ÉLÉMENTS FONDAMENTAUX DU G7 POUR LA GESTION DES RISQUES CYBER LIÉS À DES TIERS DANS LE SECTEUR FINANCIER
Octobre 2022

Contexte et portée

Les entités privées et publiques du secteur financier (ci-après « entités ») continuent d'accroître leur recours à des tiers pour soutenir leurs activités. Ces dernières années, cette prolifération s'est caractérisée notamment par le recours accru à des fournisseurs de technologies de l'information et de la communication (ci-après « fournisseurs informatiques »). Le recours à des fournisseurs informatiques peut comporter des avantages pour les entités. Il permet, entre autres, de renforcer leur résilience opérationnelle, de réduire leur dépendance à l'égard des systèmes informatiques plus anciens, et d'accroître leur potentiel d'innovation, de diversification et d'efficacité dans la fourniture de services financiers. En outre, le recours à des services informatiques externes permet aux entités de se concentrer sur leurs activités cœur de métier et de gérer efficacement leurs dépenses informatiques.

Le recours à des prestataires tiers, y compris à des fournisseurs informatiques, peut également introduire des risques cyber supplémentaires que les entités devraient prendre en compte et gérer. Ces dernières années, les incidents cyber ont montré que des parties critiques de la chaîne d'approvisionnement informatique peuvent comporter un risque cyber aussi bien pour une entité individuelle que pour le secteur financier dans son ensemble. Les incidents cyber résultant de vulnérabilités touchant des tiers peuvent, par exemple, mener à des cas de fraude, à une interruption de services, à l'accès non autorisé à des informations sensibles sur un client ou une entreprise, ou nuire à la sécurité et à la solidité des marchés financiers. Puisque l'ampleur et la complexité de ces relations ne cessent de s'accroître, comprendre, mesurer et atténuer les risques cyber pose un défi de plus en plus grand pour les entités ayant recours à des prestataires tiers.

Par relations avec des tiers, on entend, dans les présents éléments fondamentaux, toutes relations d'affaires ou contrats commerciaux conclus entre une entité et une organisation pour la fourniture d'un produit ou d'un service, que cette organisation soit une société intra-groupe ou un fournisseur externe. L'externalisation est un type important de relation avec un tiers, dans laquelle le tiers fournit à l'entité une fonction, un service ou un processus opérationnel qu'elle devrait autrement exécuter elle-même.

La chaîne d'approvisionnement informatique, au sens des présents éléments fondamentaux, comprend le réseau interconnecté de tiers qui forment l'écosystème informatique utilisé par une

entité pour la conduite de ses activités. Elle comprend également tous produits, services et infrastructures, ainsi que leurs fournisseurs, prestataires ou fabricants. Les entités peuvent envisager d'adopter une approche qui permette, dans la chaîne d'approvisionnement informatique qui soutient les opérations critiques, la détection, le rétablissement, l'évaluation continue et l'intervention en cas d'incident.

Éléments fondamentaux

Afin d'aider les entités à faire face aux risques cyber, le document *G7 Fundamental Elements of Cybersecurity for the Financial Sector* a été publié en octobre 2016 et le document *G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*, en octobre 2017. Afin de contribuer à la gestion des risques cyber liés à des tiers dans le secteur financier, le G7 a publié le document *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector* en 2018.

Pour répondre aux évolutions du secteur depuis 2018, le G7 a révisé ses éléments fondamentaux de 2018 en se concentrant non seulement sur la gestion des relations avec les tiers mais également sur la gestion de la chaîne d'approvisionnement informatique. Les éléments fondamentaux actualisés soulignent l'importance du partage d'informations et de la transparence pour faire face à des menaces en constante évolution. Afin d'attirer l'attention sur le rôle de plus en plus important des tiers dans le secteur financier, un nouvel élément fondamental (élément 7) a été ajouté.

Les entités peuvent adapter les présents éléments fondamentaux, au besoin, selon leur propre profil de risque, leurs activités, les menaces auxquelles elles sont confrontées, leur rôle dans le secteur financier ainsi 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 cyber liés à des tiers au sein d'une entité individuelle, le rôle de tiers pour le secteur financier, ainsi que la surveillance du risque cyber à l'échelle du système. En outre, les présents éléments fondamentaux considèrent la gestion des risques cyber liés à des tiers sur l'intégralité de la chaîne d'approvisionnement informatique d'une entité individuelle.

