Bureau du surintendant des institutions financières Canada
Office of the Superintendent of Financial Institutions Canada

Risque non financier et résilience opérationnelle : la montée en puissance des machines

Communication de M. Ben Gully, surintendant auxiliaire, à l'Institut C.D. Howe

Toronto (Ontario)
7 février 2019

Le texte prononcé fait foi.

Personne-ressource :

Brock Kruger
Communications et consultations
brock.kruger@osfi-bsif.gc.ca
www.osfi-bsif.gc.ca

BSIF
OSFI

Canada

Communication de Ben Gully, surintendant auxiliaire
Bureau du surintendant des institutions financières (BSIF)
à l'Institut C.D. Howe
Toronto (Ontario)
Le 7 février 2019

Introduction

Je vous remercie de m'avoir invité à vous adresser la parole aujourd'hui.

Les institutions financières accroissent leur capacité opérationnelle par une puissante combinaison de nouvelles technologies et de numérisation rapide. Ces changements modifient en profondeur leur contexte d'exploitation ainsi que les attentes à l'égard d'une saine gestion des risques.

Seules la créativité et l'imagination nous donnent une idée d'où tout cela peut nous conduire, mais ce sont le jugement et les efforts de l'être humain qui nous permettront d'y arriver.

Les progrès technologiques laissent entrevoir un avenir prometteur. Les institutions financières construisent et assoient leur réputation en respectant leurs promesses. Du point de vue prudentiel, le BSIF cherche à savoir comment les institutions s'adaptent aux changements technologiques et y réagissent. Par exemple, nous voulons savoir comment elles gèrent et atténuent les risques opérationnels que font naître les nouvelles percées technologiques.

Notre intérêt commun – et cela est d'une importance capitale – est de savoir comment ces risques peuvent miner la confiance à l'égard des institutions financières ou entacher leur réputation, car, sans cette confiance, les institutions connaîtront bien des difficultés.

Aujourd'hui, je vais vous parler de trois questions auxquelles le BSIF prête une attention particulière dans le cadre de sa réflexion sur la façon dont les technologies et la numérisation influent sur le risque opérationnel des institutions financières : la première est l'utilisation de l'analytique avancée, comme l'intelligence artificielle ou l'apprentissage automatique, la deuxième est le recours accru à des tiers pour se procurer produits et services, et la troisième est l'évolution de la sécurité de l'information face aux cybermenaces.

Le BSIF a amorcé des remaniements à l'interne pour tenir compte de ce qu'on appelle les risques non financiers. Il est à mettre en place de nouveaux moyens et une nouvelle infrastructure de contrôle de la résilience opérationnelle en tant que composante clé de la sûreté et de la solidité financières. Il nous incombe de faire connaître les mesures que les institutions financières devraient prendre, selon nous, pour accroître leur résilience dans un monde de plus en plus technologique et numérique.

L’évolution des modèles d’affaires et d’exploitation des institutions financières

Dans le contexte actuel, les institutions financières font de plus en plus appel à des entreprises technologiques pour tirer parti des nouvelles technologies financières, les f*intech*. Ces changements sont importants, ils promettent des gains d’efficience et proposent de nouvelles méthodes de gestion des activités. Mais ne vous y trompez pas, ils ont aussi le pouvoir de modifier en profondeur les modèles d’affaires et d’exploitation d’une banque ou d’un assureur.

Certaines des possibilités qui s’offrent à nous prennent la forme de stratégies d’affiliation en marque blanche, dans le cadre desquelles l’institution financière compte sur son partenaire pour obtenir des clients; autrement dit, elle n’est pas obligée d’être en contact direct avec les clients.

Il y a également les logiciels de comptabilité, les services de paie, les conseils juridiques de base ou l’offre de nouveaux services tarifés au moyen d’une plateforme. Ce sont toutes là des avenues bien éloignées des modèles d’affaires traditionnels.

Les modèles d’exploitation des institutions financières évoluent eux aussi de façon spectaculaire. La disponibilité de systèmes informatiques ouverts en remplacement des anciens systèmes traditionnels, ainsi que l’automatisation et la capacité de mettre en place des programmes qui compriment les cycles de développement technologique, auront toutes une incidence sur les choix que feront les institutions. Ces choix se traduiront par l’arrivée de nouveaux produits et services sur le marché à un rythme frénétique.

