CSA/ACVM Canadian Securities Administrators | Autorités canadiennes en valeurs mobilières

Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada

Staff Notice 21-329

Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements

March 29, 2021

Part 1. Introduction

The Canadian Securities Administrators (**CSA**) and the Investment Industry Regulatory Organization of Canada (**IIROC** and, together with the CSA, **we**) are publishing this Notice to provide guidance on how securities legislation[1] applies to platforms (**Crypto Asset Trading Platforms**, or **CTP**s) that facilitate or propose to facilitate the trading of:

- crypto assets that are securities (**Security Tokens**), or
- instruments or contracts involving crypto assets, as indicated in CSA Staff Notice 21-327 *Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto-Assets* (**CSA SN 21-327**) (**Crypto Contracts**).

This Notice also includes an overview of the applicable existing regulatory requirements and areas where there may be flexibility in how the requirements apply to CTPs, provided the key risks are addressed. Appendix A of this Notice includes a description of the key risks related to CTPs.

This Notice does not introduce new rules specifically applicable to CTPs, as CTPs are already subject to existing requirements under securities legislation in Canada. Rather, where appropriate, it provides guidance on how the existing requirements of securities legislation may be tailored through terms and conditions on the registration or recognition of CTPs and through discretionary exemptive relief with appropriate conditions. This approach allows CTPs to operate with appropriate regulatory oversight.

The overall goal of the approach outlined in this Notice is to ensure there is a balance between needing to be flexible in order to foster innovation in the Canadian capital markets and meeting our regulatory mandate of promoting investor protection and fair and efficient capital markets.

This Notice discusses CTPs that operate in a manner similar to marketplaces[2] (referred to as "**Marketplace Platforms**") and other CTPs that are in the business of trading Security Tokens or Crypto Contracts that are not marketplaces (referred to as "**Dealer Platforms**"). In some situations, a CTP may be carrying out activities that have elements of both Marketplace Platforms and Dealer Platforms, and this

[1] As defined in National Instrument 14-101 *Definitions* and includes legislation related to both securities and derivatives.

[2] A marketplace is defined in National Instrument 21-101 *Marketplace Operation* (**NI 21-101**). A marketplace is an entity that brings together the orders of multiple buyers and sellers of securities, and in some jurisdictions, parties to certain types of derivatives, using established, non-discretionary methods through which buyers and sellers agree to the terms of a trade.

Notice describes how existing regulatory requirements could apply to these CTPs. We note that, as this industry is still developing, a wide variety of CTP models are emerging. Depending on the business model and activities conducted by a CTP and the risks it creates, the regulatory treatment of one CTP may differ from another.

The guidance in this Notice focuses on CTPs that facilitate the trading of Security Tokens and/or Crypto Contracts. There may be platforms that facilitate the trading of other products or contracts that are structured as "traditional" derivatives and that also provide exposure to crypto assets (including commodity futures contracts, contracts for difference or swaps). We remind these platforms that they are subject to our jurisdiction and to existing regulatory requirements and that they should contact their local securities regulatory authority to discuss possible approaches to comply with securities legislation.[3]

In the future, the CSA plans to examine the regulatory framework that applies to dealers and marketplaces that trade over-the-counter derivatives more generally. Any proposal will be subject to the normal course process for consultation (including publication for comment).

The guidance in this Notice is intended to provide clarity regarding the steps that a CTP needs to take to comply with securities legislation, including interim steps that will allow a CTP to operate as they prepare to fully integrate into the Canadian regulatory structure. The CSA welcomes innovation. We recognize the continued evolution of fintech businesses, the infrastructure that supports such businesses, and both Canadian and foreign regulatory structures. This continued evolution may result in the tailoring of requirements or providing exemptions to accommodate their novel business and any developments, or result in alternative regulatory frameworks from the one described in this Notice being suitable for CTP business models.

Part 2. Background

Since the creation of Bitcoin in 2008, there has been growing investor interest in crypto assets and, in turn, a proliferation of CTPs that allow investors to trade these crypto assets. On March 14, 2019, the CSA and IIROC published Joint CSA/IIROC Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms* (**CP 21-402**). In CP 21-402, we outlined a proposed regulatory framework for CTPs, with a focus on Marketplace Platforms, and solicited comments in a number of areas to better understand the industry, its risks, and how regulatory requirements may be tailored for CTPs operating as marketplaces in Canada.

[3] For example, certain dealers are in the business of trading contracts for difference and similar "over-the-counter" derivative products that are currently treated as both securities and derivatives for the purposes of securities legislation in certain jurisdictions, and therefore compliance with the registration and prospectus requirements is required (in certain jurisdictions, contracts for difference and other "over-the-counter" derivative products are exclusively derivatives and therefore compliance with registration and other applicable provisions is required). Another example relates to certain foreign marketplaces operating facilities or markets that trade derivatives **(**e.g., swap execution facilities) that currently operate their business locally under an exemption from the requirement to register as an exchange. Depending on the functions or operations of the platform that is in the business of trading derivatives, the platform may be operating as a dealer, a marketplace, a clearing agency or a combination of these categories, and therefore, registration or recognition requirements will apply.

We received 52 comments in response and thank all those that provided comments. A summary of comments and responses is attached at Appendix C of this Notice.

We also met with CTPs and consulted extensively with industry stakeholders on issues specific to CTPs.

After having considered this additional information, we are providing guidance for both Marketplace Platforms and Dealer Platforms that is generally consistent with CP 21-402, but also contemplates an interim regulatory approach.

Part 3. Application of Securities Legislation to CTPs

The requirements that will be applicable to a CTP will depend on how it operates and what activities it undertakes. Generally, this will depend on whether the CTP operates as a Dealer Platform or a Marketplace Platform.

Below, we describe characteristics of Dealer Platforms and Marketplace Platforms and provide guidance on steps for CTPs to take in order to comply with securities legislation. We also provide guidance on the application process.

a. Dealer Platforms

The two most common characteristics of a CTP that suggest it would be a Dealer Platform and not a Marketplace Platform are as follows:

- it only facilitates the primary distribution of Security Tokens, and
- it is the counterparty to each trade in Security Tokens and/or Crypto Contracts, and client orders do not otherwise interact with one another on the CTP.

CTPs that are Dealer Platforms may also be engaged in other activities or perform other functions that marketplaces typically do not undertake. These include, but are not limited to:

- onboarding of retail clients onto the CTP,
- acting as agent for clients for trades in Security Tokens or Crypto Contracts, and
- offering custody of assets, either directly or through a third-party provider.

i. Registration Categories for Dealer Platforms

The appropriate category of dealer registration for a Dealer Platform will depend on the nature of its activities.

If the Dealer Platform only facilitates distributions or the trading of Security Tokens in reliance on prospectus exemptions and does not offer margin or leverage, registration as an exempt market dealer, or in some circumstances, restricted dealer may be appropriate, although this would not preclude the Dealer Platform from seeking registration as an investment dealer. Dealer Platforms may not offer margin or leverage for Security Tokens unless they are registered as an investment dealer and are IIROC members.

Similarly, Dealer Platforms that trade Crypto Contracts are expected to be registered in an appropriate dealer category, and where they trade or solicit trades for retail investors that are individuals, they will generally be expected to be registered as investment dealers and be IIROC members, subject to the interim approach described below.

In Québec, Dealer Platforms that are in the business of trading Crypto Contracts that are derivatives will be required to register as derivatives dealers under the Québec Derivatives Act (**QDA**). Dealer Platforms that also create and market derivatives must be qualified by the Autorité des marchés financiers (**AMF**) before derivatives are offered to the public.[4]

We recognize that some of the requirements under securities legislation including, as applicable, National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (**NI 31-103**) or the IIROC Dealer Member Rules may need to be tailored. Summaries of existing regulatory requirements applicable to dealers are included at Appendix C of CP 21-402.[5] In the Summary of Comments and Responses to CP 21-402, at Appendix C of this Notice, we have indicated some of the areas where we think that flexibility in the application of existing regulatory requirements may be provided. We encourage Dealer Platforms to reach out to us to discuss their business models, the appropriate registration category and how requirements may be tailored. The CSA and, as applicable, IIROC may, on application, consider discretionary exemptions from existing applicable rules where the Dealer Platform demonstrates that it can comply with the policy intent of the existing regulatory requirements in alternative ways.

Existing registered firms introducing crypto asset products and/or services are required to report changes in their business activities to their principal regulator and, in the case of investment dealers, to IIROC. The proposed changes to activities may be subject to review to assess, among other requirements, whether there is adequate investor protection. If a Dealer Platform starts conducting marketplace activities that would cause it to be considered a Marketplace Platform, the regulatory framework applicable to Marketplace Platforms will also apply.

ii. Interim approach for Dealer Platforms trading Crypto Contracts

As noted above, to foster innovation and provide flexibility, the CSA has considered an interim approach that would facilitate the development and growth of Dealer Platforms trading Crypto Contracts, while ensuring that they operate within an appropriately regulated environment. We acknowledge that in some cases the time it takes to prepare for and obtain registration as an investment dealer and IIROC membership may delay operations or impact the development of such Dealer Platform's business in this nascent industry. Further, we understand that some CTPs are interested in a testing environment to assess the technical merits of their proposed platform. Accordingly, we contemplate that, as an interim measure, a Dealer Platform that trades Crypto Contracts may operate by seeking registration as a restricted dealer, provided it does not offer leverage or margin trading. The interim approach will be time limited and the Dealer Platform must take steps during the interim period to transition to a long-term regulatory framework.

We contemplate that under this interim approach Dealer Platforms that trade Crypto Contracts will be subject to terms and conditions that will be tailored to their business model, as appropriate, and that will address key risks to clients. This approach may also involve certain limitations on the Dealer Platform's activities which will be determined by the specific facts and circumstances of the Dealer Platform.

---

[4] The marketing of each derivative must also be authorized by the AMF, and such Dealer Platforms can offer derivatives to the public only as a registered derivatives dealer, or through a registered derivatives dealer.

[5] Available at https://www.osc.ca/en/securities-law/instruments-rules-policies/2/21-402. Please note that Appendix C of CP 21-402 is not intended to be an exhaustive list of applicable requirements.

Dealer Platforms operating in New Brunswick, Nova Scotia, Ontario and Québec that trade Crypto Contracts are expected to submit applications for investment dealer registration and IIROC membership during the interim period. We expect that these Dealer Platforms will use the interim period to work actively and diligently to transition to investment dealer registration and obtain IIROC membership by the end of the interim period, which is generally expected to be two years.

In Québec, as noted above, Dealer Platforms in the business of trading Crypto Contracts that are derivatives will be required to seek registration as a derivatives dealer. Québec derivatives dealers are required to be IIROC members but, for the interim approach, Dealer Platforms may seek a time-limited exemption from this requirement. They will be subject to terms and conditions substantially similar to those imposed on Dealer Platforms registering in the restricted dealer category.[6]

Dealer Platforms seeking to continue to operate in Québec will also be expected to use the interim period to work actively and diligently to obtain IIROC membership by the end of the interim period, which is also generally expected to be two years.

The securities regulators in Alberta, British Columbia, Manitoba and Saskatchewan will consider other regulatory approaches during the interim period, as warranted. Dealer Platforms operating in these jurisdictions are expected to start the process for investment dealer registration and IIROC membership during the interim period or take other steps during the interim period, in consultation with their principal regulator, to transition to an acceptable long-term regulatory framework. The interim period is generally expected to be two years.

iii. Application Process

A Dealer Platform that only facilitates distributions or trading of Security Tokens in reliance on prospectus exemptions and does not offer margin or leverage, should submit an application for registration as an exempt market dealer or as an investment dealer.[7] Registration in these categories is contemplated under the passport system described in Multilateral Instrument 11-102 *Passport System.*

As noted above, a Dealer Platform that will trade Crypto Contracts may be registered on an interim basis in the category of restricted dealer, with certain limitations on activities as noted above.

In Québec, a Dealer Platform that trades Crypto Contracts that are derivatives should submit to the AMF, at the same time and in addition to the registration application as a derivatives dealer, an application for a time-limited exemption from the requirement to obtain IIROC membership and other obligations of derivatives dealers that may not be relevant. In addition, the Dealer Platform will be required to submit a qualification application under the QDA.

Neither the restricted dealer nor the derivatives dealer category is contemplated under the passport system, but the application and the review will be coordinated among the jurisdictions where a registration application is submitted, with a view to harmonize the terms and conditions in the CSA jurisdictions to the greatest extent possible.

---

[6] The AMF may consider, under special circumstances, granting a discretionary time-limited exemption from the qualification requirement as a transition to allow the filing of a qualification application within a certain timeframe.

[7] A Dealer Platform trading Security Tokens may be required to operate with terms and conditions on registration that appropriately address the specific risks applicable to its business model. See Appendix A for a description of risks.

Additionally, a Dealer Platform that trades Crypto Contracts,

- may need discretionary exemptive relief in the applicable jurisdictions from the prospectus requirement to facilitate the distribution of Crypto Contracts since it will be subject to the prospectus requirement in most CSA jurisdictions, and
- may need discretionary relief from the over-the-counter trade reporting requirements in the applicable CSA jurisdictions,[8] on the basis that it provides alternative reporting, if it is unable to comply with existing requirements.

