AVIS AUX MEMBRES
Nº 076-23

Le 12 juin 2023

# SOLLICITATION DE COMMENTAIRES

## MODIFICATION DES RÈGLES DE LA CORPORATION CANADIENNE DE COMPENSATION DE PRODUITS DÉRIVÉS EN MATIÈRE DE CYBERSÉCURITÉ

Le 2 février 2023, le Conseil d'administration de la Corporation canadienne de compensation de produits dérivés (la « CDCC ») a approuvé des modifications aux Règles de la CDCC afin d'introduire la notion de cybersécurité. Ces modifications ont pour objectif d'établir des exigences en matière de cybersécurité et de permettre à la CDCC de surveiller la conformité des membres compensateurs à cet égard.

Veuillez trouver ci-joint un document d'analyse de même que les modifications proposées.

**Processus d'établissement de règles**

La CDCC est reconnue à titre de chambre de compensation en vertu de l'article 12 de la *Loi sur les instruments dérivés* (Québec) par l'Autorité des marchés financiers (l'« Autorité ») et à titre d'agence de compensation reconnue par la Commission des valeurs mobilières de l'Ontario (la « CVMO ») en vertu de l'article 21.2 de la *Loi sur les valeurs mobilières* (Ontario).

Le Conseil d'administration de la CDCC a le pouvoir d'adopter ou de modifier les règles et le manuel des opérations de la CDCC. Ces modifications sont présentées à l'Autorité conformément au processus d'autocertification ainsi qu'à la CVMO conformément au processus stipulé dans la décision de reconnaissance.

Les commentaires relatifs aux modifications proposées doivent nous être présentés avant le 13 juillet 2023. Prière de soumettre ces commentaires à:

**Sophie Brault**
Conseiller juridique
*Corporation canadienne de compensation de produits dérivés*
1800-1190 av. des Canadiens-de-Montréal, C.P. 37
Montréal QC H3B 0G7
Courriel: **legal@tmx.com**

Ces commentaires devront également être transmis à l'Autorité et à la CVMO à l'attention de :

Me Philippe Lebel
Secrétaire général et directeur général
des affaires juridiques
Autorité des marchés financiers
Place de la Cité, tour Cominar
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1
Télécopieur : (514) 864-8381
Courriel : consultation-en-cours@lautorite.qc.ca

Manager, Market Regulation
Market Regulation Branch
*Ontario Securities Commission*
Suite 2200,
20 Queen Street West
Toronto, Ontario, M5H 3S8
Télécopieur : 416-595-8940
Courriel : marketregulation@osc.gov.on.ca

Pour toutes questions ou informations, les membres compensateurs peuvent communiquer avec Sophie Brault, Conseillère juridique, par courriel au sophie.brault@tmx.com**.**

George Kormas
Président

**MODIFICATION DES RÈGLES DE LA CORPORATION CANADIENNE DE COMPENSATION DE PRODUITS DÉRIVÉS EN MATIÈRE DE CYBERSÉCURITÉ**

## I. DESCRIPTION

En octobre 2021, la Banque du Canada a publié des exigences réglementaires intitulées *Cyberrésilience : attentes à l'égard des infrastructures de marchés financiers* (le « Document sur la cyberrésilience »)[1].

Aux termes de la sous-section 3.3.1 du Document sur la cyberrésilience :

***3.3.1 Risques liés aux interconnexions***
*Étant donné son importance systémique et sa position unique au sein du système financier, l'IMF devrait mettre en place des mesures de protection visant à atténuer les risques découlant des entités de son écosystème. Les contrôles appropriés pour chaque entité dépendent des résultats de l'évaluation des risques effectuée à la phase d'identification, y compris les risques associés à l'entité connectée et au type de relation qu'entretient l'IMF avec cette dernière.*

La Banque du Canada a établi qu'elle attendait de la Corporation canadienne de compensation de produits dérivés (la « CDCC ») qu'elle exerce une supervision renforcée en matière de cybersécurité à l'égard des entités externes de son écosystème (interconnexion).