La technologie permettra ou accélérera la décentralisation des participants des marchés financiers et brouillera les frontières des institutions réglementées traditionnelles. La décentralisation aura pour effet à la fois d’amplifier les risques non financiers et de diluer les responsabilités : la première conséquence devra être atténuée par la mise en place de moyens de contrôle adéquats, tandis que la seconde agira à l’encontre des fondements de la ligne directrice B-10 du BSIF voulant que ce soit à l’institution financière d’assumer les responsabilités, quelle que soit l’entente conclue avec un tiers.

La sûreté et la solidité des institutions financières dépendront en partie de la capacité des fonctions de gestion du risque de bien comprendre et de contrôler leurs activités dans un écosystème élargi de partenaires. De tels changements à la gestion des risques favoriseront la compréhension des risques non financiers dans un environnement technologique et permettront aux institutions de s’assurer que les responsabilités en matière de prise de risques restent claires et transparentes, ce qui les aidera à devenir plus résilientes face aux perturbations opérationnelles.

La preuve est faite que les risques non financiers peuvent entacher la réputation, comme le démontre la réaction du grand public et des décideurs face aux infractions au droit à la vie privée. Ce sont des facteurs qui peuvent rapidement se répercuter sur les activités d’une institution, sur sa capacité de développer ses activités et, éventuellement, sur ses résultats financiers.

À notre avis, les mesures de résilience financière traditionnellement utilisées par les gestionnaires du risque et les autorités de réglementation, telles que le capital disponible et les liquidités, ont leur utilité, car elles sont plus facilement quantifiables et généralement considérées comme un indicateur de force par les marchés et les investisseurs. Toutefois, elles pourraient ne pas suffire, à elles seules, pour gérer les tensions non financières; en fait, elles offrent probablement une réponse inadéquate aux perturbations opérationnelles pour lesquelles il y a moins d'éléments tangibles à mesurer.

Il faut donc que le BSIF et les institutions financières qu'il surveille adoptent un point de vue large de la résilience qui tient compte de l'anticipation, de la prévention, du recensement des risques opérationnels ainsi que des moyens d'intervention et de la reprise des activités.

Analytique avancée

Selon le Forum économique mondial (avril 2018), plus de données ont été créées au cours des deux dernières années que durant les 5 000 années précédentes, et ce nombre serait en hausse. Les mégadonnées sont une méga affaire.

Bien que l'utilisation de l'analytique de données ne soit pas nouvelle en soi, la puissance accrue des ordinateurs a transformé la capacité d'analyser des sources de données de plus en plus diverses et nombreuses.

Les institutions financières utilisent les mégadonnées pour diverses applications, notamment pour la mesure et la gestion du risque de crédit, la détection de la fraude, la tarification, l'optimisation du portefeuille d'investissement, les échanges avec les clients et les services-conseils à la clientèle, etc.

Les mégadonnées, combinées à l'intelligence artificielle et à l'apprentissage automatique, vont déjà bien au-delà des outils traditionnels d'informatique décisionnelle. L'analytique avancée permet de mieux comprendre le comportement des clients, de faire des prédictions ou de formuler des recommandations à des fins décisionnelles.

Cela est utile, mais comporte des risques. Il y a des risques liés à la qualité des données et des questions relatives à la gouvernance du risque de modélisation, de même que des risques liés à l'observation des règlements de protection des consommateurs et des craintes possibles en matière de confidentialité des données qui pourraient poser des risques juridiques et d'atteinte à la réputation pour les institutions financières.

Les progrès touchant l'analyse des risques sont les bienvenus et importants, mais ils exigent de nouvelles capacités en matière de gestion de risques. Les machines qui utilisent davantage de données font de meilleures prédictions et sont d'une plus grande efficacité. De fait, les machines améliorent le recensement des problèmes et réduisent les coûts.

Mais lorsque l'apprentissage automatique est utilisé au détriment de la transparence ou de la confiance, l'intervention humaine doit prendre une plus grande place et s'accompagner d'une solide remise en question, faute de quoi, la légitimité des machines et des institutions qui les emploient sera mise en doute.