Any applications for discretionary exemptive relief from regulatory requirements, including submissions regarding why that relief is appropriate, should accompany the registration application and include how key risks, including to investors and the integrity of the capital markets, are addressed.

b. Marketplace Platforms

A CTP is a Marketplace Platform if it:

- constitutes, maintains or provides a market or facility for bringing together multiple buyers and sellers or parties to trade in Security Tokens and/or Crypto Contracts;
- brings together orders of Security Tokens and/or Crypto Contracts of multiple buyers and sellers or parties of the contracts; and
- uses established, non-discretionary methods under which orders for Security Tokens and/or Crypto Contracts interact with each other and the buyers and sellers or parties entering the orders agree to the terms of a trade.

Some commenters have suggested that there is no centralized marketplace involved when a digital ledger (such as blockchain) is used to record "trades" agreed to between the parties. However, in many circumstances the individual trades on the CTP are not recorded on the digital ledger. Rather, the digital ledger is only used to record transactions where the customer delivers crypto assets to the CTP or takes delivery of crypto assets from the CTP. In our view, if the orders of multiple buyers and sellers or parties are brought together on a third-party facility, and the interaction of those orders results in a trade, that facility acts as a marketplace.

A Marketplace Platform may also perform traditional dealer functions, including holding assets and other functions like those mentioned in the preceding section on Dealer Platforms.

In any case, Marketplace Platforms are in the business of trading in securities and/or derivatives and, unless they are regulated as an exchange (as described below), should seek registration as described below.

[8] See Ontario Securities Commission Rule 91-507 *Trade Repositories and Derivatives Data Reporting*; Manitoba Securities Commission Rule 91-507 *Trade Repositories and Derivatives Data Reporting*; Multilateral Instrument 96-101 *Trade Repositories and Derivatives Data Reporting*; Québec Regulation 91-507 *respecting Trade Repositories and Derivatives Data Reporting*.

i. Regulatory Requirements for Marketplace Platforms

Similar to the manner in which alternative trading systems (**ATS**)[9] are regulated today, a Marketplace Platform will operate under the oversight of the CSA and a self-regulatory entity, as defined in NI 21-101.[10] Currently, the only self-regulatory entity that fits this definition is IIROC.

As a starting point, the concepts described in the provisions applicable to marketplaces outlined in NI 21-101, National Instrument 23-101 *Trading Rules* (**NI 23-101**) and National Instrument 23-103 *Electronic Trading and Direct Electronic Access to Marketplaces* (**NI 23-103**) are generally relevant to Marketplace Platforms and such provisions, or provisions comparable to those in NI 21-101, NI 23-101 and NI 23-103 will be applied to Marketplace Platforms.[11] In addition, we contemplate that the trading activity on a Marketplace Platform will be subject to market integrity requirements such as those in IIROC's Universal Market Integrity Rules (**UMIR**), or provisions consistent with those in the UMIR. However, we anticipate that tailoring of such requirements may be appropriate to accommodate the novel aspects of CTPs. At Appendix B, we have outlined certain core market integrity requirements that we anticipate would be relevant to trading on Marketplace Platforms.

ii. Regulatory Requirements for Marketplace Platforms that also Conduct Dealer Activities

As noted above, some Marketplace Platforms also conduct activities similar to those performed by Dealer Platforms, such as granting direct access to investors (retail and institutional), trading as a counterparty to their clients or providing custody of assets. Where a Marketplace Platform performs these functions, it would also be subject to the appropriate dealer requirements discussed above. Furthermore, depending on the circumstances and the CTP's business model, such dealer activities may have to be conducted through a separate entity or business unit which would need to meet the applicable regulatory requirements or separated through ethical walls.

For reference, summaries of the key regulatory requirements applicable to marketplaces and dealers are included at Appendices B and C of CP 21-402, respectively.[12] We note, however, that there will be flexibility regarding how the requirements will apply. Some of the above requirements will not be relevant or may necessitate customization or tailoring as a result of the functions being performed, or the operational model of, the Marketplace Platform. As is currently the case for most ATSs, certain requirements in NI 31-103 and many of the IIROC Dealer Member Rules may not apply to a Marketplace Platform that operates as a trading venue only and does not perform any dealer activities (for example, no custody or retail client on-boarding). In the context of Marketplace Platforms that also have dealer functions, IIROC and/or the CSA may, on application by a CTP, consider discretionary exemptions from existing applicable rules where the Marketplace Platform demonstrates that it can comply with the policy intent of the existing regulatory requirements in alternative ways, or where its operational model is such that compliance with the specific requirement is impractical, but the risks, described in Appendix A of this Notice, can be appropriately managed in another way.

---

[9] As defined in NI 21-101 and, in Ontario, in the *Securities Act* (Ontario).

[10] A self-regulatory entity is defined in NI 21-101 as a self-regulatory body or self-regulatory organization that (i) is not an exchange, and (b) is recognized as a self-regulatory body or self-regulatory organization by the securities regulatory authority.

[11] Certain jurisdictions intend to apply requirements that are comparable to the referenced marketplace rules and oversight structures as applicable in the circumstances to Marketplace Platforms trading over-the-counter derivatives because these rules do not extend to over-the-counter derivatives in these jurisdictions.

[12] Available at https://www.osc.ca/en/securities-law/instruments-rules-policies/2/21-402

In the Summary of Comments and Responses to CP 21-402 at Appendix C, we have indicated some of the areas where we think that flexibility in the application of existing regulatory requirements may be provided. In Appendix B we have also outlined the IIROC requirements that are expected to apply and where there may be flexibility in the application of IIROC Dealer Member Rules or the UMIR.

iii. Marketplace Platform as an Exchange

In some cases, it may be appropriate to regulate a Marketplace Platform as an exchange. For example, if a Marketplace Platform trades Security Tokens and regulates issuers of those securities, or if it regulates and disciplines its trading participants other than by merely denying them access to the platform,[13] the Marketplace Platform may be carrying on business as an exchange and would be expected to seek recognition or, if appropriate, an exemption from recognition as an exchange. In these cases, the Marketplace Platform will be expected to oversee its issuers' continuing compliance with the listing requirements of the Marketplace Platform and regulate the operations and standards of practice and business conduct of its members and their representatives, directly or indirectly.[14] The Marketplace Platform will be subject to a public interest mandate because it exercises regulatory functions and it will have to have rules requiring compliance with securities legislation and provide appropriate sanctions of violations of such rules.

iv. Interim Approach for Marketplace Platforms

We acknowledge that, in some cases, a Marketplace Platform may wish to conduct a pilot to, for example, test a novel business idea or a proposed new market, or the time it takes to prepare for obtain registration and IIROC membership may delay operations or impact the development of a Marketplace Platform's business. In these circumstances, provided that the Marketplace Platform is not offering leverage or margin and are not exchanges, it could seek registration as an exempt market dealer or restricted dealer, as appropriate, for a limited period of time. If Marketplace Platforms perform exchange functions, we would consider whether recognition as an exchange or an exemption is needed in the interim.

Marketplace Platforms operating in New Brunswick, Nova Scotia, Ontario and Québec are expected to start the process for registration as an investment dealer and IIROC membership, or the process for recognition or exemption from recognition as an exchange, as applicable, during the interim period, which is generally expected to be two years.

The securities regulators in Alberta, British Columbia, Manitoba and Saskatchewan will consider other regulatory approaches during the interim period, as warranted. Marketplace Platforms operating in these jurisdictions are expected to start the process for investment dealer registration and IIROC membership, or the process for recognition or exemption from recognition as an exchange, during the interim period or take other steps during the interim period, in consultation with their principal regulator, to transition to an acceptable long-term regulatory framework. The interim period is generally expected to be two years.

---

[13] "Discipline" involves more than just denying access, it may entail fines and reprimands and requires a disciplinary framework that offers the participant due process.

[14] An exchange may retain a regulation services provider to provide these functions. See section 7.1(2) of NI 23-101 To date, all of the equity exchanges have retained IIROC as their regulation services provider.

v. Application Process

We would generally expect that a Marketplace Platform that is not an exchange would apply for registration as an investment dealer and seek IIROC membership, unless it is pursuing the interim approach described above. The Marketplace Platform should include with its application information similar to that currently included in Form 21-101F2 *Information Statement Alternative Trading System*.[15] The process for IIROC membership is described on IIROC's website.[16]

A Marketplace Platform that is an exchange would apply for recognition as an exchange. It would submit an application describing how it meets certain criteria for recognition[17] and the information currently included in *Form 21-101F1 Information Statement Exchange or Quotation and Trade Reporting System*.[18]

A Marketplace Platform that wishes to pursue the interim approach described above would make application to applicable securities regulatory authorities for registration as an exempt market dealer or restricted dealer, as described in paragraph iv. above.

As indicated above, ensuring market integrity is critical for the management of the risks associated with trading on a Marketplace Platform. As a result, a Marketplace Platform that seeks to use the interim approach and register as a restricted dealer or exempt market dealer for a limited period of time must satisfy the regulator that it appropriately manages the risks relating to trading. Key to this is the existence of rules and processes to monitor trading and the availability of resources, including staff who understand trading activities and can monitor trading on the Marketplace Platform. Marketplace Platforms seeking to employ surveillance solutions during this interim period would need to ensure they have the requisite capabilities to do so, having regard to the marketplace they will operate and the restrictions or limitations that will be applied during the interim period.

During the period of interim registration, we anticipate imposing appropriate limitations on the types of activities undertaken by Marketplace Platforms in order to mitigate the risks, which will depend on the Marketplace Platform's operational model and the risks it presents. Such constraints could include: limits on the number and types of products traded, the types or number of participants, or on the amount invested by any particular participant.

Relevant to the determination of appropriate limitations could be:

- whether the Marketplace Platform provides any advice to participants,
- whether the Marketplace Platform trades on a proprietary basis, and
- whether there is any differentiation between client types (e.g., the sophistication and experience of the participant).

Any applications for discretionary exemptive relief from regulatory requirements, including submissions regarding why that relief is appropriate, should accompany the registration application or, in the case of

---

[15] Available at https://www.osc.ca/en/securities-law/instruments-rules-policies/2/21-101/unofficial-consolidation-form-21-101f2.

[16] At https://www.iiroc.ca/industry/registrationmembership/Pages/Becoming-a-Regulated-Marketplace.aspx

[17] The criteria and the process for becoming a recognized exchange are available at https://www.osc.ca/en/industry/market-regulation/marketplaces/exchanges

[18] Available at https://www.osc.ca/en/securities-law/instruments-rules-policies/2/21-101/unofficial-consolidation-form-21-101f1

Marketplace Platforms that are exchanges, the application for recognition or exemption from recognition as an exchange. Similar to Dealer Platforms, Marketplace Platforms that trade Crypto Contracts may also need exemptive relief from the prospectus requirement to facilitate the distribution of Crypto Contracts and from the over-the-counter trade reporting requirements.

c. Additional Considerations in the Context of Clearing and Settlement

A CTP may also perform clearing functions and may be a clearing agency or a clearing house under securities legislation. In some CSA jurisdictions:

- a registered dealer or recognized exchange is exempt from clearing agency recognition as dealers and exchanges are excluded from the definition of clearing agency
- the CTP is exempt from clearing agency recognition if the clearing functions are only an incidental component of its principal business, or
- the CTP may require recognition or need to seek an exemption from recognition as a clearing agency or a clearing house.

In order to provide flexibility in these cases, we will look at the specific risks presented by the clearing functions in order to determine whether a CTP will be required to be recognized as a clearing agency or exempted from the requirement to be recognized and what terms and conditions should apply. Certain requirements that are applicable to clearing agencies set out in National Instrument 24-102 *Clearing Agency Requirements*, such as policies, procedures and controls to address comprehensive management of risks including systemic risk, legal risk, credit risk, liquidity risk, general business risk, custody and investment risk and operational risk, may be appropriate to apply to a CTP to mitigate the risks associated with the clearing functions it performs. We anticipate imposing terms and conditions on the CTP's registration or its recognition or exemption order to address these risks. CTPs that offer clearing services should discuss these functions with the appropriate securities regulatory authority so that the appropriate approach is determined.

For Marketplace Platforms, we also note that existing requirements applicable to marketplaces in NI 21-101 require all trades executed on a marketplace to be reported and settled through a regulated clearing agency. Currently, there are no clearing agencies recognized in Canada for transactions in Security Tokens and Crypto Contracts. As a result, in some jurisdictions, Marketplace Platforms will need to apply for an exemption from the requirement in NI 21-101 and explain how the risks are otherwise addressed.

d. IIROC Membership Process for Entities with Novel Business Models

As noted above, we expect it would be appropriate that some CTPs become IIROC members. IIROC recognizes the need to be flexible and foster innovation and has therefore established a path to membership for businesses or entities with novel business models, including Marketplace or Dealer Platforms that do not necessarily fit in the existing IIROC membership structure.

The process for reviewing a membership application from an entity with a novel business model would differ from the existing IIROC processes in that IIROC would review the new elements of a Marketplace or Dealer Platform's business model and determine:

- how best to apply current requirements; and
- whether any exemptions from IIROC requirements and/or time-limited terms and conditions are appropriate.

IIROC expects that entities with novel business models would be granted membership with time-limited terms and conditions and exemptions that take into account the new aspects of the entity's operations.[19] This is in contrast with its approach to current Dealer Members, through which IIROC generally imposes all its applicable requirements without additional exceptions or terms and conditions on their membership.