Les entités et les tiers peuvent se servir de ces éléments fondamentaux comme d'un outil pour la gestion des risques cyber. 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 de la relation avec les tiers.

Les autorités au sein d'une même juridiction ou entre plusieurs juridictions 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 cyber liés à des tiers.

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

Élément 1 : Gouvernance

Les organes de gouvernance des entités sont responsables de la mise en œuvre et de la surveillance efficace de la gestion des risques cyber liés à des tiers et rendent des comptes à cet égard.

Les organes de gouvernance des entités, tels que les conseils d'administration et les instances dirigeantes, sont responsables en dernier lieu et doivent répondre de la surveillance et de la mise en œuvre de la gestion des risques cyber pour l'entité, y compris les risques posés par ses relations avec des tiers. Cela comprend la définition d'une stratégie documentée en matière de recours à des tiers, l'élaboration de politiques de gestion des risques tiers et des risques cyber, la définition d'une tolérance au risque quant aux relations avec les tiers, ainsi qu'une description claire des rôles, responsabilités et obligations de rendre compte pour la gestion des risques cyber liés à des tiers intégrée dans les fonctions de contrôle des risques de l'entité, proportionnellement au niveau de risque et à la criticité d'une activité donnée. Cela comprend également des processus appropriés de communication et de remontée de l'information à l'échelon supérieur 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 cyber liés à des tiers

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

Les entités devraient identifier, évaluer, surveiller et signaler au niveau de direction approprié les risques cyber associés à leurs tiers, et les gérer au moyen d'une approche fondée sur les risques. Elles devraient adopter des politiques et des mesures de contrôle afin de se protéger contre les risques de contagion émanant des tiers. Les entités devraient comprendre les pratiques de gestion des risques cyber utilisées par les tiers qui leur sont essentielles, y compris celles liées au recours de ces tiers 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 critiques pour leurs opérations.

Le répertoire devrait comprendre une liste de tous les tiers, les services et les fonctions qu'ils exécutent, le niveau d'accès de chaque tiers aux systèmes de l'entité, et le type de données qu'ils tiennent à jour ou traitent, le caractère sensible de ces données et leur emplacement.

Les entités devraient être capables d'identifier le niveau de criticité du tiers à l'égard des opérations de l'entité. Les facteurs qui déterminent ce niveau de criticité peuvent comprendre la mesure dans laquelle le tiers a accès aux fonctions critiques et activités cœur de métier de l'entité, et en assure

le support. Les entités sont encouragées à mener une évaluation plus approfondie de la chaîne d'approvisionnement informatique associée à leurs tiers en adoptant une approche basée sur les risques. À titre d'exemple, une étape essentielle pourrait consister à obtenir des fournisseurs de logiciels une nomenclature logicielle, telle qu'une liste de bibliothèques logicielles intégrées au logiciel et non strictement liées à la relation avec le tiers concerné (par exemple, les logiciels libres).

Évaluation des risques cyber et diligence raisonnable

Avant d'établir de nouvelles relations avec des tiers et pendant toute la durée de l'engagement, les entités mènent des évaluations des risques cyber et 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 cyber potentiels et les vulnérabilités que pourraient introduire un tiers et la chaîne d'approvisionnement informatique 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 caractère critique des opérations dont le tiers assure le support, le niveau d'accès (physique et logique) dont il dispose, le caractère sensible des données ou du système que le tiers héberge ou auxquels il a accès, de même que la méthode de connexion.

En ce qui concerne les contrôles préalables d'ensemble à mener par l'entité, les informations recueillies pourraient inclure un examen de la stratégie actuelle du tiers en matière de risque cyber et de ses performances antérieures en matière de cyber-résilience. Les entités devraient mener des contrôles préalables des risques cyber avant la conclusion des contrats ainsi que pendant la durée de l'engagement du tiers en adoptant une approche basée sur les risques, afin d'obtenir la garantie proportionnée actualisée que le programme de gestion des risques du tiers est réalisé conformément à leur environnement de contrôle, y compris aux obligations juridiques et réglementaires. Les entités peuvent envisager le recours à des évaluations communes des tiers afin de rationaliser la conduite des évaluations des risques et des contrôles préalables identifiés précédemment.

