REMIT Best Practice

A sector review on how to comply with REMIT related to inside information and market abuse.

2nd Edition

Updated: 15 January 2020

This document contains the 2nd edition of the REMIT Best Practice Report. The content of previous sections was updated and a new section on best practices regarding algorithmic trading solutions was added. The publisher of this report is the Nord Pool Group ("Nord Pool"). The following participants have contributed to the 2nd edition of the report:

- *Agder Energi Kraftforvaltning AS*
- *Centrica Energy Trading A/S (formerly NEAS Energy A/S)*
- *Danske Commodities A/S*
- *Eidsiva Vannkraft AS*
- *Fortum Power and Heat Oy*
- *Nordic Association of Electricity Traders (NAET)*
- *Skagerak Energi AS*
- *Statkraft Energi AS*
- *UPM Energy Oy*
- *Vattenfall AB*
- *Ørsted (formerly Dong Energy A/S)*
- *Nord Pool Group*

Disclaimer and rights

This 2nd edition has been prepared by Nord Pool with the participation of the above-mentioned companies and organizations.

This report is provided for information purposes only. The report does not constitute legal, technical or professional advice of any nature and may not be relied upon as such. Nothing in this report should be construed as representation or warranty, express or implied, given by either Nord Pool or any Participant as to the completeness or accuracy of information contained herein.

Any reliance by any party other than the Participants on the information contained in the report is a matter of such party's judgement and is completely at such party's own risk. Neither Nord Pool nor any Participant assumes any responsibility for any act or omission of any party as a result of relying on or in any way using information contained in the report. Neither Nord Pool nor any Participant may be liable for any loss or damage of whatsoever nature resulting from a party's reliance on or use of the information contained in this report.

Project and report information

Document details

Project no./name	REMIT Best Practice
Report finish date	15 January 2020
Accessibility	Public

Document revision history

Date	Description	Author
31 May 2017	REMIT Best Practice	Nord Pool Consulting
15 January 2020	2nd edition REMIT Best Practice Report (including a new chapter on algorithmic trading solutions)	Nord Pool Group

Nord Pool Contact details

Camilla Berg
General Counsel Nord Pool AS
market.surveillance@nordpoolgroup.com
+47 67 10 91 35

Approval

Lysaker, 15 January 2020

Preface

The Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency (REMIT) was implemented in 2011. While REMIT provides on the one hand a trustworthy level playing field for energy companies, it led on the other hand to an increased risk and burden to comply with strict compliance obligations. The consequence of misconduct can potentially be severe. More guidance and a common approach to compliance with REMIT has been asked for by many market participants.

The Agency for the Cooperation of Energy Regulators (ACER) has published guidance[1] on how to interpret REMIT and guidance on specific market abuse types[2]. This report is not a substitute to ACER's guidance but is meant as a guide to best practice on how market participants may ensure that they have implemented the right measures to comply with REMIT and by that limit the risk of misconduct. The report describes options that may provide guidance for market participants on how to develop and maintain an effective compliance regime under REMIT and how to comply with the requirements and prohibitions related to inside information and market abuse.

The 2nd edition of the report is based on input and knowledge sharing of ten market participants, one sector organisation and staff from the Nord Pool Group with long experience within REMIT and market monitoring. The participants are market actors of various sizes and types, and together their experience and various points of view gave valuable input and, in the end, a balanced report for a common approach on REMIT compliance. It is difficult to find an approach to compliance that fits all varieties of market participants, but the aim has been to make a report that could give guidance to all types of market participants and a presentation of the central points of consideration when building an entity-specific compliance manual. **That being said, the authors of this report are of the view that each market participant is best placed to assess the compliance risks that it faces and to design a compliance regime that in an appropriate manner addresses those risks, taking into account the nature, size and complexity of its business and the nature and range of trading in wholesale energy products.**

[1] Guidance on the application of Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency

[2] For the time being Guidance Note 1/2017 on wash trades, 1/2018 on transmission capacity hoarding and 1/2019 on layering and spoofing.

Table of Contents

1 Introduction

The aim of this report is to give a best practice guidance on how to comply with some key parts of REMIT. The ACER Guidance states that "*The Agency is of the opinion that market participants should develop a clear compliance regime*" fitted to ensure compliance with the various REMIT requirements. This report will be a guide on how to achieve this.

Section 2 focuses on how to develop and implement a compliance regime. The ACER 4th Guidance chapter 10 is used as a base to highlight main elements of a compliance regime.

Section 3 focuses on market abuse related challenges under REMIT. Section 3.1 describes how to identify and handle inside information, including measures to prevent abuse and how inside information should be published. Section 3.2 focuses on recommendations on measures to prevent market manipulation, both intentional and unintentional. Section 3.3 discusses and recommends how market participants may ensure compliance under REMIT when using algorithmic trading solutions.

The target audience for this report are market participants covered by the REMIT regulation. Focus is primarily on electricity, but the concepts described can to a large extent be applied also for gas. Market participants under REMIT may vary significantly in size and complexity, and the complexity in securing compliance may also differ significantly. This Best Practice report is only a guidance, and each market participant must make its own assessment of how to ensure compliance. It is possible to achieve compliance also without following the practice described in this document.

Other relevant laws and regulations for the target audience could be e.g. the Market Abuse Regulation (MAR), the recast of the directive on markets in financial instruments (MiFID II), and competition law. This report will only touch upon a few selected parts of MiFID II for the purpose of comparison between the regulation of physical and financial instruments. It is therefore important to highlight that other and stricter requirements may exist in these regulations than what is described here under REMIT.

REMIT also contains obligations regarding reporting of orders and transactions. This report will not provide any best practice guidance on this, as this is rather of an operational nature and the complexity of the detailed reporting obligation would overburden this guidance.

2 Compliance regime

REMIT does not set out any form of requirements for having a compliance regime. The regulations describe requirements, prohibitions and sanctions, but not how to comply with the regulation. However, the ACER Guidance states the following:

> The Agency is of the opinion that market participants should develop a clear compliance regime towards real time or close to real time disclosure of inside information and the further REMIT requirements, beyond compliance with existing Third Package transparency obligations. NRAs should consider the following best practice example of such compliance regime for market participants, but taking into account the market participant's size and trading capacity

Text box 1 From ACER Guidance chapter 10

In addition to the recommendations from ACER, a compliance regime will support market participants in conforming with rules and policies, creating a secure framework for employees and contributing to a fair and level playing field for trading activities by giving trust to the market. Further, a proper compliance regime will help avoid or minimise the risk of monetary fines and other regulatory sanctions and potential civil law claims. It will also help avoid or minimise the risk of loss of reputation as for instance bad press or bad customer experience.

Based on the above, each market participant should develop a compliance regime specifically adapted to their organisation, where the specific risks faced by the market participant should make the basis for how to prioritise the compliance work.

Ensuring compliance with REMIT is a complex task that requires the market participant to actively address and manage the risks involved taking into account the nature, size and complexity of its business, and the nature and range of trading in wholesale energy products. It requires a strong compliance culture, adequate and clear policies and procedures, regular training of employees and proper documentation of implemented measures.

In the following we will describe some main pillars to be included in a compliance regime adopted to ensure compliance with the various rules related to market abuse and disclosure of inside information under REMIT. **It is important to emphasise that there is no "one-size-fits-all" approach to compliance**. In this report, we therefore only point at and give examples of some compliance practices that have proved to be good and effective, and which we consider to be a best practice approach. When developing a compliance regime, market participants are recommended to ensure that such regime is properly adjusted for the size and set-up of their organisation and their business' trading capacity.

WHY IMPLEMENT A COMPLIANCE REGIME?

- Ensure compliance with REMIT requirements
- Contribute to a fair and level playing field for trading activities
- Avoid or minimise the risk of regulatory measures
- Avoid loss of reputation
- Shield employees, management and company from criminal sanctions
- Shield company from civil liabilities

2.1. What could a compliance regime look like?

Neither REMIT nor ACER prescribe a particular compliance regime or requirements in respect of a compliance regime. As stated above it is important to emphasise that there is no “one-size-fits-all” approach to compliance. Each market participant must develop a compliance regime adapted to the specificities of its own organisation. In particular, the size and the complexity of the market participant and its trading capacity must be considered. Naturally, there will be significant differences on a compliance regime for small and non-complex market participants compared to large and complex market participants.

However, the ACER Guidance sets out the following pillars in a best practice compliance regime:

i) Compliance objectives; the compliance with REMIT requirements, namely the registration, disclosure and reporting obligations and the market abuse prohibitions; see art. 2.1.1.

ii) Compliance culture; the creation of a corporate culture to comply with REMIT requirements; see art. 2.1.2.

iii) Compliance organisation; the definition of roles and responsibilities in the internal organisation; see art. 2.1.3.

iv) Compliance risks; the identification / assessment of concrete compliance risks; see art. 2.1.4.

v) Compliance programme; the identification of concrete actions to define compliant/non-compliant behavior; see art. 0.

vi) Communication; the communication of the rules and regulations to be observed, see art. 2.1.6.:

- internal communication and training concept (raising the awareness of employees)

- external communication and reporting to the Agency/NRAs
- reporting processes: internal reports on compliance, reporting of infringements, status of current processes, etc.

vii) Monitoring improvements: internal controls, audits, reporting lines for monitoring results; documentation of processes and actions; see art. 2.1.7.

In this report, we have chosen to follow the structure of the ACER Guidance on how to set up a proper compliance regime.

2.1.1. Compliance objectives

> Compliance objectives: the compliance with REMIT requirements, namely the registration, disclosure and reporting obligations and the market abuse prohibitions

Text box 2 From ACER Guidance chapter 10

The first element in a well-functioning compliance regime is to **define the objectives**. The ACER Guidance points at objectives that are important in relation to compliance with REMIT.