IIROC will apply this application review process for novel business models to a Marketplace or Dealer Platform that demonstrates:

- a new business model which presents unique features not consistent with current IIROC membership categories;
- that it has a business plan or road map; and
- potential investor benefits.

As part of the application review process for novel business models, IIROC will:

- assess the applicable requirements for the Marketplace or Dealer Platform by reviewing their underlying policy objectives and determine whether the applicable requirements need to be modified in the context of a CTP's new business model;
- collaborate with the Marketplace or Dealer Platform to ensure it develops appropriate policies and procedures to comply with applicable IIROC requirements;
- place limits on the activity, products and/or number of clients, as appropriate; and
- conduct surveillance of trading activities as appropriate.

The review of these novel businesses will be conducted in partnership with the CSA, to ensure consistency of approach, coordination and agreement with respect to novel approaches to manage risks.

It is important that we continue to foster innovation but also promote investor protection and support fair and efficient markets. As CTPs and the environment within which they operate continue to evolve, we will continue to monitor this space and assess whether the approach described in this Notice for regulating CTPs remains appropriate and evolves with the industry.

Part 4. Complying with Securities Legislation

We encourage CTPs to consult with their legal counsel and to contact staff of their local securities regulatory authority on the appropriate steps to comply with securities legislation and IIROC rules.

As the technology and operational models of CTPs continue to evolve, the CSA and IIROC welcome continued dialogue with CTPs and stakeholders on issues that are developing and possible ways of complying with requirements and additional areas where flexibility may be appropriate.

We remind CTPs operating from outside Canada that have Canadian clients that they are expected to comply with Canadian securities legislation. CSA members may take new enforcement actions or continue existing actions against CTPs that do not and/or have not complied with Canadian securities legislation.

[19] IIROC will work with the CSA to determine whether any of the terms and conditions imposed by the CSA will continue to apply in the form granted by the CSA or in a modified form.

Part 5. Questions

Please refer your questions to any of the following CSA and IIROC staff:

Amanda Ramkissoon Senior Regulatory Adviser, OSC LaunchPad Ontario Securities Commission aramkissoon@osc.gov.on.ca	**Ruxandra Smith** Senior Accountant, Market Regulation Ontario Securities Commission ruxsmith@osc.gov.on.ca
Gloria Tsang Senior Legal Counsel, Compliance and Registrant Regulation Ontario Securities Commission gtsang@osc.gov.on.ca	**Timothy Baikie** Senior Legal Counsel, Market Regulation Ontario Securities Commission tbaikie@osc.gov.on.ca
Lise Estelle Brault Senior Director, Data Value Creation, Fintech and Innovation Autorité des marchés financiers Lise-estelle.brault@lautorite.qc.ca	**Serge Boisvert** Senior Policy Advisor Autorité des marchés financiers Serge.boisvert@lautorite.qc.ca
Nataly Carrillo Senior Policy Advisor Autorité des marchés financiers nataly.carrillo@lautorite.qc.ca	**Sophie Jean** Executive Advisor, Supervision of Intermediaries Autorité des marchés financiers Sophie.Jean@lautorite.qc.ca
Denise Weeres Director, New Economy Alberta Securities Commission Denise.weeres@asc.ca	**Katrina Prokopy** Senior Legal Counsel, Market Regulation Alberta Securities Commission Katrina.prokopy@lautorite.qc.ca
Cathy Tearoe Senior Legal & Policy Counsel New Economy Alberta Securities Commission Cathy.tearoe@asc.ca	**Dean Murrison** Executive Director, Securities Division Financial and Consumer Affairs Authority of Saskatchewan Dean.murrison@gov.sk.ca
Michael Brady Manager, Derivatives British Columbia Securities Commission mbrady@bcsc.bc.ca	**Rina Jaswal** Senior Legal Counsel, Capital Markets Regulation British Columbia Securities Commission jaswal@bcsc.bc.ca
Peter Lamey Legal Analyst, Corporate Finance Nova Scotia Securities Commission peter.lamey@novascotia.ca	**Chris Besko** Director, General Counsel The Manitoba Securities Commission chris.besko@gov.mb.ca
David Shore Legal Counsel, Securities Division Financial and Consumer Services Commission (New Brunswick) david.shore@fcnb.ca	**Sonali GuptaBhaya** Director, Market Regulation Policy IIROC sguptabhaya@iiroc.ca
Victoria Pinnington Senior Vice President, Market Regulation IIROC vpinnington@iiroc.ca	

APPENDIX A
CTP RISKS AND APPLICABLE REGULATORY REQUIREMENTS

The introduction of CTPs to the market brings with it the introduction of risks, both to the market and its participants. Like traditional dealers and marketplaces, the regulatory requirements applicable to CTPs will be focused on managing and addressing those risks. Below we discuss in more detail the key risks relating to CTPs.

a. Safeguarding Investor Assets where a Dealer Platform or Marketplace Platform has Custody

Some Dealer Platforms and Marketplace Platforms may have custody of assets (or private keys). A key risk respecting CTPs that perform this function is the risk of loss of those assets. We recognize that the mechanism for "custody" in the crypto asset context may be different between business models, yet a risk of loss, theft or bankruptcy remains. We are of the view that safeguarding investor assets is critical, and CTPs will be expected to manage the associated risks.

Managing risks

Existing regulatory requirements for market participants with custody activities are included in NI 31-103 and in IIROC rules (see Appendix B for additional detail). Dealer Platforms and Marketplace Platforms that offer custody services must manage this risk by measures that would ensure the security of their participants' assets, including the following:

- properly segregating their participants' assets and private keys from their own;
- maintaining adequate record-keeping to be able to confirm participants' holdings at all times;
- maintaining policies and procedures to protect participants' assets and private keys from theft or loss, including policies and procedures governing when participants' assets are placed in and removed from cold storage and how private keys are created and stored;
- maintaining policies and procedures covering segregation of duties and key person risk;
- having sufficient financial resources and insurance, including insurance against the risk of loss, or alternative risk mitigation strategies;
- conducting due diligence before retaining a custodian;
- requiring that the CTPs have access to necessary books and records, and monitor the custodian's ongoing performance, internal controls and compliance with regulatory requirements; and
- sufficient risk mitigation regarding the custody of Securities Tokens or crypto assets underlying Crypto Contracts such as obtaining an independent report from a reputable accounting firm providing assurance on the suitability of the design of, and operating effectiveness of, the custodian's controls around the systems and processes in place to safeguard participants' assets (e.g. System and Organization Controls (SOC) 2 Type 1 and 2 report for service organizations).

We acknowledge that this is an evolving market and new custodial models may emerge over time. We will review such models on a case-by-case basis in order to assess whether the risks associated with asset custody are properly addressed. In the process, we will consider the practices identified in the responses to comments and as developed by the industry from time to time.

b. Access to Marketplace Platforms

This relates to the risk that a Marketplace Platform does not have fair and transparent criteria regarding access to its services to ensure that it does not unreasonably discriminate between participants. The Marketplace Platform will be required to ensure they do not unreasonably prohibit, condition or limit access to its platform. It will also be required to articulate who can access the Platform and make transparent its access requirements.

Managing risks

Existing regulatory requirements relating to access are found in Part 5 of NI 21-101. Section 5.1 of NI 21-101 requires that a Marketplace Platform not unreasonably prohibit, condition or limit access by participants to its Platform. This does not mean a Marketplace Platform has to admit any person seeking access but would prohibit a Marketplace Platform from unreasonably discriminating between its participants. It would also require a Marketplace Platform to articulate who can access the Platform, apply the criteria fairly and on a non-discriminatory basis, and document grants and denials of access. Access requirements are required to be transparent and be made available on a Marketplace Platform's website.

c. System Resiliency, Integrity and Security Controls

System resiliency, reliability and security controls are important for investor protection and market integrity, especially when the CTP maintains custody of participant's assets including through holding the private keys. System failures or inadequate protection against cyber-attacks may result in a CTP's participants being unable to access their crypto assets or may lead to losses due to theft.

Managing risks

Currently, marketplaces are required by Part 12 of NI 21-101 to have adequate internal and information technology controls over their trading, surveillance and clearing systems and information security controls over these systems. It is expected that these would cover cyber-resilience, security threats and cyber-attacks. Marketplaces are also required to maintain business continuity and disaster recovery plans. They must also engage an external auditor to conduct an independent systems review (**ISR**) to assess whether they have adequate internal and information technology processes and controls.

As noted in the responses to the Summary of Comments at Appendix C, we acknowledge the need to consider flexibility in applying the NI 21-101 requirements to Marketplace Platforms, and will consider alternative approaches to demonstrating system integrity, reliability and security where the risks are otherwise appropriately managed. We would consider each Marketplace Platform request on a case-by-case basis in order to determine the scope of its ISR, or whether an exemption, subject to terms and conditions as necessary, is appropriate.

d. Transparency about the CTP's Operations and the Crypto Assets Traded on the CTP

It is important that participants on a CTP understand its operations. This enables them to make informed decisions regarding whether and how to participate on the CTP and what risks they are willing to take.

CTPs will be required to provide adequate transparency regarding, among others, its operations, fees, conflicts of interest policies and procedures and any referral arrangements on its website.

Managing risks

Under NI 21-101, a marketplace is required to make transparent, on its website, a description of how its orders are entered, interact and are executed, the order and trade information disseminated, the hours of operations, its fees, its affiliates' fees, access requirements, conflicts of interest policies and procedures as well as any referral arrangements between the marketplace and its service providers. We expect Marketplace Platforms to also make this information publicly available, in order to allow their participants to make informed decisions. The information that should be disclosed includes:

- a description of the crypto assets trading on the Marketplace Platform including, where applicable, references to underlying projects;
- custodial arrangements and risks;
- ownership of the Marketplace Platform;
- conflicts of interest, including how they are managed, especially if the operator of the Marketplace Platform will trade on the marketplace against, or in competition with, clients' orders;
- rules for trading and, if applicable, for choosing which crypto assets will be admitted to or removed from trading on the Marketplace Platform; and
- policies for handling of forks, airdrops and other relevant events.

This additional information suggested by the commenters is useful, as it would ensure that a complete description of a Marketplace Platform's operations and risks is provided to existing and prospective participants. Marketplace Platforms may also disclose additional information, if necessary.

While Marketplace Platforms will have flexibility with respect to the content of information that will be ultimately disclosed, we will review their disclosure to determine whether it provides a Marketplace Platform's participants with all the information they need to understand how the Marketplace Platform operates, the products traded on it, the risks and whether it presents that information in a format that is understandable by the participant, in particular if retail investors have direct access to the Platform.

e. Market Integrity and Price Discovery

"Market integrity" risk relates to the risk that Marketplace Platforms may be susceptible to manipulative and deceptive trading. This may result from, for example, a lack of reliable pricing information for crypto assets, manipulative or fraudulent activity by one or more participants in buying and/selling crypto assets, or even manipulative or fraudulent activity involving other marketplaces which are trading the same crypto asset. It also relates to investor confidence, where investors know that rules regulating market conduct are set and those rules are appropriately monitored and enforced.

Managing risks

Those trading on marketplaces are required to comply with rules governing trading and marketplaces are required to take steps so that trading activities are monitored and the rules are enforced. NI 21-101 and NI 23-101 set out the overarching securities laws. Equity exchanges have adopted UMIR, which govern trading in much more detail, and the exchanges have outsourced monitoring and enforcement of

these rules to IIROC. The trading activities on other marketplaces that trade securities are also governed by UMIR (for equity securities) and monitored and enforced by IIROC, as a regulation services provider. In contrast, derivatives exchanges or marketplaces often have their own trading rules and conduct their own surveillance and enforcement.

Our expectation is that the starting point for the trading rules applicable in the context of a Marketplace Platform trading Securities Tokens or Crypto Contracts will be the requirements in UMIR. However, we recognize that in certain cases some specific aspects of UMIR may not be applicable. In other cases, trading on a Marketplace Platform may introduce additional risks not contemplated under UMIR. The determination of which UMIR provisions are relevant to Marketplace Platforms is currently on-going and is likely to evolve as the trading environment for Securities Tokens and Crypto Contracts evolves. We expect that the broad provisions prohibiting manipulating and deceptive activities would apply and other rules would be crafted to relate specifically to trading of Securities Tokens and Crypto Contracts. Given their experience in acting as a regulation services provider for various existing securities marketplaces, IIROC is well positioned to perform the monitoring of trading and compliance with securities legislation and UMIR in the context of CTPs.

f. Direct Access by Retail Investors

Some Dealer Platforms and some Marketplace Platforms offer access directly to retail investors. If CTPs on-board retail investors directly, there is a risk that the investors may purchase or trade products that they do not understand or are not suitable for them. However, if the CTP trading Crypto Contracts is not providing any recommendations or advice to participants, we may consider discretionary exemptive relief, allowing them to operate in a manner similar to an order execution only dealer. IIROC has issued guidance with respect to the limitations that apply to OEOs.[20] Additional restrictions may be applied to CTPs that are granted an exemption from suitability requirements.

CTPs may also be exposed to participants who are using the Marketplace Platform for money laundering or other illegal purposes and will be expected to have appropriate anti-money laundering (**AML**) and counter-terrorist financing (**CTF**) policies and procedures.

