GROUPE DES SEPT (G7) – ÉLÉMENTS FONDAMENTAUX POUR LA GESTION DES RISQUES CYBERNÉTIQUES LIÉS À DES TIERS DANS LE SECTEUR FINANCIER

Contexte et portée

Les entités du secteur privé et public dans le secteur financier (ci-après « entités ») font appel à des tiers pour diverses raisons. Les tiers introduisent des défis supplémentaires quant à la gestion des risques cybernétiques pour les entités avec lesquelles ils sont en relation. Les incidents cybernétiques découlant de la vulnérabilité des tiers peuvent mener à des cas de fraude, à une interruption de services ou à l'accès à des informations sensibles sur un client ou une entreprise. Puisque la taille, la complexité et l'interconnexion des tiers et leur utilisation ne cessent d'augmenter, cerner les risques cybernétiques liés aux tiers pose un défi de plus en plus grand aussi bien pour chaque entité sur une base individuelle que pour le système financier dans son ensemble.

De plus, il se peut que les entités n'aient pas encore développé de techniques robustes pour gérer les risques liés aux tiers auxquels elles ont recours, ce qui contribue à accroître la complexité de la gestion des risques cybernétiques.

Par tiers, on entend des organisations qui ont noué des relations d'affaires ou ont conclu des contrats commerciaux avec une entité afin de lui fournir un produit ou un service. L'externalisation est un type important de relation avec un tiers, lui permettant de fournir à l'entité une fonction, un service ou un processus opérationnel que celle-ci devrait autrement exécuter elle-même.

Éléments fondamentaux

En vue d'aider à gérer les risques cybernétiques, le document *Groupe des sept – Éléments fondamentaux pour la cybersécurité du secteur financier* a été publié en octobre 2016 et le document *Groupe des sept – Éléments fondamentaux pour l'évaluation efficace de la cybersécurité dans le secteur financier*, en octobre 2017.

Afin de contribuer à la gestion des risques liés à des tiers dans le secteur financier, le G7 a élaboré le document *Éléments fondamentaux pour la gestion des risques cybernétiques liés à des tiers dans le secteur financier.* Il s'agit d'éléments fondamentaux que les entités peuvent adapter, au besoin, selon leur profil de risques, leurs opérations, les menaces auxquelles elles sont soumises, leur rôle dans le secteur de même que leurs cadres juridique et réglementaire. Ces éléments ne sont pas contraignants, n'invalident aucun cadre existant, ni n'empêchent leur adaptation continue.

Les éléments fondamentaux ci-dessous prennent en compte le cycle de vie de la gestion des risques cybernétiques liés à des tiers au sein des différentes entités ainsi que la gestion des risques cybernétiques liés à des tiers pouvant avoir des conséquences systémiques. Les entités et les tiers peuvent se servir de ces éléments comme d'un outil pour la gestion des risques cybernétiques. Ce faisant, les entités devraient adopter une approche proportionnelle qui prend

en compte la taille, la nature, la portée, la complexité et l'importance systémique potentielle des risques cybernétiques. Les autorités au sein d'un même territoire de compétence ou entre plusieurs territoires de compétence peuvent se servir de ces éléments fondamentaux pour élaborer leurs actions de politique publique, de réglementation et de supervision, en vue de gérer les risques cybernétiques liés à des tiers.

Cycle de vie de la gestion des risques cybernétiques liés à des tiers

Élément 1 : Gouvernance

Les organes de gouvernance des entités sont responsables de mettre en œuvre et d'effectuer une surveillance efficace de la gestion des risques cybernétiques liés à des tiers et de rendre des comptes à cet égard.

Les organes de gouvernance des entités, tels que les conseils d'administration et les instances dirigeantes, sont ultimement responsables et doivent répondre de la surveillance et de la mise en œuvre de la gestion des risques cybernétiques pour l'entité, y compris les risques posés par ses tiers. Ceci comprend le développement d'une stratégie et d'une analyse de tolérance au risque quant aux relations avec les tiers ainsi qu'une description claire des rôles, des responsabilités et des obligations redditionnelles pour la gestion des risques cybernétiques liés à des tiers. De plus, cette surveillance comprend une communication et une transmission à l'échelon supérieur adéquates dans le cours normal des activités, à tous les niveaux de l'entité et entre l'entité, le tiers et les autorités concernées.

Élément 2 : Processus de gestion des risques concernant les risques cybernétiques liés à des tiers

Les entités disposent d'un processus efficace de gestion des risques cybernétiques liés à des tiers, tout au long du cycle de vie de la gestion des risques posés par les tiers.

