ISACA
China Hong Kong Chapter

Securities and Futures Commission
54/F, One Island East
18 Westlands Road, Quarry Bay
Hong Kong

22 March 2023

Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators licensed by the Securities and Futures Commission

ISACA Hong Kong Chapter would like to provide our comments to the "Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators" (the Consultation Paper). The Consultation Paper outlined ten specific questions, and our comments focus on the three specific questions that concern the risk and control of technologies relevant to operators of virtual asset trading platforms.

If there are specific areas that you wish to seek further clarification, please let us know and we would be delighted to discuss with you.

Submission by ISACA China HK Chapter

Question 3: What other requirements do you think should be implemented from an investor protection perspective if the SFC is minded to allow retail access to licensed VA trading platforms?

Part III of the Consultation Paper sets out the due diligence that need to be performed by Virtual Asset Trading Platform (VATP) Operators:

> *a) A licensed platform operator should ensure that its own **internal controls**, systems, technology and infrastructure could support and manage any risk specific to that virtual asset.*
>
> *b) The licensed platform operator is expected to conduct a **smart contract audit** for virtual assets based on blockchains with a smart contract layer unless the platform operator demonstrates that it would be reasonable to rely on a smart contract audit conducted by an independent auditor. The audit should focus on reviewing whether the smart contract layer I s subject to any security flaws or vulnerabilities. (paragraphs 48a and 48b of the Consultation Paper)*

ISACA's comments & recommendations

It is important to note that as of this point in time, there are no standards or baseline criteria in relation to virtual asset related audit. Individual audit firms would adapt and extend existing auditing and technology governance standards, such as COBIT, to address specific circumstances of the entity to be audited.

Information Systems Audit and Control Association China Hong Kong Chapter Limited
Address: Room 2001, 20/F, Wellborne Commercial Centre, 8 Java Road. North Point, Hong Kong
Tel: (852) 2528 3772
Fax: (852) 2520 0069
Email: info@isaca.org.hk
http://www.isaca.org.hk

ISACA
China Hong Kong Chapter

With this new licensing regime, and given there is no precedent for auditing VSTPs, it is important for the SFC to collaborate with the audit profession, specifically the AFRC and the HKICPA, to develop more specific guidance to support future audits in related areas, such as in relation to the expected internal control framework for VATPs; technical audit approach/considerations specific to VASPs; smart contract audit approach and related criteria/standards, etc.

The SFC may be aware of controversies surrounding "proof-of-reserves" where "AUPs (Agreed Upon Procedures)" were referred to as "Audits", and questions raised by the community eventually led to the firm that performed such work having to withdraw their published reports and suspended their work with crypto companies on proofs-of-reserves reports. This clearly illustrates the need for objective standards and guidance to avoid any misunderstanding.

In additional to considering the technical aspects of tokens to be admitted for trading, VATPs should also ensure related technological components are safe, particularly with respect to any digital wallets supported or provided by VATPs.

Question 6: Do you have any suggestions for technical solutions which could effectively mitigate risks associated with the custody of client virtual assets, particularly in hot storage?

> *"Further, as access to a virtual asset is effected by the usage of a private key, custody of virtual assets primarily concerns the safe management of the private keys. A platform operator should establish and implement written internal policies and governance procedures for private key management to ensure all cryptographic seeds and keys are securely generated, stored and backed up." (paragraph 19a of the Consultation Paper)*

ISACA's comments & recommendations

The security and control of virtual asset rests with the "safe management of the private keys". This is similar to safeguarding the passwords for ATM, e-banking, and credit card transactions in traditional banking services.

It is important to point out that cryptographic key management plays a crucial role in the secure operation of crypto asset and blockchain technology. Following the "same business, same risks, same rules" principle, the SFC may consider adopting the security recommendations from Payment Card Industry Security Standards Council (PCI SSC, https://www.pcisecuritystandards.org/about_us/) and HKMA on Distributed Ledger Technology (https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/20171024e1.pdf, and https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/20171025e1a1.pdf), where Hardware Security Modules (HSM) are explicitly mentioned. According to the HKMA Whitepaper "...an HSM is a technology solution for safeguarding and managing digital keys".

A sustainable cryptographic operation will rely on sound key management as well as the robustness of the underlying algorithms. In light of the advancement of quantum computing, the SFC should also take heed of the "The Quantum Computing Threat: Risks and Responses" (https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-34/the-quantum-computing-threat-risks-and-responses). The SFC may consider requiring VATPs to address

Information Systems Audit and Control Association China Hong Kong Chapter Limited
Address: Room 2001, 20/F, Wellborne Commercial Centre, 8 Java Road, North Point, Hong Kong
Tel: (852) 2528 3772
Fax: (852) 2520 0069
Email: info@isaca.org.hk
http://www.isaca.org.hk

ISACA
China Hong Kong Chapter

"quantum-resistant" and "crypto-agility" in the design of their cryptographic solutions, so as to ensure the Quantum Threat is adequately addressed.

Question 8: Do you have any comments on how to enhance the other requirements in the VATP Terms and Conditions when they are incorporated into the VATP Guidelines?

ISACA's comments & recommendations

An important consideration is investor education; VATPs should have the obligation to educate investors on security considerations in connection with key and wallet management, much in the same way as banks remind customer on cyber security risks.
Further, notwithstanding the requirement for VATPs to disclose potential conflicts of interest regarding employees' dealings, one additional consideration is for VATPs to disclose their interest in virtual asset projects, particularly in connection with the virtual assets (tokens) they admit.

Other Consideration
The Consultation Paper outlined the general principles that VATPs should follow in their selection of auditors.

> *Accounting and auditing: A platform operator is required to exercise due skill, care and diligence in selecting auditors, and consider their* ***experience, track record and capability*** *in auditing virtual asset related businesses and platform operators. Further, a platform operator should submit an auditor's report in each financial year which contains a* ***statement on whether applicable regulatory requirements have been contravened.*** *(paragraph 19d of the Consultation Paper)*

ISACA's comments & recommendations

The Virtual Assets industry is relatively new to Hong Kong, and few audit firms have the requisite experience, track record and capability. It is therefore important for the SFC to clearly specify the desired/required capability that the auditor should demonstrate to be qualified to provide audit services to VATPs. This capability framework would also serve as a reference for the training and skilling-up of audit professionals.

About ISACA
ISACA® (www.isaca.org) is a global professional association and learning organization that leverages the expertise of its more than 165,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. The ISACA China Hong Kong Chapter is entering its 40th anniversary this year serving both the community and our members.

ISACA China Hong Kong Chapter

Information Systems Audit and Control Association China Hong Kong Chapter Limited
Address: Room 2001, 20/F, Wellborne Commercial Centre, 8 Java Road, North Point, Hong Kong
Tel: (852) 2528 3772
Fax: (852) 2520 0069
Email: info@isaca.org.hk
http://www.isaca.org.hk