CTPs will be subject, when appropriate, to know-your-client and suitability requirements and will be required to have policies and procedures for AML and CTF.

Managing risks

Dealer Platforms and Marketplace Platforms that offer direct access to investors will be subject to the know-your-client and suitability requirements applicable to registered dealers. They would also have to have policies and procedures for AML and CTF. We understand that many CTPs already have AML and CFT procedures in place and comply with Financial Transactions and Report Analysis Centre's (**FINTRAC**) *Proceeds of Crime (Money Laundering) and Anti-Terrorist Financing Act*.

[20] Available at: https://www.iiroc.ca/Documents/2018/54df3aa0-06d8-48fd-8e93-ce469be1c650_en.pdf

g. Conflicts of interest

CTPs may have conflicts of interest that arise from the commercial interests of the CTP, its owners and operators, the businesses that raise capital on the CTP, if applicable, and the participants that trade on it. CTPs will be required to identify, manage and disclose potential conflicts of interest.

Managing risks

CTPs will be required to identify, manage and disclose potential conflicts of interest. They will be subject to the conflicts of interest provisions such as those in NI 31-103 or NI 21-101, as applicable, and, if they are IIROC members, also subject to the conflicts of interest provisions in IIROC's Dealer Member Rules and the UMIR.

APPENDIX B
SUMMARY OF IIROC REQUIREMENTS APPLICABLE IN THE CONTEXT OF CTPS

Requirements consistent with the core market integrity provisions of UMIR would apply, including:

- Part 2 – Abusive Trading including UMIR 2.2 Manipulative and Deceptive Activities. UMIR 2.3 Improper Orders and Trades
- Part 4 – Front Running
- UMIR 5.3 – Client Priority
- Part 6 – Order Entry and Exposure including UMIR 6.4 Trades to be on a Marketplace
- Part 7 – Trading in a Marketplace including: UMIR 7.1 Trading Supervision Obligations, UMIR 7.2 Proficiency Obligations, UMIR 7.3 Liability for Bids, Offers and Trades, UMIR 7.5 Recorded Prices, 7.11 Variation and Cancellation and correction of Trades, UMIR 7.12 Inability to Rely on Marketplace Functionality, UMIR 7.13 Direct Electronic Access and Routing Arrangements
- Part 8 – Principal Trading
- Part 9 – Trading Halts, Delays and Suspensions
- Part 10 – Compliance including: UMIR 10.9 Power of Market Integrity Officials, UMIR 10.11 Audit Trail Requirements, UMIR 10.12 Retention of Records and Instructions, UMIR 10.14 Synchronization of Clocks, UMIR 10.16-10.18 Gatekeeper Obligations
- Part 11 – General exemptive relief, review or appeal of market regulator decisions, indemnification and limited liability of the market regulator

As noted earlier, these requirements may be tailored to reflect the business models of the CTPs or the products they trade.

IIROC Rules that would apply include:

Custody

- DMR 17 – Dealer Member Minimum Capital, Conduct of Business and Insurance
- Form 1 – General Notes and Definitions, (d) “acceptable securities locations”
- Form 1 – General Notes and Definitions, (h) “regulated entities”
- DMR 2000 – Segregation Requirements
- DMR 2600 – Internal Control Policy Statements

Insurance Coverage

- DMR 17 – Dealer Member Minimum Capital, Conduct of Business and Insurance
- DMR 400 – Insurance
- DMR 2600 – Internal Control Policy Statements
- Form 1 – Schedule 10, Insurance

Know Your Client

- DMR 1300 – Supervision of Accounts
- DMR 2500 – Minimum Standards for Retail Customer Account Supervision

DMR 2700 – Minimum Standards for Institutional Customer Account Opening, Operation and Supervision

Appropriateness

- IIROC Rule 3211 (Note: This becomes effective December 31 , 2021) As per IIROC Guidance Note 18-0076 – Guidance on Order Execution only Services and Activities, an initial appropriateness standard does apply to OEO accounts. The standard is higher with respect to certain products such as CFDs.

Suitability

- DMR 1300 – Supervision of Accounts (not applicable if the firm operates in an OEO capacity)

Conflicts of Interest

- DMR 42 – Conflicts of Interest

Relationship Disclosure

- DMR 3500 – Relationship Disclosure

Margin

- DMR 17 – Dealer Member Minimum Capital, Conduct of Business and Insurance
- DMR 100 – Margin Requirements
- IIROC Notice 08-0074 – Margining of a Security that is not covered in Dealer Member Rule 100 or Form 1
- DMR 2600 – Internal Control Policy Statements

Regulatory Financial Reporting

- Form 1
- DMR 17 – Dealer Member Minimum Capital, Conduct of Business and Insurance
- DMR 100 – Margin Requirements
- DMR 200 – Minimum Records
- DMR 2600 – Internal Control Policy Statements
- DMR 1800 – Commodities Futures Contracts and Options (for some of the cases based on products)
- DMR 1900 – Options (for some of the cases based on products)
- DMR 2900 – Proficiency and Education

Fair Pricing and Best Execution

- DMR 3300 – Best Execution of Client Orders

Research Restrictions and Disclosure Requirements

- DMR 3400 – Research Restrictions and Disclosure Requirements

Registration

- DMR 7 – Dealer Member Directors and Executives
- DMR 18 – Registered Representatives and Investment Representatives
- DMR 38 – Compliance and Supervision
- DMR 2900 – Proficiency and Education

Anti-Money Laundering

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (**PCMLTFA**)[21]

Note: IIROC Rules, which will replace the current Dealer Member Rules, are expected to come into effect on December 31, 2021. At the same time, IIROC rules pertaining to Know Your Client, Suitability, Product Due Diligence, Know Your Product, Conflicts of Interest and Relationship Disclosure will be amended to reflect the Client Focused Reforms effective December 31, 2021.

[21] Although this is not an IIROC rule, but rather federal legislation, IIROC is it still responsible for testing IIROC Dealers compliance with Canadian AML law and regulations.

Appendix C
Summary of comments and responses
Joint CSA-IIROC Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms*

1. List of Commenters

	Commenter
1.	Allan C. Hutchinson
2.	Dr. Stephen Castell (Castell Consulting)
3.	Eric Swildens
4.	Atlantic Blockchain Company
5.	Piotr Piasecki
6.	Canadian Foundation for Advancement of Investor Rights
7.	Investor Advisory Panel (Neil Gross)
8.	Leede Jones Gable Inc.
9.	Crowdmatrix Inc.
10.	Brane Inc.
11.	Omega Securities Inc. and 4C Clearing Corporation
12.	Wall Street Blockchain Alliance
13.	Raymond Chabot Grant Thornton LLP
14.	Bull Bitcoin Inc. and Satoshi Portal et al.
15.	Durand Morisseau LLP and IJW & Co.
16.	Paradiso Ventures Inc.
17.	Aquanow
18.	Jonathan Hamel
19.	Coinsquare Capital Markets
20.	Dominion Mining Company and Bitcanuck
21.	Chamber of Digital Commerce Canada
22.	Fidelity Clearing Canada ULC
23.	Fern Karsh
24.	Roger Miller
25.	Tritum Inc. (John Willcock)
26.	DV Chain, LLC (Dino Verbrugge)
27.	Payward Canada Inc. and Affiliates (Kraken)

28.	State Street Corporation (James J. Biancamano)
29.	Octonomics (Elisabeth Prefontaine)
30.	The Canadian Bankers Association
31.	Vakeesan Mahalingam
32.	Global Digital Finance
33.	SoapBox Network Inc.
34.	Investment Industry Association of Canada (Annie Sinigagliese)
35.	Chartered Professional Accountants of Canada (Gordon Beal)
36.	Catalx Exchange Inc.
37.	KNOX Industries
38.	TD Securities
39.	The Jersey Company (Robert Young)
40.	ViewFin Canada (Adnan Tahir)
41.	ComplyChain Solutions (Adnan Tahir)
42.	Canadian Digital Asset Coalition
43.	TMX Group Limited (Deanna Dobrowsky)
44.	Alloy Blockchain Solutions
45.	Blockchain Technology Coalition of Canada
46.	National Digital Asset Exchange
47.	Bitvo
48.	National Crowdfunding & Fintech Association of Canada
49.	CC Corporate Counsel Professional Corporation
50.	Anonymous
51.	Fiach_Dubh (Reddit)
52.	Market Data Company (Alexander Izak Levesque)

2. Terminology

Airdrop - a crypto-asset airdrop refers to a distribution of a crypto-asset to digital wallets (often for no financial consideration).

Decentralized exchange – refers to a marketplace where trades occur directly between users (peer-to-peer) through an automated process.

Fork - refers to a change of the code in the underlying protocol which is incompatible with the previous version. This results in different versions of the protocol.

Multi signature wallet – a wallet that requires multiple keys to authorize a transaction.

Proof of stake – a concept where an individual can mine or validate block transactions according to how much they hold in crypto assets.

Proof of work – refers to a consensus algorithm on DLT.

Wallet/Hot Wallet (or Hot Storage)/Cold Wallet (or Cold Storage) - A crypto-asset wallet is an address, defined by its public key, which can send and receive related crypto assets. It is secured by a private key which may only be known by the wallet owner and must be used to sign a transaction before it can be sent. Hot storage (or a hot wallet) is connected to the internet, while assets stored in cold wallets have no online connectivity.

3. Abbreviated terms:

Anti-Money Laundering (**AML**)

Anti-Terrorist Financing (**ATF**)

Application Programming Interface (**API**)

Business Continuity Plan (**BCP**)

Canadian Derivatives Clearing Corporation (**CDCC**)

The Canadian Depository for Securities Limited (**CDS**)

Canadian Deposit Insurance Corporation (**CDIC**)

Canadian Investor Protection Fund (**CIPF**)

Canadian Standard on Assurance Engagements (**CSAE**)

The Commodity Futures Trading Commission (**CFTC**)

Committee of Sponsoring Organizations of the Treadway Commission (**COSO**)

Control Objectives for Information and Related Technologies (**COBIT**)

Crypto asset trading platforms (**CTP**)

Distributed Ledger Technology (**DLT**)

Enterprise Risk Management (**ERM**)

Financial Industry Regulatory Authority (**FINRA**)

Hardware Security Modules (**HSM**)

Information Security Management System (**ISM**)

Internal Controls over Financial Reporting (**ICFR**)

International Organization of Securities Commission (**IOSCO**)

International Organization for Standardization (**ISO**)

Investment Industry Regulatory Organization of Canada (**IIROC**)

Know Your Client (**KYC**)

Money Service Business (**MSB**)

National Institute of Standards and Technology (**NIST**)

New York Department of Financial Services (**NYDFS**)

Over-the-counter (**OTC**)

Personal Information Form (**PIF**)

Portfolio Manager (**PM**)

Principal Regulator (**PR**)

Regulatory Framework for CTPs proposed in CP 21-402 (**Proposed Framework**)

Risk Assessment Questionnaire (**RAQ**)

Securities Exchange Commission (**SEC**)

Swap execution facility (**SEF**)

Self-regulatory organization (**SRO**)

Universal Market Integrity Rules (**UMIR**)

*Other undefined abbreviated terms should be understood to have generally accepted industry meanings.

Topic	Summarized Comment	Response
General comments		
Support for the proposed regulatory framework	Several commenters indicated support for the Proposed Framework. A few commenters agreed that the existing regulatory framework for dealers and marketplaces, with some	We thank the commenters for their support.

described in CP 21-402 (Proposed Framework)	modifications, could be extended to CTPs and noted that a different regime could create arbitrage opportunities.	
Principles to consider in developing regulation for CTPs	Several commenters noted principles that the CSA and IIROC should consider in developing the regulatory framework for CTPs. These include: • regulation should be principles based, outcome focused, flexible and technology neutral to ensure that it is the least intrusive on innovation as possible; • regulation should be proportionate to allow innovative firms in the development stages to succeed while protecting investors or businesses may leave to other jurisdictions; a regulatory "light touch" approach should be taken to avoid stifling the development of new technologies; • regulation should consider the entire crypto-asset ecosystem, the different entities in the space (centralized and decentralized CTPs, custodial and non-custodial CTPs, custodial and non-custodial wallets, payment processors, etc.) and the multiple functions they perform; • requirements should mirror existing frameworks where appropriate; • to the extent possible, regulation should be harmonized across Canada and consistent with global regulation and international best practices; and • requirements should protect participants from counterparty risks and cover market integrity, surveillance, fair pricing, custody, clearing, disclosure of conflicts of interests, and systems and business continuity planning. Many commenters suggested that further consultation and collaboration with the industry is required before developing a framework for CTPs that appropriately balances innovation and ecosystem growth with the objective of protecting participants and market integrity. A few commenters suggested the establishment of a task force of industry experts to work with policy makers and regulators (in the policy areas of finance, economic development, innovation, consumer protection and privacy), including the Department of Finance, FINTRAC and the CRA, to study and review each aspect of a CTP and the broader regulatory framework and objectives and to ensure that regulations are aligned, consistent and not overly burdensome.	We thank the commenters for these suggested principles. We have considered many of these principles and will continue to keep them at the forefront of any additional regulatory work. Securities legislation is principles based and may evolve as the industry evolves. We have conducted extensive consultations with industry participants, both through the public comment process to CP 21-402 and through our ongoing discussions with industry participants, including CTP representatives. We will continue to consult with and work with CTPs to understand new business models and developments in the industry. The approach applies existing regulatory requirements, to the extent these requirements are appropriate and relevant in light of the CTPs' functions and the risks they introduce to the market. Although the scope of jurisdiction set out in CSA Staff Notice 21-327 in Canada may be broader than some international jurisdictions, our approach to regulating those platforms that fall within our jurisdiction, i.e. applying our existing regulatory framework, but tailoring it as appropriate, is consistent with that taken in foreign jurisdictions