Les règles actuelles ne mentionnant pas explicitement d'exigences en matière de sécurité de l'information et de cybersécurité, la CDCC propose de modifier ses règles afin d'y inclure des exigences en matière de cybersécurité et des pouvoirs de surveillance à l'égard des contrôles de sécurité que les membres compensateurs doivent mettre en place. De plus, la CDCC propose de modifier ses règles pour permettre l'imposition de sanctions autres que le statut de membre non conforme (qui peut entraîner une suspension) dans le contexte de ces nouvelles exigences en matière de cybersécurité.

À moins que d'autres définitions ne soient précisées dans la présente analyse, tous les termes clés qui y sont employés ont le sens qui leur est attribué dans les règles, le manuel des opérations, le manuel des risques et le manuel de défaut (les « Règles »).

---

1 URL : https://www.banqueducanada.ca/wp-content/uploads/2021/10/Cyberresilience-attentes-egard-infrastructures-marches-financiers.pdf

## II. MODIFICATIONS PROPOSÉES

La CDCC propose par les présentes de modifier l'article 1A02 (« Critères d'adhésion ») de la règle A-1A et d'ajouter deux nouveaux articles à la règle A-2 (articles A-225 et A-226) en vue d'introduire la notion de cybersécurité. Ces modifications ont pour objectif d'établir des exigences en matière de cybersécurité et de permettre à la CDCC de surveiller la conformité des membres compensateurs à cet égard.

Ces modifications n'auront aucune incidence sur le manuel des opérations, le manuel des risques et le manuel de défaut de la CDCC.

## III. ANALYSE

### a. Contexte

L'écosystème de la CDCC comprend deux principaux groupes d'entités externes, soit les prestataires de service ou fournisseurs et les membres compensateurs. Les premiers sont encadrés de manière exhaustive par diverses politiques internes de TMX et de la CDCC et ne sont pas concernés par la présente analyse. Toutefois, aucun processus semblable n'est en place à la CDCC concernant les membres compensateurs. La CDCC a réalisé un examen des risques liés à la cyberrésilience qui pourraient être posés par ses membres compensateurs et mené des travaux en vue de se doter de mécanismes adéquats de surveillance des membres compensateurs et de leurs contrôles de cybersécurité, comme indiqué dans le Document sur la cyberrésilience.

Le Bureau de la sécurité de l'information de TMX a effectué un examen complet de la manière dont les membres compensateurs se connectent à la CDCC. Cette évaluation des menaces et des risques (EMR) a fait porter la méthodologie d'EMR sur l'efficacité des mesures de sécurité qui protègent les connexions des membres compensateurs de la CDCC. La portée de l'évaluation s'est étendue aux actifs informatiques dont se servent les membres compensateurs pour se connecter à la CDCC et accéder aux données et aux rapports liés à leurs activités. La nature de la connectivité des membres compensateurs à la CDCC limite le risque qu'un membre compensateur introduise un cyberrisque à la CDCC. Compte tenu du « faible » risque existant selon cette évaluation, le Bureau de la sécurité de l'information a élaboré une série de contrôles de sécurité obligatoires en se fondant tant sur Document sur la cyberrésilience que sur les pratiques adoptées par des infrastructures de marchés financiers semblables sur d'autres territoires[2].

À compter de 2023, les membres compensateurs seront tenus d'attester annuellement qu'ils sont dotés des contrôles obligatoires.

2 Rapport d'avril 2012 intitulé Principes pour les infrastructures de marchés financiers (les « PIMF ») publié par le Comité sur les paiements et les infrastructures de marché et l'Organisation internationale des commissions de valeurs - https://www.bis.org/cpmi/publ/d101_fr.pdf

**b. Objectifs**

Les modifications proposées des règles devraient présenter trois avantages : a) démontrer la conformité de la CDCC aux exigences réglementaires énoncées dans le Document sur la cyberrésilience; b) conférer à la CDCC le pouvoir d'exiger que les membres compensateurs mettent en place des contrôles de sécurité donnés; et c) réduire les risques auxquels la CDCC pourrait être exposée du fait de l'insuffisance des contrôles de cybersécurité et de sécurité des technologies introduits dans ses activités par un ou des membres compensateurs.

**c. Analyse comparative**

La CDCC a réalisé une analyse comparative des renseignements publics sur les pratiques exemplaires d'IMF semblables en matière de cybersécurité. Cette analyse avait pour objectif de déterminer la meilleure démarche à suivre pour mettre à jour les règles de la CDCC afin d'y inclure des exigences en matière de gestion des risques de sécurité, comme l'exige le Document sur la cyberrésilience.