This report will focus on the market abuse prohibitions, namely insider trading, including not spreading inside information and publication of inside information, and market manipulation. The compliance objectives could also embrace registration and reporting of orders and transactions under REMIT as well as objectives following from other regulations applicable to the market participant, but these are not included in this report.

2.1.2. Compliance culture

> Compliance culture: the creation of a corporate culture to comply with REMIT requirements

Text box 3 From ACER Guidance chapter 10

The second element in a well-functioning compliance regime according to the ACER Guidance is to create a **corporate culture** to comply with REMIT. A culture that encourages a commitment to comply with the REMIT requirements is important for the success of compliance. There are some areas a market participant should be particularly aware of in order to ensure it has a culture for compliance.

It is important that focus on compliance is **embedded in the management**. Without active support from the management, there is a risk that the market participant will not succeed in creating a culture for compliance. In general, a successful implementation of a compliance regime depends on a sound compliance culture.

As part of a compliance culture, the following points are important to consider:

i) the market participant has a compliance function with **sufficient resources**,
ii) the market participant has **adequate policies and procedures** to ensure compliance and detect non-compliance,
iii) the compliance function takes a **risk-based approach** for efficient use of resources,
iv) the compliance function establishes a **compliance programme** with priorities determined by a risk assessment and
v) **adequate communication** of the legal framework and internal rules/guidelines, including training of employees and regularly and ad-hoc reporting to the management.

These elements will be handled further in the report. Each market participant must find the relevant approach to ensure a strong compliance culture. However, to highlight the importance of compliance in the business, two points could be considered:

- The **market participant's values** may have a link to compliance to highlight the importance of compliant behaviour

- The **market participant's strategy** may have a link to compliance

As a part of the compliance culture, it is important to have employees with the right incentives for ethical behaviour and to reduce the risk of wilful and intentional market abuse. Two measures can be considered:

- Background Checks
    - For traders and other key personnel**, basic background checks** may be performed. This may include an identity check and checking references. Other measures may also be taken to ensure that persons recruited possess the relevant competence, and that they act with the necessary integrity and do not have a criminal record making the person unsuitable for the position. It is up to each market participant to decide how broad such a background check should be.

- Remuneration
    - The **choice of remuneration system**, especially for traders and compliance personnel, may influence the risk of market abuse taking place.

- Traders may have a remuneration system where bonus is dependent on the profits made by traders. This is often considered necessary to create sufficient incentives for traders, but it may also make traders more inclined to commit insider trading or manipulate the market. To mitigate the risk of such actions, the market participant may take into consideration the structure and composition of their remuneration system and bonus scheme, including performance bonus, incentives related to compliance and reduction of bonus in case of breach of REMIT and internal policies and guidelines, considering the seriousness of a breach and degree of negligence.
- The remuneration structure of compliance personnel should not compromise their independence or create conflicts of interest. The remuneration structure may be based on company-wide performance criteria but should not directly depend on the performance of the trading department.

2.1.3. Compliance organisation

Compliance organisation: the definition of roles and responsibilities in the internal organisation (e.g. responsibilities for the REMIT requirements (centralised vs. decentralised), internal vs. external reporting lines, internal vs. external interfaces, provision of resources: human / technical (IT Systems) resources)

Text box 4 From ACER Guidance chapter 10

The third element in a well-functioning compliance regime is to make sure the compliance function is **properly organised and staffed**. Again, it is no "one-size-fits-all". The set-up of a compliance function must be adjusted to fit the market participant's needs and what kind of risks the market participant faces. However, some general principles are recommended:

- The compliance function should have **clearly defined roles and responsibilities.** Dependent on the size and complexity of the market participant's activities it is advisable to have a department or at least one person responsible for compliance with REMIT. The responsibility of compliance may also be one part of the tasks of one employee, if sufficient independence can be achieved. The role and responsibility of the compliance personnel/person should be clearly defined and communicated to the organisation.

- The compliance function should be staffed with **sufficient people with sufficient business knowledge and competence**, and have sufficient resources in terms of IT support etc. It is advisable that compliance personnel have knowledge of the daily operation/trading activities in addition to in-depth knowledge of the REMIT requirements. This could be supported by having the

compliance officer sitting close to or physically located at the operation/trading desk. The compliance personnel will by this be involved and learn about the trading activities whilst the traders may be more encouraged to ask questions and discuss relevant matters, they experience in their daily work with the compliance personnel. Compliance could also participate in trading status meetings and the like. The compliance function needs to have sufficient knowledge of relevant business activities of the market participant. It is therefore recommended to ensure early involvement of the compliance function in decision making processes. In addition, the compliance function should have sufficient resources for participating in industry associations, trainings etc.

- The compliance function should be **independent** from the business it advices, monitors and controls. Ideally the compliance function should as second line of defence (see art. 2.1.7) also be separated from other controlling units like internal auditing (third line of defence) and risk controlling. This is best practice for large and complex market participants, whilst for smaller or non-complex market participants it could be proportionate to combine the compliance function with internal audit and risk controlling.

- The compliance function should have the **authority required** for such a function and the **support of the management** to be able to perform its tasks, i.e. have the authority to implement procedures and report compliance failures. It is important that focus on compliance is embedded in the management. Without active support from the management, there is a risk that the market participant will not succeed in creating a culture for compliance. The importance of compliance should be communicated from management both on a general level and by concrete messages, for instance clearly stating that insider trading and market manipulation are not tolerated. Management may also demonstrate its commitment to compliance through concrete actions by allocating sufficient resources to the compliance function, implementing guidelines and procedures based on advice from the compliance function, ensuring that employees understand their compliance obligations and regularly assess and evaluate the effectiveness of the compliance regime followed by necessary changes. This could be done by e.g. having a dedicated employee as a compliance officer, or for smaller market participants, have an employee with a written job description that includes management of compliance as one task. Management could support the compliance organisation by requiring that traders sign a written statement whereby traders undertake to comply with applicable laws, rules and regulations as well as internal compliance measures.

- The compliance function should have **unlimited access** to all necessary information, documents, IT systems etc. needed for the regular compliance tasks such as incident investigation and controls.

- The compliance function should have a **direct reporting line** to senior management at an appropriate level, depending upon the size and structure of

the market participant. The manager to whom compliance reports must be responsible for the conduct of the overall business unit or the company – i.e. there should be no middle management with competing incentives involved.

- The compliance function should be **involved in significant changes of the organisation** involving business units subject to REMIT requirements. The compliance function should also be involved in development of new products, or changes to existing products, entering new markets, areas or countries, and any other relevant changes.

- The compliance function should always be **informed** about significant market and regulatory developments. This may be achieved by participation in associations, conferences, working groups within the industry etc. Such fora will also strengthen the competence of the compliance staff.

- The compliance function should ensure that all parts of the compliance activities (including interpretations and considerations) are **documented** by the compliance function or the business as applicable. This includes procedures, instructions and actions taken from compliance or the business**.** Documentation is key to provide evidence of what has been communicated, decided, monitored and controlled. This applies to all types of market participants, both small and large.

2.1.4. Compliance risks

Compliance risks: the identification / assessment of concrete compliance risks

Text box 5 From ACER Guidance chapter 10

The fourth element in a well-functioning compliance regime is to conduct **risk assessments** to prioritise the compliance effort and to ensure a risk-based compliance approach. To be able to set up an effective compliance regime with the right measures, it is important to have a clear picture on what compliance risks the market participant faces. Therefore, each market participant should perform a risk assessment. Once again, it is pointed out that there is no “one-size-fits-all”. The risk assessment must be adjusted to fit the market participant’s needs. However, some general principles can be highlighted:

- The compliance function may on a regular basis do an assessment of the market participant’s compliance areas and its risk exposure
    - Identify the relevant compliance areas (activities)
    - Identify the main source/areas for compliance risks
    - Identify existing controls (particularly existing internal controls)
    - Identify the key stakeholders for the identified compliance- and risk areas to help with input regarding the relevant business activities and compliance risks

- The compliance function may do interviews with key stakeholders within the company
    - Acquire a description of the activities of the business unit
    - Pre-structured questions, e.g. to identify the potential flow of inside information
    - Open questions to receive additional concerns/suggestions

The risk assessment could be based on the impact of a possible incident and the likelihood of this happening and may also include existing controls. For each risk area, the likelihood of it to happen can be assessed together with the consequence of the risk occurrences. On this basis, the risk should be graded. The approach to the risk assessment should take into consideration the market participant's size and complexity. The assessment may also consider results of any previous monitoring activities and relevant findings of the compliance and audit functions.

When assessing the compliance risks, results can be divided by descriptions (e.g. low, medium, high or very high), colours or numbers. What risk level is acceptable for each area/activity is for each market participant to decide.

A risk assessment is a good starting point for the determination of the compliance programme, including the compliance plan, and for ensuring that the right compliance measures are implemented to reduce the risks. In particular, high-risk areas should be addressed and managed so that they are kept at an acceptable level.

It is important to be aware that different market participants have different risks, and that risks and consequences may also vary between different parts of the market participant.

The risk assessment should at least include an assessment of all the types of market abuses, that are described in chapter 8 in the ACER Guidance on REMIT as well as in the separate ACER Guidance Notes on specific market abuse types[3], and the obligation to publish inside information. In appendix 1, an example of how a risk mapping could look like is provided. Note that this is a fictitious example with fictitious numbers and not based on a real-life risk assessment.

[3] For the time being Guidance Note 1/2017 on wash trades, 1/2018 on transmission capacity hoarding and 1/2019 on layering and spoofing.

