

SENIOR SUPERVISORS GROUP

Algorithmic Trading Briefing Note

April 2015



BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY



OSFI
BSIF



BANCO DE ESPAÑA
Eurosystem

TABLE OF CONTENTS

I. INTRODUCTION AND MARKET EVOLUTION 1

II. KEY RISKS.....2

III. KEY CONTROL PRINCIPLES AND SOUND PRACTICES.....3

IV. NEXT STEPS: QUESTIONS FOR FIRMS AND SUPERVISORS4

V. CONCLUSION6

EXECUTIVE SUMMARY

High-frequency trading (“HFT”), or high-speed trading¹ (“HST”), a type of algorithmic (or “algo”) trading, is now a well-known feature of the global market landscape. In many markets, a small number of firms may account for a large proportion of trading volume. Although it has been argued that HFT has lowered investors’ trading costs by reducing bid-ask spreads, the risk that HFT activity specifically, and algorithmic trading more generally, poses to firms and the financial markets has sparked debate and raised concern among market participants and regulatory agencies globally. This is, in part, owing to the speed of trading and, therefore, the pace at which exposures may accumulate intraday at financial institutions. Indeed, unexpected events linked to algorithmic and high-frequency trading have caused significant volatility and market disruption, leading to heightened debate around the risks these activities pose to the functioning of global markets. The complexity of market interactions among HFT firms and other market participants increases the potential for systemic risk to propagate across venues and asset classes over very short periods of time.

This briefing note focuses on how risks associated with algorithmic trading are monitored and controlled at large financial institutions during the trading day. While market structure and trading rules differ by jurisdiction and asset class, we seek to identify risks common to algorithmic trading and to suggest questions that supervisors might

¹ For purposes of this paper, the terms “high-speed trading” and “high-frequency trading” refer to automated trading conducted at millisecond or microsecond speeds throughout the trading day.

The Senior Supervisors Group (SSG) is composed of the staff of supervisory agencies from ten countries and the European Union: the Canadian Office of the Superintendent of Financial Institutions, the European Central Bank Banking Supervision, the French Prudential Control and Resolution Authority, the German Federal Financial Supervisory Authority, the Bank of Italy, the Japanese Financial Services Agency, the Netherlands Bank, the Bank of Spain, the Swiss Financial Market Supervisory Authority, the United Kingdom’s Prudential Regulatory Authority, and, in the United States, the Office of the Comptroller of the Currency, the Securities and Exchange Commission, and the Federal Reserve.

The SSG acknowledges the important contributions of Caleb Roepe, George Wyville, and Stephanie Losi to this briefing note.

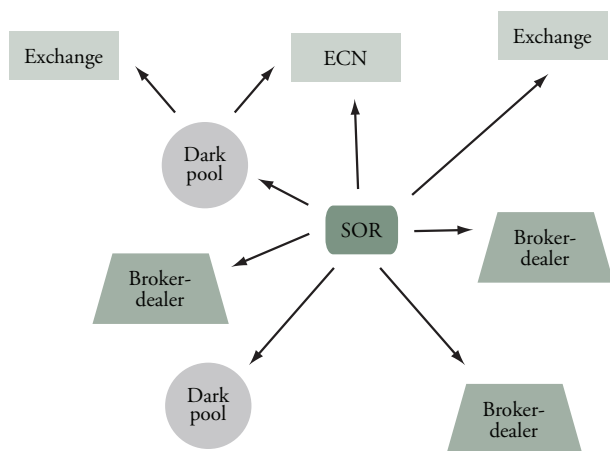
consider as they monitor or examine this activity. Further, by setting forth risk-based principles and questions that firms already engaged in algorithmic trading can use to assess their controls over this activity, we aim to facilitate an informed conversation about sound risk management practices and renew market participants’ focus on improving risk management of this activity.

Key supervisory concerns center on whether the risks associated with algorithmic trading have outpaced control improvements. The extent to which algorithmic trading activity, including HFT, is adequately captured in banks’ risk management frameworks, and whether standard risk management tools are effective for monitoring the risks associated with this activity, are areas of inquiry that all supervisors need to explore. Further, algorithmic trading activity has expanded beyond the U.S. equity markets to other markets and asset classes, including futures, foreign exchange, and fixed-income markets. Thus, our supervisory approach needs to remain flexible and adaptable to address growth and evolution of this activity.