Les sociétés suivantes comptent parmi les organisations examinées : Depository Trust & Clearing Corporation (la « DTCC »), National Securities Clearing Corporation (la « NSCC »), Options Clearing Corporation (l'« OCC »), CME Clearing (la « CME ») et Eurex Clearing (l'« Eurex »).

Les chambres de compensation comparables ne communiquent pas publiquement d'information détaillée sur les contrôles de sécurité qu'elles exigent de leurs membres compensateurs. Toutefois, l'analyse comparative a permis d'établir qu'une pratique généralement acceptée consiste à imposer aux membres compensateurs de mettre en œuvre un programme de sécurité rigoureux, dont l'efficacité doit être attestée par un dirigeant du membre compensateur, comme le chef de la sécurité de l'information, le chef de l'information ou le chef de la technologie.

Le programme de sécurité des membres doit régulièrement faire l'objet d'un audit par un tiers indépendant. Dans le cadre de leur processus de vérification en matière de cybersécurité, la DTCC et la NSCC exigent notamment de leurs membres compensateurs qu'ils mettent en œuvre un programme de sécurité fondé sur l'une des principales normes internationales ou américaines en matière de sécurité, comme l'ISO27001 ou le NIST Cybersecurity Framework. Ce programme de sécurité doit être continuellement en vigueur et à jour, et être régulièrement audité. Chaque membre est tenu de remplir l'attestation en matière de sécurité au minimum tous les deux ans et de répondre à tout avis de non-conformité dans un délai de 180 jours.

L'OCC utilise un formulaire d'attestation en matière de cybersécurité et un processus semblable à ceux de la DTCC. Elle exige que chaque membre compensateur remplisse et dépose un formulaire confirmant l'existence d'un programme de cybersécurité des systèmes informatiques approuvé par la haute direction ou le conseil d'administration du membre.

La CME n'a pas publié d'exigences expresses à l'intention de ses membres. La quasi-totalité des règles publiées sur son site Web porte sur les affaires, les obligations juridiques et la mise en exécution des règles, mais on n'y trouve aucune règle portant précisément sur la sécurité.

L'Eurex n'a pas publié d'exigences expresses à l'intention de ses membres. Elle attend de ses membres qu'ils disposent d'un personnel suffisamment compétent, y compris des personnes-ressources pour la résolution des problèmes urgents, mais ne mentionne pas de cyberincidents potentiels. Les membres sont « obligés » de mettre à niveau toute norme technique conformément aux exigences d'Eurex. Il peut s'agir d'exigences en matière de sécurité, mais le contenu précis des exigences (le cas échéant) n'est pas public.

Conclusions

- Les IMF examinées ont opté pour un mécanisme d'attestation (plutôt que des audits informatiques en profondeur ou des évaluations techniques sur place).
- Aucune des IMF examinées n'a publié la liste explicite de ses exigences en matière de contrôles de cybersécurité. Elles renvoient aux normes internationales de sécurité de haut niveau.
- En règle générale, le délai accordé aux membres pour qu'ils remédient à tout manquement est de 180 jours.
- Les sanctions pécuniaires en cas de manquement ne sont pas précisées.

**d. Analyse des incidences**

**i. Incidences sur le marché**

Les modifications proposées n'auront aucune incidence sur le marché.

**ii. Incidences sur les systèmes technologiques**

Nous ne nous attendons pas à ce que les modifications proposées des règles nécessitent ou entraînent des changements pour les systèmes technologiques. Elles pourraient avoir une légère incidence sur le plan des ressources humaines. Le processus d'attestation étant nouveau et touchant tous les membres compensateurs (ce qui génère du travail de gestion), nous nous attendons à ce qu'il faille augmenter les ressources affectées aux fonctions de gestion des relations avec la clientèle et de sécurité informatique.

**iii. Incidences sur les fonctions de négociation**

Les modifications proposées n'auront aucune incidence sur les règles ou les systèmes de négociation de la Bourse de Montréal.

