Algorithmic trading – governance and controls

Project report

AFM - Public

Publication date: 02 April 2021

The Dutch Authority for the Financial Markets

The AFM is committed to promoting fair and transparent financial markets.

As an independent market conduct authority, we contribute to a sustainable financial system and prosperity in the Netherlands.

Contents

1. 2020 Algo-project

Context

In the last decade, the nature of trading has changed for the vast majority of transactions from point-and-click trading to automated trading via an algorithm. A great many of these trades are carried out at a high frequency, currently even within nanoseconds (a billionth of a second).

The high degree of automation (and for some firms also the high frequency at which trading takes place), makes it very important that both investment firms (IFs) and trading venues (TVs) have the right controls in place and sound procedures for the development and testing of algorithms and trading engines. Good governance should be embedded in all phases (development, pre-trade, real time monitoring, post-trade) of algorithmic trading to mitigate any operational risks and, if necessary, any incidents that may occur.

Incidents involving an algorithm may have and have already had a major impact on the confidence in and the efficient functioning of capital markets. A rogue algorithm, failure of platform controls, failure of emergency controls like the kill-functionality, unclear lines of communication, failure of real-time monitoring, concealed trading activities or a cyber-security incident are all real-life examples of controls not doing what they are designed to do: preventing market disruptions.

Since the 2010 flash crash, regulators have implemented and refined regulations aimed at preventing incidents and controlling algorithms. In the past few years, several regulators have looked into organisational controls of algorithmic trading implemented by firms, most notably the FCA in 2018, the Hong Kong Market Authority in 2019, and IOSCO in 2020. In addition, the amount of academic literature on the effects and risks of algorithms and the interplay between them, on capital markets and their structure, and the possible response on the part of regulators, has increased greatly.

The aim of the AFM's 2020 Algo-project is to help prevent a possible future market disruption originating from algorithmic trading. We therefore took the following steps: i) we assessed firms' compliance with regulations with regard to algorithmic trading and controls by analysing self-assessments, ii) we performed deep-dives at several firms and trading venues to gain a thorough understanding of these parties and their practices for controlling algorithms, as well as identifying and addressing any gaps in their practices, iii) we extrapolated findings that (may) apply to or may benefit the sector as a whole or help focus the sector's attention on the algo-controls and the AFM's expectations (this publication), and iv) we proposed improvements and addressed issues with the current legislation through the MiFID-review.

Project approach

For firms trading algorithmically, organisational requirements of controls, processes, procedures, and governance of investment firms which trade algorithmically are laid down in the Delegated

Regulation 2017/589 (RTS6). For trading venues which allow or accommodate algorithmic trading, these requirements are laid down in the Delegated Regulation 2017/584 (RTS7).

The approach taken by the AFM consisted of two phases: in phase I, a part of the annual self-assessments of these regulatory technical standards (RTS) at the proprietary trading firms and trading venues under its supervision were analysed.

In phase II, a deep dive was performed at a limited number of firms and trading venues. After analysing supporting documentation and evidence with regard to the set-up and actual embedment of processes, the analysis was performed based on an average of 5 interviews with the firms' experts on particular topics (grouping several RTS articles together): compliance, software development, platform controls, market abuse regulation, IT-security, testing, Member Due Diligence.

This analysis focused mainly on legal requirements of organisations with respect to algorithmic trading (controls, processes, governance, etc.) applying to both investment firms and trading venues. It should be noted that this research did *not* look into any short- or long-term risks and effects (different types of) algorithms have or may have on the markets.

Report

In this report, the AFM shares its findings and expectations with regard to different aspects of RTS6 and RTS7. This report will probably be of particular interest to compliance officers, risk departments, and persons in the business responsible for implementing and upholding processes and controls as per the RTS requirements.

Main findings and expectations

Expectations

In general: the scope of the areas covered by the RTS is broad, ranging from governance to development to testing, and from system resilience to IT security, but are all centred on the theme of algorithmic trading. The RTS requirements have been in force since 2018; the AFM expects investment firms and trading venues to have become familiar with the details of the RTS requirements and to have all of the necessary/required controls, processes, reviews and documentation as per these requirements in place so as to avoid market disruptions and market manipulation caused by algorithmic trading.