2.1.5. Compliance programme

> Compliance programme:
> the identification of concrete actions to define compliant/non-compliant behavior

Text box 6 From ACER Guidance chapter 10

The fifth element in a well-functioning compliance regime is the **compliance programme**. In the ACER Guidance, this is described as the identification of concrete actions to define compliant/non-compliant behaviour. In this report, "compliance programme" is used in a wider perspective. Based on the performed assessment of the identified compliance risks, existing internal controls and previous findings, a compliance programme (including a compliance plan) with concrete actions to address the identified compliance risks should be developed. The main aim of the compliance programme is to define and implement actions to prevent, detect and mitigate the risks. In addition, the aim is to prioritise the concrete actions and ensure a risk-based approach. The programme should be tailored to fit each market participant's size and structure. Co-owned/operated companies and joint ventures should also have their own compliance programme defined and well documented, either by co-owned company's own personnel, by the owners, or a third party.

A compliance programme should cover three main pillars. First pillar consists of measures to **prevent** breaches from happening. The preventive measures should be appropriate and proportionate and be based on the results of the performed risk assessment and previous findings. Secondly, it is important to be able to **detect** possible breaches. It is recommended to implement compliance activities and controls, monitoring and routines for possible breaches of REMIT. Thirdly, to ensure effective compliance the market participant should ensure an adequate **response** to specific incidents or matters that may occur.

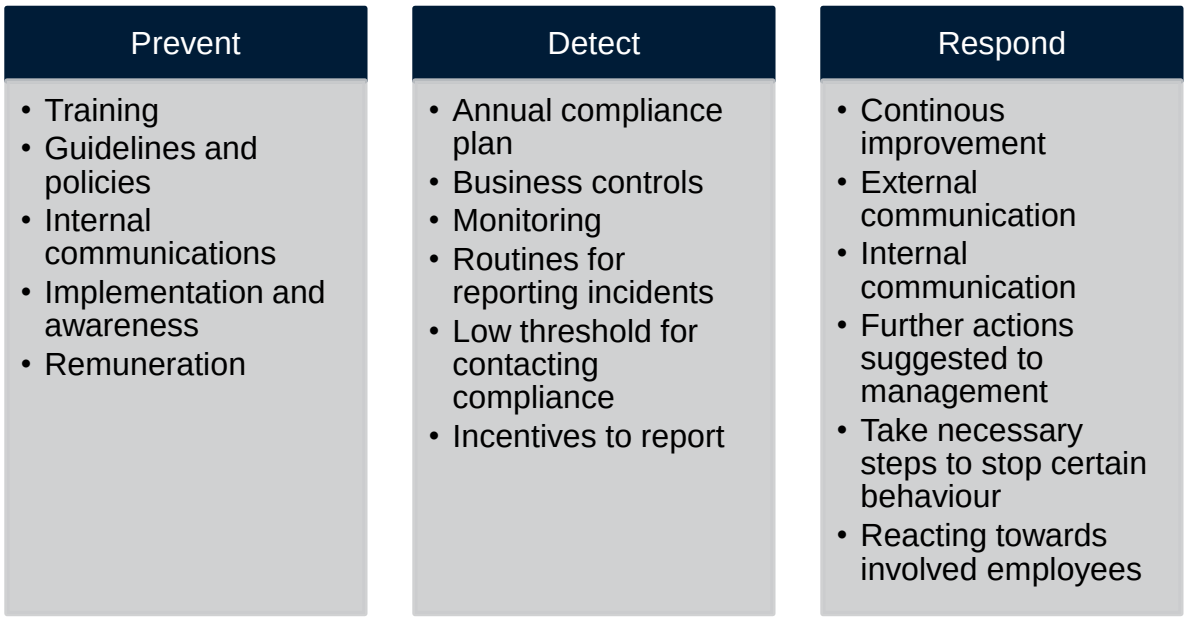

Figure 1 Prevent, detect and respond

The compliance programme should cover all the three targets above with specific emphasis on prevention. The points above are handled in other chapters of this report.

Compliance plan

Market participants are recommended to always develop a plan for the coming year. It should be adjusted to fit each market participant's size and commercial activities. The compliance plan should be based on the risk assessment, existing controls and previous findings and should over a reasonable period cover all compliance areas. For each chosen area in the annual compliance plan the following parameters could be addressed:

- Assessment of activity
- Compliance risk
- Period
- Relevant department
- Relevant person responsible
- The source for compliance (e.g. guidelines, interviews or samples of Urgent Market Messages)
- Type of control
- Conclusion
- Completion
- Implementation of new regulation or new interpretations/practice

When having a plan with priorities it is possible to explain why some actions are prioritised, and to review the compliance work. It should also be noted that other tasks than those in the compliance plan need to be prioritised in case of unforeseen events. All compliance functions regardless of the size of the market participant should make a year-end compliance report to management. This report should cover inter alia what has been done, what are the concerns, have there been any breaches, how many incidents in the past year, and what has been achieved and not with the dedicated resources. In the end, it is the management who owns the risk, approves the plan and devotes resources.

2.1.6. Communication

Communication:
the communication of the rules and regulations to be observed:
- internal communication and training concept (raising the awareness of employees);
- external communication and reporting to the Agency/NRAs;
- reporting processes: internal reports on compliance, reporting of infringements, status of current processes, etc.

Text box 7 From ACER Guidance chapter 10

The sixth element in a well-functioning compliance regime is to have proper **communication** in place. The ACER Guidance points at some communication procedures to consider.

Internal communication including internal reporting processes and training

Internal communication can be divided into three main parts:

- Communication from the compliance function to the business:
  - Training
  - Lessons learned
  - Information regarding regulations, new routines and developments

- Communication from the business to the compliance function

- Communication from the compliance function to management

Communication from the compliance function to the business
Compliance typically requires a conscious approach from a large number of employees. To succeed, there has to be a clear and effective communication to ensure that employees understand rules and regulations, internal procedures and routines, the importance of compliance, and the commitment of the market participant.

Communication from the compliance function to the business includes training. Regular training is essential to provide the business and the relevant employees with up-to-date knowledge of REMIT and how REMIT applies to their day-to-day activities. It is vital that employees are aware of what kind of behaviour that can constitute a breach of REMIT. All market participants, regardless of resources, should therefore set up a tailored training programme for their company. The aim of such programme should be to put the business and the relevant employees in a position where they possess sufficient knowledge to avoid potential breaches of REMIT. To ensure that there is no breach of the rules, both compliant and non-compliant behaviour should be defined. There is a variety of different training methods. E-training, classroom-training, real scenario training, topic-specific training, general Q&A's, external, internal etc. It is recommended to tailor the training with a view to the size of the organisation, the type and scale of its trading activities and the need for publishing inside information. Another important part when tailoring the training programme is also to assess the experience level and knowledge of the employees to develop training suited for the people involved.

Further, it should be considered to have an end-of-training assessment that requires employees to achieve a particular score to pass, taking into account the relevant activity, the complexity and risk assessment.

Finally, both the training attendance, the content of the training, and the results from the end of training assessment should be documented. If the results from the training assessment are not sufficiently strong, measures should be considered.

For some market participants, it may be sufficient to have regular distribution of up-to-date guidelines with every relevant employee having to sign that he/she has read and understood the content in addition to the possibility and encouragement to ask questions if anything is unclear.

Market participants may wish to create a compliance workspace/tracking tool, a system for setting out the highest risk compliance areas for the company and update the tool when necessary. This may help ensure that compliance is integrated as part of the company's way of doing business and, thereby, seen as a positive process rather than merely a function producing lists of prohibitions.

An example on how to set up a tailored training programme is found in Appendix 2.

TRAINING CONCEPT – KEY POINTS

- Set up a tailored training programme based on the company's needs and risk-groups of employees
- Training should take into account the specific risk profile and experience and knowledge of the employees
- Training should be performed regularly
  - In addition
    - When there are developments in market practice or regulatory updates
    - On an ad-hoc basis after incidents either internally or externally
- Not a generic or one size-fits-all training: Different roles – different needs
- Tests may be performed to ensure that the participants of the training have understood the training. Tests could require employees to achieve a particular score to pass
- The training attendance should be documented, as well as the content of the training

Communication from the business to the compliance function

To prevent potential compliance issues, visibility of the compliance function in the company is important, and the market participant should support an environment that encourages employees to discuss compliance concerns and report compliance issues. Employees should be encouraged not to hesitate to contact compliance for advice and in case of compliance incidents.

To detect and prevent potential compliance issues, a low threshold for contacting compliance personnel with any concerns, possible breaches or other issues that might arise is advisable. It should be clearly defined and communicated how employees should report potential compliance issues, and who they can report to. The regular reporting will normally go to the immediate manager and will be handled within the normal lines of reporting in the company. In addition, all compliance issues should be reported to the compliance function. Procedures to handle such notifications are advisable:

- The compliance function must take all notifications seriously and handling of such issues should have a high priority to prevent or minimise any further damage. Notifying persons should not be subject to any retaliation for notifying according to existing procedures

- Compliance should report the number of notifications received and their nature to management

- Review of the notification handling procedures may be executed regularly, for example through a self-assessment from Compliance, and/or through internal audit

- The reporting scheme may also include a whistleblowing scheme where anonymous reporting is possible and where the whistleblower is protected

Communication from the compliance function to management

Reporting processes should cover reporting to management in respect of results of the compliance plan and additional compliance reviews. Reporting could be done annually (or with quarterly updates) and ad hoc in case of important incidents or other important matters. Such reports may gather monitoring insights to review the efficiency of the compliance framework.

External communication and contact with authorities

A market participant may become aware of an error or other types of incidents that could potentially be a breach of REMIT. Regardless of the risk of the regulatory authorities discovering the potential breach, an approach where market participants report potential abuses could be mitigating in case of an investigation. It **may** turn out positive to give the NRA an explanation of a potential breach before they potentially start an investigation. A proactive notification of a breach, although not a legal requirement, may have a positive impact on whether and which sanctions might be applied. In addition, a proactive approach could also improve the trust and cooperation with the NRA. To do this, it is advisable to have a policy for when, how and by whom NRAs should be contacted. The same approach could be considered in respect of the market surveillance departments of the affected PPAT(s), including dual notifications.