**iv. Intérêt public**

La CDCC est d'avis que les modifications proposées ne sont pas contraires à l'intérêt public. Les modifications proposées des règles serviront l'intérêt public, puisqu'elles réduiront le risque qu'un cyberincident porte atteinte aux fonctions de négociation et de compensation. Les pouvoirs additionnels de supervision en matière de cybersécurité sont également dans l'intérêt du public, en ce qu'ils permettraient de surveiller les risques que les parties externes sont susceptibles d'introduire pour les IMF. Cette démarche répond aux attentes du public et des

membres compensateurs, qui demandent des règles claires, en phase avec les pratiques exemplaires des autres chambres de compensation et conformes aux PIMF.

## IV. PROCESSUS

Les modifications proposées, de même que la présente analyse, doivent être approuvées par le conseil d'administration de la CDCC, puis présentées à l'Autorité des marchés financiers, conformément au processus d'autocertification réglementaire, ainsi qu'à la Commission des valeurs mobilières de l'Ontario, conformément aux règles énoncées à l'appendice A de l'annexe C de l'ordonnance de reconnaissance de la CDCC datée du 8 avril 2014 (dans sa version modifiée de temps à autre). Les modifications proposées et l'analyse seront également soumises à la Banque du Canada, conformément à l'accord de surveillance. Après avoir été soumises aux commentaires du public, les modifications proposées devraient entrer en vigueur au cours du deuxième trimestre de 2023.

## V. DOCUMENTS JOINTS

- Annexe 1 : Règles modifiées

**ANNEXE 1 : MODIFICATIONS PROPOSÉES DES RÈGLES**

**VERSION AFFICHANT LES MODIFICATIONS**

**CORPORATION CANADIENNE DE COMPENSATION DE PRODUITS DÉRIVÉS**

**RÈGLES 202X**

[…]

**RÈGLE A-1A – ADHÉSION À LA SOCIÉTÉ**

[…]

**Article A-1A02 – Critères d'adhésion**

Chaque candidat qui souhaite devenir un membre compensateur doit satisfaire aux critères qui peuvent être adoptés par le Conseil à l'occasion, dont les critères suivants :

a) le candidat doit satisfaire aux exigences minimales en matière de résilience financière en vigueur à ce moment-là, applicables à un membre compensateur, conformément à l'article A-301 ou, dans le cas d'un candidat au titre de membre compensateur à responsabilité limitée, aux exigences minimales en matière de résilience financière applicables à l'admission à titre de membre compensateur à responsabilité limitée, conformément à l'article A-1B04;

b) le candidat doit exercer ou projeter d'exercer des activités de compensation d'options, de contrats à terme visés par des opérations boursières ou de compensation d'opérations sur titres à revenu fixe ou d'autres opérations IMHC par l'intermédiaire de la Société;

c) le candidat doit démontrer à la Société que ses installations opérationnelles et son personnel sont adéquats et que les membres de son personnel sont en nombre suffisant et ont la compétence nécessaire pour la transaction rapide et ordonnée des affaires avec la Société et d'autres membres compensateurs, et pour la conformité aux exigences prévues par les présentes règles;

d) sauf si l'entité demande l'adhésion à titre de membre compensateur à responsabilité limitée, le candidat a effectué, auprès de la Société, le dépôt de base dans le fonds de compensation selon le montant et dans les délais prescrits par les règles et il a signé et fait parvenir à la Société une convention en la forme prescrite par le Conseil.

e) sauf si l'entité demande l'adhésion à titre de membre compensateur à responsabilité limitée, le candidat a effectué, auprès de la Société, ses contributions de liquidité supplémentaire initiales au fonds de liquidité supplémentaire selon le montant et dans les délais prescrits par les règles et le manuel des risques;~~.~~

f) le candidat doit satisfaire aux exigences en matière de cybersécurité en vigueur à ce moment-là conformément à l'article A-225.

[…]

**RÈGLE A-2 – EXIGENCES DIVERSE**

[…]

**Article A-225 - Exigences en matière de cybersécurité**

Tout membre compensateur doit se doter d'un programme et d'un cadre de cybersécurité complets concernant les cybermenaces susceptibles de nuire à son organisation et protéger la confidentialité, l'intégrité et l'accessibilité de ses systèmes et de ses données.

