CENTRE DE DROIT
BANCAIRE ET FINANCIER

IOSCO

Les bonnes pratiques en matière d'*outsourcing*

Par Yannick Caballero Cuevas le 15 novembre 2021

L'*International Organization of Securities Commissions* (IOSCO) a récemment publié une mise à jour des principes en matière d'*outsourcing* établis en 2005 pour les intermédiaires du marché financier (*market intermediaries*), et en 2009 pour les bourses. Cette actualisation est due aux nouveaux développements technologiques et à l'évolution récente dans le domaine de l'externalisation.

Tout d'abord, le champ personnel de ces principes a été élargi. Ceux-ci s'appliquent non seulement aux entités précitées, mais également aux plates-formes de négociation (notamment les systèmes multilatéraux de négociation), aux participants sur les marchés financiers agissant pour leur compte et aux agences de notation (ci-après : les entités réglementées). Le rapport contient aussi une analyse approfondie de l'utilisation de l'externalisation et du *cloud computing* par les agences de notation.

Ce rapport relève ensuite les différents risques de l'*outsourcing* pour les entités réglementées. Parmi ceux-ci, on peut citer la perte de contrôle dans l'exécution des tâches externalisées, le risque accru de cyber-incidents et de fuite de données, ou encore les risques pour la résilience opérationnelle des entités réglementées.

Sept grands principes en matière d'externalisation sont proposés. Ceux-ci peuvent être regroupés en trois catégories, à savoir les principes en matière de sélection du prestataire de services, les principes en matière de contrôle et de supervision du prestataire et finalement les principes s'appliquant à la résiliation des rapports contractuels.

Pour la sélection des prestataires, le rapport préconise la conduite d'un audit. Celui-ci permet notamment d'identifier les potentiels confits d'intérêts, d'évaluer les compétences du prestataire, d'identifier les tâches devant être externalisées et déterminer les risques transfrontaliers liés à l'externalisation. Cet audit facilitera également la rédaction du contrat qui devra répondre aux risques critiques et matériels des tâches externalisées, tout en prévoyant des règles de conflit en matière de droit applicable et de for juridique.

Concernant le contrôle et la supervision du prestataire, le rapport recommande aux entités réglementées et à leurs prestataires de prendre des mesures appropriées pour protéger les données clients contre toute fuite et s'assurer de la résilience du système utilisé. Parmi les mesures proposées, nous trouvons la mise en place de sauvegardes périodiques, la conduite de tests réguliers du système informatique pour évaluer l'efficacité des mesures de cyber-

sécurité, ou encore l'établissement de procédures d'urgence pour le prestataire ou de plans de récupération en cas de sinistre. Ces mesures devront tenir compte des différentes législations applicables, surtout en cas d'externalisation transfrontalière.

Un autre principe aidant à la supervision est l'accès sur demande aux données, aux systèmes informatiques, aux locaux et au personnel du prestataire. Cet accès permet de contrôler la bonne exécution de la tâche externalisée au regard du contrat et des réglementations applicables. Les auditeurs et autorités de surveillance des entités réglementées devront également avoir un droit d'accès. Ainsi, il est suggéré de prévoir une clause contractuelle accordant un droit d'inspection. Il est prévisible que la rédaction de cette clause fera l'objet d'âpres négociations, puisque l'entité réglementée souhaitera avoir le droit d'inspection le plus étendu, tandis que le prestataire limitera celui-ci au strict nécessaire, afin de protéger ses secrets d'affaires. Cette problématique pourrait apparaître en lien à l'accès ou non d'algorithmes *in-house* utilisés par le prestataire pour l'exécution des tâches externalisées.

Finalement, le rapport recommande de prévoir des clauses contractuelles qui déterminent quand une résiliation peut être opérée, à quelles conditions et quand la résiliation prend effet. Ces clauses permettent d'instaurer une période transitoire avant la fin des rapports contractuels. Les parties devront également prévoir des procédures pour le transfert des données à l'entité réglementée ainsi que leur suppression.

En conclusion, ces principes n'ont rien de révolutionnaires, mais clarifient les bonnes pratiques à adopter lorsqu'une tâche est externalisée auprès d'un prestataire. D'ailleurs, on remarque que de grands principes en matière de sécurité de l'information deviennent incontournables comme la résilience des systèmes face aux cyber-incidents. Ces principes peuvent donc inspirer plus d'une institution au moment d'externaliser ses tâches.