Generally, it is recommended that the compliance function should manage the contacts with the authorities in REMIT related matters, and compliance should always be involved when corresponding with authorities in these matters, or jointly with Legal where deemed necessary.

It is recommended that the policy includes guidelines or routines for what to consider when handling contact with the authorities (and possibly the market surveillance departments of a PPAT) in the following situations:

- When the market participant or an employee has (potentially) breached REMIT
    - When making such guidelines, the following may be taken into account:
        - Principles for what kind of breaches and the seriousness of such breaches that should be reported
        - Take into consideration the risks for the relevant employee
        - Intentional market abuse compared to unintentional

- When there are doubts regarding how to interpret REMIT

    - Routines for both urgent matters and more fundamental questions

- When an authority approaches the market participant or employees
    - Routines for who should be contacted and who may communicate with the authorities.

- When a market surveillance team approaches the market participant or employees
    - Routines for who should be contacted and who may communicate with the market surveillance team.

- When for example a trader detects suspicious behaviour from another market participant
    - Routines for when, who and to whom such suspicious behaviour should be reported.

One specific situation is an unannounced inspection at the market participant's premises (dawn raid). It is recommended to have a short manual available describing how to handle this kind of situation. The rules and regulations relating to such unannounced inspections may differ between different jurisdictions and this should be taken into account when developing such a manual.

A manual may include the following topics:

1. What is an unannounced inspection?
    - Purpose of an unannounced inspection
    - The regulatory authorities that are entitled to carry out unannounced inspections
    - The extent of an unannounced inspection
    - Copies of documents

2. Precautionary measures in case of an unannounced inspection:
    - Calling in the primary responsible person
    - Calling in legal assistance (surveillance persons and external legal advisor)
    - Internal communication
    - Gathering of inspectors/civil servants
    - Surveillance of inspectors/civil servants
    - IT-specialists
    - A report of the inspection

3. After the inspection

The manual could also include specific instructions to reception desk, primary responsible, surveillance persons and IT-specialists. An example of such instruction is found in Appendix 3

2.1.7. Monitoring improvements

Monitoring improvements: internal controls, audits, etc.; reporting lines for monitoring results; documentation of processes and actions

Text box 8 From ACER Guidance chapter 10

The seventh element of a well-functioning compliance regime is to have **monitoring procedures** in place and make improvements based on the monitoring. This part will cover both **preventive** measures and **detection** of possible infringements.

Three lines of defence

It is recommended to implement a compliance regime for monitoring purposes based on the "three lines of defence". With respect to REMIT, it is recommended to ensure that the business operations handle risk management and internal control within the first line, compliance is in place as a second line of defence, and internal audit as a third line of defence. However, the need for this must be assessed in relation to the size and complexity of the market participant, and for smaller market participants it may for example be relevant to combine compliance and internal audit within one unit.

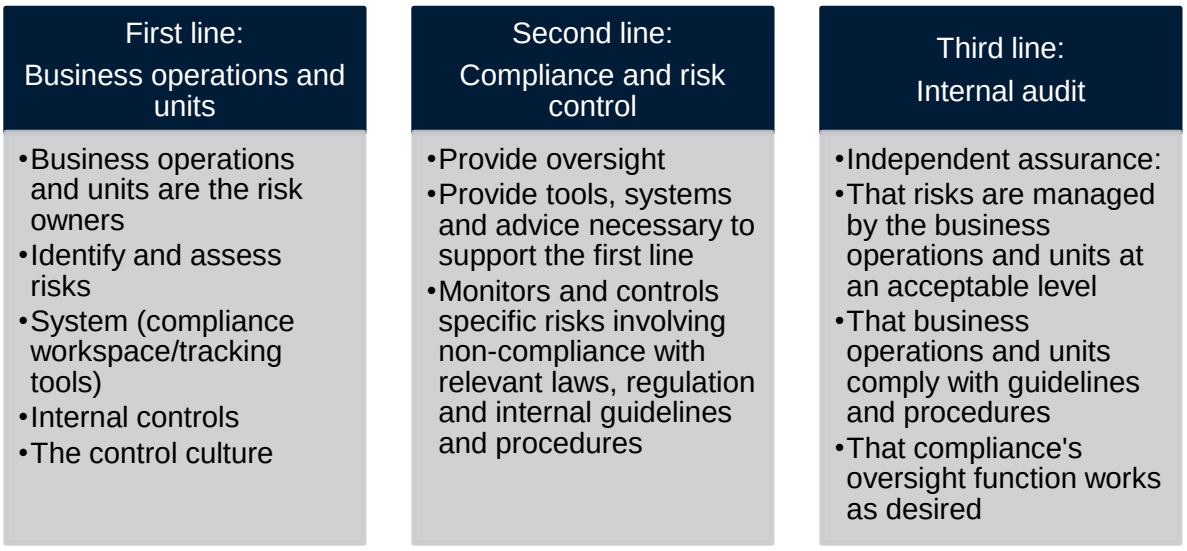

Figure 2 Three lines of defence

<u>Monitoring of the business by the compliance function</u>

Depending on the nature of the trading activities, it may be relevant to implement routines for monitoring of the trading activity. This may be manual or automated monitoring, and it may be continuous or ad-hoc monitoring. Irrespective of the type of

monitoring implemented, it is important that the traders know that their trading activities may be subject to monitoring, as this may have a disciplinary effect.

Self-assessment

Regular assessments of the compliance regime should be conducted. To be able to maintain an effective compliance regime over time, it is recommended to both measure the performance of the compliance regime and update it on a regular basis. The required measures will depend on the activities of the market participant, and the implemented measures should be proportionate. The aim for the assessment should be to ensure that the compliance regime continues to be "fit for purpose", uncover compliance gaps and failures and to identify necessary updates that must be implemented.

In addition to periodic reviews of the risk assessments and the compliance plan, market participants should review and if relevant, update their risk assessments and compliance plan in the following instances:

- Changes to legislation and other pertinent rules (e.g. REMIT 2.0, new or updated ACER Guidance)
- New or changes in practice from NRAs or ACER
- Upon the occurrence of non-compliant incidents

A suitable measure to respond to the above situations could be, for example, a corresponding change to guidelines and training (where required by changes to regulation or practice) or change in processes and training (where existing processes have resulted in or not prevented compliance incidents).

The compliance function should work together with the business to optimise and prioritise the monitoring and compliance reviews.

Internal audit

Market participants may also conduct regular or ad hoc internal audits of the compliance function which may reveal any needs for updates of the compliance regime. This report does not address how to conduct internal audits as this is an area where extensive guidance already exists. Instead, it is recommended to conduct basic internal audits based on available international standards for the professional practice of internal auditing. Such standards may serve as a guidance, but the measures implemented should be reasonable and proportionate for each individual market participant.

CHECKLIST COMPLIANCE REGIME

- Defining compliance objectives
- Create a compliance culture
    - Embedded in management
- Compliance organisation
    - Clearly defined roles and responsibilities
    - Sufficient people with sufficient business knowledge and competence
    - Ensure sufficient independence
    - Authority and support from management
    - Access to information
    - Direct reporting line to management
    - Involved in significant changes in the organisation
    - Documentation procedures
- Risk assessment
- Compliance programme
    - Prevent, Detect, Respond
    - Compliance plan
- Communication and training
- Monitoring and improvements
    - Three lines of defence

3 Specific challenges related to market abuse and publication of inside information under REMIT

3.1. Inside information

The starting point is the compliance regime as described under section 2 and special attention should be given to chapter 3.3 when using algorithmic trading solutions. The aim of this chapter is to particularly point at what kind of measures market participants need to be aware of and address in their regime to ensure compliance with REMIT when it comes to handling of inside information. Again, it is no “one-size-fits-all”, and each market participant must tailor their compliance regime accordingly. But regardless of the type and size of the company, all market participants should have a clearly documented strategy on how to handle inside information. Another important point is to have efficient and good documentation routines to be able to show the information flow in case of an inquiry from NRAs or for own investigation purposes.

In the following, recommendations are given for how to handle inside information prior to publication, how to avoid insider trading and how to ensure efficient publication routines.

The definition of *inside information* is set out in REMIT Article 2.

> Definition:
> ‘inside information’ means information of a precise nature which has not been made public, which relates, directly or indirectly, to one or more wholesale energy products and which, if it were made public, would be likely to significantly affect the prices of those wholesale energy products.

Text box 9 REMIT Art. 2 Definition of Inside information

The first step for a market participant to comply with the requirements related to inside information under REMIT is to be able to identify the types of information which qualify as inside information. When inside information is identified, it is important to be aware of the three types of market abuse related to the possession of inside information as described in the prohibition against insider trading:

- ***Using*** *inside information in trading*
- ***Spreading*** *of inside information*
- ***Recommending*** *or* ***inducing*** *based on inside information*

The prohibition of *insider trading* is set out in REMIT Article 3.

Prohibition of insider trading

1. Persons who possess inside information in relation to a wholesale energy product shall be prohibited from:

(a) using that information by acquiring or disposing of, or by trying to acquire or dispose of, for their own account or for the account of a third party, either directly or indirectly, wholesale energy products to which that information relates;

(b) disclosing that information to any other person unless such disclosure is made in the normal course of the exercise of their employment, profession or duties;

(c) recommending or inducing another person, on the basis of inside information, to acquire or dispose of wholesale energy products to which that information relates.

Text box 10 REMIT Art. 3 Prohibition of Insider Trading

The obligation to publish inside information to the market is set out in REMIT Article 4. “Publication in an effective and timely manner”. The ACER Guidance has stated that “a timely manner" normally means as soon as possible, but at the latest within one hour if not otherwise specified in applicable rules and regulations.

