CHARTERED PROFESSIONAL ACCOUNTANTS CANADA
COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Chartered Professional Accountants of Chartered Professional Accountants of Canada
277 Wellington Street West Toronto (ON) CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
www.cpacanada.ca

Comptables professionnels agréés du Canada
277, rue Wellington Ouest Toronto (ON) CANADA M5V 3H2
T. 416 977.3222 Téléc. 416 977.8585
www.cpacanada.ca

April 16, 2024

c/o

The Secretary
Ontario Securities Commission
20 Queen Street West 22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
Email: comments@osc.gov.on.ca

Me Philippe Lebel
Secrétaire et directeur général des affaires juridiques, Autorité des marchés financiers
Place de la Cité, tour Cominar
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1
Fax: 514-864-6381
E-mail: consultation-en-cours@lautorite.qc.ca

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumers Services Commission, New Brunswick
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Office of the Superintendent of Securities Service Newfoundland and Labrador
Office of the Superintendent of Securities, Northwest Territories
Office of the Superintendent of Securities, Yukon Territory
Superintendent of Securities, Nunavut

To whom it may concern:

Re: Proposed Amendments to National Instrument 81-102 Investment Funds Pertaining to Crypto Assets

Chartered Professional Accountants of Canada (CPA Canada) appreciates the opportunity to comment on the Canadian Securities Administrators (CSA) proposed amendments to National Instrument 81-102 *Investment Funds* (NI 81-102) and proposed changes (the CP Changes) to Companion Policy 81-102CP *Investment Funds* (81-102CP) (collectively referred to as the Proposed Amendments and CP Changes) which seeks feedback on how the existing regulatory framework in NI 81-102 needs to be adapted to properly account for the unique aspects of crypto assets as an investment product for publicly distributed investment funds.

We support the CSA initiative to provide investment fund managers with greater regulatory clarity concerning investments in crypto assets, which may facilitate new product development in the space while also ensuring that appropriate risk mitigation measures are built directly into the investment fund regulatory framework.

CPA Canada is one of the largest national accounting bodies in the world representing more than 220,000 members. It works collaboratively with the provincial, territorial and Bermudian CPA bodies, as it represents the Canadian accounting profession, both nationally and internationally. This collaboration allows the Canadian profession to champion best practices that benefit business and society, as well as prepare its members for an ever-evolving operating environment. CPA Canada also actively supports the independent structure of accounting, audit and assurance, and sustainability standard setting in Canada by providing funding, staff and other resources. CPA Canada also issues guidance and thought leadership on a variety of matters, including but not limited to audit and assurance, financial reporting and sustainability.

In formulating our response on specific aspects of the Proposed Amendments and CP Changes, we have drawn on our knowledge of audit and assurance practices and unique challenges related to auditing crypto assets. We also solicited input from our extensive network of volunteers representing members from accounting firms with expertise in the areas of crypto assets, blockchain, and system and organization controls (SOC) reporting. This includes our Crypto-Asset Auditing Discussion Group, facilitated by CPA Canada and involves representatives from the Auditing and Assurance Standards Board (AASB) staff, the Canadian Public Accountability Board (CPAB), CPA provincial practice inspection, and the auditing firms.

Overall Comments

We see continued interest in crypto assets and recognize this consultation is extremely important and the issues raised in the Proposed Amendments and CP Changes are critical for investor protection.

Emerging financial technology is a key area of focus for CPA Canada. We believe transparent and auditable crypto asset trading and custodial services are critical, and that the accounting profession plays a vital role in building public confidence in these areas.

CPA Canada is committed to supporting our members and other stakeholders in the crypto asset ecosystem by working with industry experts, the CSA, academia, and accounting and auditing and assurance standards setters through our various committees and working groups. Some of our recent educational initiatives include the following publications on auditing crypto-assets to support audit practitioners in applying Canadian Auditing Standards (CAS) in the crypto asset industry:

- Third-party service provider considerations
- Relevance and reliability of information from a blockchain
- Are tests of controls needed for the ownership assertion?