Structure des contrats

Les contrats que les entités concluent avec leurs tiers comprennent des clauses visant à appuyer la gestion des risques cyber et incluent les risques cyber résultant de la sous-traitance.

Les entités devraient s'assurer que les obligations juridiques, les exigences des autorités compétentes ainsi que leurs propres attentes sont prévues dans un contrat avant d'entamer une relation avec un tiers.

Parmi les clauses liées à la cybersécurité, les entités pourraient inclure la portée de la relation, les niveaux de service, les droits d'accès, d'information et d'audit dont disposent l'entité et ses autorités compétentes, les dispositions en matière de *reporting*, les exigences quant à la fréquence

et aux types de tests de cyber-résilience (tests d'intrusion, test d'intrusion fondés sur la menace (*threat-led penetration testing*), par exemple), les conditions relatives à l'emplacement, au stockage, à la conservation, au transfert et à la suppression des données, la sous-traitance et, dans la mesure du possible, les dispositions relatives à la chaîne d'approvisionnement informatique et les options de résiliation. Sauf disposition contraire de la loi, les accords contractuels devraient faire en sorte que l'entité et les autorités compétentes reçoivent les informations nécessaires pour évaluer les risques cyber 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 de déclaration à l'entité de tout incident dans la chaîne d'approvisionnement informatique pouvant avoir des répercussions négatives sur le profil de risque cyber du tiers, dont les cyber-incidents, 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 manière continue leur performance vis-à-vis des normes prévues au contrat en matière de gestion de leurs risques cyber.

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 relatifs aux vulnérabilités et risques significatifs du tiers, son environnement opérationnel et les répercussions de toute cyber-menace ou cyber-incident. Les entités devraient régulièrement surveiller les performances des tiers afin de déterminer si elles répondent aux attentes prévues par le contrat. L'entité pourrait collecter et analyser des mesures du risque cyber 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, elle devrait envisager une surveillance plus stricte et plus fréquente, et une surveillance suffisante.

Les entités devraient apprendre continuellement et renforcer leur capacité à répondre aux risques cyber liés aux tiers et aux chaînes d'approvisionnement informatiques, lesquels évoluent constamment.

Élément 3 : Dispositif de réaction aux incidents

Les entités établissent et mettent en œuvre des dispositifs de réaction aux incidents, qui incluent les tiers essentiels.

Le dispositif de réaction aux incidents établi par l'entité devrait inclure des méthodes pour détecter et recueillir les informations sur les cyber-incidents impliquant des tiers et de communiquer avec ces derniers et les autorités compétentes. Le dispositif devrait également prévoir les rôles et

responsabilités ainsi que les événements déclencheurs de *reporting* aux autorités compétentes, y compris les équipes nationales de réponse aux cyber-incidents.

Des exercices périodiques peuvent aider à identifier les faiblesses, à mettre à l'épreuve la cyber-résilience et à évaluer le caractère approprié des mesures d'intervention et de rétablissement. Dans la mesure du possible, le dispositif de réaction aux incidents devrait être testé par les entités, les tiers et les partenaires concernés. dispositif de réaction aux incidents devrait être mis à jour afin de prendre en compte les changements organisationnels et les retours d'expérience.

Élément 4 : Plan de continuité et stratégies de sortie

Les entités disposent de plans de continuité d'activité et de stratégies de sortie suffisants pour gérer les situations où les performances des tiers ne répondent pas aux attentes en matière de cybersécurité ou si ces tiers présentent des risques cyber qui dépassent l'appétence au risque de l'entité.

Les entités devraient élaborer et tenir à jour des plans de continuité et des stratégies de sortie viables qui garantissent leur capacité à assurer leurs fonctions essentielles. Les scénarios ayant une incidence sur le risque cyber de l'entité peuvent inclure la survenue d'un événement opérationnel important lié au tiers, les changements intervenus dans la capacité du tiers à exercer ses activités, dans sa stratégie commerciale ou opérationnelle, et/ou dans sa performance. Les options possibles incluent la ré-internalisation du ou des services, ou leur attribution à un autre tiers. Une entité devrait évaluer les options qui conviennent le mieux à ses opérations et qui favorisent le plus la sécurité et la solidité du système financier et limitent les préjudices aux clients.