Obligation to publish inside information

1. Market participants shall publicly disclose in an effective and timely manner inside information which they possess in respect of business or facilities which the market participant concerned, or its parent undertaking or related undertaking, owns or controls or for whose operational matters that market participant or undertaking is responsible, either in whole or in part. Such disclosure shall include information relevant to the capacity and use of facilities for production, storage, consumption or transmission of electricity or natural gas or related to the capacity and use of LNG facilities, including planned or unplanned unavailability of these facilities.

Text box 11 REMIT Art. 4 Obligation to publish inside information

It is recommended that market participants implement measures to ensure that:

i) Inside information is identified and information flows are mapped; chapter 3.1.1
ii) Inside information is protected; chapter 3.1.2

iii) Inside information is not used for market abuse; chapter 3.1.3
iv) Inside information is published; chapter 3.1.4

3.1.1. Identification of inside information and mapping of information flows

It is recommended to implement measures to be able to **identify possible inside information**. Different market participants might have different types of inside information. Each market participant should identify what kind of information they might possess that could constitute inside information. Each market participant should go through the specificities for its company to:

- Identify all facilities (production/consumption/transmission) the market participant owns or is responsible for and specify in which situations inside information might occur

- Identify what kind of situations exist in general, not related to specific facilities, where inside information occurs or might occur (such as having access to customer orders)

- Identify stress points/parts of the organisation that are vulnerable for information leaks – intentionally and non-intentionally

- Map information flow to identify any information that could contain or qualify (or potentially qualify) as inside information

- Identify in what kind of situations the market participant might receive inside information from other third parties

Based on the above, each market participant should develop a guidance on what kind of information may constitute inside information for the market participant. Specific thresholds may be defined, and these could be differentiated in situations with strained power balance. Market participants may need to use informal thresholds for operational purposes so that personnel dealing with UMMs can respond to situations quickly. However, we advise to be cautious with wholesale reliance on “thresholds” per se. ACER and some NRAs have specifically refused to give threshold indications and have emphasised that each situation requires individualised assessment. Market participants who work with operational thresholds ought to be mindful to differentiate between a threshold suitable to normal market conditions versus a strained market situation in which much lower limits could affect market prices.

In addition, a clear description of the process of identifying inside information and the point in time when it arises, should be implemented. This should also include descriptions on how to handle cases where it is uncertain whether a specific set of information constitutes inside information or not.

3.1.2. Handling of inside information

REMIT has a specific prohibition of spreading inside information to any other person, unless it is made in the normal course of employment, profession or duties, and a specific prohibition of trading based on inside information. This implies that inside information must be kept confidential, both externally and internally.

A market participant may receive inside information on different levels:

- Information related to **the market participant's own company** where the market participant is solely responsible for publication of the information

- Information related to **other market participants** where the market participant is not responsible for publishing the information

- Information related to **co-owned companies**, **co-operating companies, joint ventures** etc. where market participants share the responsibility for publication of inside information

Market participants are recommended to have measures in place for protection of inside information in all cases regardless of the origin of the information and of which market participant the information relates to.

How to ensure confidentiality of inside information until it is published to the market will differ between market participants. However, some general advice will be given in the following.

Internal Instructions/guidelines

Guidelines and clear instructions are key when dealing with inside information. Market participants are recommended to make sure to have proper written guidelines and instructions on how to deal with inside information. The instructions may contain:

- List of functions authorised to routinely receive inside information

- Specification of responsibilities for handling inside information

    - There should be a dedicated team responsible for publishing inside information

- Specification on how to handle inside information
    - Internal communication process with definition of the point in time the information arises
    - Not spread to any unauthorised personnel prior to publication
    - No advice shall be given based on inside information
    - Not used for trading
    - What to do if you receive inside information by accident e.g. from a third party

- Facilitate publishing of inside information

Information barriers/Chinese Walls

Above is a description of possible procedures and routines that ensures that inside information is kept within a specific group, which means that no one outside the specific group can gain access to the information.

However, it may also be important for the market participant to arrange for a certain group, especially traders, to be excluded from access to inside information in order to ensure that no trade stops would be required because of leaks of inside information, or the number of trade stops would be kept to a minimum.

This arrangement aims at preventing information from reaching the trading environment and is strongly recommended if the market participant wants to continue trading when possessing inside information.

If the market participant wants to continue trading when holding inside information, it is recommended to include the following:

- It should be ensured that persons involved in trading are not authorised to gain access to inside information prior to publication.

- Traders should be physically separated from any persons authorised to gain access to inside information.

- If the personnel handling inside information is situated in the same building as traders, additional measures may be necessary to document that inside information is not accessible to traders, e.g. access controls to the trading desk with logging.

If trading while holding inside information, the need for additional checks and detection work of the compliance function increases, and it is recommended that regular compliance checks are executed to detect possible weaknesses in the information barrier/Chinese Walls.

There is no clear definition of an information barrier/Chinese Walls and how to implement it efficiently. The crucial point is to have sufficient routines and documentation to ensure that the barrier is effective and serves its purpose.

IT-systems

It is essential when setting up measures to protect inside information to ensure that sufficient restrictions are implemented in the relevant IT systems. This may include:

- Documentation of which systems may contain inside information and who has access to these systems

- Ensure that unauthorised personnel cannot gain access

- Training, clear restrictions and clear instructions for relevant IT personnel may be considered depending on the market participant's IT-structure and size

Third party inside information

In some cases, market participants may receive inside information from third parties, for example information from TSOs that affects or could affect the market participant, or information from an up-river production unit. According to REMIT, a market participant is only required to publish information if it relates to the participant's own business[4]. It is therefore critical to be able to correctly assess if the information is correct, and whether the market participant is obliged to publish the information or not. If it is concluded that the information is inside information, but not related to the market participant but a third party, the following may be done:

- Protect the information. In particular, prevent information from being used in trading, and ensure that it can be documented how the information has been handled.
    - Prevent the information from reaching the trading floor.
    - If a trader on the trading floor receives inside information: he/she should immediately leave the trading floor to ensure that no trading is done, and that the information is not spread to others. It is recommended to immediately contact compliance who can consider further actions.
    - Consider if it is necessary to stop relevant trading based on, or having a connection to, that information.

- Contact the owner of the information to ensure that the information is published or will be published. For publication of third party inside information see chapter 3.1.4 (Situations where there are multiple market participants responsible for publication of information).

- In specific situations, it may also be possible to contact the TSO to agree with them that the market participant can trade while holding inside information according to the exemption in REMIT Article 3.4 (b) – see also chapter 3.1.3 under "Exemptions".

[4] By own business is meant: "in respect of business or facilities which the market participant concerned, or its parent undertaking or related undertaking, owns or controls or for whose operational matters that market participant or undertaking is responsible, either in whole or in part" – REMIT Article 4

Confidentiality agreements for external contractors

It is recommended to implement confidentiality agreements with external contractors when such are involved in for instance building of new production facilities or involved in other processes where they might gain inside information. It is then essential to ensure that they are aware of what kind of information to keep confidential.

3.1.3. Measures to prevent insider trading

Market participants must have implemented routines to prevent the use of inside information when trading. A part of this is to have awareness training and internal instructions to avoid breaches of the prohibition against insider trading.

Mapping of products/markets relevant to different types of inside information

The prohibition against insider trading relates to trading based on inside information. This means that it is allowed to trade other wholesale energy products when holding inside information, provided that the inside information does not relate to the product traded. Consequently, it is important that the traders are certain that the respective information is not related to the product(s) traded.

For instance, if there is a planned maintenance at a power plant in the future, and it is unlikely that this information could be relevant for day-ahead or intraday products (not likely to significantly affect the prices of the relevant wholesale energy products), it should not be necessary to stop trading. However, allowing for trading while holding inside information may constitute an additional risk for the market participant, and it is therefore recommended to have clear instructions and routines for how to conduct such trading to avoid any unintentional or intentional abuse. It should be included in the internal guidelines if and when the market participant allows trading when holding inside information, including procedures (approval requirements) and documentation requirements.

It is recommended to map all products and markets relevant for different types of inside information the market participant may hold.

Tracking of information

It is important for a market participant to be able to track who has had access to inside information and at what point in time. This is especially important if a market participant wishes to allow trading in related products while the market participant itself holds inside information and where traders do not have access to the inside information. One way to mitigate this inherent risk is to ensure that safeguards are in place. Measures may include, among others, the following:

- Record telephone conversations of relevant staff (e.g. traders)
- Map the flow of inside information and include a log of staff/employees who have received the information and the date/time when they received it
  Document the setup and functionality of relevant information barriers (Chinese walls) around the information flow
- Establish periodic/systematic checks over the above procedures, document how any incidents have been handled, and what the market participant has done to remedy the situation as well as to make the procedures more robust.

Being able to document how inside information has been handled is of the utmost importance in the event an NRA or the market surveillance department of a PPAT wishes to investigate. A market participant must be able to demonstrate that its procedures were resilient enough not to allow trading on inside information.

Information barrier/Chinese walls around traders

To create information barriers/Chinese walls around traders is another measure for protecting the inside information to be used when trading. Please refer to the information above regarding “Tracking of information”.

Trade-stop

There is always a risk that traders get access to inside information. Thus, even if the market participant has organised information barriers, a trade-stop mechanism may be necessary in case the information barriers are not effective. Trade-stop and similar prevention measures should also be put in place if information barriers have not been implemented and traders can have access to inside information.
The trade-stop mechanisms may be manual routines, where the relevant trader leaves the trading floor and informs the manager (without explaining the reason) and compliance (explaining the reason) that he/she has become an insider and not being allowed on the trading floor before approved by compliance. More structured measures may also be implemented. These are some examples of trade-stop mechanisms:

- Alarm/light that is manually switched on when in possession of inside information, or potential inside information, with instructions in the internal guidelines only to switch off the alarm/light when the information is assessed and deemed not to be inside information, or when inside information has been published

- Push-notifications by phone call, SMS and/or e-mail with instructions to stop trading

- IT-systems that prevents traders from doing anything in the trading system whilst in an insider position or a potential inside position

Documentation need: It is recommended that the routines for trade stop are documented, including when the alarm/lights goes off, who has triggered the alarm if in use, and when the alarm/lights have been switched off again. It may also be relevant to include documentation of to whom, or to which products, the trade stop applies. Regardless of which measures the market participant has implemented, it should be documented how to ensure that inside information is not used in trading.