Tout membre compensateur doit a) régulièrement mettre à jour les processus liés aux risques prévus par son programme et son cadre de cybersécurité sur la base d'une évaluation des risques ou de l'évolution des systèmes technologiques, de ses activités, du contexte de risque ou du cadre réglementaire; et b) mettre en œuvre les pratiques exemplaires du secteur et appliquer les principales normes mondiales en matière de sécurité pour protéger l'interface et/ou la connectivité entre ses systèmes et ceux de la CDCC, afin de prévenir l'interruption ou la contamination des systèmes de la CDCC en cas d'incident de sécurité le touchant.

La Société peut, de la manière et à la fréquence qu'elle décidera, à sa seule discrétion, examiner le programme et le cadre de cybersécurité du membre compensateur et faire toutes les recommandations qu'elle juge nécessaires ou souhaitables. Le membre compensateur doit suivre lesdites recommandations dans le délai prescrit par la Société.

Chaque membre compensateur doit indemniser, dégager de toute responsabilité et tenir la CDCC couvertes ainsi que ses affiliés et ses filiales de même que leurs associés, administrateurs, fiduciaires, dirigeants, employés et mandataires respectifs de l'ensemble des dommages ou pertes subis par l'un, plusieurs ou l'ensemble de ceux-ci, de tous frais ou dépenses occasionnés pour eux, de toute responsabilité leur incombant ou de toute action intentée contre eux (y compris les honoraires des avocats engagés pour les conseiller ou les défendre) par suite d'un manquement de ce membre compensateur aux exigences en matière de cybersécurité.

Si la Société doit corriger ou modifier ses systèmes, de quelque manière que ce soit, en raison d'une atteinte à la cybersécurité d'un membre compensateur ou de l'accès par un tiers aux systèmes du membre compensateur, la Société a le droit de recouvrer directement auprès de ce membre compensateur tous les frais et dépenses occasionnés par cette correction ou cette modification.

Le membre compensateur qui ne se conforme pas à cette règle ou procédures est également passible de mesures disciplinaires conformément aux présentes règles

**Article A-226 - Mesures liées à la cybersécurité**

Si elle détermine qu'un membre compensateur manque aux exigences en matière de cybersécurité, la Société peut, au lieu de prendre les autres mesures énoncées aux présentes, imposer à celui-ci les mesures de redressement suivantes :

1. une amende d'au plus 50 000$;
2. l'obligation de nommer, à ses frais, un auditeur acceptable pour la Société, chargé de rédiger un rapport sur son état de cybersécurité et sur les mesures correctives qu'il devrait prendre pour satisfaire aux exigences de cybersécurité. L'auditeur doit communiquer son rapport à la Société et au membre compensateur.

Si le membre compensateur continue de manquer à toute exigence en matière de cybersécurité ou ne prend pas les mesures correctives voulues à la satisfaction de la Société, cette dernière peut prendre toute autre mesure énoncée à l'article A-226 ou toute autre mesure prévue par les règles.

**ANNEXE 1 : MODIFICATIONS PROPOSÉES DES RÈGLES**

**VERSION AU PROPRE**

**CORPORATION CANADIENNE DE COMPENSATION DE PRODUITS DÉRIVÉS**

**RÈGLES 202X**

[…]

**RÈGLE A-1A – ADHÉSION À LA SOCIÉTÉ**

[…]

**Article A-1A02 – Critères d'adhésion**

Chaque candidat qui souhaite devenir un membre compensateur doit satisfaire aux critères qui peuvent être adoptés par le Conseil à l'occasion, dont les critères suivants :

a) le candidat doit satisfaire aux exigences minimales en matière de résilience financière en vigueur à ce moment-là, applicables à un membre compensateur, conformément à l'article A-301 ou, dans le cas d'un candidat au titre de membre compensateur à responsabilité limitée, aux exigences minimales en matière de résilience financière applicables à l'admission à titre de membre compensateur à responsabilité limitée, conformément à l'article A-1B04;

b) le candidat doit exercer ou projeter d'exercer des activités de compensation d'options, de contrats à terme visés par des opérations boursières ou de compensation d'opérations sur titres à revenu fixe ou d'autres opérations IMHC par l'intermédiaire de la Société;

c) le candidat doit démontrer à la Société que ses installations opérationnelles et son personnel sont adéquats et que les membres de son personnel sont en nombre suffisant et ont la compétence nécessaire pour la transaction rapide et ordonnée des affaires avec la Société et d'autres membres compensateurs, et pour la conformité aux exigences prévues par les présentes règles;

d) sauf si l'entité demande l'adhésion à titre de membre compensateur à responsabilité limitée, le candidat a effectué, auprès de la Société, le dépôt de base dans le fonds de compensation selon le montant et dans les délais prescrits par les règles et il a signé et fait parvenir à la Société une convention en la forme prescrite par le Conseil.