Responses to Consultation Questions:

After reviewing the specific questions in the Proposed Amendments and CP Changes, we have elected to provide a response to question 4 only. We also offer a few additional separate feedback points for your consideration, following our response to question 4.

4. Custody - The Proposed Amendments include a requirement that custodians or sub-custodians that hold crypto assets on behalf of an investment fund obtain an annual assurance report prepared by a public accountant that assesses the design and effectiveness of various internal controls and policies concerning their obligations to custody crypto assets. The CP Changes clarify that obtaining a SOC-2 Type 2 will be considered to comply with the requirement, without prescribing that specific report. We are seeking feedback regarding other assurance reports that may be comparable to a SOC-2 Type 2 that we should also consider sufficient for complying with this requirement. We are also seeking feedback regarding the appropriate scope of any reporting to be provided under this requirement.

Summary of Custody-related Recommendations

Listed below is a summary of our recommendations for the Proposed Amendments and CP Changes related to custodians or sub-custodians (herein referred to as Crypto Custodians) and the annual assurance report. Each recommendation is explained in greater detail further below, along with additional background information, for the CSA's consideration.

We recommend the CSA:

A. Establish expectations regarding the scope and/or a baseline set of high-level control objectives or system requirements that may be relevant in a controls assurance engagement for a Crypto Custodian. Examples of the types of controls that may be required to mitigate the unique risks relevant to these types of entities are included below. In establishing the scope of the assurance engagement, consider what assurance report options may exist. For example, consider whether a SOC 1 report, covering the expected scope and control objectives, may be appropriate (or necessary) in addressing regulatory expectations for controls assurance as an alternative or in addition to a SOC 2 report.

B. Reference which Canadian assurance standard should be used by the independent professional accountant when performing the SOC engagement, to enhance clarity of the requirements and consistency in practice.

C. Clarify intent regarding whether the assurance report must be prepared by an independent professional accountant, such as a CPA assurance practitioner, and use consistent terminology in both the Proposed Amendments (public accountant) and CP Changes (external auditor).

D. Add more specificity regarding the annual assurance report coverage period for scenarios where the SOC engagement reporting period does not align with the financial year-end; for example, including specificity on the minimum period covered by the SOC report and on the maximum number of months that the SOC reporting period can differ from the financial year.

System and Organization Controls (SOC) Assurance Engagements

System and Organization Controls (SOC) reports are assurance reports issued by practitioners who are engaged directly by a service organization (in this case the Crypto Custodian) to conduct a SOC assurance engagement. There are different types of SOC assurance engagements, and each is designed for a specific purpose and for different users. For the purposes of this response, we provide background information on both SOC 2 engagements (referred to in the Proposed Amendments and CP Changes) and on SOC 1 engagements.

SOC 2 engagements address controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy and may also provide additional relevant information related to aspects of the IT environment, depending on the scope of the SOC engagement. In Canada, SOC 2 engagements are performed in accordance with the Canadian Auditing and Assurance Standards Board's (AASB) Canadian Standard on Assurance Engagements (CSAE) 3000, *Attestation Engagements Other Than Audits or Reviews of Historical Financial Information* and use the American Institute of Chartered Public Accountants (AICPA) Trust Services Criteria (TSC) for Security, Availability, Processing Integrity, Confidentiality, and Privacy and the AICPA Description Criteria Section 200. It is important to highlight that the risks and corresponding controls covered in a SOC 2 report may not be designed, implemented or tested with the purpose of addressing the user entity's[1] internal control over financial reporting and therefore may not be relevant for an independent financial statement auditor for use in their audit.[2].

SOC 1 engagements are performed in accordance with a specific subject-matter standard, CSAE 3416, *Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, which requires compliance with CSAE 3000. SOC 1 engagements are typically most relevant to independent financial statement auditors, as they address the controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting.

CSAE 3000 and CSAE 3416 are included in the "Other Canadian Standards" section of the *CPA Canada Handbook - Assurance*. Herein, we will refer to SOC 1 and SOC 2 reports for simplicity.