Exemptions

There are some exemptions from the prohibitions against insider trading. One exemption is set out in Article 3(4)(b).

> 4. This Article shall not apply to:
> (b) transactions entered into by electricity and natural gas producers, operators of natural gas storage facilities or operators of LNG import facilities the sole purpose of which is to cover the immediate physical loss resulting from unplanned outages, where not to do so would result in the market participant not being able to meet existing contractual obligations or where such action is undertaken in agreement with the transmission system operator(s) concerned in order to ensure safe and secure operation of the system. In such a situation, the relevant information relating to the transactions shall be reported to the Agency and the national regulatory authority. This reporting obligation is without prejudice to the obligation set out in Article 4(1);

Text box 12 REMIT Art. 3(4)(b) Exemption from the prohibition against insider trading

It is an opening to trade whilst holding inside information to cover immediate physical loss. It is unclear in what situations this exemption is valid and safe to use, and it is recommended to be careful when using this exemption, and to consider alternative approaches to cover the loss instead of through trading when holding inside information.

If the exemption is to be used, the following measures should be taken in advance to reduce the risk of breaching REMIT:

- Analyse and list in which situations the exemption may be used

- Include in the internal guidelines, if use is possible for the relevant market participant and the relevant business units. If possible, to use and in case of exceptional use, Compliance should be involved as soon as possible

- Have clear instructions on how and when to report to ACER and the NRA when the exemption is used. Consider whether the market surveillance department of the affected PPAT(s) should be informed as well.

- The report should be given through the notification platform provided by ACER
    - Contact persons and details should be decided beforehand
    - A copy of the notification should be taken before submitting the form to ensure that the content of the report is documented
    - The receipt received from the notification platform should be kept

According to REMIT, the exemption can only be used if one of the below requirements are fulfilled:

"- where not to do so would result in the market participant not being able to meet existing contractual obligations; or
- where such action is undertaken in agreement with the TSO(s) concerned in order to ensure safe and secure operation of the system."

It is recommended that the requirement that forms the grounds for claiming the exemption is documented. It should also be documented that the requirement is fulfilled.

3.1.4. Publication of inside information

Inside information in accordance with REMIT Article 4 should be published in an effective and timely manner following the ACER Guidance. All market participants are recommended to develop and implement guidelines and procedures for publication of inside information. It is important to know that all market participants could be in a position where they must publish inside information even though they do not have any physical assets. All market participants trading in the physical market are recommended to be prepared for publishing information to the market. This implies having i.e. instructions or agreements, training and access to a UMM reporting system in place.

It is generally recommended to publish inside information on an inside information platform (IIP). This is in line with the latest update on ACERs Guidance on the application of REMIT (updated 16th July 2019). An IIP makes all the individual inside information from each market participant available on a central platform and thus, improves the transparency in the market.

Different functions within the market participant can be responsible for publishing inside information:

- Trading desk
- Dispatch centre/control centre
- Production/consumption site
- Other departments within the market participant
- Outsourced to a third party

The determination of the responsible person or function may depend on the size and set-up of the market participant. It is essential that the responsibilities and procedures are clear and included in the internal guidelines.

As a general principle, it is advisable that the persons sitting closest to the information are responsible for the publishing. However, this should be weighed against the challenge of ensuring that they have the necessary insight and competence to be able to effectively fulfil the requirements for effective and timely publication pursuant to REMIT.

Market participants having many power plants often find it beneficial that inside information is published by the central dispatch centre as this allows for building a stronger competence amongst the persons responsible for publishing. Large power plants may arrange the information to be published directly from the plant. This may allow for faster publication and can also reduce the number of persons involved, and thereby the risk of market abuse. The optimal solution may differ from market participant to market participant and must be assessed on an individual basis.

Further, publishers should have sufficient training to ensure that publication can be executed according to the regulation. Regular use of a test environment to practise the publication may be considered.

In all cases, it is recommended to include in the internal guidelines or to have separate guidelines containing the following:

- It should be defined where the market participant publishes inside information and which tools to use

- Specific instructions on what kind of information the publication should contain in different situations
    - Many market participants have developed “templates” with standard wording to be used in various specified situations
    - Include at least information as stated in the ACER Guidance

- It should state alternative procedures in case of any issues with the system used for publication

- Routines should be in place to ensure that inside information is published as soon as possible, and at the latest within one hour

- Routines should be in place to keep track on messages published to the market, any updates to the messages, and routines on how to ensure that messages at all times are up to date

Exceptionally delay publication of inside information

The obligation to publish inside information contains a requirement that it shall be published in an effective and timely manner. In respect of timely manner, the ACER Guidance refers to as close to real time as possible with an hour time limit. However, there could be some occasions where it might be relevant to delay the publication. One potential example of this could be a situation where permanent shutdown of a production/consumption site is planned, and there is a need for a HR-process for affected employees. Another example could be in a situation where safety must be given priority over publication. These are only examples, and their compliance with REMIT has to be assessed on a case by case basis. In REMIT Article 4(2), there is an opening for delaying the publication of inside information:

> 2. A market participant may under its own responsibility exceptionally delay the public disclosure of inside information so as not to prejudice its legitimate interests provided that such omission is not likely to mislead the public and provided that the market participant is able to ensure the confidentiality of that information and does not make decisions relating to trading in wholesale energy products based upon that information. In such a situation the market participant shall without delay provide that information, together with a justification for the delay of the public disclosure, to the Agency and the relevant national regulatory authority having regard to Article 8(5).

Text box 13 REMIT Article 4(2) Delay public disclosure of inside information

A best practice approach to handle such a situation is:

- To ensure that necessary processes and procedures are implemented in advance so that compliance can be ensured when it is decided that information should be delayed

- Documentation of who has access to the information when
  - Drafting insider lists
  - Ensuring confidentiality

- Inform ACER and the relevant NRA(s) about the delayed publication
  - Use the reporting solution on the ACER platform

- Ensure that no information reaches trading personnel, or alternatively, stop trading

Situations where there are multiple market participants responsible for publication of information

Situations where several market participants are responsible for publishing inside information may occur when:

- there are several owners of a production/consumption facility/company
- when publication is outsourced to a third party
- where the owner/operator are not the same legal party/entity
- where the balancing responsibility has been allocated to another party
- the production/consumption facility is affected by work on the transmission network

If more than one market participant has a responsibility to publish the inside information, they can publish the information separately, or they can coordinate the publication. If published separately, there is a significant risk of ending up in a situation where the information is not published identically which could lead to significant challenges. Therefore, it is best practice in such situations to coordinate the publication, typically by having one party publishing on behalf of all responsible parties.

It is important to be aware that it is not possible to outsource the legal responsibility of publishing inside information, regardless of how the agreement is constructed. It is therefore recommended to have good routines to ensure that the party who is publishing information on a market participant's behalf has sufficient knowledge (be aware that a third-party publisher might not have an advanced level of knowledge of the market participant's facilities), competence and routines to be able to fulfil the publication obligation.

The parties are recommended to enter into a written contract where rights and responsibilities of each party are clearly defined. Explicit courses of actions and contact persons may also be described in the agreement.

An agreement to outsource the task of publishing inside information should always include the right for the owner of the information to publish the information himself if they consider this necessary in fulfilling their obligations. This may be relevant for situations where the parties do not agree on whether a certain information shall be published or not.

A best practice approach when others publish information on your behalf, is to monitor the information published and continuously assess the need for changes in the procedures or the agreement.

In cases where publication is outsourced to a third party which does not have a separate responsibility to publish the information according to REMIT, further measures may be considered, i.e. as requiring that the market participant has internal controls or requiring documentation to be available in the event of a request from an NRA.

In cases when a production/consumption facility is affected by work on the transmission network, it is the responsibility of the transmission network owner to publish inside information related to the transmission network. The owner of the production/consumption facility could consider contacting the transmission network owner to clarify who will publish a UMM. If the transmission network owner does not publish that information, but the owner of the production/consumption facility considers it inside information, it is considered best practice that the owner of the production/consumption facility publishes a UMM focusing on the consequence for its own assets. Such a UMM would typically be of the type “Other Market Information”. The message should not provide detailed information on the work on the transmission network or the facilities not owned by the publisher to reduce the risk of publishing erroneous information.

To handle inside information publication in cases where there are several owners involved may be challenging. There might for instance be multiple companies participating in board meetings or operational meetings where inside information needs to be discussed. It is therefore important that the co-owners have instructions or guidelines on how to handle inside information or possible inside information, including who is responsible for publication on behalf of the owners to ensure effective and timely publication and to avoid multiple and potentially inconsistent publications which could mislead the market.

CHECKLIST INSIDER TRADING

- Identifying inside information
    - A process for identifying inside information
    - Risk assessment – what are the risks for the company?
    - Specification of possible inside information
- Handling of inside information
    - Routines for protecting inside information
        - May include also contracts with external companies, such as contractors/suppliers
    - Routines for handling cases when receiving inside information that does not relate to your own business or assets
- Measures to prevent insider trading
    - Tracking of information
    - Information barriers/Chinese walls
    - Trade stop
    - Specific routines related to usage of exemptions from the prohibition of insider trading
- Routines for publishing inside information
    - May include routines for delayed publication
    - If relevant should also include handling of situations where more than one company is responsible for publication

3.2. Market manipulation

The aim of this chapter is to point out measures market participants should consider including in their compliance regime to ensure compliance with REMIT with respect to market manipulation. The starting point is the overall compliance regime, including the compliance programme and compliance plan as described under section 2 and special attention should be given to chapter 3.3 when using algorithmic trading solutions. As already mentioned, there is no “one-size-fits-all” solution, and each market participant must tailor their compliance regime accordingly. Regardless of the type and size of the market participant, all market participants should have clearly documented internal policies and guidelines on how to prevent market manipulation. Another important point is to have robust documentation routines to be able to evidence the compliance plan in event of an inquiry from NRAs or the market surveillance department of a PPAT.