Le BSIF s'emploie lui aussi à parfaire ses outils, ses compétences et son programme de formation afin de faire face à l'avenir. C'est aussi pour lui l'occasion de procéder à une transformation numérique. Il ne saurait en être autrement, car il doit continuer de placer la barre très haut pour les institutions financières et d'évaluer leur supervision de l'analytique avancée, y compris l'utilisation de l'intelligence artificielle et de l'apprentissage automatique.

Le BSIF s'appuie en cela sur des principes fondamentaux relatifs à la gouvernance du risque de modélisation qui préservent la transparence et, en fin de compte, la légitimité perçue des résultats analytiques.

Écosystème de tiers

Les institutions financières se tournent de plus en plus vers des tiers pour se procurer produits et services – grâce aux progrès technologiques – pour tirer avantage de leur efficience et de leurs économies d'échelle. L'écosystème tiers gagne rapidement en importance et en diversité, ce qui signifie que les frontières des institutions financières traditionnelles deviennent de plus en plus poreuses. Fait important, certaines de ces ententes avec des tiers ne correspondent manifestement pas à la définition classique d'entente d'impartition, telle que l'entend le BSIF.

Les clients des services financiers ont toujours eu un grand pouvoir de négociation et pourraient donc insister pour obtenir des ententes-cadres personnalisées en matière de services. Avec l'infonuagique et d'autres solutions sur mesure, les tiers auxquels les institutions font appel peuvent chercher à mettre en place un modèle universel. L'adoption de conditions universelles pourrait se traduire, pour les institutions financières, par une perte de contrôle sur les services. De plus, dans de nombreux pays, ces tiers fournisseurs ne font l'objet d'aucune réglementation.

Ce qu'il faut craindre ici, c'est que les risques que courent les tiers se propagent rapidement et menacent leurs partenaires d'une perturbation des activités et entachent la réputation de l'institution financière.

Bien que les tiers offrent une plus grande capacité, ils altèrent la transparence de la gestion des risques. C'est pourquoi le BSIF s'attend à ce que les institutions financières comprennent et gèrent en toutes circonstances les risques rattachés aux ententes qu'elles concluent avec des tiers.

Nous nous attendons à ce que les institutions contrôlent elles-mêmes la qualité des pratiques de gestion des risques de leurs tiers et à ce qu'elles étudient les conséquences que celles-ci pourraient avoir sur leur résilience opérationnelle.

Vu l’augmentation du nombre de marchés avec tiers, il peut y avoir concentration des risques lorsque des institutions financières commencent à ne compter que sur quelques fournisseurs de services. Le BSIF craint que la position dominante d’un fournisseur donné dans un certain créneau ne se répercute, par effet de dépendance, sur l’ensemble du secteur des services financiers. Cela n’est pas sans importance, car la résilience du système financier dépendrait en fin de compte des activités d’un petit nombre d’entreprises technologiques actives en dehors du secteur des services financiers.

En préparation de la possibilité grave, mais plausible, d’un environnement de risque non financier, le BSIF recueille de l’information sur les types et l’importance des liens de dépendance des institutions financières avec des tiers fournisseurs de services.

Dans le cadre de ces travaux, nous mettrons l’accent sur la résilience opérationnelle, la technologie du nuage et la sécurité de l’information. Il ne s’agira pas d’un examen unique et ponctuel, car notre travail se poursuivra au fur et à mesure que l’écosystème de tiers évoluera.

Cybersécurité

Compte tenu du volume croissant de données numérisées et de l’amélioration de l’accès à celles-ci grâce aux nouvelles technologies, la sécurité de l’information est de plus en plus exposée au cyberrisque.

La cyberrésilience d’une institution tient à sa capacité de bien déceler les inévitables intrusions, d’intervenir et de reprendre ses activités. Le rythme effréné du changement et la persistance des menaces nécessitent des améliorations constantes des pratiques de gestion du cyberrisque.

Bon nombre des cyberattaques signalées jusqu’ici ont été perpétrées par le biais des services bancaires numériques – paiements frauduleux, hameçonnage de données ou vol d’identité par courriel, prises de contrôle automatisées de comptes. Les institutions financières doivent aussi considérer leurs tiers comme étant une source de risque et de dommages éventuels.