In addition to the AFM's expectation concerning the self-assessment method, the AFM expects investment firms engaging in algorithmic trading activities and trading venues that allow these activities to have this annual review embedded in a yearly review cycle. A firm's or venue's controls should be assessed in detail based on all applicable elements of the respective RTS, the self-assessment and validation report should be signed off on by senior management, and the firm or venue should take steps to address issues as needed.

Main findings

At the in-scope proprietary trading firms engaging in algorithmic trading activities, the AFM observed at a majority of firms a substantial improvement in the way the self-assessments are performed (both in terms of the structure and the level of detail provided in describing how a firm is compliant).

For the in-scope trading venues which allow algorithmic trading, there is considerable room for improvement when it comes to the annual RTS7 self-assessments: the AFM expects venues to follow the structure of the RTS and describe in detail the way in which the venue is compliant with the requirements of the RTS article.

In addition, the AFM wants to underline in particular that there is room for improvement at both firms and trading venues when it comes to the testing of (single) algorithms to determine their contribution to disorderly trading conditions. The AFM expects firms to properly test single algorithms/trading strategies to determine their possible impact on the capital markets (especially as regards their contribution to disorderly trading conditions) and for trading venues to i) have members certify that an algorithm has been properly tested in this regard and ii) offer a simulation environment to accommodate it.

In conclusion

The trend of trades done algorithmically is still upwards and as technology continues to progress algorithms may become more advanced. This has an impact on both the market (micro-)structure and on the nature of the (operational) risks. This project should be understood as part of a continuing effort on the part of the AFM in this area.

2. Structure of this report

The report starts with the findings of the project with respect to the select group of investment firms before presenting the findings and expectations for the trading venues. First, phase I findings and expectations will be described, followed by phase II findings and expectations. The report then follows the same structure for the findings and expectations as regards trading venues.

Investment firms

Phase I

The self-assessments received were analysed with regard to the following sub-topics:

1. Structure and degree of detail of the self-assessment
2. General organisational requirements
3. Compliance function
4. Security and limits to access

Phase II

Following the phase II deep-dive for investment firms, the AFM made several observations regarding the following sub-topics:

1. Governance and compliance – Articles 1, 2
2. Intra-group outsourcing – Article 4
3. Algo-development and testing – Articles 5, 7, 8, 11
4. MAR surveillance – Article 13
5. IT security – Article 18

The sections on each sub-topic begin with an observation and conclude with an expectation (if applicable).

Trading venues

Phase I

The project focused mainly on the structure and the self-assessments of the trading venues; findings and expectations on this topic are described.

Phase II

Following the phase II deep-dive for trading venues enabling or allowing algorithmic trading through their systems and for which Delegated Regulation (EU) 2017/584 (also known as RTS7) is applicable, the AFM had several observations regarding the following sub-topics:

1. Governance and compliance
2. Member due diligence
3. Testing
4. Platform controls
5. IT-security

The section on each sub-topic begins with an observation and concludes with an expectation (if applicable).

3. Sector findings – investment firms - phase I

3.1 Structure and level of detail of self-assessments

All firms followed the structure of the RTS6 articles in their self-assessments. Not all firms immediately provided substantial detail concerning the way in which they were compliant with the requirements of the articles.

1. The AFM expects firms to follow the structure of the RTS articles when assessing their own compliance
2. The AFM expects firms to describe in detail the way in which they are compliant with the requirements of the article.

3.2 General findings with respect to Article 1 General organisational requirements

Article 1 states that firms are required to have a governance framework in place for the development and deployment of and updates to trading algorithms which is proportionate to the nature, scale and complexity of its business. The AFM considers the requirements as laid down in Article 1 of key importance for mitigating the risk of algorithmic trading incidents occurring in financial markets.

In general, the self-assessments indicate that firms have increased the maturity of their organisation as regards the development, deployment and subsequent updates of trading algorithms compared to last year's assessments.

1. The AFM encourages firms to continue to clearly lay down an organisational structure for the development, deployment and subsequent updates of trading algorithms, thereby ensuring a sound segregation of tasks and responsibilities.
2. The AFM expects firms to continue to thoroughly assess how concealed unauthorised trading activity has been prevented.

3.3 General findings for Article 2 Role of the compliance function

Article 2 requires investment firms to ensure that the compliance function has an understanding of both the systems and single algorithms. The AFM wants to emphasise the importance of the level of knowledge and skills of the compliance staff and of continuous training in the algorithmic trading for key personnel, including the control functions.

