Sound risk management practices for algorithmic trading

The HKMA undertook a round of thematic examinations focused on algorithmic trading (algo-trading) in 2019. This note sets out the HKMA's expectations on AIs' risk management for algo-trading activities, including some sound practices adopted by the more advanced institutions as observed by the HKMA in the thematic examinations.

Governance and oversight

1. <u>Proper governance and risk management frameworks</u> – AIs should put in place proper governance and risk management frameworks for overseeing and managing the risks associated with algo-trading activities and ensuring that these risks are within their risk appetite.

   The more advanced institutions have established dedicated governance bodies comprising representatives from all the major functions involved in algo-trading (e.g. front office, control function, finance, information technology and operations). These governance bodies are provided with sufficient information including management information and other reports (e.g. incident reports) to facilitate their oversight of the institutions' algo-trading activities.

   Senior management, risk and compliance functions of the more advanced institutions receive adequate training on a regular basis to get acquainted with algo-trading and the risks involved so that they are able to raise sensible challenges throughout the development, testing and implementation of the algorithms. In addition, given the specific nature of algo-trading, these institutions have set out clearly the respective roles and responsibilities of the first, second and third line of defence related to their algo-trading activities. In cases where the underlying algorithms or systems are adopted from their headquarters,

these institutions' local management do not place undue reliance on their headquarters' oversight but are actively involved in managing the risks associated with their algo-trading activities through, for instance, local governance bodies which mirror the setup at the group level. They also have sufficient representation in the algo-trading governance bodies at the group level to directly participate in the discussion and deliberation on relevant risk management and implementation issues and provide inputs from a local perspective.

2. <u>Effective and independent control function</u> – AIs should establish or assign a control function, which acts as the second line of defence independent of the front office, to manage the risks associated with algo-trading activities.

    For the more advanced institutions, the control function plays a proactive role in the key processes throughout the life cycle of the algorithms, including development, testing and approval of algorithms, design and implementation of pre-trade and post-trade controls and kill functionality, handling of incidents and regular reviews of algorithms and relevant controls. The control function is staffed with algo-trading experts who are given sufficient authority to challenge the front office and equipped with the tools needed to properly discharge their duties (e.g. system access for activating the kill switch to suspend algo-trading if warranted).

3. <u>Regular reviews of algorithms and relevant governance and controls</u> – AIs' first and second line of defence should conduct regular reviews (at least once a year) to evaluate the performance of the algorithms implemented, and whether the relevant governance, systems and controls, and business continuity planning remain adequate and effective.

    For the more advanced institutions, these reviews cover all the key processes throughout the life cycle of the algorithms and are guided by the governance bodies overseeing algo-trading activities. The results of the reviews are extensively discussed by the governance bodies and the discussions provide a

basis for formulating appropriate actions to strengthen the risk management for algo-trading. Where relevant, the review results are reported to these institutions' headquarters not only for attention but also for necessary actions to be taken at the group level.

4. <u>Regular internal audit reviews</u> – AIs' internal audit function, being the third line of defence, should perform regular reviews of algo-trading activities to ensure that these activities are subject to proper governance and the risks arising from these activities are adequately and effectively managed.

For the more advanced institutions, algo-trading is treated as a separate business area from general treasury activities in their regular audit programme and a tailor-made scope of review is developed to cater for the specific risks associated with algo-trading. The internal audit staff of these institutions possess sufficient knowledge on algo-trading and are capable of performing their reviews effectively.

Development, testing and approval

5. <u>Effective framework governing development and testing of algorithms</u> – AIs should establish an effective framework governing the development and testing of algorithms to ensure they behave as intended, and comply with the relevant regulatory requirements and the institutions' internal policies. AIs' staff responsible for developing and testing the algorithms should possess the requisite expertise and experience.

For the more advanced institutions, the robustness and resilience of algorithms and the relevant monitoring and controls are tested to ensure that they will work effectively under stressed market conditions and will not disrupt market functioning at any time. If any changes are to be made to an algorithm currently in use, these institutions would not merely test the changes in isolation. They would perform comprehensive tests on the updated algorithm as if it were a new algorithm. Some of the more advanced institutions also appoint an individual as a

project leader to oversee the entire development and testing processes to ensure that the processes are well coordinated and performed in a consistent manner across different algorithms.

6. <u>Robust algorithm approval policy and procedures</u> – AIs should put in place robust approval policy and procedures to ensure that new algorithms or changes to the algorithms currently in use are subject to proper testing, reviews and challenges before they are implemented. Some institutions' trading systems have algo-trading functionalities which are not activated at the inception of those systems. For these cases, AIs should ensure that the algo-trading functionalities are subject to a proper approval process before activation.

    For the more advanced institutions, standardised approval templates are used to ensure that sufficient information is consistently provided to staff assigned with the approval authority to facilitate effective evaluation of new algorithms or changes to the algorithms currently in use. Where appropriate, these institutions would take extra steps during the approval process to ensure the evaluations are adequate, such as additional expert reviews to assess the appropriateness of complex algorithms.