		We acknowledge the comment suggesting regulation should be harmonized across Canada and note that, given that the regulatory framework outlined in the Notice is based on existing regulatory requirements set out in various National Instruments. CSA members recognized the importance of harmonization and strive to develop a harmonized approach.
Concerns about the applicability of securities and/or derivatives regulation to CTPs	Concerns about the Proposed Framework included: • securities or derivatives regulation is not appropriate for CTPs that allow the trading of crypto assets that operate solely as a form of payment. The current regulatory framework for marketplaces may not be the appropriate starting point as it does not achieve the right balance for crypto assets that are not securities and have different inherent risks; • different crypto-assets have distinct classifications and purposes which need to be examined individually; • CTPs that facilitate the trading of non-securities, such as bitcoin, are MSBs and should be regulated as such; • the Proposed Framework is responsive to abusive businesses and risks alone, however addressing abuses in the crypto industry with rules designed for securities marketplaces could create additional risks; • there should be a focus on actual and material risks with a tiered approach used to establish the requirements that should apply as the risks increase or other requirements become more relevant; • the Proposed Framework creates barriers for new entrants and new business models and does not consider the potential impact of a stifling of innovation and the use of DLT; • a balance needs to be struck to ensure that Canadian CTPs are not at a competitive disadvantage as a result of the high costs of domestic compliance with requirements that may not be relevant; and • foreign CTPs may stop providing services to Canadians and, as a result, Canadian CTPs may be locked out of their ability to source liquidity from global markets;	Securities legislation applies to CTPs that trade products that are securities or derivatives, including in the situation described in CSA SN 21-327. A CTP, like other market participants, may be subject to various forms of regulation e.g., AML, MSB, deposit-taking regulations, privacy, in addition to being subject to securities legislation. We have reviewed the securities regulatory-related risks introduced by CTPs and how these risks can be addressed through existing principles-based securities regulatory requirements. We contemplate that requirements will be tailored to address the unique risks. We recognize the need to be flexible in order to foster innovation. We also recognize the need to have an appropriate level of regulatory oversight in order to provide investor protection and foster fair and efficient markets.

	another comment was made, however, that foreign CTPs should be prohibited from doing business in Canada if they do not comply with the Proposed Framework.	Many of the CTPs we have seen conduct activities that are similar to those of dealers or existing equity marketplaces. Where CTPs trade Security Tokens or Crypto Contracts, we are of the view that the approach we describe in this Notice - based on the existing regulatory framework applicable to marketplaces and dealers with flexibility to take into account bespoke business models - is appropriate. Regulatory requirements will be tailored depending on the functions and operational model of a CTP, which may include providing exemptions from existing requirements circumstances justify it.
Alternatives to the Proposed Framework	Commenters suggested a number of approaches, including: • self-regulation combined with industry certifications; it was noted that number of leading CTPs in the U.S. have collaborated to create the Virtual Commodity Association with the goal of forming a self-regulatory organization specifically for virtual commodity exchanges and custodians to work with the CFTC; • establishment of a quasi-autonomous non-governmental organization (**QUANGO)** that is comprised of a full range of stakeholders, but is separate from the government, with some ties. The commenter noted that QUANGO could adopt best practices and voluntary registration as the first step; and • federal regulation - crypto assets that are not securities should be regulated at the federal level to limit regulatory burden and confusion. A few commenters suggested that the focus of regulators should be on consumer education and the development of industry standards as an alternative approach to the Proposed Framework. One of the commenters suggested developing standards with bodies like the Canadian Standards Association or the Canadian Centre for Cybersecurity.	We note that industry participants may form, and some have already formed, associations that provide guidance and best practices for their members. Where the products traded on a CTP are securities or derivatives, the regulation of the CTP necessitates consistency in application with other types of marketplaces so that we can ensure that the risks are appropriately managed and a level playing field is maintained where appropriate. That being said, the applicable requirements will be considered based on the functions performed. We agree with the importance of investor education. The CSA has already published, over time, various investor alerts regarding trading in crypto assets.

Question 1: The Consultation paper notes that the CSA is evaluating the specific facts and circumstances of how trading occurs on Platforms to assess whether or not a security or derivative may be involved and lists several factors we are considering. Are there factors in addition to those listed that should be considered?		
Classification of crypto assets	Several commenters suggested that there needs to be a comprehensive taxonomy for different crypto assets. Many commenters indicated that there needs to be further clarification on which crypto assets are securities, so that market participants are aware of the applicable requirements. It was suggested that the lack of clarity over when securities legislation applies may cause projects and businesses to move to jurisdictions that offer greater clarity. A few commenters highlighted factors to be considered in assessing whether a CTP is subject to securities legislation. Some commenters provided comments on the meaning of "delivery" in the context of CTPs. A couple of commenters suggested the CSA should consider the approach of the CFTC and their proposed interpretation of "actual delivery".	There are various ways of categorizing crypto assets for different purposes. Unfortunately, this will not necessarily assist with an assessment of the application of securities legislation. The definition of "security" is broad and inclusive. The definition of "derivative" is similarly broad. Further, on January 16, 2020, we published CSA Staff Notice 21-327 that provides guidance on some of the factors to be considered for determining whether securities legislation applies even where the crypto asset is not itself a security or derivative. This guidance is largely consistent with the CFTC's interpretation of "actual delivery" with differences to account for the specific limitations on jurisdiction within the *U.S. Commodity Exchange Act.*

Question 2: What best practices exist for Platforms to mitigate the risks outlined in Part 3 of the Consultation Paper? Are there any substantial risks which we have not identified?		
Comments on best practices	Best practices suggested by commenters to mitigate the risks outlined in CP 21-402 included: *Safeguarding of crypto assets* • multi-signature wallets, segregation of accounts and segregation of duties; • custodial services should be separated from other services; • custody should only be provided by IIROC dealers, banks or trust companies; • third-party custodians should maintain a certain reserve ratio; • a majority of assets should be held in cold-storage; • CTPs should operate on a "full reserve basis" with segregated accounts; • CTP could set aside some of its profits (in fiat or crypto) in a segregated account intended to be an emergency re-capitalization fund which it could deploy to recoup losses in the event of a hack; *Policies and procedures* • CTPs should have well documented policies and procedures and internal controls in place including, but not limited to, adequate disaster recovery and business continuity planning protocols; *Disclosure* • CTPs should be required to provide disclosure to participants on the CTP, including in the following areas: o information about the crypto assets available for trading on the CTP; o the selection criteria for admitting a crypto asset for trading on the CTP; o policies for managing hard and soft forks; o CTP rules and practices including frequently asked questions; o ownership, possession and control parameters; o conflicts of interest including whether the CTP trades as principal; o fees; o trading limits; o how prices are determined; o crypto assets that have been stolen or were involved in a fraud, as reported by investors; and o risks related to the CTP's operations, safeguarding of crypto assets and trading;	We thank the commenters for providing suggestions for best practices that would help manage the risks outlined in CP 21-402. We will consider these best practices in assessing whether the CTP complies with applicable requirements. It is our intention to be flexible, so that the principles-based requirements can be met through different means, as long as the risks introduced by CTPs are addressed.

	Security and compliance • employees should go through extensive background checks; • CTP executives should be required to pass certain amended regulatory exams and should certify that the CTP is in compliance with applicable rules and regulations; • attestation by CTP participants that the controls required by the user are in place and working; *Conflicts of interest* • CTP employees should be prohibited from trading on information that gives them an advantage over non-employees; *Cybersecurity and system resiliency* • regular testing for adequacy of security controls and vulnerabilities; • mandatory implementation of processes and procedures like those that exist for traditional marketplaces, such as enterprise risk management, information security management systems and control frameworks (COSO and COBIT); *Order and trade transparency* • requiring users and related parties to be identified so that CTPs can identify fake trading volume; • use of central information processors, like those used for marketplaces; *Reporting* • CTPs should be required to provide third-party reports on volume and trade data; *Client confidentiality* • access to participants' confidential information should require two-factor identification and be limited to a small number of CTP employees that are required to have access to perform their duties; • "zero-knowledge proofs" or technologies such as RingCT could be used to ensure the confidentiality of participants' trades; • CTPs should consider whether trades could be executed between parties without the CTP knowing the identity of the parties, but rather by trusting a third-party that has verified the identity of the parties so that sensitive information is not required to be sent to a CTP that may not have the proper security in place to store user data;	

	Prudential requirements • capitalization requirements should be imposed on business models where customer assets are held in omnibus or commingled accounts; *Insurance* • appropriate and sufficient insurance coverage is important to mitigate the key risks associated with CTPs; *Independent reviews* • regular financial and technology audits should be conducted on CTPs, both internally and by third-parties, as well as audits of underlying assets where the CTP permits the trading of crypto assets that are digital representations of a tangible asset; and • regular on-site field reviews by regulators.	
Other substantial risks	Commenters noted a number of risks: *Safeguarding crypto assets* • there are risks related to multi-signature implementation, key management and asset verification; • risks related to the transfer of crypto assets including address verification and transaction approvals; *Insider fraud* • greater risk of delay in detecting insider fraud given CTPs are often involved in all aspects of a trade; *Lack of policies and procedures* • many CTPs lack policies and procedures to detect and monitor fraud and AML activities within and across CTPs; *Fake trading volume* • the practice of creating inflated trading volumes, particularly for CTPs that issue their own tokens *Lack of reliable banking services*	We thank the commenters for highlighting these risks. We believe that the approach outlined in the Notice will help mitigate the risks identified, to the extent that they are applicable to CTPs. For example: • *risk of lack of policies and procedures* – CTPs will be required to establish and maintain policies and procedures that ensure compliance with securities legislation and manage the risks associated with their business. • *risk of artificially higher trading volume due to practices such as wash trading* – CTPs will be required to comply with requirements in NI 21-101 to maintain fair and orderly markets; Platform participants will be required to comply with the UMIR (as amended as may be necessary to accommodate the unique

	• risks related to the use of third-party payment processors and off-shore banks, including that funds may become frozen or lost when relationships are terminated or there is reliance on suppliers in risky jurisdictions outside of Canada; • the lack of a reliable banking partner may also create barriers to audits, insurance and efficient price discovery *Forked crypto assets* • forks can come with different security and economic implications as they may be unsupported by the CTP's infrastructure or the new wallets may introduce security vulnerabilities to the CTP; *Initial Coin Offerings (**ICO**) and Initial Token Offerings (**ITO**)* • risk of pump and dump schemes for crypto assets that are created through ICOs and ITOs; • misappropriation by founders of funds raised through ICO/ITO; and *Decentralization* • decentralization will result in heightened risks due to the diffusion of accountability; that tracking the risk will become more and more difficult unless guidelines are well developed now.	features of CTPs and the crypto assets they trade) which, among others, prohibit manipulative and deceptive trading activities and the entering of orders with the goal of creating a false or misleading appearance of trading activity or interest in a particular security. • *risks associated with security and vulnerability due to forks* – CTPs will be required to have adequate systems and information technology controls, including controls over the security of their systems, and to provide disclosure of risks where the DLT has undergone a fork or other irreversible change.
Question 3: Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?		
General comments	A number of commenters have indicated that Toronto is quickly becoming a hub for innovation and investments in DLT. A few commenters have cautioned that firms will leave Canada to jurisdictions with lower barriers to entry if regulation is too costly, onerous or restrictive. It was noted that, without domestic access, Canadian investors will increase the use of foreign CTPs with potentially heightened risks. One commenter, however, cautioned against adopting approaches in jurisdictions with more accommodating policies. Other comments raised included: • views that there are no leading global approaches yet; • it is mostly non-G20 countries that have adopted tailored frameworks that create more room for innovation.	As we indicated in CP 21-402, many jurisdictions globally are applying their existing regulatory requirements to regulate CTPs that trade products that fall within their regulatory jurisdictions. We are of the view that the approach described in the Notice, which leverages existing regulatory requirements, is consistent with the approaches taken in other jurisdictions. We note that, to the extent that foreign CTPs are accessed by Canadian clients, we would consider a

		registration or exemption regime for those CTPs depending on the regulatory regime applicable and whether the risks are addressed.
Global approaches that should be considered	Commenters suggested the CSA and IIROC consider approaches taken in the following jurisdictions: • Asia Securities Industry and Financial Markets Association's (ASIFMA) guidance; • Abu Dhabi; • Australia; • Bahamas; • Bahrain; • Barbados - it was noted that Barbados does not intend to regulate utility tokens (or protocol tokens) as securities and has also developed legislation that is focused on the security of CTPs; • Bermuda – Digital Asset Business Act (DABA) - it was noted that DABA is a comprehensive regulatory regime that provides regulatory certainty and consumer protection without sacrificing innovation; • Estonia; • France - it was noted that the AMF has adopted a draft bill (action plan for business growth and transformation) that establishes an optional visa regime for ICOs and an optional license regime for crypto asset service providers; • Germany; • Gibraltar – it was noted that the Gibraltar Financial Services Commission (GFSC) requires that any company "storing or transmitting value belonging to others" using DLT, including CTPs, be licensed by the GFSC. The GFSC regulations cover obligations of DLT providers to have adequate infrastructure in place for AML and CFT, solvency, corporate governance and cybersecurity; • Japan; • Mauritius – it was noted that Mauritius has developed a regulatory framework for custodial services by working with industry experts; • Malta - it was noted that Malta was implementing certification programs to facilitate the creation of a set of credentialed advisors that could serve as a second vetting layer for industry participants. • Singapore; • Switzerland; • UK; • United States	We thank the commenters for these suggestions. We have and are continuing to monitor closely regulatory developments and approaches in other jurisdictions, including the countries that are part of the G20 and also those identified in the responses to CP 21-402.