The AFM has found that most firms' compliance staff have at least a general understanding of the algorithmic trading systems and a particular role in the algorithmic trading and development. The self-assessments further indicate that at most proprietary trading firms, compliance staff either have direct access to the kill functionality or are in contact with other staff who have access to it. Merely having a kill functionality is not enough to comply with this article.

The AFM expects firms to specify whether the compliance function or elements thereof are outsourced to a third party. In the case of an outsourced compliance function, the firm should evaluate how it can ensure that data privacy will be guaranteed and the compliance function can be audited.

3.4 General findings for Article 18 Security and limits to access

Article 18 requires investment firms to have the appropriate IT security and access limits in place that are in line with the risk strategy. Due to the increasing digitizationof the financial services sector in combination with rising levels of cybercrime, the AFM considers adequate management of information security risks of utmost importance. The AFM expects firms to take the appropriate measures (inter alia as per Article 18) to guarantee the continuity and reliability of their IT and provision of information, and to limit the impact of any security incidents.

The AFM is pleased to see that the security and reliability of IT systems are important considerations for investment firms. Most firms have set up and maintained adequate arrangements for information security.

However, the AFM's findings also show that there is room for improvement, especially regarding the incorporation of cyber risk in firms' overall risk strategy.

The AFM expects that

1. due to the critical role of IT, firms identify risks to their IT systems, implement the appropriate control measures, and develop an appropriate response plan.
2. firms have procedures and processes in place to handle material breaches of firms' security measures including promptly notifying the AFM in case of an incident.

4. Sector findings – investment firms – phase II

4.1 Governance and compliance – Articles 1, 2

There were no specific findings in this area, which may be due to the AFM's heightened interest in this aspect during last year's analysis.

The AFM observes that:

1. Firms have expanded the risk and compliance functions, including by hiring staff with a background in algorithmic trading activity.
2. The risk and compliance functions are embedded in the policies and procedures with regard to the algorithmic trading activities.
3. The risk and compliance staff are sufficiently knowledgeable about the algorithmic trading activities.

4.2 Intra-group outsourcing – Article 4

Attention to intra-group outsourcing has become more important now that several Brexit-firms operate on the basis of an AFM licence as these firms tend to outsource several key activities to other entities in the group. The requirements with regard to intra-group outsourcing are by and large the same as for outsourcing to third parties.

1. The AFM expects firms to have SLAs in place with the entities to which activities are outsourced, with a clear description of the legal (RTS6) requirements and obligations of both entities, as well as provisions on assuring continuity of the critical services.
2. The AFM expects firms to monitor the obligations and functioning of the outsourcing contracts and policies.
3. The AFM wants to emphasise that, in line with the requirements of Article 4 of RTS6, firms should make sure that sufficient knowledge to evaluate the (quality of the) service exists and remains within the firm.
4. The AFM expects the dependency of (on?) critical key activities and mitigating actions to be included in firms' business continuity planning.
5. The AFM expects firms to own all the relevant documentation and data and ensure sufficient knowledge exists within the Dutch entity to evaluate the quality of algorithmic trading services offered by the intra-group entities.

4.3 Algo-development and testing – Articles 5, 7, 8, 11

Trading algorithm: variety of interpretations

The term "trading algorithm" plays a central role in RTS 6. The AFM observes that different trading firms can have different interpretations of what constitutes a single trading algorithm. Some trading firms point out that a trading algorithm should always encompass a single trading strategy, as it is able to operate without dependencies on other trading algorithms. Others point out that one and the same trading algorithm can be used in various trading strategies, and that the combination of such trading algorithms constitutes a single trading strategy.

The AFM notes that a clear interpretation of what a trading firm considers to be a single trading algorithm is important for various reasons. For example, if a trading firm were to introduce a new trading strategy consisting of various trading algorithms, the trading firm might want to test the trading algorithm in conjunction with the other trading algorithms to measure the full effect of the new trading strategy on disorderly trading conditions. On the other hand, if a trading firm regarded a single trading algorithm as reflecting a single trading strategy, this might result in a different approach to testing.

1. The AFM encourages firms to define what is considered one trading algorithm and apply the definition consistently throughout the development/testing/deployment cycle.