e) sauf si l'entité demande l'adhésion à titre de membre compensateur à responsabilité limitée, le candidat a effectué, auprès de la Société, ses contributions de liquidité supplémentaire initiales au fonds de liquidité supplémentaire selon le montant et dans les délais prescrits par les règles et le manuel des risques;

f) le candidat doit satisfaire aux exigences en matière de cybersécurité en vigueur à ce moment-là conformément à l'article A-225.

[…]

**RÈGLE A-2 – EXIGENCES DIVERSE**

[…]

**Article A-225 - Exigences en matière de cybersécurité**

Tout membre compensateur doit se doter d'un programme et d'un cadre de cybersécurité complets concernant les cybermenaces susceptibles de nuire à son organisation et protéger la confidentialité, l'intégrité et l'accessibilité de ses systèmes et de ses données.

Tout membre compensateur doit a) régulièrement mettre à jour les processus liés aux risques prévus par son programme et son cadre de cybersécurité sur la base d'une évaluation des risques ou de l'évolution des systèmes technologiques, de ses activités, du contexte de risque ou du cadre réglementaire; et b) mettre en œuvre les pratiques exemplaires du secteur et appliquer les principales normes mondiales en matière de sécurité pour protéger l'interface et/ou la connectivité entre ses systèmes et ceux de la CDCC, afin de prévenir l'interruption ou la contamination des systèmes de la CDCC en cas d'incident de sécurité le touchant.

La Société peut, de la manière et à la fréquence qu'elle décidera, à sa seule discrétion, examiner le programme et le cadre de cybersécurité du membre compensateur et faire toutes les recommandations qu'elle juge nécessaires ou souhaitables. Le membre compensateur doit suivre lesdites recommandations dans le délai prescrit par la Société.

Chaque membre compensateur doit indemniser, dégager de toute responsabilité et tenir la CDCC couvertes ainsi que ses affiliés et ses filiales de même que leurs associés, administrateurs, fiduciaires, dirigeants, employés et mandataires respectifs de l'ensemble des dommages ou pertes subis par l'un, plusieurs ou l'ensemble de ceux-ci, de tous frais ou dépenses occasionnés pour eux, de toute responsabilité leur incombant ou de toute action intentée contre eux (y compris les honoraires des avocats engagés pour les conseiller ou les défendre) par suite d'un manquement de ce membre compensateur aux exigences en matière de cybersécurité.

Si la Société doit corriger ou modifier ses systèmes, de quelque manière que ce soit, en raison d'une atteinte à la cybersécurité d'un membre compensateur ou de l'accès par un tiers aux systèmes du membre compensateur, la Société a le droit de recouvrer directement auprès de ce membre compensateur tous les frais et dépenses occasionnés par cette correction ou cette modification.

Le membre compensateur qui ne se conforme pas à cette règle ou procédures est également passible de mesures disciplinaires conformément aux présentes règles

**Article A-226 - Mesures liées à la cybersécurité**

Si elle détermine qu'un membre compensateur manque aux exigences en matière de cybersécurité, la Société peut, au lieu de prendre les autres mesures énoncées aux présentes, imposer à celui-ci les mesures de redressement suivantes :

1. une amende d'au plus 50 000$;
2. l'obligation de nommer, à ses frais, un auditeur acceptable pour la Société, chargé de rédiger un rapport sur son état de cybersécurité et sur les mesures correctives qu'il devrait prendre pour satisfaire aux exigences de cybersécurité. L'auditeur doit communiquer son rapport à la Société et au membre compensateur.

Si le membre compensateur continue de manquer à toute exigence en matière de cybersécurité ou ne prend pas les mesures correctives voulues à la satisfaction de la Société, cette dernière peut prendre toute autre mesure énoncée à l'article A-226 ou toute autre mesure prévue par les règles.