	○ a few commenters indicated that due to the close alignment between Canadian and U.S. markets, the approach of the SEC should be considered (whose position is that CTPs trading in crypto assets that are securities should be registered with FINRA as a broker dealer); ○ a few commenters also pointed to the approach by Wyoming state where a bill was enacted exempting utility tokens from being classified as securities; ○ a few commenters have also suggested the approach taken by the NYDFS; ○ one commenter suggested considering guidance issued by the US Financial Crimes Enforcement Network (FinCEN) regarding the application of regulation to certain business models involving crypto assets; and ○ a few commenters cited self-regulatory efforts in the United States including the creation of the virtual commodity association (VCA).	
Global approaches that should not be considered	Some commenters suggested that the following approaches should not be considered: • NYSDF's BitLicense – it was noted that the BitLicense hampers investors and has caused CTPs to leave NY state and blacklist residents of NY state; • Malaysia - a few commenters cautioned against sweeping regulations, such as Order 2019 in Malaysia, which specifies that all digital currencies be classified as securities; and • China and Vietnam – one commenter expressed that an outright ban on crypto assets should not be considered as it will result in the creation of an underground network and would not advance the goal of protecting Canadian investors.	We thank commenters for their suggestions. We note that we are not considering an outright ban on crypto assets. As indicated above, we have published CSA Staff Notice 21-327 that provides guidance on when entitlements to crypto assets that are not themselves securities or derivatives, may be considered securities or derivatives.
Question 4: What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.		
General comments	A few commenters were of the view that CTPs should not be allowed to have their own custody systems and one commenter noted that custody of crypto assets should be limited to regulated entities, such as banks and trust companies. One commenter, however, indicated that using third-party custody services will increase costs for the CTP and its participants. Another commenter identified jurisdictional risk in using foreign third-party custodians.	The risk that investors' assets are not appropriately safeguarded is one of the key risks identified in CP 21-402. We expect that standards to mitigate risks associated to the safeguarding of assets will evolve as the industry evolves and we intend to continuously consider the appropriate tools and mechanisms to ensure the safety of client assets.

		For example, where CTPs outsource custody services to third-party providers, they will also be subject to the requirements applicable to dealer or marketplaces that outsource key services or systems to a service provider set out in NI 31-103 or NI 21-101, respectively, which include ensuring that the securities regulator has access to all data, information and systems maintained by the third-party service provider. The purpose of these requirements is to ensure CTPs have policies and procedures to evaluate and approve outsourcing agreements and monitor the ongoing performance of the service provider.
Minimum standards that should be met by CTPs that offer custody services and for those using third-party custodians	One commenter suggested that CTPs should be provided the flexibility to choose the minimum standards they must maintain so long as they are able to demonstrate the adequacy of such standards. Most commenters, however, provided suggestions on minimum standards that could be adopted both by CTPs that provide custody services and by those using third-party custodians. They included: • segregation of assets; • maintaining a majority of assets in cold storage; • ensuring privacy of data and cybersecurity; • verification of assets; • imposing special capital requirements or, if financially feasible, insurance to protect assets, • requiring ISO 27001 and ISO 27017 certification if cloud-based technology is used; • requiring National Institute of Standards and Technology (NIST) minimum level 3 certification; it was noted that NIST also has standards for generating public and private cryptographic keys that should be considered; • requiring standards similar to other financial market infrastructures, such as those outlined by the Committee on Payment and Settlement Systems of IOSCO;	Since the requirements under securities legislation are principles based, CTPs will have the flexibility to implement different mechanisms as long as they can confirm that the risks associated with safekeeping of investors' crypto assets are adequately managed. The suggestions provided will be helpful for the CSA when evaluating whether CTPs' internal controls and policies and procedures regarding custody are adequate. We would expect that, at a minimum, CTPs will seek to ensure the following as part of their custody solution: • control over access to investors' assets; • segregation of investors' assets from the CTP's own assets;

	• requiring the Crypto Currency Security Standard published by the Crypto Currency Certification Consortium, which provides guidance for security best practices for crypto assets; and • imposing requirements similar to those of the SEC.	• verification of crypto assets; • use of cold storage for a majority of participants' crypto assets; and • adequate levels of insurance or alternative risk management strategies.
Best practices for CTPs offering custody services	Commenters suggested a number of best practices for CTPs offering custody services, as follows: *System controls* • maintaining and demonstrating robust system design, specifically intended to avoid "single points of failure"; • clearly documenting and following policies and procedures; and • enterprise risk management and financial and systems controls, regardless of whether CTPs self-custody or use a third-party custodian for their participants' assets; *Internal controls* • ensuring that a sufficient number of senior management has access to wallets; • restricting access to crypto assets to personnel that undergo background and criminal checks; • recording access to funds on tamper-proof logs residing outside of the CTP and making such records available to participants; • requiring multiple signatures in order for transactions to be completed; • a "Dead Man Switch", where the former responsibilities of a deceased individual can get transferred safely to a trusted third party; *Segregation of client assets* • segregating client assets from the assets of the CTP and, in the case of third-party custodians, from assets of other businesses stored by the custodians; • one commenter noted that client assets should be held separately for each client; *Storage of client assets* • generating and managing digital wallet keys offline for the lifetime of the key, on dedicated hardware (such as HSMs) that have received a rating of FIPS 140-2 Level 3 or higher; it was noted, however that HSMs, while used pervasively in the industry, may be appropriate for lower value, high volume-high speed transactions in which	We thank commenters for the suggested best practices identified. As noted above, we are of the view that it is important to allow CTPs' flexibility to implement their own processes, policies and procedures, as long as the risks introduced when they offer custody services are managed and adequately disclosed. Consequently, we will consider these suggestions when evaluating whether a CTP has implemented adequate custody arrangements, including adequate internal controls, policies and procedures over custody services.

	the storage of information is ephemeral but not for long-term storage of high value crypto assets; • maintaining redundant sites to protect participants' assets; • storing assets in multiple geographic locations; • a CTP's corporate headquarters should not store or contain crypto assets of material value; • limiting the storage of crypto assets to Canada to manage potential jurisdiction risks; • ensuring no two keys for the same wallet are present on a single device; • maintaining a majority of crypto assets in cold storage; it was further suggested that the private keys should be maintained on a computer or hardware device that has never been on the internet and is physically secured in a vault; • giving participants a choice in whether to store their assets on the CTP or in their own wallets; • maintaining fiat currency with a regulated financial institution located in a trusted jurisdiction; *Other* • establishing voting pools where multiple CTPs get together to secure one another's funds; with this concept, a CTP on its own would not be able to move funds, even its own funds; CTPs would cross-audit one another and will be responsible for countersigning transactions; • requiring CTPs to have proof of reserves (proof that a CTP maintains a minimum amount of assets); • establishing limits for the level of assets that can be maintained in hot wallets; one commenter indicated that only amounts required to facilitate daily trading liquidity on the CTP and those needed to satisfy withdrawal requests made by customers should be held in the hot wallet; • limiting withdrawals to a specific, narrowly defined timeframe (for example, allowing withdrawals only once a day); • for CTPs that use third-party custodians, implementing a reconciliation process between its internal accounts and the assets custodied by the third parties; • custody of digital assets should be limited to regulated custodial entities (banks and trust companies). This is necessary because of risks in "hybrid" nature of platform operations; and • development of a standardized settlement cycle, reconciliation requirements and dispute adjudication procedures.	

CTPs that retain third-party custodians	Comments specific to CTPs that retain third-party custodians were as follows: • CTPs should be required to conduct thorough due diligence on third-party custodians before retaining them; • CTPs should conduct ongoing due diligence to ensure agreements with custodians are being fulfilled as expected; • CTPs should disclose to their participants the use of third-party custodians • there should be requirements that third-party custodians be insured for theft and subject to regular external security audits; • users should be enabled to verify their funds by using view keys or moving the funds to temporarily show that they are actually under their control; and • there is jurisdiction risk when using foreign third-party custodians. A few commenters noted that third-party entities should: • provide verification of policies and procedures regarding conflicts of interest, fair access, segregation of participants' assets and insider theft; • issue independent audit reports on internal controls; • verify assets and issue a report; and • verify that there is full segregation of crypto assets for each client.	As noted above, Dealer Platforms will be subject to the requirements applicable to custody in Division 3 of NI 31-103 or, if they are Marketplace Platforms, those applicable to marketplaces that outsource key services set out in section 5.12 of NI 21-101. The suggestions regarding third-party entities may be helpful for CTPs in determining whether they have adequately assessed a third-party service provider.

Question 5: Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?		
Scope of SOC 2 reports	• Some commenters noted it is important for regulators to understand the scope of SOC 2 reports, since not all cover the same scope of controls; • One commenter noted that the scope and baseline of controls be determined before options regarding how to provide assurance over the design and effectiveness of these controls can be considered; the same commenter indicated that, once this is done, the CTP can decide whether to obtain a SOC 1 or SOC 2 report; • It was also suggested that regulators could review the scope proposed by a CTP on a case by case basis; • It was noted that, currently, SOC 2 reports are based on the Trust Service Criteria, but regulators should require that a SOC 2 report cover certain controls such as those related to system availability, processing integrity, confidentiality and privacy, as well as regulatory controls such as those related to client acceptance, transaction processing and custody; • One commenter indicated that the Trust Service Criteria should be supplemented by other frameworks dealing with a specific subject matter, for example, the NIST 800-53 *Cloud Controls Matrix* when reporting on cloud solutions; and • One commenter noted that the issuance of SOC2 Type I and Type II reports is not an adequate measure of safety for this industry. A number of commenters indicated that it is not possible that CTPs provide an unqualified opinion in a SOC 2 Type I or Type II report until it has been in operation for a reasonable period of time and suggested that a SOC 2 Type I report should be accepted for a period covering the initial operations (for example, six months), and a SOC 2 Type II report thereafter.	We thank commenters for their suggestions. It is our intention to focus the SOC 2 reports on critical systems for example, custody, order entry, and order execution systems. The determination of critical systems for a particular CTP will be dependent on the functions provided by the CTP. The scope of the SOC 2 reports will be discussed with each CTP at the time that the independent systems review is being planned. We acknowledge that CTPs may not be able to provide an unqualified opinion for a SOC 2 report at the time of launch. We will consider other possible mechanisms to obtain the necessary assurance.
Alternatives to SOC 2 reports	Commenters suggested a variety of ways for CTPs to provide assurance to regulators that a CTP has controls in place to ensure that investors' crypto assets exist and are properly protected, and that transactions are verifiable. These include: • regulators having special teams dedicated to emerging technology, including blockchain, that would, among other things, conduct reviews to ensure that investors' assets exist and are properly segregated and protected; • establishing an SRO with a division that specifically deals with this issue;	We thank commenters for their suggestions. It is our intention to generally require third-party systems reviews to be conducted on an annual basis once operations begin to provide assurance to regulators that a CTP has appropriate internal controls in place, similar to the existing requirements for marketplaces.

	• regulators engaging a third party that offers security evaluation services to the government and industry; • accepting reports from qualified experts which are not necessarily auditors, as long as relevant qualifications concerning independence and expertise can be established (similar to mining experts); • accepting SOC 1 reports with the appropriate scope and control objectives; it was noted, however, that a SOC 1 report should be required in addition to a SOC 2 report, because it focuses on a service organization's controls likely to be relevant to an audit of financial statements, which may include controls over custody systems if they are relevant to financial reporting; • requiring frameworks such as COSO, COBIT or CSAE 3000; • accepting a SOC 2 Type I report alone; • accepting SOC 3 Type I and Type II reports, as these are easier for investors to understand; • performing audits of specified procedures that are designed to target key areas of risk and security concerns; and • requiring CTPs to provide 'Proof of Reserve'.	If it is not possible to provide a SOC 2 report, CTPs may propose alternatives to provide regulators with this assurance. Such alternatives may be acceptable if the appropriate or a similar level of comfort is provided. In our view, from an investor protection perspective and given the high risk associated with safekeeping of investors' assets, it is especially important for CTPs that offer custody services to provide a third-party report on relevant controls. CTPs outsourcing such services would have to ensure that the service entity to which the custody functions were outsourced can provide such a report. That said, as indicated above, there will be flexibility on the types of entities qualified to provide custody and the scope of the reviews, as long as the risks are addressed and required assurance is provided.
Question 6: Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?		
Benefits associated with CTPs maintaining participants' assets	Commenters noted the following benefits associated with CTPs maintaining participants' assets: • CTPs have security and technology resources that individuals do not have; • there is no risk of participants losing their own private keys as a result of participant error; • investors may not be interested in maintaining wallet technology; • lower fees (for example, there are no on-chain transaction fees, no mining verification costs); • higher speed of trading (because there is no on-chain transaction verification	We thank the commenters for these responses. While it is not our intention to mandate how crypto assets are held, these considerations will help us better understand the risks associated with CTPs' operations and whether they have the proper processes to manage these risks.