‘market manipulation’ means:

(a) entering into any transaction or issuing any order to trade in wholesale energy products which:
  (i) gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of wholesale energy products;
  (ii) secures or attempts to secure, by a person, or persons acting in collaboration, the price of one or several wholesale energy products at an artificial level, unless the person who entered into the transaction or issued the order to trade establishes that his reasons for doing so are legitimate and that that transaction or order to trade conforms to accepted market practices on the wholesale energy market concerned; or
  (iii) employs or attempts to employ a fictitious device or any other form of deception or contrivance which gives, or is likely to give, false or misleading signals regarding the supply of, demand for, or price of wholesale energy products;

  or

(b) disseminating information through the media, including the internet, or by any other means, which gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of wholesale energy products, including the dissemination of rumours and false or misleading news, where the disseminating person knew, or ought to have known, that the information was false or misleading.

[…]

Text box 14 REMIT Article 2(2) Definition of Market Manipulation

The definition of market manipulation is found in REMIT Article 2. In general terms, market manipulation can happen either through orders and transactions in wholesale energy products or through disseminating information in any way that could give false or misleading signals.

Prohibition of market manipulation

Any engagement in, or attempt to engage in, market manipulation on wholesale energy markets shall be prohibited.

Text box 15 REMIT Article 5 Prohibition of Market Manipulation

REMIT Article 5 prohibits market participants in the wholesale energy market to manipulate the market. The ACER Guidance provides examples and interpretations of the definition of market manipulation. How to interpret REMIT is found in the ACER Guidance and is not described in this report. The report discusses possible approaches on how to be compliant with the interpretation of REMIT found in the ACER guidance.

Common causes for market manipulation include:

- Intentional manipulation to increase profits
- Unintended or negligent manipulation
  - Unawareness of what is prohibited
  - Technical or human errors
- Spreading information
  - Insufficient or wrong information

It is recommended to implement procedures to address the above listed causes. In the following, measures are divided in three categories:

i) General measures to prevent market manipulation; chapter 3.2.1
ii) Measures to prevent market manipulation through orders and transactions; chapter 3.2.2
iii) Measures to prevent market manipulation through spreading false or misleading information; chapter 3.2.3

3.2.1. General measures to prevent market manipulation

Market participants should implement measures to **reduce the risk of employees manipulating** the market, including control measures as described in section 2. Some measures to avoid both intentional and unintentional market manipulation include risk assessment and awareness training. The most important step to prevent market manipulation is to ensure that the employees are **aware** of what kind of behaviour could be manipulative. All market participants should have mandatory trainings for traders as described in section 2. These should also include training on

specific market manipulation scenarios. Another important step to prevent market manipulation is to conduct a market abuse risk assessment as described in section 2. For market manipulation, the risk assessment should be based on all types of market manipulation described in the ACER Guidance on REMIT and the separate guidance notes on specific market abuse types[5]. In addition, it should be considered whether other types of manipulation are relevant.

3.2.2. Measures to prevent market manipulation through orders and transactions

Specific measures aiming at preventing market manipulations through orders and transactions are addressed below.

Documentation procedures; documentation of trading mandates

It is important to have good documentation procedures on all implemented measures. The level of details should be proportionate and not unreasonably burdensome. It is recommended that traders should have a clear mandate and clear instructions on how to trade, where the risk of manipulating the market is taken into consideration. The mandates should be documented. It is recommended that market participants document deviations from the trading mandate.

In case of any investigations either internally, from NRAs or PPAT's it is important to have diligent routines regarding documentation of the trading mandates. In addition, it is advisable for the traders themselves to document their behaviour in situations where they enter into, or have entered into, unusual or exceptional transactions or made unusual or exceptional profit/loss, or if there have been other unusual or exceptional situations or market conditions that may attract the interest of regulatory authorities and/or the market surveillance department of PPAT(s). In such cases, the market participant may benefit from being able to document the background for their behaviour. Such unusual or exceptional circumstances could be:

- High/low prices
- Exceptional deals by any measure
- A profitable trade before important information is published
- Trades outside the standard or common spread

Sufficient documentation is important to be able to explain transactions and relevant circumstances in case of investigations. Compliance should have full access to such documentation.

[5] For the time being Guidance Note 1/2017 on wash trades, 1/2018 on transmission capacity hoarding and 1/2019 on layering and spoofing.

Internal instructions and procedures

Instructions and procedures on what a trader can and cannot do should be developed and communicated to all relevant personnel. This should be **dynamic** and updated when there is any new development internally or externally in the market.

Routines to prevent errors when trading

A risk for market participants trading in the wholesale energy market is the risk of **trading errors**. When trading in the wholesale energy market, errors, for instance when placing orders, can have significant impact on the market and may constitute market manipulation. Market participants are therefore recommended to have routines and procedures in place to prevent unintentional and negligent manipulation.

The measures implemented may differ depending on the business of the market participant and the nature of the product traded. For example, the day-ahead auction, where orders are placed just once a day, and where errors may have a very large market impact, may require specific measures that are not needed in a continuously traded market.

Internal controls should be in place to ensure that all orders placed are correct. This could be automatic alarms/checks, manual checks or a combination of these. Some exchanges offer the flagging of self-trades in line with the description of best practices in Chapter 5 in ACER's guidance on wash trades. Such a functionality may be used to reduce the risk of sending false or misleading signals to the market when performing self-trades.

Some examples for day-ahead auction trading that could be implemented:

- Compare orders with previous day's orders
- Check whether the orders placed equal the orders in your internal system
- Four-eyes principle: the orders may be checked by another person before submitting them
- As far as possible avoid manual steps (copy/paste) in planning /bidding process in order to avoid human mistakes
- Submit "safety bids" for at least d+2 in order to always have a bid in case of IT- or other disturbances
- Check that orders are logical, i.e. that fields contain values or that purchase volumes are not increasing with increased price
- Automatic alerts, for instance if the orders deviate significantly from normal

- After the auction
    - Check whether the result corresponds with the expected result – production plan

Typically, not all the measures above will be relevant for all market participants.

Specific issues to be aware of

It is recommended that the market participant develops a specific list of behavioral issues to be aware of to avoid market manipulation. Such a list can be helpful in exemplifying what the market abuse prohibition means in practice. Below are some examples of issues that may be included in such a list:

- Never coordinate trading activities or discuss pricing strategies with other market participants – no cooperation or attempt of cooperation or information sharing

- There should be a real desire to trade behind all orders – never place an order designed not to be executed

- Do not place orders with the intention of affecting reference prices

- Consider how you offer your available capacity into the total market
    - Even if not all available capacity is offered in every market segment, it is recommended that the total available capacity is always offered in all market segments combined, unless there is a legitimate reason for not offering all available capacity.

- Ensure that publication of information is always correct

- Ensure that orders placed are always correct

3.2.3. Measures to prevent market manipulation through spreading false or misleading information

In addition to manipulating through orders and transactions, market manipulation can also happen through **spreading false or misleading information**. This type of manipulation can be done by a much wider group than just traders and separate measures are therefore required.

It is important to ensure that **inside information is published correctly** to the market. Wrong or misleading inside information may be considered market manipulation (and not only a violation of the requirement to publish inside information in an effective and timely manner). If a mistake is discovered in a published UMM and

such mistake is REMIT relevant, a correction should be published as soon as possible. For inside information and publication of inside information see section 3.1.

In principle, anyone within a market participant may spread false or misleading information to the market. To mitigate the risk of this happening, some measures could be relevant:

- A policy on how to handle communication with the media
    - Only authorised persons can communicate with the media, for instance:
        - Communication personnel
        - Management
        - Board of directors
        - Others
    - Processes to ensure that information is correct and precise
        - Do not spread rumours

- Relevant persons should have specific awareness training to ensure that they do not send false or misleading signals

- A policy for staff on information given in social media and other for a

SPECIFIC MEASURES TO AVOID MARKET MANIPULATION

- General
    - Risk assessment and awareness training
        - Based on business model and trading activities
        - Should as a minimum include all types of market manipulation in the ACER Guidance
        - Other types of manipulative behaviour
    - Trading mandates
        - Develop and document
        - Mandate for traders
    - Instructions and procedures
        - Dynamic Q&A

- Negligent or unintentional market manipulation
    - Routines to prevent erroneous trading

- Spreading false or misleading information
    - Ensure routines to secure the quality of inside information published
    - Policy on communicating with the media
    - Policy for employees on social media/fora etc.

3.3. Algorithmic trading solutions

3.3.1. Background

The starting point for this chapter, similar to the previous chapters on inside information and market manipulation, is the compliance regime described under section 2. The aim of this chapter is to discuss and recommend a governance model around algorithmic trading[6] of wholesale energy products to ensure compliance with REMIT.

It is important to highlight that other and stricter requirements may exist for algorithms that trade in wholesale energy products, but fall under financial regulation, compared to the recommendations in this chapter. These algorithms should comply with requirements set out under the recast of the directive on markets in financial instruments (MiFID II) as well as other relevant financial regulation.

While neither REMIT nor any of ACER's guidance currently set out specific requirements for algorithmic trading solutions, REMIT does contain general market abuse prohibitions. There is therefore an implicit expectation that any algorithm deployed by a market participant is subject to robust governance such that it neither abuses the market nor creates disorderly conditions.

By contrast, MiFID II stipulates specific and detailed requirements for trading venues and firms to implement in relation to algorithmic trading. These requirements came into force in January 2018. In addition, ESMA developed various regulatory technical standards (RTS), one being RTS 6 with the background in MiFID II Art. 17.