Les entités devraient déterminer, évaluer et surveiller les risques cybernétiques associés à leurs tiers et les gérer au moyen d'une approche basée sur les risques. Les entités devraient adopter des politiques et des mesures de contrôle afin de se protéger contre les risques de contagion émanant des tiers. En outre, les entités devraient comprendre les pratiques de gestion des risques cybernétiques, adoptées par les tiers qui leur sont essentiels, y compris dans les situations où les tiers nouent à leur tour des relations d'affaires avec leurs propres tiers, tel que dans le cas de recours à des sous-traitants.

Établissement d'un répertoire des tiers et de leur niveau de criticité

Les entités tiennent à jour un répertoire de leurs tiers et savent dans quelle mesure ces tiers sont indispensables à leurs opérations.

Le répertoire devrait comprendre une liste de tous les tiers, les services et les fonctions qu'ils exécutent, le type de données qu'ils tiennent à jour ou traitent, le caractère sensible de ces données et le niveau de criticité à l'égard des opérations de l'entité.

Évaluation des risques cybernétiques et contrôles préalables
Avant de nouer une nouvelle relation d'affaires avec un tiers, les entités mènent des évaluations des risques cybernétiques et mènent des contrôles préalables en examinant si ces relations sont conformes à leur stratégie de cybersécurité.

Les entités devraient évaluer et gérer, d'une part, les risques cybernétiques potentiels ainsi que les vulnérabilités qu'un tiers pourrait introduire dans leur environnement opérationnel, et, d'autre part, les risques associés à la capacité d'un tiers à livrer un produit ou à exécuter un service. Les entités pourraient examiner les facteurs de risques tels que le niveau d'accès qu'a le tiers aux ressources de l'entité (physiques et logiques), le caractère sensible des données ou du système auquel accède le tiers de même que la méthode de connexion.

Quant aux contrôles préalables à menés par l'entité, les renseignements recueillis pourraient comprendre un examen des performances antérieures du tiers en matière de cyberrésilience. Les entités devraient exiger que leurs tiers mènent des contrôles préalables qui soient conformes à leur propre cycle de vie des risques cybernétiques. Les entités peuvent envisager le recours à des évaluations communes des tiers afin de réaliser des gains d'efficience dans l'exécution des évaluations des risques et des contrôles préalables identifiés précédemment.

Structuration des contrats
Les contrats que les entités concluent avec leurs tiers comprennent des clauses visant à appuyer la gestion des risques cybernétiques.

Les entités devraient s'assurer que les obligations juridiques, les exigences des autorités concernées et leurs propres attentes sont prévues dans un contrat avant d'entamer une relation d'affaires avec un tiers. Cela pourrait comprendre des clauses liées à la conservation, au transfert et à l'élimination des données confidentielles.

Parmi les clauses liées à la cybersécurité, les entités pourraient inclure la portée de la relation, les normes de rendement, les droits d'accès et d'audit, les dispositions en matière de rapports et de sous-traitance et les options de résiliation. À moins de dispositions contraires dans la loi, les dispositions contractuelles devraient faire en sorte que l'entité et les autorités concernées reçoivent les renseignements nécessaires pour évaluer les risques cybernétiques découlant des relations avec les tiers, y compris lorsqu'un changement important est apporté à l'exécution du service prévu au contrat. En outre, les attentes en matière d'établissement de rapports liés aux cyberincidents à l'intention des entités devraient être énoncées dans les contrats.

Surveillance continue
Les entités surveillent les changements concernant la criticité et les risques posés par les tiers et examinent de façon continue leur performance vis-à-vis les normes prévues au contrat en matière de gestion des risques cybernétiques.

La surveillance devrait être proportionnelle à l'importance du risque et prendre en compte les changements concernant la nature de la relation avec le tiers. La surveillance continue pourrait porter sur les changements quant aux vulnérabilités et risques significatifs du tiers, son environnement opérationnel et les répercussions de toute cybermenace ou cyberincident. Les

entités devraient examiner les contrats, afin de déterminer si les tiers s'acquittent de leurs tâches telles qu'elles ont été prévues. L'entité pourrait collecter et analyser des mesures du risque cybernétique et des indicateurs de risque dans le cadre de la surveillance.

Lorsque le tiers fournit des fonctions essentielles ou présente un niveau de risque substantiel pour l'entité, une surveillance plus rigoureuse et fréquente et une supervision adéquate devraient être considérées. Les entités devraient apprendre continuellement et renforcer leur capacité à répondre aux risques cybernétiques liés aux tiers, lesquels évoluent constamment.

Élément 3 : Intervention en cas d'incident
Les entités établissent et mettent en œuvre des plans d'intervention en cas d'incident, qui comprennent les tiers essentiels.