	• participants are able to sell crypto assets quickly in response to market developments, which better allows them to manage market risk; • holding multiple participants' assets allows a CTP to aggregate multiple trades easier and ensure that large orders can be cleared in a simple fashion, without triggering a lot of small, on-chain transactions; • requiring CTPs to hold participants' assets in individual segregated wallets could publicly reveal confidential information about the participants' holdings, trades and counter-parties; • holding participants' crypto assets would mitigate the risk that a participant selling crypto assets will fail to complete a sale; and • for crypto asset to fiat trading, a centralized party is needed to store and distribute the fiat to investors.	
Challenges and concerns associated with CTPs holding crypto assets for their customers	A few commenters indicated challenges and concerns associated with CTPs holding crypto assets for their customers, including: • the fact that facilitating the transfer of crypto assets in and out of a CTP is viewed by many third parties (insurance providers, banks etc.) as a high-risk activity from both a money laundering and fraud perspective; • there is an expectation for CTPs holding private keys to keep up with events such as "hard forks", "airdrops" and "dividends", which would require additional programming and technical modifications by the CTP; • CTPs may not be qualified custodians or use the services of a qualified custodian and may not utilize acceptable controls, • CTPs may not segregate participants assets from the CTP's assets; • CTPs may become target for attacks by hackers when they hold a large quantity of crypto assets; and • the creation of difficulties for legal ownership determination.	We thank the commenters for these responses. They raise important considerations that will help regulators understand the risks associated with CTPs holding crypto assets for their investors, and whether they have adequate processes to ensure that the investors' assets are safe.

Question 7: What factors should be considered in determining a fair price for crypto assets?		
Comments on factors to consider in determining a fair price	A number of commenters noted that pricing should be determined by supply and demand in the market, and that market forces will ensure that CTPs have an economic incentive to maintain fair prices. Commenters listed factors that should be considered in determining a fair price for crypto assets. They included: • for ICO tokens, the progress made on the underlying technology and the type and purpose of the utility underlying a crypto asset; • whether the founding members or representatives of the crypto asset are active participants on social media and respond quickly and appropriately to questions and critiques; • the bid and the ask, for crypto assets that do not derive their value from underlying products; • for tokens backed by an asset, such as gold or a fiat currency, the asset and liquidity of the token; • whether the underlying asset produces dividends; • mining costs and difficulty of mining; • the number of tokens issued / that will be issued and whether there is a small group that has possession or control of a large portion of the issued tokens; • volume of crypto assets that cannot be traded (e.g., lost, locked up in a smart contract, hack or ICO); • transaction speed and cost; • price of other / related crypto assets; • legitimate level of trading volume / liquidity, and the mix of types of order flow; • jurisdiction and regulatory oversight for a particular CTP or crypto asset; • use of liquidity pools and arbitrage bots; • shorting and / or margin trading can have benefits in preventing market manipulation (and thus efficient pricing that is in line with other CTPs and creates a more consistent global price for digital assets); and • third party reference data (reliable and vetted).	We thank commenters for describing the factors that should be considered in determining a fair price for crypto assets. Where the CTP or an affiliate is trading on the CTP as principal, the CTP will be required to provide participants a fair price. In addition, a CTP will be expected to not do anything that interferes with a fair and orderly market, which would include offering unfair prices. IIROC's fair pricing requirements allow dealers flexibility in determining what policies and procedures are needed, as long as they meet the requirement to provide a fair price. In the context of their oversight, regulators review their policies and procedures to assess whether they are adequate.

Question 8: Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?		
Pricing sources that may be used by CTPs to determine a fair price	While one commenter indicated that they were not aware of any pricing sources that were reliable, many commenters suggested a number of pricing sources that could be considered, including: • Coinmarketcap.com (it was noted, however, that this source can simply add or remove data from specific CTPs only); • Poloniex (for less liquid crypto assets); • Bloomberg (which encompasses data from large CTPs such as Coinbase, Kraken and Bitstamp); • a weighted average of prices on the large CTPs (examples given were Coinbase, Bitfinex, Binance) or CTPs with high depth of the market. It was noted, however, that an approach where prices are aggregated across CTPs may not be adequate because there may be misleading trading activity; • MV Index Solutions GmbH (MVIS), an index provider based in Frankfurt and regulated as an index administrator by BaFin, as they administer the MVIS CryptoCompare Bitcoin Index • the CME CF Bitcoin Reference Rate published by the CME and the CME CF Bitcoin Real Time Index (BFTI); • the Ethereum Reference Rate and Real-Time Index; and • Brave New Coin has indices supported by NASDAQ.	We thank the commenters for the responses. We will be considering this information.
Factors that should be used in determining whether a pricing source is reliable	One commenter indicated that key signs that a pricing source is unreliable are: fake volume, increasing volume without an increasing number of users and consistent uniform volume that is not consistent with what is expected on a CTP. One commenter noted that a pricing source is reliable if the price is established based on the most recent legitimate transaction completed. Another commenter stated that the onus is on a CTP to communicate their best execution strategy and provide sufficient data to substantiate based on own methodology. Another commenter noted that regulators should focus on global markets that afford same level of protection to arrive at a "consolidated national (global) best bid/offer".	We thank commenters for the input on means of determining whether a pricing source is reliable.

Question 9: Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?		
Circumstances under which a CTP may be permitted to set their own rules and monitor trading activities on their CTP	A few commenters were of the view that CTPs should not monitor their own trading activities. One commenter suggested that a CTP be required to retain a regulation services provider (RSP), at least initially, and use its own surveillance system in parallel. If the two monitoring regimes produce the same results, then the CTP may be permitted to conduct its own surveillance. One commenter raised questions regarding IIROC's capacity to surveil and supervise these CTPs if multiple applicants become registered. Another small subset of commenters expressed that it is reasonable for CTPs to set and enforce their own rules and noted that CTPs have already started to monitor their own trading. It was noted that a number of CTPs are currently using Nasdaq's proprietary monitoring software (SMARTS). Some thought that this should be allowed at least until such time as regulatory authorities are able to provide full market oversight. Most commenters, however, supported an approach where the CTP (or a third party that is not a regulator) would monitor trading activities, subject to regulatory oversight. Commenters noted that this could be done in a few different ways, for example: • by allowing the CTP to monitor compliance with marketplace specific rules and activities but also requiring the CTP to engage an RSP such as IIROC to conduct market surveillance; • allowing CTPs to monitor for manipulative and deceptive trading, with regular reporting of transactions to the RSP; and • allowing CTPs to monitor their own trading, subject to regulatory access and oversight where the activities are relatively straightforward and the CTP presents a relatively low risk.	We thank commenters for their responses. We remain open to options regarding surveillance of trading activities under the interim approach to regulation described in the Notice, provided these are appropriate and adequate for the marketplaces operated. We expect IIROC to monitor trading of the Marketplace Platforms it regulates to ensure, among others, a consistent level of regulatory oversight across Marketplace Platforms and, where appropriate and trading activities are similar, to existing marketplaces.

Question 10: Which specific market integrity requirements should apply to trading on Platforms? Please provide specific examples.		
Comments on the UMIR that should apply to CTPs	The responses varied. A small number of commenters thought that the UMIR in its current form should apply to trading on CTPs. Some commenters thought that, while the entire UMIR may not apply, or may need to be modified to account for specific nuanced elements of CTPs (such as the fact that they operate outside of regular market hours), at least some of the provisions of the UMIR should apply, such as: • Part 2 – Abusive Trading • Part 3 – Short Selling • Part 4 – Front Running • Part 5 – Best Execution • Part 6 – Order Entry and Exposure • Part 7 – Trading on a Marketplace • Part 8 – Client Principal Trading • Part 10 – Compliance	We contemplate that, generally, the trading activity on a Marketplace Platform will be subject to the UMIR or requirements consistent with those in the UMIR, although tailoring of such requirements may be appropriate to accommodate the novel aspects of CTPs.
Prohibition of dark trading and short selling activities	Three commenters cautioned against prohibiting short selling and margin trading without doing further analysis on their prevalence and significance. It was noted that short-selling activities may help crypto assets become legitimate assets in the mainstream financial markets, provide a means of stability and risk management, and prevent market manipulation.	As noted in CP 21-402, CTPs will not be allowed to permit dark trading or short selling activities, or to extend margin to their participants in the near term. We will revisit this once we have a better understanding of the risks introduced by CTPs to the market and how these risks are managed.

Question 11: Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?		
Comments on crypto-asset market surveillance tools	While one commenter noted that there are no reliable third-party surveillance tools currently in the market, others gave the following examples: • Blockchain.com; • Etherscan.io; • Nasdaq's SMARTS market surveillance technology; • the Irisium Surveillance platform from Cinnober; • specialized blockchain analysis such as Elliptic, CipherTrace or Chainalysis, which can trace transactions; • surveillance software that can monitor "Know Your Transaction"; and • FinCEN.	We thank the commenters for these responses. As we noted above and in the Notice, we have proposed an interim approach to regulation for CTPs that need more time before IIROC membership can be obtained. We will consider these surveillance tools in assessing whether the CTP is adequately managing their risks.
Question 12: Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?		
	Commenters noted the following risks: • where transactions are conducted wallet-to-wallet, investors may not be dealing with a trusted counterparty; • trading occurring outside of displayed venues; • inflated transaction volumes on CTPs; • the global nature of the business; • the highly technical nature of the business; • security risks; • anonymity of wallets; • money laundering / terrorism financing; and • not all cryptocurrencies have surveillance software.	We thank commenters for identifying these risks. We will take them into consideration in determining the appropriate surveillance for CTP trading.
Question 13: Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.		
Circumstances under which an exemption from the ISR requirement may be appropriate	While two commenters indicated that there are no circumstances where an exemption to provide an ISR by a CTP would be appropriate, most commenters supported some flexibility in applying the requirement. Other commenters indicated that ISRs can be prohibitively expensive for small firms, and that there should be flexibility depending on the level of complexity and risk of the CTP.	While there should be some flexibility in applying the requirement for an ISR, the reliance on critical systems for trading and management of client assets is a key risk for CTPs. For this reason, we are of the view that the right balance needs to be struck to

	Commenters noted the following circumstances in which such an exemption may be appropriate: • where the CTP is decentralized and matches and settles the transactions without holding private keys and its participants use a multi signature wallet; • if there is regular and independent self-assessment of internal controls conducted by the CTP, the CTP provides reports of its monitoring of controls, no significant issues are identified, and exposure is limited; and • for CTPs that leverage well established third-party systems (such as cloud-based infrastructure, trade matching engines and surveillance tools developed by traditional equity market providers). Other comments included: • marketplaces should voluntarily submit ISRs for the next five years until patterns can be observed and a generalized approach conceived; and • There should be a transitional period to determine whether an ISR is needed.	ensure the reliability, resilience and security of these systems. We may consider exemptions from the requirement to conduct third party systems reviews on critical systems where assurance is provided that the risks are appropriately being managed and that systems and controls used are assured to be reliable, resilient and secure.
Services that should be included or excluded from the scope of an ISR	One commenter noted that the scope of an ISR should be determined by insurance providers, as policies are priced partly on the basis of independent system reviews. Other commenters noted the following services that should be included in the scope of an ISR: • custodial services; • system capacity to handle changing market conditions; • robustness of BCP and DRP; and • effectiveness of incident reporting and remediation.	The purpose of ISRs is to provide regulators with independent assurance that CTPs have adequate internal and information technology controls for its critical systems. While insurance providers may price their policies partly based on independent system reviews, the scope of any independent reviews they require may not be similar and not transparent to regulators. For these reasons, we are of the view that it would be inappropriate to rely on ISRs whose scope is dictated by insurance providers. As indicated above, we agree that custodial services should always be included in the scope of an ISR. We may consider exemptions for other non-critical functions, in certain circumstances.

