Oversight on recognised market operators

Given that recognised markets are non-intermediated markets that onboard investor-clients directly, the SC's role is to supervise the recognised market operator's (RMO) compliance with among others, the *Guidelines on Recognized Markets* (RMO Guidelines), *Guidelines on Prevention of Money Laundering and Terrorism Financing for Capital Market Intermediaries* and *Guidelines on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing for Capital Market Intermediaries* (TFS-PS Guidelines). In addition, RMOs are also expected to monitor and mitigate cyber security and IT infrastructure risks in compliance with the *Guidelines on Management of Cyber Risks* (Cyber Risk Guidelines).

For information on the Thematic Regulatory Assessment on Digital Asset Exchanges, please refer to Figure 4.

FIGURE 4

THEMATIC REGULATORY ASSESSMENT ON DIGITAL ASSET EXCHANGES

BACKGROUND

The SC adopts a risk-based approach to the oversight of RMOs. Given the risks associated with digital asset, money laundering, terrorism and proliferation financing as well as risks of cyber security threats and systems disruptions, the SC completed the thematic regulatory assessment on three digital asset exchanges (DAX) in August 2021. It is imperative for DAXs to ensure that relevant processes, procedures, practices, and systems are in place to drive a well-functioning market infrastructure for the integrity and reputation of the Malaysian capital market.

OBSERVATIONS

Generally, RMOs have an adequate understanding of their Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) risk and technology and cyber risk obligations prescribed under the various SC Guidelines and are broadly compliant with the obligations stipulated in the Guidelines.

AREAS OF IMPROVEMENT

The following key areas have been identified, among others, for further enhancements:

- Board and senior management are required to assume greater accountability on anti-money laundering (AML) policies and procedures, technology systems management as well as to ensure consistency of practice with the policies and procedures that are in place
- Strengthen documentation and record-keeping to improve the effectiveness of compliance functions
- Ensure adequate access controls in the database and digital asset wallets