I. INTRODUCTION AND MARKET EVOLUTION

Algorithmic trading has grown and evolved in response to the many changes that have taken place in the market landscape since electronic communications networks (ECNs) became established in the late 1980s into the 1990s. Advancements in trading technology, along with regulatory developments, have played a role in fundamentally changing the structure of markets and the way that securities and derivatives are traded. HFT activity, for example, benefited from technology that reduced delay, or latency, to the markets. In addition, by co-locating their servers with market servers at an exchange or dark pool data center, algorithmic traders, including HFT firms, increased the speed at which they could access the markets. The decimalization of pricing helped in the advancement and development of certain forms of algorithmic trading, such as HFT. Meanwhile, alternative trading systems (ATS) and dark pools began to attract volume and grow market share. Changes in the market landscape, such as growth in the number of electronically traded markets, also played a role in the expansion of,

Model of U.S. Equity Market Structure



and investments in, algorithmic trading. The combination of these and other factors facilitated the overall growth in algorithmic trading; however, no single factor explains the growth and evolution of the different subsets of algorithmic trading.

What is quite clear, however, is that algorithmic trading is a pervasive feature of markets in many countries, each with its own regulatory structure. Often associated with the equities market, HFT, for example, spans asset classes and traded products across jurisdictions and trading venues. HFT in foreign exchange (“FX”) and rates markets, which have different regulatory controls than equities markets, has grown substantially over the past decade. Additionally, firms engaging in algorithmic trading activity have benefited from a fragmented market structure in at least one way—by arbitraging prices between different trading venues. Many traders’ roles also changed as algorithmic trading evolved and expanded. Instead of making order execution decisions based on valuation models or in the course of making a market or facilitating clients’ orders, traders now use trading strategies based on algorithms to arbitrage price differences across related products and trading venues and take advantage of liquidity, or lack thereof, in different markets. Traders can adjust an algorithm within certain boundaries (for example, tuning an algorithm to trade more or less aggressively), but actual orders are generated by the algorithm based on response to market signals. For instance, many banks employ algorithms designed to execute trades without significantly impacting market prices.

Although certain types of algorithmic trading may reduce perceived bid-ask spreads, algorithmic trading also increases operational risk at individual firms and across the financial system. For example, an algorithmic strategy may fail to maintain risk exposure within a specified threshold during volatile market conditions, or fail to return to an allowable risk position. An undetected failure with one market participant’s algorithmic trading strategy can increase, or further transmit, risk to another firm, or to the markets more generally. As algorithms and their interactions grow in both number and complexity, various types of algorithmic trading may increase systemic risk.

II. KEY RISKS

Risks associated with algorithmic trading, including HFT, have been covered extensively in numerous forums, such as the International Organization of Securities Commissions (IOSCO) consultative report² and market regulator roundtables³ and concept releases⁴. We will not repeat the discussion of the risks already covered in these reports and forums. Instead, we take the opportunity in this briefing note to lay out four risks commonly associated with algorithmic trading:

1. **Systemic risk may be amplified.** An error at a relatively small algorithmic trading firm may cascade throughout the market, resulting in a sizable impact on the financial markets through direct errors or the reactions of other algorithms to the error. Clearinghouses and central counterparties (CCPs) may also be affected by erroneous trades, though their degree of exposure to clearing members may be limited depending upon the product category involved and the nature of the events.⁵

² <http://www.iosco.org/library/pubdocs/pdf/IOSCOPD354.pdf>

³ <http://www.sec.gov/news/otherwebcasts/2012/ttr100212-transcript.pdf>

⁴ <http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/federalregister090913.pdf>

⁵ In addition to numerous procedural safeguards and financial resources designed to anticipate and absorb extreme but plausible exposures, clearinghouses and CCPs have in place, or are developing, safeguards specifically designed to control exposures that may arise as a result of erroneous trades.