Le plan d'intervention en cas d'incident établi par l'entité devrait comprendre des façons de cerner et de recueillir les renseignements sur les cyberincidents impliquant des tiers et de communiquer avec ces derniers et les autorités concernées. Le plan devrait également prévoir les rôles et responsabilités ainsi que les événements déclencheurs de rapports aux autorités concernées, y compris les équipes nationales de réponse aux incidents cybernétiques.

Des exercices périodiques peuvent aider à cerner les faiblesses, à mettre à l'épreuve la cyberrésilience et à évaluer le caractère adéquat des mesures d'intervention et de rétablissement. Dans la mesure du possible, le plan d'intervention en cas d'incident devrait être testé par les entités, les tiers et les partenaires concernés. Le plan d'intervention en cas d'incident devrait être mis à jour afin de prendre en compte les changements organisationnels et les leçons apprises.

Élément 4 : Plan de contingence
Les entités disposent de plans de contingence pour gérer les situations où les performances des tiers ne répondent pas aux attentes en matière de résultats liés au cyberespace ou si ces tiers présentent des risques cybernétiques qui dépassent l'appétence au risque de l'entité.

Les entités devraient évaluer et utiliser un plan de contingence afin de soutenir leur capacité à maintenir les fonctions essentielles à la suite d'un cyberincident lié à un tiers. Dans le cadre des options liées à ce plan, les entités devraient déterminer des solutions de rechange appropriées et viables dans l'éventualité où les tiers ne peuvent assurer les fonctions essentielles. Il se pourrait que la mise en œuvre de ces solutions de rechange soit nécessaire rapidement, ce qui nécessiterait d'envisager que les fonctions et les services opérationnels soient retransférés à l'entité ou attribués à un ou plusieurs autres tiers. Dans la mesure du possible, les entités devraient inclure des clauses de résiliation dans les contrats avec les tiers. Les entités devraient également examiner et évaluer les plans de contingence des tiers essentiels et comprendre la façon dont ces plans sont validés.

Surveillance des risques cybernétiques à l'échelle du système et coordination intersectorielle

Élément 5 : Surveillance des risques pouvant avoir des conséquences systémiques

Les relations avec des tiers font l'objet d'une surveillance à l'échelle du secteur financier et les sources de risques cybernétiques liés à des tiers qui pourraient avoir des conséquences systémiques sont évaluées.

L'évaluation des risques cybernétiques liés à un tiers dépasse l'entité en soi. Lorsqu'un tiers assure une fonction essentielle pour une entité d'importance systémique ou lorsque plusieurs entités font appel à des tiers communs (risque de concentration), les risques liés à des tiers pourraient avoir des conséquences systémiques. Ces risques devraient être cernés et évalués afin qu'ils puissent être gérés.

Même lorsqu'un tiers n'assure pas une fonction essentielle pour une entité d'importance systémique, si le même tiers est en relation avec plusieurs entités, un risque de concentration pourrait en résulter. De la même façon, l'offre de plusieurs services par un tiers pourrait entraîner un risque global ou additionnel.

Les mesures destinées à gérer ces risques et à améliorer le partage d'information peuvent inclure l'agrégation des renseignements sur les tiers portant sur l'ensemble des entités et l'identification des points de défaillance uniques, d'un risque de concentration ou des canaux de contagion. La substituabilité des tiers pourrait être envisagée pour se protéger contre ces risques. Afin de s'assurer que ces mesures sont efficaces, les entités et les autorités concernées devraient s'efforcer d'améliorer l'échange de renseignements sur les relations avec les tiers à l'échelle du secteur financier.

Élément 6 : Coordination entre les secteurs

Les risques cybernétiques associés aux dépendances à l'égard des tiers entre différents secteurs sont identifiés et gérés par ces différents secteurs.

Le secteur financier dépend des tiers dans d'autres secteurs. Un cyberévénement perturbateur dans un de ces secteurs peut avoir des répercussions sur la capacité des entités à exécuter leurs principales fonctions opérationnelles. Des mesures appropriées devraient être prises en vue de faciliter la coordination entre les secteurs pour identifier et gérer ces risques cybernétiques.

Les efforts visant à améliorer l'échange de renseignements entre les différents secteurs en matière de risques cybernétiques devraient être encouragés, de manière à ce que les entités puissent surveiller et gérer ces risques issus de tiers dans d'autres secteurs.

Les entités des secteurs public et privé devraient travailler en collaboration avec leurs homologues dans d'autres secteurs et au sein de forums sur les infrastructures essentielles afin de promouvoir une saine gestion des risques cybernétiques, d'accroître la cyberrésilience, de promouvoir l'échange de bonnes pratiques, le cas échéant, de mener des actions conjointes.