Other comments	One commenter noted that the existing requirement in subsection 12.4(2) of NI 21-101 regarding the resumption of operations following the declaration of a disaster by a marketplace should not apply to CTPs trading digital securities, as they trade a few unique securities.	We note that the requirement in subsection 12.4(2) of NI 21-101 requires that a marketplace have policies and procedures for resumption of operations of their systems. The requirement allows for flexibility in circumstances where this is not possible.
Question 14: Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?		
Disclosure specific to trades between a CTP and its participants	Commenters indicated that CTPs should disclose that the CTP acted as principal and any discrepancies between the trade and the terms of an equivalent trade, if that trade were to be made on the market. It was also suggested that designated market makers on a CTP should have unique identifiers, so that participants can identify trades executed against a market maker.	CTPs should disclose all conflicts of interest, including those that would arise when a CTP trades as principal. We will consider the suggestion that designated market makers should have unique identifiers to allow participants to identify trades against a market maker. We note that currently, designated market makers trading on equity exchanges do not have unique identifiers to the public but IIROC is able to identify them in its surveillance system.
Question 15: Are there any particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?		
Conflicts of interest related to the multiple functions performed by CTPs	Multiple commenters noted that the combination of the multiple functions that may be performed by CTPs, specifically, acting as a marketplace, clearing agency, dealer and custodian, presents conflicts of interest. Commenters indicated that these conflicts could be managed in a number of ways, including: • by bifurcating a CTP's role as a dealer and marketplace; • by providing transparency of these functions, risks and mitigating controls; • by separating the functions of order matching, market making and deposit taking; • by limiting access by proprietary trading desk to customer information; and • careful consideration of the market making function. Some commenters believed that CTPs should not be permitted to provide custody of participants assets to avoid operational conflicts.	We thank the commenters for the responses. It is not our intention to mandate how a CTP will structure its operations, as this would be inconsistent with our goal of facilitating innovation that benefits investors and our capital markets. Rather, CTPs are required to comply with the applicable requirements, and we will assess the risks introduced by the CTPs and

	Other conflicts of interest identified included: • participants' funds may not be segregated from the funds of the CTP; • the CTPs may trade as principal (although one commenter thought this could have benefits, such as increased liquidity); • CTPs have more information than their participants (for example, they hold information of previous participants) and may develop derivative information; • CTPs may have information about their participants' upcoming trades, which could lead to front running; • CTPs and their employees may have access to non-public information, including information related to which crypto assets will be listed on the CTP and could trade on that knowledge; • CTPs may issue their own security tokens that are also traded on the CTP; • CTPs may receive payments in exchange for listing certain crypto assets; • Potential use or sale of investor information (including data on specific holdings); and • payment for order flow**.**	whether they have the internal controls and processes in place to address them. As noted in the Notice, CTPs will be required to identify and manage potential conflicts of interest. Their policies and procedures, including those dealing with conflicts of interest, will be examined by regulators both in the context of reviewing their initial application for registration and/or IIROC membership and on an ongoing basis, as part of our regulatory oversight. These comments will help us better understand the full range of potential conflicts of interest that may arise at a CTP and whether they have appropriate policies and procedures to manage them.
Question 16: What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to maintain? Please explain.		
Types of insurance coverage a CTP should be required to maintain	Approximately a quarter of the commenters that responded to this question thought CTPs should be required to maintain full insurance. A few commenters thought CTPs should not be required to have insurance and noted that requiring insurance would be prohibitive to small start-up CTPs. Other comments included: • there should be insurance for hot and warm wallets, but it is debatable whether insurance is needed for assets held in cold wallets, especially if appropriate controls and policies are put in place, as evidenced by a SOC 2 report; • the appropriate nature and extent of the insurance will vary with the circumstances, considering the nature of the risks, other forms of risk transfer and risk mitigation processes in place at the CTP; • insurance should be optional, and the market should decide the right mix of insurance and security; and • a cautious approach to insurance requirements should be taken.	We thank the commenters for the responses. We will consider the need for insurance and the type in the context of the functions performed by a particular CTP. However, we are of the view that CTPs will likely require insurance where they have custody or control over client assets unless they can demonstrate an adequate alternative risk mitigation strategy. Such insurance should cover specific risks including, but not limited to, the risk of theft and cyber-attacks.

	Most commenters provided feedback on the types of insurance that should be required. This included: • the same insurance required for traditional dealers and custodians; • crime and theft insurance coverage for all fiat funds and crypto assets, regardless of the method of storage; • crime and theft insurance if CTPs are holding material amounts of crypto assets in hot wallets; • errors and omissions and cybersecurity insurance; • insurance in case of death or incapacity of a key holder; • financial Institution Bonds to cover employee dishonesty, forgery, vendor-related fraud and theft; • cyber insurance to protect impact of damages to computer systems (outages & failures); and • director and officer insurance.	
Question 17: Are there specific difficulties associated with obtaining insurance coverage? Please explain.		
	Many commenters noted a number of difficulties associated with obtaining insurance coverage. The main concern identified was that it is difficult and expensive for CTPs to obtain any type of insurance (hot wallet, cold storage, theft and other). It was noted that few insurance providers are willing to cover CTPs, and those that do charge high premiums (one commenter noted that premiums can be 1-2% of the insurable assets). Commenters also noted that: • the market for underwriting the risks associated with crypto assets is limited and the underwriters' understanding of the technology and industry remains limited; • insurance companies are hesitant to work with CTPs, largely because the money laundering risks; • there is no historical and actuarial data in the crypto markets to determine appropriate premiums; • CTPs are not able to have the stringent controls expected by insurance providers; • coverage for cyber theft is expensive and does not provide a significant degree of protection to customers; and • cold wallets are not insured by all insurers. One commenter noted, however, that CTPs are becoming increasingly able to obtain insurance for the assets they custody and gave the examples of Coinbase, Bakkt and BitGo.	We acknowledge the concerns raised regarding the ability to obtain insurance coverage. We will continue to monitor this over time. Acknowledging the current possible difficulties in obtaining insurance, there will be flexibility regarding the type and level of insurance required, as long as the risks associated with the custody of client crypto-assets are addressed.

Question 18: Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?		
Member-funded insurance	A large number of commenters that responded to this question indicated that there should be member funded insurance such as CIPF or CDIC. Commenters noted their expectation that, if required to register as an IIROC dealer, CTPs will be CIPF members. One commenter suggested a form of self-insurance where CTPs contribute premiums to compensate participants in cases of loss, and such premiums are based on trading volume, history of losses, quality of audit reports, use of RSPs, or whether the CTPs provides custody.	CTPs that will be IIROC dealer members will be CIPF members. CIPF will assess the coverage it offers on a case by case basis. While we do not intend to mandate how CTPs compensate participants in cases of loss, we will consider their processes in our assessment of the type and level of insurance they will be required to maintain.
Alternatives to insurance coverage	Commenters listed a number of alternative measures that could be considered equivalent to insurance coverage. These included: • robust practices, policies and procedures with respect to handling participants' assets; • an adequate level of capitalization, so that a loss of assets can be absorbed by the CTP; • segregation of participants' assets from a CTP's assets (although it was noted that this constitutes an inherent safeguard that offers investor protection in the event of bankruptcy, but not theft); • a fund maintained by the CTP that is funded using a percentage of the trading fees or the CTP's profit (many commenters suggested a fund similar to the Secure Asset Fund for Users established by Binance); • maintaining fiat balances in amounts equivalent to the crypto assets held on behalf of participants in hot wallets; • maintenance of participants' and CTPs' crypto asset across multiple wallets, to distribute the risk and responsibility of security, reducing the amount of insurance required; • proof of distributed authority, key management systems, Dead Man's Switch; • decentralized CTPs with multi signature wallets for participants; • maintaining 95-100% of the balances in cold wallets, to mitigate the risk of hot wallet theft; • insurance intermediation platforms, which involve the use of crypto assets as a form of premium that participants can exchange with the CTP in return for an insurance	We thank the commenters for the responses. We will consider these measures in assessing the level and type of insurance that should be maintained by CTPs.

	policy being placed with an insurer; the CTP acts as a digital provider of insurance intermediation services and still relies on the traditional insurance market; • evidence of funding, such as bonds, letters of credit or sufficient working capital, • the investors' own insurance; and • a card with security features, which could be printed by Canadian Mint, which would be loaded with crypto assets; the investor is the only one that can store and access the assets.	
Question 19: Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?		
Models of clearing and settlement for CTPs	Commenters identified the following models for matching trades and clearing and settling transactions: • CTPs maintain an internal ledger that maintains a record of all transactions; once matched, transactions are settled on the blockchain; • the decentralized model, where users' orders are matched with each other on a CTP, but the CTP does not, at any point in the transaction, hold users' funds; • a central counterparty clearing system with net settlement similar to CDS or CDCC; and • new technology is being developed that will allow holders of one crypto asset to swap or trade with a holder of another crypto asset on the blockchain, without the involvement of any third party.	We thank the commenters for providing information on other models for matching trades and clearing and settling transactions.
Risks and concerns introduced by the models of clearing and settlement for CTPs	Commenters noted that: • where CTPs perform both clearing and custody functions, there is counterparty risk and credit risk (for example, if participants are permitted to trade on margin, with settlement at a later date); it was noted that counterparty risk could be mitigated, for example, by the imposition of a requirement for participants to pre-fund trading accounts with fiat currency before completing a trade; • with respect to the new technology that permits holders of one crypto asset to swap with a holder of another crypto asset on the blockchain, there is the risk that the technology could be flawed and funds lost through a technical error; at the same time, there is reduced risk of a third-party losing funds; • the use of currently available clearing houses or establishing identical requirements for new CTPs ignores the value and reasons for using distributed ledger; and • all models of clearing and settling crypto assets presently utilized by CTPs introduce a centralized point of failure. One commenter stated that decentralized models have less cyber-security risk.	We thank the commenters for these responses. We will consider these risks in assessing the requirements that should apply to CTPs performing clearing and custody functions.

Question 20: What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these risks could be mitigated.		
	Commenters identified the following differences between the traditional model of clearing and settlement and the decentralized model: • all transactions that take place on the distributed ledger are permanent and irreversible; • there is a higher possibility of human error in the traditional model, where settlement occurs days after the trade, with trade matching and payments occurring in a more manual and costly model; • there is significant systemic risk in the traditional model, due to concentration of this risk in one entity; • counterparty risk is eliminated on decentralized CTPs, however participants have no way of knowing who they are trading against, which makes it difficult to manage compliance risks; • the key risk for transactions settled on a decentralized model is ensuring delivery versus payment; the payment is made when the client deposits fiat or crypto assets as the means to purchase a crypto asset. The delivery and settlement are confirmed by receipt of the crypto asset at the custodian, verifiable "on-chain" by anyone running a node, including a custodian; • when transactions are executed on a distributed ledger, the assets may become lost if there is a software bug in the smart contract development or deployment; • identity fraud is easier in a digital ecosystem; complete decentralization may not provide sufficient KYC/AML protection, and has not evolved to the point where it provides frictionless AML controls; and • with the decentralized model trades are cleared in real time, where in a traditional model it is subsequent to the trade day. One commenter indicated that the risk associated with not having third-party clearing and settlement could be mitigated by having a hybrid model where CTPs maintain an internal ledger and transactions are also executed on the blockchain.	We thank the commenters for these responses. We will consider these differences, and the specifics of the decentralized model of clearing and settlement, in determining the appropriate clearing and settlement requirements that should apply to CTPs.
Question 21: What other risks could be associated with clearing and settlement models that are not identified here?		
	One commenter noted risks specific to stable coins, which may be backed by complex systems of collateral. The commenter noted that, if the underlying asset crashes, there is a risk that a cascade of smart-contracts are triggered, and a large volume of clearing and settlement is executed. Additional comments on other risks associated with clearing and settlement included: • faster asset and payment movement create higher turnover on networks; • reputational risk;	We thank the commenters for the responses and note that we will consider these specific risks in determining the appropriate clearing and settlement requirements that should apply to CTPs.

	• inter-organizational settlement (complexity) risk in using CTPs like Ripple or Ethereum to settle interbank transfers; • regulatory risks (no designated regulatory body monitoring transactions); and • liquidity and timing risk with decentralized exchanges.	
Question 22: What regulatory requirements (summarized at Appendices B, C and D), both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and rationale.		
Regulatory requirements that should apply to CTPs	One commenter stated that its it more productive to start with the risks and then identify the relevant requirements. Commenters indicated that the following regulatory requirements, should also apply to CTPs: • transparency of a CTP's operations, including how orders are entered and executed; • daily reconciliations between CTP and third-party data; • disclosure of a CTP's governance structure; • disclosure of the CTP's rules; • disclosure of the CTP's fees; • disclosure of conflicts of interest; • transparency of crypto assets traded, including its features, attributes, use, value, risk factors and the method of valuation; • daily reporting of funds, transactions and volumes; • the requirement to send account statements to participants on a regular basis, and at least quarterly; • trading information should be confidentially maintained; • recordkeeping; and • the principle of fair and orderly markets but interpreted in the context of CTPs.	We agree and note that this is the approach we have taken in developing the regulatory framework applicable to CTPs. We will continue to evaluate the risks and the appropriate regulatory requirements as the industry evolves. We thank commenters for the suggestions. We are of the view that the approach, which is based on the Marketplace Rules and NI 23-103, will cover these requirements.
Regulatory requirements that should not apply or should be modified – suitability requirements	One commenter indicated that all the requirements applicable to dealers may be relevant, with the exception of suitability if no advice or recommendations regarding the buying and selling of specific crypto assets are made by the CTP. Another commenter suggested that new categories of qualified investors be introduced, in the spirit of democratizing investments.	The suitability requirements will apply to Dealer Platforms, but where a Dealer Platform only offers Crypto Asset Rights and is not providing recommendations or advice, we may consider whether, similar to order-execution-only platforms, an assessment at onboarding may be more appropriate compared to trade-by-trade suitability.

Regulatory requirements that should not apply or should be modified	Comments included: • capital requirements should only be imposed on CTPs where the participants' assets are held in omnibus or commingled accounts; • capital adequacy requirements for CTPs should be modest where the CTP does not custody participants' assets; and • there should be exemptions from the requirement to clear and settle trades through a recognized entity.	The CSA and IIROC will consider each CTP's operational model, risks introduced and how these risks are managed by the CTP to determine what regulatory requirements should apply or be modified. Flexibility in the application of regulatory requirements would be achieved through exemptions from existing requirements where justified.