2. **Algorithmic trading desks may face a significant amount of risk intraday without transparency and robust controls.** Proprietary and agency trading desks at financial institutions generally have risk reporting and risk controls in place to limit and control risk exposure acquired over the course of the trading day. However, at any institution, intraday risk controls may not be robust, reporting may not be complete or timely, or limit breaches may not be transparent to senior risk officers. As such, an unintended accumulation of a large position during the trading day may result in a firm taking on significant exposure before end-of-day risk processes take effect. Also, technology failures, exceptional or unanticipated market conditions, or an unexpected failure of an algorithm during the day could force a firm to carry significantly more risk overnight than it had intended, and without timely senior risk management oversight.
3. **Internal controls may not have kept pace with speed and market complexity.** Malfunctions and outages at financial institutions and critical entities such as exchanges are not new, but their potential impact can be amplified. Further, many banks' prime brokerage businesses have algorithmic and HFT firms as clients, and the risk controls and monitoring efforts across these businesses vary widely among banks and are evolving to keep pace with this type of client activity.
4. **Without adequate controls, losses can accumulate and spread rapidly.** Examples of rapid-impact events include the 2010 Flash Crash (a large-order execution algorithm operating in an unexpected way), the 2012 Facebook IPO (an exchange system problem), and the 2012 Knight Capital incident (the malfunction of an order routing system). As follow-ups to these events, published regulatory enforcement actions highlighted control shortcomings related to insufficient testing⁶, and new rules and recent proposals by market regulators have aimed to increase control strength.⁷

⁶ <http://www.sec.gov/litigation/admin/2013/34-69655.pdf> (NASDAQ Facebook IPO) and <http://www.sec.gov/litigation/admin/2013/34-70694.pdf> (Knight Capital).

⁷ <http://www.sec.gov/rules/sro/nms/2012/34-67091.pdf> (Limit Up-Limit Down) and <https://www.sec.gov/rules/proposed/2013/34-69077.pdf> (proposed Regulation SCI).

III. KEY CONTROL PRINCIPLES AND SOUND PRACTICES

The following is a list of principles for supervisors to consider when assessing practices in and key controls over algorithmic trading activities, including HFT, at banks. These key controls and practices are both preventative and detective in nature, and are the underpinnings of an overall risk management framework.

Controls must keep pace with technological complexity and trading speeds. A multilayered “defense-in-depth” strategy, which increases control redundancy and diversity, can reduce the risk that an erroneous or destabilizing order will reach financial markets. Defense-in-depth is a concept from the information security field that calls for multiple controls at multiple points in a process. For example, algorithmic trading controls should exist prior to algorithm launch or change deployment, during the trade lifecycle, and during the incident response process. Firms need to have controls that cover all aspects of the trading process, including order generation, order handling, and order execution.

Governance and management oversight can limit exposure to losses and improve transparency. One sound practice is to establish firm-wide governance for algorithmic trading controls being aligned with the firm's stated risk appetite framework and apply it consistently within the firm. Without such consistently applied governance, differences in controls across desks can introduce unnecessary risk for a firm and can represent a lost opportunity to identify and implement best practices across all desks.

Testing needs to be conducted during all phases of a trading product's lifecycle, namely during development, rollout to production, and ongoing maintenance.

- Initial testing: Firms wishing to deploy a new or updated strategy or algorithm must first conduct simulations and non-live testing within a trading venue testing environment. Appropriate testing helps to ensure that algorithms pass the risk management controls required by the firm and the exchange.
- Controlled rollout: The algorithms should be rolled out in a controlled and cautious fashion. Initially, a firm should self-impose price and position limits as well as limits on the number of instruments and venues where the algorithm is deployed.

- Ongoing testing: Firms should test systems and controls to ensure that they can withstand significant or elevated market volumes and external events that could exert stress on those systems and controls.

When assessing control depth and suitability, management should ensure sufficient involvement of control functions (such as Compliance, Technology, Operations, Legal, Controllers, and Market Risk) as well as business-unit management. All stakeholders should have a voice at the table in determining the right balance between risk and controls. Control functions and developers both need to understand the inherent risks that algorithmic trading poses to ensure that the proper controls are in place. Defense-in-depth also gains strength when different layers within a firm play a role.

IV. NEXT STEPS: QUESTIONS FOR FIRMS AND SUPERVISORS

In this briefing note, we address three specific oversight levels: business unit or desk management; control functions and senior management; and the board. For each level, we present questions that supervised firms can use to self-assess their current control state and risk appetite. As a corollary, supervisors also may consider asking firms these or similar questions.