A. The Importance of Establishing Expected Controls and SOC Report Type

Before determining the appropriate assurance approach, it is vital to first identify the controls required at a Crypto Custodian to mitigate the risks related to Crypto Custodians (i.e., Section 6.7 of the Proposed Amendments and Subsection 8.3(2) of the CP Changes which addresses processes relating to security and other measures pertaining to its custody obligations). To ensure your intended objectives for the Proposed Amendments and CP Changes are met and to enable consistency in practice, we recommend that the CSA establish expectations regarding the scope and/or a baseline set of high-level control objectives or system requirements that may be relevant in a controls assurance engagement for a Crypto Custodian.

The baseline control objectives/system requirements (herein referred to as 'controls') expected may include, among others, those that would be intended to manage and mitigate the custodial risks, including processes

[1] A user entity is an entity hat uses a service organization and whose financial statements are being audited

[2] For further information, refer to the AICPA's Auditing Interpreta ion No. 1, "Considera ions Related to the Use of a SOC 2 Report in an Audit of a User En ity's Financial Statements" at https://www.aicpa-cima.com/resources/download/interpretation-no-1-of-au-c-section-402

and controls to safeguard the assets. Examples of areas that may be necessary to address in a Crypto Custodian's SOC engagement to mitigate the unique risks relevant to these types of entities may include:

- cryptographic key creation, key security and key management controls, and
- custody and record-keeping controls (e.g., reconciliation to the blockchain) that ensure investors' crypto assets exist, are appropriately segregated and protected, and that ensure transactions with respect to those assets are verifiable.

CPA Canada has prepared guidance on third-party service provider considerations to assist auditors of financial statements that contain material crypto asset balances and whose entity engages with a third party (e.g., custodian) to transact and/or hold their crypto assets[3]. Although the scope of controls at a Crypto Custodian relevant to audits of user-entity financial statements may differ from the scope of controls expected by you as the regulator, our guidance may inform further changes to your regulatory framework in NI 81-102. Part 2 of this paper in particular may be helpful to you in considering the minimum risks and relevant controls you would determine necessary as part of the scope of the required SOC engagement.[4]

The SEC's Custody Rule is also one example of how you may specify what is appropriate from a control scoping standpoint without being too prescriptive.

Once you have established the scope and/or baseline of controls expected, options to provide assurance over the design and operating effectiveness of those controls can be explored. The CP Changes notes that the CSA is of the view that a SOC 2, Type 2 report for a Crypto Custodian will satisfy the requirements in the Proposed Amendments, though other comparable reports may also be considered from time to time. While one way to provide assurance on such controls may be through the issuance of SOC 2 reports, not all SOC 2 reports have the same scope of controls. As mentioned above, if the SOC 2 report does not cover the scope of controls you expect, then it will not provide the assurance you are seeking.

For example, a minimum scope SOC 2 report may cover only those controls required to meet the Security category of the TSC (or a subset thereof) and would exclude the additional criteria and controls for system Availability, Processing Integrity, Confidentiality, and Privacy. Conversely, a SOC 2 engagement that evaluates and reports on all five criteria may not be necessary to satisfy the requirements in the Proposed Amendments. In addition, you may wish to require specific regulatory controls for such Crypto Custodians (see the 2018 SOC 2 Description Criteria[5] and 2017 Trust Services Criteria[6] for details) to help ensure the controls covered in the SOC 2 report meet your expectations.

As an alternative (or in addition) to SOC 2 reporting which you have suggested in the CSA Notice, a SOC 1 report, with the appropriate scope and control objectives, may be sufficient (or necessary) in addressing regulatory expectations for controls assurance. SOC 1 reports are often used to provide controls assurance

---

[3] https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/third-party-controls-crypto-audit-considerations

[4] The AICPA has also issued technical ques ions and answers related to the inclusion of information about controls over cryptographic keys in management's description of a service organization's system in a SOC 1 report at https://www aicpa-cima.com/resources/download/aicpa-tqas-9560-01-to-06

[5] https://www.aicpa-cima.com/resources/download/get-description-criteria-for-your-organizations-soc-2-r-report

[6] https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022

for traditional custody and exchange services, so it is unclear why they may not also be suitable for a Crypto Custodian, provided the appropriate scope and control objectives are covered. For financial statement audits of entities who use Service Organizations (including traditional or Crypto Custodians) as defined by Canadian Auditing Standards, auditors will typically look to obtain a SOC 1 report to understand the entity's system of internal control relevant to the preparation of the financial statements.

