfmcmahan@deloitte.ca

Bruno Melo
Associé, Conseils en gestion des risques
416-601-5926
brmelo@deloitte.ca



Mariama Zhouri
Directrice principale, Conseils en gestion des risques
514-393-7317
mzhouri@deloitte.ca

Nous souhaitons remercier les professionnels du service à la clientèle de Deloitte ci-dessous pour leur point de vue et leur contribution au présent rapport :

Jas Anand, directeur principal, Conseils en gestion des risques, Deloitte Canada
Andrea Barragan-Verduzco, conseillère principale, Conseils en gestion des risques, Deloitte Canada
Olivia Chiu, directrice principale, Conseils en gestion des risques, Deloitte Canada
Sandeep Chopra, directeur principal, Conseils en gestion des risques, Deloitte Canada
Robert Cranmer, directeur de service, Conseils en gestion des risques, Deloitte Canada
Judit Halin, associée, Conseils en gestion des risques, Deloitte Canada
Umang Handa, directeur principal, Conseils en gestion des risques, Deloitte Canada
Stefanie Ruys, directrice principale, Conseils en gestion des risques, Deloitte Canada
Betty Tien, directrice principale, Conseils en gestion des risques, Deloitte Canada
Slava Trefilin, conseillère principale, Conseils en gestion des risques, Deloitte Canada
Helen Zhang, directrice, Conseils en gestion des risques, Deloitte Canada
Zeshan Choudhry, associé, Conseils en gestion des risques, Deloitte Royaume-Uni
Scott Martin, directeur principal, Centre de stratégie en réglementation d'EMEA, Deloitte Royaume-Uni
David Strachan, chef du Centre de stratégie en réglementation d'EMEA, Deloitte Royaume-Uni
Pierre Lapointe, associé, Conseils en gestion des risques, Deloitte Canada
Jacques Guvlekjian, conseiller principal, Conseils en gestion des risques, Deloitte Canada

CENTRE *de*
STRATÉGIE EN RÉGLEMENTATION
AMÉRIQUES

Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans de nombreux secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500[MD] par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Pour en apprendre davantage sur la façon dont les quelque 264 000 professionnels de Deloitte ont une influence marquante – y compris les 9 400 professionnels au Canada – veuillez nous suivre sur **LinkedIn**, **Twitter** ou **Facebook**.

Deloitte.