Disorderly trading conditions: variety of interpretations

Article 5.4 of RTS 6 states:

“The methodologies referred to in paragraph 1 shall ensure that the algorithmic trading system, trading algorithm or algorithmic trading strategy:

(a) does not behave in an unintended manner;

(b) complies with the investment firm’s obligations under this Regulation;

(c) complies with the rules and systems of the trading venues accessed by the investment firm;

(d) does not contribute to disorderly trading conditions, continues to work effectively in stressed market conditions and, where necessary under those conditions, allows for the switching off of the algorithmic trading system or trading algorithm.”

The AFM notes a variety of interpretations of the term “unintended manner” RTS6, art.5.4(a)) and “disorderly trading conditions” (RTS, art.5.4(d)). Furthermore, the AFM notes that the interpretations – and the means for testing for them – appear to overlap substantially with other articles/terms in RTS 6.

The AFM observes that some trading firms test whether or not their algorithms contribute to “disorderly trading conditions” by making sure their messages get processed properly at the corresponding trading venue (potentially overlapping with “conformance testing”, or Article 6 in RTS 6). Some trading firms try to make sure their algorithms don’t contribute to “disorderly trading conditions” by ensuring the appropriate pre-trade controls are in place (Article 8) or by having an automated surveillance system to detect market manipulation (Article 13).

1. The AFM expects firms to have an interpretation of “disorderly trading conditions” as it will allow for testing this requirement explicitly. The AFM refers to Recital 11: Testing against disorderly trading conditions should be designed with a view to

specifically addressing the reaction of the algorithm or strategy to conditions that may create a disorderly market.

4.4 MAR – Article 13

False positives versus not many positives in alerting

The AFM notices that trading firms might experience difficulties in adjusting their alerting models so as to ensure the appropriate (number of) alerts are received. On the one hand, trading firms might want to be alerted to all actions that could be indicative of market manipulation, which might result in a relatively large number of alerts (including many that do not indicate market manipulation). On the other hand, setting the alerting models so that they are too stringent, might result in some cases of market manipulation not being detected.

1. The AFM notes that – above all – a detection system should detect all cases of (possible) market manipulation and cover all trading activities (as per Article 13.3).
2. That system should firstly be focused on identifying true positives and, secondly, on turning up the smallest possible number of false positives and negatives (as per Article 13.5.); the latter should be assessed at least annually.

Cross-asset class detection

The AFM notes that many trading firms use exclusively single-instrument detection models, i.e., the models look at potential market manipulation within the scope of a single financial instrument.

1. The AFM encourages trading firms – taking the variety of asset classes traded into account – to use models that take trading behaviour across various financial instruments into account. The reason for this is that even though market manipulation might not be apparent when looking at traders’ behaviour with respect to one instrument when looking at the behaviour with regard to both instruments at the same time, relevant signals might be produced.

Dynamic alerting

The AFM notes that some trading firms use a “static” threshold for their alerting, meaning: irrespective of recent volatility/stress in the market, an alert will be produced if a certain fixed threshold is exceeded. This might result in many alerts being generated during times of volatility or stress in the market. The AFM observes that some trading firms use “dynamic” alerting, which dynamically changes alerting thresholds based on recent trends in the market.

4.5 IT security – Article 18

1. An investment firm shall implement an IT strategy with defined objectives and measures which:

(a) is in compliance with the business and risk strategy of the investment firm and is adapted to its operational activities and the risks to which it is exposed;

(b) is based on a reliable IT organisation, including service, production, and development;

(c) complies with effective IT security management.

It is important for any firm to consider how its IT can assist with business activities and support the continuity, security and efficiency of its key processes. A formal IT strategy, aligned with the business and risk strategy, and subject to regular review, can aid a firm in ensuring that its IT and systems are able to meet business and regulatory demands.

The AFM observes that while most firms have defined objectives, goals and measures concerning the continuity, reliability and security of their IT and provision of information, few of them have compiled these in a documented plan aligned with their broader business strategy.

Inadequate strategic IT oversight makes a firm more likely to incur both business and compliance risk.

1. The AFM expects firms to document an IT strategy, taking into account the requirements of Article 18(1) RTS6.
2. Firms should set up and maintain appropriate arrangements for physical and electronic security that minimise the risks of attacks against its information systems and that includes effective identity and access management. Those arrangements shall ensure the confidentiality, integrity, authenticity, and availability of data and the reliability and robustness of the firm's information systems.
2. Due to the increasing digitization of the financial sector and rising occurrences of cyber threats, the AFM considers appropriate control measures regarding physical and electronic security to be of utmost importance.