Risk monitoring and controls

7. <u>Comprehensive and prudent pre-trade controls</u> – AIs should have in place a comprehensive set of pre-trade controls for algo-trading activities to ensure risks are managed prudently. Examples of pre-trade controls include risk limits based on the institution's capital, trading strategy and risk tolerance; price collars which block orders that do not satisfy pre-defined price parameters; checking of repeated and rejected orders; and limits on maximum order value or volume to prevent uncommonly large orders from entering the order book.

    For the more advanced institutions, the pre-trade controls are more granular (e.g. control limits vary by client and by trading strategy) and are reviewed regularly to

take account of the latest market conditions. In establishing and reviewing the pre-trade controls, these institutions perform detailed analyses to ensure that the controls are prudent and in line with their risk appetite.

8. <u>Robust post-trade controls</u> – AIs' front office and independent control function should conduct real-time monitoring of algo-trading activities. The relevant systems should have the capability of providing real-time alerts to assist staff in identifying limit excesses, activation of kill functionality and other abnormal trading activities (e.g. trading continues after the kill functionality is activated). Automated surveillance tools should be in place to detect suspicious activities and possible conduct issues (e.g. signs of potential market manipulation).

   The more advanced institutions have established alerts that are more stringent than the control limits (e.g. 80% of the respective control limits) to provide early warning signals. These institutions have a dedicated team for monitoring algo-trading activities and production of structured management information reports on these activities for review by the relevant governance bodies and senior management.

9. <u>Proper kill functionality to suspend trading</u> – AIs should put in place a proper kill functionality as an emergency measure to suspend the use of an algorithm and cancel part or all of the unexecuted orders immediately in case of need. There should be a robust framework governing the activation of the kill functionality and the subsequent re-enablement of algo-trading.

   The kill functionality of the more advanced institutions can be activated at various levels (e.g. at the system, algorithm, trader and client level). This can minimise the disruptions to other algo-trading activities which are not related to the underlying reasons for activating the kill functionality. For a kill functionality which requires manual activation (commonly referred to as a "kill switch"), these institutions provide detailed guidance to the relevant staff on the circumstances under which the switches should be activated. For a kill functionality which is

activated automatically based on predefined triggers (commonly referred to as a "circuit breaker"), these institutions review these triggers regularly to ensure they remain appropriate.

10. Effective business continuity arrangements – AIs should establish a robust business continuity plan to set out contingency measures for dealing with possible adverse scenarios where algo-trading systems cannot function normally due to, for instance, a break-up in data feed to these systems or other forms of system malfunctioning. These contingency measures should include fall-back solutions (e.g. alternative arrangements to execute orders) and should be subject to regular testing to ensure they are effective and staff are familiar with the business continuity plan.

For the more advanced institutions, tailor-made business continuity plan covering a wide range of scenarios is developed for each major type of algorithms having regard to the purposes of the algorithms (e.g. making investment decisions, executing trade orders and market-making), and the markets and products to which the algorithms are applied.

11. Adequate controls on access rights – AIs should put in place proper security controls on the physical and electronic access to algo-trading systems to ensure that only authorised staff are given access to these systems. These security controls should include the use of reliable techniques to authenticate the identity of staff and application of differentiated access controls according to the staff's responsibility and authority. Staff departure or transfer resulting in changes in responsibility and authority should be timely reflected in these security controls. Staff's access records and activity logs should be subject to regular reviews to identify any unauthorised access to or improper use of the systems.

The more advanced institutions have established a dedicated policy governing the access controls for algo-trading systems, specifying the rights of access that should be given to the relevant staff at different stages of life cycle of algorithms,

including development, testing, migration from testing to the production environment and implementation.

12. Robust incident-handling policy and procedures – AIs should establish robust policy and procedures for handling incidents related to algo-trading. Any such incidents and the associated remedial actions should be properly escalated. Sufficient information should be provided to the governance bodies and other responsible staff to facilitate their review of the incidents and the adequacy and effectiveness of the remedial actions. Remedial actions should be implemented timely with proper audit trails.

For the more advanced institutions, incidents related to algo-trading are investigated thoroughly and the results of the investigation are extensively discussed by the governance bodies. In the light of the nature and root causes of the incidents, these institutions may initiate a holistic review of all relevant algorithms and the associated controls to avoid reoccurrence of similar incidents in other algorithms.

Documentation

13. Proper documentation for audit trials – AIs should maintain proper documentation to provide sufficient audit trails on the key processes throughout the life cycle of algorithms.

For the more advanced institutions, clear documentation standards and templates have been developed for the development, testing and approval processes, design and implementation of pre-trade and post trade controls, handling of incidents, and regular reviews of the performance of algorithms and effectiveness of the relevant risk controls. These institutions store the documentation in a centralised database which is accessible only to authorised personnel.

14. Comprehensive inventory of algorithms – AIs should establish and maintain a

comprehensive inventory to document all the algorithms implemented and the relevant key information, such as a brief description of the algorithms and the trading strategies involved, owner, approver and approval date, implementation date, names of systems where the algorithms are implemented, scope of application (e.g. market and product type), review records and the applicable risk controls.

The more advanced institutions maintain two inventories, one for the algorithms implemented and another for the applicable risk controls. This allows all the key information on the risk controls to be included in the dedicated inventory and facilitates the identification of any inconsistencies in the risk controls across the implemented algorithms.