Il n’y a rien de sorcier dans ce qui rend une institution résiliente au cyberrisque. La résilience opérationnelle aux cybermenaces passe par la sécurisation du périmètre de l’entreprise, l’utilisation de configurations sécurisées, le contrôle de l’accès utilisateur, la protection contre les logiciels malveillants, la gestion des correctifs, etc.

Ces mesures peuvent sembler aller de soi, mais l’application de pratiques éprouvées de gestion du risque informatique a permis aux institutions de mieux gérer les menaces qui les guettaient. Le changement périodique des mots de passe, le fait de ne permettre qu’un accès privilégié à l’information essentielle et la réalisation périodique de test d’intrusion comptent pour beaucoup dans la promotion de la résilience et l’amélioration continue.

Ces mesures ne sont qu'une partie de la solution. L'amélioration des mesures préventives n'aboutira pas à grand-chose si l'on ne réfléchit pas à la façon de se remettre d'un incident.

Nous continuerons de surveiller la capacité des institutions financières à s'autoévaluer et à réagir face aux cyberincidents. Les tests de résilience opérationnelle qu'effectueront les entreprises joueront un rôle essentiel et nous savons que nous avons du travail à faire pour concevoir nos outils et nos techniques dans ce domaine.

Le BSIF peaufine son propre protocole interne d'intervention en cas de cyberincident et il collabore et assure la coordination avec le nouveau Centre canadien de cybersécurité en prévision d'un éventuel incident de sécurité nationale.

En augmentant le nombre d'acteurs intervenant en cybersécurité, nous répartissons la charge de travail en proportion de la propagation des risques. Ensemble, nous avons de meilleures chances de mettre à profit les données et les résultats des analyses de ces événements et ainsi améliorer la façon dont nous détectons ces menaces et intervenons.

Réaction du BSIF

Voici dix ans qu'a eu lieu la crise financière mondiale et, depuis, les efforts visant à accroître la résilience du système face aux tensions financières ont été considérables. Toutefois, nous sommes à la croisée des chemins en matière de gestion des risques et de surveillance.

Bien que la résilience financière doive demeurer au cœur de nos préoccupations, il faut aussi prêter attention à la gestion des risques non financiers, car le relèvement des fonds propres n'améliorera pas la résilience face à une cyberattaque ou à l'interruption des services d'un tiers.

De nouveaux outils seront nécessaires pour gérer les nouveaux risques. Le BSIF ne ménage aucun effort pour élaborer ces nouveaux outils et jeter les bases de la collaboration avec d'autres experts, tant au pays qu'à l'étranger.

Nous analysons et évaluons les bonnes pratiques de résilience opérationnelle face aux menaces non financières. En améliorant nos connaissances, nous serons en mesure d'exercer une meilleure surveillance et d'intervenir plus efficacement face aux risques auxquels les institutions sont confrontées. Notre objectif est clair : en arriver à une compréhension commune de ce qui constitue une gestion efficace des risques dans un monde caractérisé par la maturité technologique.

Conclusion

Il existe plusieurs façons de voir l'avenir.

La technologie est porteuse de nouveaux profits et des gains d'efficience qui jouent un rôle important dans la poursuite du succès, l'innovation et la stabilité financière.

Si l’on ne prête attention qu’aux profits, il existe une réelle menace que les risques ne soient pas décelés ou gérés, entachant ainsi la réputation des institutions financières.

Les machines rendent les entreprises plus productives et plus compétentes; toutefois, le jugement humain continuera de définir l’efficacité globale de la gestion des risques dans un avenir prévisible.

Ce qui diffère le présent du passé, c’est jusqu’où nous pouvons voir dans l’avenir. Cette période de prévision s’amenuise en raison du rythme des avancées technologiques et de la numérisation.

Il est essentiel d’assurer un dialogue ouvert avec les spécialistes du risque, les experts en technologie et en science des données et d’autres experts pour favoriser notre propre stabilité. Je suis heureux d’avoir été invité aujourd’hui et je compte bien poursuivre le dialogue sur cet important sujet.