2. Most firms have implemented relevant control measures and procedures. However, the measures are not always based on effective risk assessment, making it impossible to determine the adequacy of the implemented security arrangements. Moreover, procedures are often not standardised and formally documented nor are they subject to appropriate review, which poses substantial security risks.

1. The AFM expects firms to perform security risk assessments, allowing them to assess, identify and modify their security posture and enabling the organisation to handle security threats and risks in a risk-based manner. In addition, it is recommended that firms draft standard operating procedures in relation to their physical and electronic security arrangements.

3. An investment firm shall promptly inform the competent authority of any material breaches of its physical and electronic security measures. It shall provide an incident report to the competent authority, indicating the nature of the incident, the measures taken following the incident and the initiatives taken to avoid similar incidents from occurring in the future.

All firms investigated take the notification requirement of Article 18(3) RTS6 into account. However, not all firms have formalised the notification requirement in a standard operating procedure. Furthermore, determining what constitutes a material breach is not always based on objective criteria. These deficiencies carry substantial business and compliance risks.

1. The AFM recommends that firms implement an incident classification policy and draft standard operating procedures for notifying the relevant national competent authorities in case of material breaches of their physical and electronic security measures.

4. An investment firm shall annually undertake penetration tests and vulnerability scans to simulate cyber-attacks.

The AFM is pleased to observe that firms in scope undertake annual penetration tests and vulnerability scans.

5. An investment firm shall ensure that it is able to identify all persons who have critical user access rights to its IT systems. The investment firm shall restrict the number of such persons and shall monitor their access to IT systems to ensure traceability at all times.

Identity and access management are often the first line of defence when it comes to threats to information and systems. Due to the ubiquity of mobile computing and on-demand access to applications and data, appropriate system access controls and data access controls are essential.

While all firms have implemented identity and access management, the level of maturity varies substantially by firm.

1. The AFM expects firms to implement appropriate identity and access control measures, considering authentication, authorisation and accounting mechanisms, and best practices such as the principle of least privilege.

5. Sector findings – trading venues – phase I

5.1 Structure and degree of detail of self-assessments

The AFM expects the self-assessments to look at trading venues' compliance with all the applicable requirements laid down in RTS7 and include a bespoke analysis of this. The analysis should be substantiated with enough detail to assess the trading venue's findings/evaluation.

Not all requirements apply to all types of trading venues. Recital 5 of the Delegated Regulation states:

(5) Requirements should be laid down with respect to the systems of trading venues allowing or enabling algorithmic trading. However, their specific application should take place in conjunction with a self-assessment to be conducted by each trading venue since not all trading models present the same risks. Therefore, some organisational requirements may not be appropriate for certain trading models although their trading systems could be supported to a certain extent by electronic means. In particular, the specific requirements to be set in relation to request-for-quote systems or hybrid systems should be considered according to the nature, scale and complexity of the algorithmic trading activity undertaken. Equally, more stringent requirements should be established by the trading venues where appropriate.

1. The AFM expects trading venues to follow the structure of the articles of RTS7; and
2. The AFM expects trading venues to explain in adequate detail per article how the trading venue either
    a. complies with the requirements laid down in the articles of RTS7, or;
    b. why the article is not applicable to the activities of the specific trading venue.

6. Sector findings – trading venues – phase II

6.1 Governance and compliance – Articles 3, 4.

Governance - Article 3

As part of their overall governance and decision-making framework, trading venues have to establish and monitor their trading systems by means of a clear and formalised governance arrangement. Part of this arrangement involves the analysis of technical, risk and compliance issues when taking critical decisions.

The AFM notes that, although trading venues have decision-making frameworks, the definition of "critical decision" is not established consistently at the trading venues. As a consequence, there is a risk of failing to recognise critical decisions on time and hence, taking decisions at an incorrect level.

Another part of the governance arrangement relates to having effective procedures for the communication of information such that instructions can be sought and implemented in an efficient and timely manner.

This requirement refers to internal lines of communication. The AFM observes that even though lines of communication exist, these are not in all cases established in effective procedures.

1. The AFM advises trading venues to establish a definition of critical decisions within the decision-making framework.
2. The AFM expects trading venues to establish effective procedures for communication according to the requirements of Article 3.

Compliance - Article 4

The words "compliance function" and "compliance staff" in Article 4 refer to persons or a team or department dedicated to the compliance of the trading venue with official requirements. These persons, this team or this department function as the independent second line of defence within the trading venue.

