1. Are there factors in addition to those noted in Part 2 that we should consider?

<No Comment>

2. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?

- Problem: Individuals have the ability to create Initial Coin Offering (ICO) or Security Token Offering (STO), and platforms have the ability to create initial exchange offerings (IEO)s. Due to their ease of creation, and users inability to determine if projects are real, creates many risks. One risk is the ICO/IEO/STO founders have many tokens and can use them to pump and dump a platform's market. Another risk is ICO/IEO/STO founders create a fake company and use their worthless cryptocurrency to purchase other cryptocurrency or fiat.
    - Potential Solution: On regulated platforms only allow approved cryptocurrencies. An "approved cryptocurrency" could be different depending on: if the cryptocurrency is centralized or decentralized, that cryptocurrencies consensus mechanism, and likelihood that the founders (if the cryptocurrency was centralized) are creating a real product.

- Problem: An exchange could be initiating trades between itself to create transaction volume on that exchange.
    - Potential Solution: Internal controls must be in place and used, users of the exchange must be verified, and parties related to the exchange must be identified.

- Problem: Exchanges keep user data on site, and may not have appropriate safeguards to secure that information (Driver licences, utility bills, etc.)
    - Potential Solution: Using a service like Verified.Me to confirm a user rather than sending sensitive information to an entity that might not have proper security in place to store user data.

- Problem: Some cryptocurrencies are susceptible to a 51% attack. That is why most cryptocurrency exchanges have a minimum confirmation height for a deposited cryptocurrency before it can be traded on that exchange.
    - Potential Solution: Before a cryptocurrency is accepted for trading on an exchange there should be a minimum amount of confirmations. The amount of confirmations for each cryptocurrency should be different, and based on a type of economic model (i.e. if the cost of a 51% attack is $1 million dollars based on the amount of confirmations needed, network hashing power and current price, then total deposits over x amount being confirmed by the exchange should take longer so that an attack

would be more costly than the benefit that would be received from the attack.). The amount of confirmations needed for each cryptocurrency should be dynamic and conservative.

- Problem: Banks submit suspicious transaction reports to FINTRAC for fiat transactions; however, there is no reports submitted for suspicious cryptocurrency transactions. This has the potential for people in illicit activities to wash their money through a platform.
    - Proper regulation and infrastructure needs to be in place to deal with these types of transactions, but a potential short-term solution could be to:
        - #1 – Only allow current transactions to the platform where the 2nd prior transaction is more than a day old, and transactions where the 2nd prior transaction is less than a day old to not accept the transaction to the platform. This will prevent individuals from creating multiple addresses in order hide the source of the cryptocurrency right before they post the transaction to the exchange. Some exceptions that could shorten this time could be "when received from an approved exchange that is follow these regulations" also some things that could increase the time might be "When crypto assets were involved in a mixing service or atomic swap".
        - #2 – Also have a reporting page where investors can indicate crypto assets have been stolen or were involved in a fraud. This will be tricky to manage as people could use this site to mess around with legitimate crypto assets. Therefore, the identity of the individual would need to be known, proof of ownership (can be proved by signing addresses where incident happened from), and a report of what happened.

- Problem: To my knowledge bank accounts involved in cryptocurrency activities cannot be opened in Canada, and owners of exchanges open bank accounts in other countries to get around this problem. This causes many issues, as an exchange in Canada that has Canadian assets do not hold those assets in Canada.
    - Potential Solution: Provide a way for platforms to hold funds in Canada

- Problem: As mentioned there are no suspicious transaction reports for cryptocurrencies, and the source of an asset is just as important when talking about fiat as it is when talking about cryptocurrencies.

  For example, if someone received fiat for human trafficking, we would want to treat cryptocurrency received for human trafficking in the same way. This is a direct causality (i.e. proceeds of human trafficking = cryptocurrencies).

However, we also need to think of indirect causality when discussing this topic (i.e proceeds of human trafficking were used to create a cryptocurrency mining facility, and this mining facility produces newly minted cryptocurrencies).

  - Potential solution: Source of cryptocurrencies would need to be provided and could potentially be audited. So there would need to be some potential regulations around this auditing process.

- Problem: Retailers may accept cryptocurrencies for goods and services, but allow cryptocurrencies from illicit services. The retailer might then try to sell the cryptocurrencies on the platform and the platform rejects the transaction.

  - Potential solution: If a retailer uses a cryptocurrency payment processor that payment processer could be responsible to have KYT, and reject cryptocurrency from an illicit source.

Many of the above problems echo the report "Why We Fail to Catch Money Launderers 99.9 percent of the Time" released on May 7, 2019: https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/Final%20for%20release%20e-brief_291_web%20%28003%29.pdf

3. Are there any global approaches to regulating Platforms that are 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.

Some applicable standards to consider, are those of the Cryptocurrency Certification Consortium: https://cryptoconsortium.org located at: https://cryptoconsortium.github.io/CCSS/ (Full disclosure I have my CBP from this body).

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' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

To determine the minimum amount of cryptocurrency an exchange controls, and the amount of liability the exchange has from holding its customers cryptocurrencies a Proof-of-Reserve may be performed. Auditors preforming normal audit testing with proof-of-reserve testing could provide assurance. Proof-of-reserve only works from an assurance standpoint if all cryptocurrencies offered by an exchange are reviewed at the same point in time. More information on proof-of-reserve can be found at:

a. https://www.lopp.net/pdf/princeton_bitcoin_book.pdf "Bitcoin and Cryptocurrency Technologies" Pages 115 to 118
b. https://www.kraken.com/proof-of-reserves-audit

6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet?

The question depends of the services the platform provides. If a platform only offers crypto to crypto trading there is no challenge in structuring an exchange to allow an investor to send crypto from their wallet to receive another type of crypto directly to that investor's wallet. However, for crypto to fiat transactions this does pose challenges as a centralized party is needed to store and distribute the fiat of the investors.

What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?

1. There is the benefit of convenience in allowing an investor to store their assets on a platform. If the investor did not want to store their cryptocurrencies on an exchange, they would need to create an address for that particular cryptocurrency, and then need to safe guard it (i.e. create a backup of the private key/seed, and physically secure it against thief).
2. If the assets are kept on a platform the investor can react quicker to market changes.
3. History has shown that storing cryptocurrencies on a platform is less safe than an individual personally holding their cryptocurrencies.

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?

<No Comment>

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?

<No Comment>

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

<No Comment>

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?

In addition to know your customer (KYC), there is surveillance software that allows for know your transaction (KYT). KYT can allow exchanges to reject cryptocurrency from address or known illicit activities or frauds.

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?

At this time not all cryptocurrencies have surveillance software. This creates a risk of not being able to track some cryptocurrencies.

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.

<No Comment>

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

<No Comment>

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?

<No Comment>

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

<No Comment>

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 that are equivalent to insurance coverage?

<No Comment>

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 could be mitigated.

<No Comment>

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

<No Comment>

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 the rationale.

<No Comment>