Business-Unit/Desk-Management Level

What degree of role overlap is permitted among traders, strategists, and developers?

Situations in which front-office traders, strategists, and developers lack clearly defined role boundaries can result in insufficient oversight and create conflicts of interest. Management should consider the risks of allowing traders to develop their own algorithms; of allowing developers to test their own code; and/or of allowing developers to deploy their own code into production. All of these situations run counter to separation-of-duties principles and may increase the likelihood of errors. Fast-paced, iterative development environments require heightened controls.

Does the unit adhere to firm-wide policies and processes?

If front-office trading desks develop their own processes such as change management rather than following

firm-wide processes, risk may exceed the level intended by senior management and the board. Therefore, independent risk management functions should review and approve any changes and should inform senior management and/or the board of these exceptions. Moreover, independent risk management should revisit desk-specific procedures periodically.

Does the unit seek advice from independent control functions to ensure that compensating controls are effective and functioning as intended?

If resource or personnel constraints prevent a trading desk from implementing optimal controls, the likelihood of generating erroneous or destabilizing orders increases. The business unit should establish compensating controls to mitigate both firm-specific and systemic risk. Independent control functions at the firm should verify, approve, and periodically reassess the adequacy of these compensating controls.

What types of risk reports does the unit produce, and who in the firm receives those reports?

If business units do not provide transparency about risk taken intraday, senior management and the board may remain unaware of the business's full risk profile. To provide transparency, trading desk management should develop appropriate reports (for example, intraday profit and loss) for independent risk management and/or senior management and the board.

Control-Function and Senior-Management Level

Does an independent risk management function communicate with senior management about the level of intraday risk taken by each desk at the firm? Can independent risk management effectively challenge the front office if they identify excess risk?

In line with the recommendation that desk management should develop appropriate risk reports, independent risk management should review those reports and ensure that senior management is aware of the level of intraday risk taken across the firm. In addition, independent risk functions should be robust enough to develop their own key risk indicator reports and provide them to a chief risk officer, risk committees, or similar management governance bodies. If risk managers feel that the exposure created by certain business activities or transactions is too great given the firm's risk appetite, they should have the power to delay or decline activity pending senior management briefing

and consideration. In particular, senior management must have an understanding of how rapidly positions can accumulate intraday. Independent risk management and/or senior management also should engage with and challenge business units as needed to ensure that intraday risk exposure remains within acceptable limits.

Are control-related functions such as Technology, Operations Management, and Compliance aware of the controls in place on trading desks, and do they view those controls as sufficient? Do they have the ability to mandate stronger controls if they perceive gaps or weaknesses?

If control functions have only limited input or insight into front-office controls, firms may miss opportunities to align with industry best practices. They may, furthermore, face losses or liability if a control gap allows an erroneous or destabilizing order to reach financial markets. Robust involvement in the control-setting process by control functions can foster productive discussion about the optimal balance of control strength and innovation pace, resulting in a stronger, more resilient overall business. Furthermore, control functions are key secondary and tertiary lines of defense for firms. Their own control frameworks can be important supplements and complements to those of the front office.

Who receives reports on major incidents and/or losses? Is senior management aware of glitches and incidents? How does the firm communicate lessons learned from any incidents and/or losses?

Near-misses that are not reported represent lost opportunities to strengthen controls broadly across a firm. By reporting near-misses through firm-wide incident management systems, even when no financial loss has occurred, firms gain the opportunity to mitigate control weaknesses before those weaknesses cause harm to the firm or to financial markets. Firms should effectively communicate any lessons learned to the entire organization so that controls can be upgraded across trading desks and so that senior management can be sure that trading activity does not result in undue risk to the firm or the financial system.

Does senior management understand how incident responses are affected by exceptional circumstances (such as busting trades) that differ among trading venues and clearing/settlement firms?

In a market-wide incident, best-case scenarios tend to occur when trading venues, market participants, and

clearing/settlement firms have clear rules and procedures that enable them to respond rapidly and effectively to events.⁸ Different trading venues and clearing/settlement firms have different rules and procedures for exceptional circumstances, such as for busting trades or halting trading. A financial institution's risk exposure under these exceptional circumstances can be significant. To manage exceptional circumstances and assess and manage risk rapidly and effectively, senior management must understand in advance how exceptional circumstances, such as busting trades, are handled at each trading venue and the impact on the firm's risk position.