1. The AFM expects the compliance function and compliance staff to be independent and to function as a second line of defence.

6.2 Member due diligence – Article 7

The AFM observes that trading venues have onboarding policies and procedures in place to structure the onboarding process and the necessary reviews before applications are sent to a separate body for (senior management) approval. In addition, the AFM observes that trading venues have structured procedures for annual risk-based assessments and follow-up audits in place.

The venue should act as its own gatekeeper and should make sure that the important controls on algorithmic trading are in place together with their prospective members. The AFM observes that not all trading venues check these controls before accepting prospective members. This requirement applies to both MiFID firms and non-MiFID-firms.

1. The AFM expects trading venues to perform a due diligence with respect to the requirements of Article 7.1 (i.e. pre- and post-trade controls, policy on kill functionality, qualified key staff) before prospective members are granted access to the venue.

6.3 Testing – Article 10

Disorderly trading conditions: different interpretations/implementations

The AFM notes that there are a variety of interpretations of the term and “disorderly trading conditions” (RTS 7, Article 10.2). The AFM observes that some trading venues tend to check for “disorderly trading conditions” by making sure the orders received get processed appropriately (potentially overlapping with “conformance testing” in Article 6 of RTS 6). Some trading venues tend to focus on having appropriate pre-trade controls or having an automated surveillance system in place to detect market manipulation to make sure algorithms don’t contribute to “disorderly trading conditions”.

1. The AFM points out the importance of trading venues establishing a clear interpretation of “disorderly trading conditions” (as opposed to the means to test it and as opposed to other terms in RTS 6 or 7). See also the next finding and expectation.

Certification of trading algorithms – Article 10

The article requires trading venues to have their members certify that the algorithms they deploy have been tested to avoid contributing to or creating disorderly trading conditions prior to the deployment or a substantial update of a trading algorithm or trading strategy and explain the means used for that testing.

The AFM observes significant variation among trading venues as regards the rigour of the testing of trading firms’ compliance with Article 10.1 of RTS 6. In particular, the quality of the explanations (as provided by trading firms regarding the testing of trading algorithms) deemed sufficient by trading venues varies. As with the testing of the trading system which is covered in Article 8, the testing of trading algorithms in order to avoid disorderly trading conditions is important. The AFM expects trading venues to assume their role in this regard as per the requirements of Article 10. The AFM wants to emphasise that this requirement is separate from any requirements concerning conformance testing (these requirements are set out in Article 9).

1. The AFM expects trading venues to require their members to certify that an algorithm, a new strategy, or an updated algorithm has been tested to avoid contributing to or creating disorderly trading conditions prior to the deployment.
2. The AFM expects members to explain to the trading venue the means they used for testing whether or not their trading algorithms contribute to or create disorderly trading conditions.

Scenario testing: various levels of sophistication

The AFM observes significant variation among trading venues as regards the realism/sophistication of scenarios in their testing environment provided to trading firms to test trading algorithms. These range from ad-hoc order books (generated by the trading venue at the request of a trading firm) to markets generating orders in real-time, allowing trading firms to trade with particular orders.

The AFM observes that trading venues have difficulty creating simulation facilities which reproduce the production environment, including disorderly trading conditions, as realistically as possible.

1. The AFM encourages trading venues to explore innovative ways to make their simulation environments more realistic so that they are in line with the requirements.

6.4 Platform controls – Articles 18-20

Pre- and post-trade controls

As regards the prevention of disorderly trading conditions caused by the trading venue, the AFM observes that the trading venues in scope have appropriate controls and other arrangements in place to ensure compliance with the requirements of this article. Trading venues regularly test the relevant controls, and related policies and procedures are subject to periodic review.

Regarding mechanisms to manage volatility, trading venues have adequate controls in place to automatically halt or restrict trading. Trading venues have dedicated the appropriate resources to monitoring activities and have the required processes for manual intervention.

With respect to pre-trade and post-trade controls, trading venues have implemented the appropriate controls, which are monitored systematically. Pre- and post-trade controls are updated according to changing market circumstances.

1. The AFM would like to stress the importance of platform controls for the functioning of the financial markets. Trading venues should remain diligent when it comes to the design and implementation of adequate controls and arrangements, as well as the

testing and monitoring of these controls. Furthermore, trading venues should regularly review whether the allocation of resources to ensure the proper functioning of these controls and arrangements is still sufficient.