It may be possible to develop a set of regulatory requirements for Crypto Custodians that could be used as either System Requirements for SOC 2 reporting, or Control Objectives for SOC 1 reporting, and allow the Crypto Custodian to decide whether to obtain a SOC 1 or SOC 2 report, or a combination thereof depending on the objectives and intended users.

B. Clarity on Assurance Standards Applied

The Proposed Amendments and CP Changes refer to a SOC 2 Type 2 Report prepared in accordance with the framework developed by the American Institute of Chartered Public Accountants (AICPA). While SOC 2 engagements use the Trust Services Criteria, a set of criteria established by the AICPA's Assurance Services Executive Committee, in Canada, a SOC 2 Type 2 Report would be prepared in accordance with CSAE 3000, as issued in the *CPA Canada Handbook - Assurance*. We recommend the Proposed Amendments and CP Changes be updated to reference which assurance standard should be used when performing the SOC engagement, to enhance clarity of the requirements and consistency in practice. Moreover, firms that perform SOC engagements and apply CSAE 3000 are also required to apply Canadian Standard on Quality Management 1, which deals with a firm's responsibilities to design, implement and operate a system of quality management for audits or reviews of financial statements, or other assurance or related services engagements. For your reference, CPA Canada has prepared a guide for performing SOC 2 engagements, which was adapted from the AICPA version to meet Canadian standards[7].

C. Clarity on Who can Perform the Assurance Engagement

The Proposed Amendments refer to the Crypto Custodian's assurance report being prepared by a *public accountant*. The CP Changes refer to the assurance report being prepared by an *external auditor*. We recommend the requirements be revised to clarify the CSA's intent regarding whether the assurance report must be prepared by an independent professional accountant, such as a CPA assurance practitioner. In addition, there may be confusion with usage of the term *external auditor*, as it may imply the same auditor/practitioner would perform both the audit of financial statements and the controls assurance engagement of the Crypto Custodian.

Further, it may also be beneficial to incorporate appropriate qualifications of the practitioner performing the assurance engagement as part of the requirements.

D. Period Covered by the SOC Report

While the Proposed Amendment in Section 6.7 requires the Crypto Custodian to obtain an assurance report within 60 days after the end of its most recently completed financial year, we recommend adding more specificity regarding the coverage period for scenarios where the SOC engagement reporting period does not align with the financial year-end; for example, including specificity on the minimum period covered by the

[7] https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/internal-control/publications/soc-2-guide

SOC report (e.g., at least 6 months of the financial year-end), and on the maximum number of months that the SOC reporting period can differ from the financial year (e.g., coverage period must be no earlier than 3 months before the financial year-end).

It is important to note that if the reporting period does not align well with typical user entities' year-ends, the practitioner may not be able to rely upon the SOC report or may require the custodian to produce two SOC reports each year, each for a different purpose.

Other Considerations

We recommend that further clarification or consideration may be needed for the following:

- Defining a fungible vs. non-fungible crypto-asset within the Proposed Amendments and/or CP Changes, as this impacts the accounting treatment and disclosures in the financial statements.
- How the CSA defines a 'recognized exchange', recognized by a securities regulatory authority in a jurisdiction of Canada, in the context of NI 81-102 and the crypto-asset industry.
- Requirements or issues concerning crypto-asset staking.
- The CSA's thought process for allowing cryptographic keys to be stored in omnibus accounts given that regular mutual funds under NI 81-102 are required to be held in segregated accounts.
- Whether the CSA also considered amending or is intending to amend NI 81-106 for these instruments, in addition to NI 81-102.

We appreciate the opportunity to participate in this consultation and would be happy to meet to discuss our comments further. Please do not hesitate to contact Kaylynn Pippo, Director, Audit and Assurance [redacted] or myself.

Regards,

[redacted]

Rosemary McGuire, CPA, CA
Vice President
Member Experience