Les plans de continuité et les stratégies de sortie devraient être testés au besoin et dans la mesure du possible. Les entités devraient également comprendre et valider les plans de continuité de leurs tiers critiques, ainsi que les politiques et normes de gouvernance qui sous-tendent ces plans et stratégies.

Surveillance des risques cyber 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 cyber liés à des tiers qui pourraient avoir des conséquences systémiques sont évaluées.

L'évaluation des risques cyber liés à un tiers dépasse l'entité elle-même. 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 cyber liés à ce tiers pourraient avoir des conséquences systémiques. Ces risques systémiques devraient être identifiés et évalués afin de pouvoir être maîtrisés.

Même lorsqu'un tiers n'assure pas une fonction essentielle pour une entité d'importance systémique, si le même tiers fournit des services à 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 entités devraient identifier, évaluer et surveiller le risque de concentration de leur point de vue concernant leur recours à des tiers et partager les informations pertinentes avec les autorités compétentes.

Les autorités compétentes devraient essayer d'identifier, d'évaluer et de surveiller le risque de concentration et le risque systémique potentiel au niveau de l'entité, ainsi qu'au niveau sectoriel le cas échéant. S'agissant des approches relatives aux risques systémique et de concentration, les autorités compétentes devraient envisager de mettre en œuvre des mesures appropriées pour gérer ces risques et améliorer le partage d'informations, telles que l'agrégation des renseignements sur les tiers au niveau de l'ensemble des entités et l'identification de points de défaillance uniques, de risques de concentration ou de canaux de contagion. La substitution partielle d'un autre tiers pourrait être envisagée pour limiter ces risques. Afin de s'assurer que ces mesures sont efficaces, les entités, les tiers et les autorités compétentes sont encouragés à améliorer le partage d'informations sur les relations avec les tiers à l'échelle du secteur financier.

Élément 6 : Coordination entre les secteurs

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

Le secteur financier dépend de tiers situés dans d'autres secteurs. Un incident cyber perturbateur dans un de ces secteurs pourrait 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 cyber.

Les efforts visant à améliorer l'échange d'informations entre les secteurs en matière de risques cyber devraient être encouragés, afin que les entités puissent surveiller et gérer ces risques issus de tiers situés dans d'autres secteurs.

Les entités et les autorités compétentes devraient continuer de chercher des opportunités de collaborer avec leurs homologues dans d'autres secteurs et au sein de forums sur les infrastructures critiques afin de promouvoir une saine gestion des risques cyber, d'accroître la cyber-résilience, de promouvoir l'échange de bonnes pratiques et, le cas échéant, de mener des actions conjointes.

Élément 7 : Tiers vis-à-vis du secteur financier

Les tiers qui établissent des relations contractuelles avec une entité devraient être conscients que les exigences de ces entités en matière de gestion des risques pourraient avoir des implications pour leur offre de services et de biens.

Les entités demeurent responsables du fonctionnement sûr et solide des services qui leur sont fournis par des tiers. Toutefois, les tiers devraient aider les entités en identifiant, évaluant, surveillant et atténuant les risques cyber ainsi qu'en respectant les exigences associées en matière de gestion des risques. Cela vaut tout particulièrement pour les tiers intervenant en support des services informatiques et de cybersécurité. En ce sens, les tiers devraient mettre à disposition les informations nécessaires pour faciliter la gestion efficace des risques cyber, y compris du risque cyber lié à des tiers. Cela comprend les informations susceptibles d'affecter une entité et ses clients, telles que les informations liées à des incidents significatifs, l'intention de mettre un terme à la fourniture d'un service ou au support d'un service ou d'un produit, et l'intention de nouer une relation avec des tiers à caractère critique ailleurs dans la chaîne d'approvisionnement informatique.

Les prestataires tiers sont encouragés, le cas échéant, à utiliser les présents éléments fondamentaux pour maîtriser les risques émanant des tiers auxquels ils ont eux-mêmes recours dans la chaîne d'approvisionnement.