Consultation questions:

1. Are there factors in addition to those noted above that we should consider?

A: None

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

- there presently exist protocols which have baked into them KYC-based trade restrictions. Those can be extended as needed simply by amending the smart contracts.

- a comprehensive set of rules for the Platforms, and a positive disclosure obligation on the Platforms can go a long distance in mitigating the risks associated with processes, policies and procedures (trade order, conflicts, token security controls, record-keeping, etc.).

- similarly, a standardized (or relatively so) disclosure form can be created that token-issuers must complete and must be kept by the Platform for each token it trades, and that form be provided to each investor prior to completion of any token purchase (complete with a click-box acknowledgement that the form has been read to the investor's satisfaction).

- rules regarding custody can be created. For example, each investor must be clearly presented with the choice to have its tokens stored in its own wallet, or on that of the Platform; Platforms may be allowed to aggregate multiple investors' tokens, but not co-mingle them with Platform's tokens. It may also be determined best that Canadian investors' tokens, if stored by the Platform, must be stored in a cold wallet physically located in Canada.

- an audit function must be introduced with reporting on Platforms' compliance with this set of rules.

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

No comment.

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.

No comment.

5. Other than the 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' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

No comment.

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 Platforms holding or storing crypto assets on their behalf?

- Speed of completion of trades may be affected if crypto is held in a participant's wallet, if the participant also retains the private key (and not the exchange)

- the participant's wallet may be less secure than that of the exchange, and therefore more prone to hacks, especially in the case of hot wallets

- the participant may be more likely to lose (or have fewer safeguards/redundancies to prevent against the loss of) private keys than an exchange

- for all of the above reasons, it may be preferable to have the Platform store crypto assets on behalf of investors

7. What factors should be considered in determining a fair price for crypto assets?

No comment.

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?

- Coin Market Cap is widely recognized as a fair resource for a token price. There are also a number of leading exchanges. Often, in M&A transactions, the accepted value of crypto is that as stated in coin market cap, and, should that not be available, the average price of the average in-day price of three leading exchanges.

- Reliability of a pricing source can be assessed based on the degree of variance between the price in question, and that found in the already-accepted authorities. Trading history on a particular exchange may also be a factor in determining price reliability.

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?

- perhaps not initially – if a Platform wants to conduct its own monitoring, it should be required to use an RSP initially, and use its own monitoring system as a duplicate tool. If the 2 regimes yield the same or materially similar results over a stated period of time, then the Platform would have established the case for the use of its own monitoring tool, and the RSP can drop off. However, regulators would retain the right to conduct audits of these Platforms' monitoring systems.

10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.

- trading order practices must be implemented – ie: if a bid has several possible matches, it would be paired to the first-posted ask; there would be no discretion as to how trade partners are paired.

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?

- No comment.

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?

- No comment.

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

- No comment.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

- If the Platform is the counterparty to the trade, this must be disclosed.

15. Are there 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?

- Many Platforms also issue their own security tokens that would be traded on the Platforms. Platforms would be able to use token supply management to offer price support, and primary token sales by the Platform (from treasury) would always be in conflict to secondary market trades by token holders if both were allowed to occur at the same time. Perhaps it would be necessary to not allow both primary and secondary trades to occur at the same time, meaning that the Platform would have to complete its primary token issuance in order for the tokens to trade on the Platform’s secondary market.

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

- This may be something that the market can decide. Rather than mandate what type of insurance is required, make it mandatory that all Platforms disclose the type and amount of insurance they carry for the benefit of their participants. In that way, participants will select out those Platforms that carry inadequate levels of coverage, and will also select out those that have coverage that is more expensive than they are willing to pay for.

17. Are there specific difficulties with obtaining insurance coverage? Please explain.

- No comment.

18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

- There could be a form of self-insurance, whether on an individual Platform basis or respecting the industry as a whole, where all Platforms contribute premiums to a central repository, where they are held to compensate participants in cases of loss. The size of premiums assessed against a Platform can be based on trade volume, history of losses (or absence of losses), quality of audit reports, use or non-use of RSP’s, whether Platform does or does not maintain custody of crypto, etc.

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?

- No comment.

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 different risks may be mitigated.

- No comment.

21. What other risks are associated with clearing and settlement models that are not identified here?

- No comment.

22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

- No comment.