Are incident response processes up-to-date, effective, and communicated to senior management?

Markets, market participants, and clearing entities should regularly review their risk management and operational risk policies and procedures to ensure that they reflect the latest best practices and to keep response teams current and coordinated within the firm's risk management framework. All parties should be aware of their responsibilities and have established procedures (that are tested regularly) for coordinating with markets and clearing agencies in responding to market incidents. All incident responses must integrate well with market-wide rules and protocols so that events and risks are managed in a timely, effective manner.

Are control functions prepared to execute trading incident response processes?

Control functions such as Compliance and Internal Audit risk uncoordinated responses to trading incidents if advance preparation is insufficient. Appropriate, comprehensive, timely, and coordinated incident reporting and response procedures are required. "Break glass"⁹ and other similar procedures for worst-case scenarios must be documented and tested. Procedures for responding to erroneous trade executions differ by venue and should be understood at all levels of the firm.

⁸ Regulators have imposed rules and procedures on markets, clearing agencies, and individual firms to mitigate the risk of, and implement coordinated responses to, trading events, such as single stock price swings, or market-wide volatility. Furthermore, the Securities and Exchange Commission's market access rule (Rule 15c3-5) requires broker-dealers to have risk management controls and supervisory procedures (especially credit and operational risk) with market access.

⁹ A break-glass procedure refers to an added layer of control over emergency or nonroutine action, which automatically notifies others as the process is triggered.

Board and Executive Level

Are the board and key management risk committees aware of the level of intraday risk taken across the firm?

If the board and executive-level risk committees are not informed of the level of risk taken intraday across the firm, risk may increase beyond the level intended by the board. Senior management should leverage information provided by desk-level management and independent risk management to communicate to executive risk committees and to the board the level of intraday risk taken firm-wide. This information can inform the board's oversight, discussion, and decisions on risk.

Are key governance bodies such as the board, audit committees, and control committees aware of the types of controls in use on trading desks, and does the board view those controls as sufficient?

Because trading incidents can have significant firm-specific and market-wide impact, boards of directors should have, at a minimum, high-level knowledge of the types and sufficiency of controls in use. Boards should request this information from senior management, and senior management should be able to collect the information across desks and present it to the board from a risk perspective. Other management committees, such as audit or control committees, can be additional resources to provide oversight of incidents and related follow-up activities occurring within the firm.

Does the board receive reports on significant near-misses and incidents?

Senior management should inform the board about near-misses and low-impact incidents that highlight critical control weaknesses. In doing so, management gives the board an opportunity to assess whether it is still comfortable with the firm's controls as well as its trading strategies and risk.

V. CONCLUSION

Firms and supervisors can assess control strength and identify areas for improvement through the application of traditional risk management principles, involving stakeholders from control functions as well as business management. This effort should ensure transparency into front-office trading activities for senior management and the board.

Market structure is evolving with the implementation of new rules and regulations. In the United States, the introduction of swaps execution facilities (SEFs) is moving over-the-counter derivatives onto exchanges through electronic platforms. Many view this as a growth opportunity for HFT firms. In the European Union, the amended Markets in Financial Instruments Directive (MiFID II) is introducing new regulation for algorithmic trading and traders. Cross-asset-class interconnections are becoming more significant as more markets become algorithmically traded, and both trading and compliance systems must handle increasing complexity. The effects of errors or attacks could amplify risk in highly interconnected markets.

While we have not addressed the question of permissibility in this note, firms, supervisors, and public authorities continue to weigh the costs versus benefits of different subsets of algorithmic trading. We encourage greater discussion in the near term given the scale of risks associated with this type of trading activity. The immediate need for stronger controls is paramount. While it is not possible to eliminate risk entirely, firms should strive to reduce risk by applying strong, layered controls. With senior management and boards aware of risks being taken at the desk level, risk-taking activity can be better monitored and controlled. Thus, transparency is imperative. By setting forth risk-based principles and questions for our supervised firms, we aim to facilitate thoughtful discussion and action.