Halting functionality: necessity of adequate testing

The AFM observes that some trading venues have experienced issues when it comes to their ability to automatically halt trading. Not being able to halt market activity whenever necessary is a serious issue that can have significant and negative consequences.

1. The AFM expects any trading venue to have mechanisms in place to automatically halt or constrain trading. These functionalities should be tested under all relevant scenarios.

6.5 IT security and limits to access – Article 23

1. Trading venues shall have procedures and arrangements in place for physical and electronic security designed to protect their systems from misuse or unauthorised access and to ensure the integrity of the data that is part of or is transmitted through their systems, including arrangements that allow the prevention or minimisation of the risks of attacks against the information systems as defined in Article 2(a) of Directive 2013/40/EU of the European Parliament and of the Council.

The trading venues in scope of the deep dive have the appropriate security procedures and arrangements in place to ensure compliance with the requirements of Article 23 RTS7. Overall, trading venues have demonstrated that they have dedicated an adequate amount of resources to information security.

2. In particular, trading venues shall set up and maintain measures and arrangements for physical and electronic security to promptly identify and prevent or minimise the risks related to:

(a) unauthorised access to their trading system or to a part thereof, including unauthorised access to the work space and data centres;

(b) system interferences that seriously hinder or interrupt the functioning of an information system by inputting data, by transmitting, damaging, deleting, degrading, altering or suppressing such data, or by rendering such data inaccessible;

(c) data interferences that delete, damage, degrade, alter or suppress data on the information system, or render such data inaccessible;

(d) interceptions, by technical means, of non-public transmissions of data to, from or within an information system, including electromagnetic emissions from an information system carrying such data.

The trading venues in scope have suitable measures and arrangements in place to ensure compliance with this Article. Most information security measures and arrangements are determined at group level, taking local circumstances into account. Risk ownership and awareness within the group and the local entity are considered adequate.

1. The AFM expects that trading venues remain diligent and to subject their information security policies, controls and procedures to regular review taking any changes in the security threat landscape into account.
2. Due to a shift to working from home, the AFM expects trading venues to continue their efforts to strengthen their endpoint security across systems and networks, and increase their information security awareness activities where necessary.
3. Trading venues shall promptly inform the competent authority of incidents of misuse or unauthorised access by promptly providing an incident report indicating the nature of the incident, the measures adopted in response to the incident and the initiatives taken to avoid similar incidents from occurring in the future.

The in-scope trading venues have demonstrated their compliance with incident reporting requirements. The AFM expects firms and venues to remain compliant with these requirements and evaluate compliance on a regular basis.

7. Annex

7.1 Articles in scope of deep-dive – proprietary trading firms

Articles in scope of deep-dive – proprietary trading firms
Organisational requirements
Article 1 - General organisational requirements
Article 2 - Role of the compliance function
Article 3 - Staffing
Article 4 - IT outsourcing and procurement
Testing and deployment of trading systems and strategies
Article 5 - General methodology
Article 7 - Testing environments
Article 8 - Controlled deployment of algorithms
Post-deployment management
Article 11 - Management of material changes
Means to ensure resilience
Article 12 - Kill functionality
Article 13 - Automated surveillance system to detect market manipulation
Article 16 - Real-time monitoring
Article 18 - Security and limits to access

Articles in scope of deep-dive – trading venues

Articles in scope - trading venues
General organisational requirements
Article 3 - Governance of trading venues
Article 4 - Compliance function within the governance arrangements
Capacity and resilience
Article 7 - Member due diligence
Article 8 - Testing of trading systems
Article 10 - Testing the members' algorithms to avoid disorderly trading conditions
Article 12 - General monitoring obligations
Article 14 - Periodic review of the performance and capacity of the algorithmic trading systems
Article 18 - Prevention of disorderly trading conditions
Article 19 - Mechanisms to manage volatility
Article 20 – Pre- and post-trade controls
Article 23 - Security and limits to access

The Dutch Authority for the Financial Markets
T +31(0)20 797 2000 | F +31(0)20 797 3800
PO Box 11723 | 1001 GS Amsterdam
www.afm.nl

The text of this publication has been compiled with care and is informative in nature. No rights may be derived from it. Changes to national and international legislation and regulation may mean that the text is no longer fully up to date when you read it. The Dutch Authority for the Financial Markets is not liable for any consequences - such as losses incurred or lost profits - of any actions taken in connection with this text.