In its REMIT Quarterly Q4/2018, ACER discusses the possibility to apply best practices from financial regulation to wholesale energy markets. This chapter is based on the same idea and uses MiFID II as inspiration and a starting point for a best practice governance model around algorithmic trading. The Articles of RTS 6 cited in textboxes throughout this section are for information only. The content of RTS 6 is reviewed and the measures that we consider relevant for the purpose of this report are discussed in the text of the respective sections[7]. It is, however, important to balance the level of governance around the trading activity of algorithms with the risk of creating a regulatory barrier to entry (especially for smaller- and medium-sized market participants).

---

[6] The terms "algorithmic trading solution", "algorithmic trading" and "algorithm" will be used interchangeably in this chapter.

[7] This report does not repeat all the requirements for algorithmic trading under the financial regulation as these can be found directly in the regulation. If a specific article is not mentioned and the content of that article is neither discussed, then the authors of this report did not consider the provision relevant for the current state of the wholesale energy market (for example Chapter III on "Direct Electronic Access" or Chapter V on "High-Frequency Algorithmic Trading Technique and Final Provisions").

We believe that each market participant is best placed to assess the compliance risks that it faces when introducing algorithmic trading and to design a compliance regime that in an appropriate manner addresses those risks, taking into account the size and complexity of the algorithmic trading activity. We would like to state again, that there is no “one-size-fits-all” approach.

3.3.2. Definition of algorithmic trading

Definition of algorithmic trading according to MiFID II:
‘Algorithmic trading’ means trading in financial instruments where a computer algorithm automatically determines individual parameters of orders such as whether to initiate the order, the timing, price or quantity of the order or how to manage the order after its submission, with limited or no human intervention, and does not include any system that is only used for the purpose of routing orders to one or more trading venues or for the processing of orders involving no determination of any trading parameters or for the confirmation of orders or the post-trade processing of executed transactions.

Text Box 16 from MiFID II Art. 4 point 1 (39)

Definition of algorithmic trading according to REMIT Quarterly Q4/2018:
Algorithmic trading is trading with limited or no human intervention that is based on a computer algorithm automatically determining individual parameters of orders.

Text Box 17 from REMIT Quarterly Q4/2018

ACER used a shortened version of the definition of algorithmic trading in MiFID II in the REMIT Quarterly Q4/2018. We find it natural to use the definition provided by ACER when discussing algorithmic trading on wholesale energy markets. It is, however, our understanding that ACER’s definition is not to be considered broader than the definition in MiFID II. Similar to MiFID II, we, for example, do not assess a system, that is only used for the purpose of routing orders to one or more trading venues, as algorithmic trading.

The table below briefly describes two examples to clarify how we understand the line between algorithmic and non-algorithmic trading. Firms should however assess their use of trading strategies on a case by case basis in order to determine whether they use algorithms to ensure proper governance:

Algorithmic trading	Non-algorithmic trading
Any computer program that reacts to any market signal(s) and decides, based on pre-defined parameters or machine learning, whether to initiate an order, the timing, price or quantity. For example, a computer program that provides liquidity on both buy and sell side. The algorithm may choose to update the offered spread based on e.g. trading behaviour of other market participants. It may also choose to insert new orders when an active order gets filled. It reacts, thus, to market signal(s) and decides whether to initiate an order and at which prices.	Iceberg orders and other order types provided by the trading venue do not qualify as algorithmic trading by the market participant. Based on the Q&A by European Securities and Markets Authority (ESMA)[8]: • The use of algorithms which only serve to inform a trader of a particular trading opportunity is not considered as algorithmic trading, provided that the execution is not algorithmic.

MiFID II requires firms to notify competent authorities about the usage of algorithms[9]. It mentions further the need to identify orders generated by algorithmic trading[10]. Several market participants have already started to use algorithmic trading solutions and we are of the opinion that it is not necessary to notify regulatory authorities of such usage unless it is required by law or a clearly stated wish by the regulators.

It should, however, be considered good practice to be able to identify which orders and transactions are generated by an algorithm. This can be done in the internal records kept by each market participant, but the best practice approach would be to make this identification available to the trading venues as well as ACER and regulators. One possible solution could be to use a data field that is already today reported under REMIT, e.g. the Data Field No (3) “ID of the trader” (according to TRUM[11]) as identified by the organised market place (e.g. “IDAPI_Algo_Powertrading_01”). This is, however, dependent on the technical solutions provided by the trading venue.

The identification of orders placed by algorithm(s) is also a prerequisite for the effective use of the kill-functionality (see further details regarding the “kill functionality” in chapter 3.3.7 on “Post-deployment management”).

[8] Q&A on Market Structure Issues: Part 3 (Question 7) https://www.esma.europa.eu/file/50174/download?token=8LnokgxS

[9] MiFID II Art. 17 point 2

[10] MiFID II recital point 67

[11] Transaction Reporting User Manual by ACER

3.3.3. General organisational requirements

RTS 6 specifies the organisational requirements of firms engaged in algorithmic trading and starts by setting out general organisational requirements.

Art. 1

(a) clear lines of accountability, including procedures to approve the development, deployment and subsequent updates of trading algorithms [..]

(b) effective procedures for communication of information […] such that instructions can be sought and implemented in an efficient and timely manner

(c) *a separation of tasks and responsibilities of trading desks on the one hand and supporting functions, including risk control and compliance functions, on the other.*

Art. 2 (1):
An investment firm shall ensure that its compliance staff has at least a general understanding of how the algorithmic trading systems and trading algorithms of the investment firm operate.

Art. 3 (1):
An investment firm shall employ a sufficient number of staff with the necessary skills to manage its algorithmic trading systems and trading algorithms and with sufficient technical knowledge of:

(a) the relevant trading systems and algorithms;
(b) the monitoring and testing of such systems and algorithms;
(c) the trading strategies that the investment firm deploys through its algorithmic trading systems and trading algorithms;
(d) the investment firm's legal obligations

Art. 14 (1):
An investment firm shall have business continuity arrangements in place for its algorithmic trading systems which are appropriate to the nature, scale and complexity of its business.

Art. 18 (1) and (2):
An investment firm shall implement an IT-strategy.
[…]
An investment firm shall set up and maintain appropriate arrangements for physical and electronic security.

Text Box 18 with excerpts from RTS 6

It is best practice to establish a clear and formalised governance model with clear lines of accountability and effective procedures for communication of information in line with Article 1 of RTS 6.

With regards to the separation of responsibilities of trading desks and supporting functions, we would like to reiterate our recommendation from point 2.1.3 above: dependent on the size and complexity of the market participant's algorithmic trading activities it is advisable to have a department or at least one person responsible for compliance with REMIT. The responsibility of compliance may also be one part of the tasks of one employee, if sufficient independence can be achieved.

The market participant should in any case have sufficient staff who have the necessary skills and technical expertise to be able to fulfil their assigned tasks. That implies that every staff member, that plays a more than marginal role in the lifecycle of a trading algorithm, should have a general understanding of how the algorithm works. Some staff members will of course have a more expert knowledge on certain aspects, for example developers on the exact technical implementation of the trading strategy. Compliance and Risk functions may not have to have the same expert knowledge as developers, but they need to understand the algorithm well enough in order to be able to challenge the developers on the practical implications of the algorithm.

Similarly, relevant staff should have the necessary understanding of REMIT with special attention to the prohibitions against insider trading and market manipulation. This is of particular importance in the design phase of the algorithm (see chapter "Design recommendations").

Further, the market participant should also ensure that it is adequately staffed with employees who have the required technical skills to manage its trading systems and algorithms on an ongoing basis (see further details in chapter 3.3.8 on "Monitoring").

Each market participant is best suited to decide on the exact governance model (including the need for business continuity arrangements and a separate IT-strategy), but it is advisable and recommended to ensure on an ongoing basis that the algorithmic trading solutions are at all times fit-for-purpose. This means, as a minimum, that the market participant can at all times withdraw an algorithm from the market (see further details regarding the "kill functionality" in chapter 3.3.7 on "Post-deployment management") and that the market participant should decide and document which persons have access rights to deploy an algorithm and change the coding/trade parameters of the algorithm(s).

3.3.4. Design recommendations

Art. 12 (1):
An investment firm shall be able to cancel immediately, as an emergency measure, any or all of its unexecuted orders submitted to any or all trading venues to which the investment firm is connected ("kill functionality").

Art. 15 (1):
An investment firm shall carry out the following pre-trade controls on order entry for all financial instruments:
(a) price collars […]
(b) maximum order values […]
(c) maximum order volumes […]
(d) maximum message limits […]

Art. 15 (3):
An investment firm shall have in place repeated automated execution throttles which control the number of times an algorithmic trading strategy has been applied.

Art. 17 (2):
Post-trade controls […] shall include the continuous assessment and monitoring of market and credit risk of the investment firm in terms of effective exposure.

Text box 19 with excerpts from RTS 6

During the entire design phase (from concepting to technical implementation), the involved staff members should be aware and have a thorough understanding of the market abuse prohibitions in REMIT (i.e. Art. 3 on insider trading and Art. 5 on market manipulation). This can be ensured through appropriate training sessions on relevant market abuse types.

It is considered best practice to assess how the proposed trading strategy will affect the market. Additionally, market participants should assess whether the combination of the different trading strategies may send false or misleading signals to the market.

Moreover, market participants should have the ability to immediately stop any trading activity by an algorithm. This should be achieved by a kill functionality, as required in RTS 6 (see further details regarding the kill functionality in chapter 3.3.7 on "Post-deployment management"). An extra feature could include a suspend functionality. The suspend functionality would only stop new order and trade activity by the algorithm but leave all unexecuted orders in the market. This may be less disruptive to the market and the preferred option under certain circumstances.

In terms of trade parameters, the description of pre- and post-trade controls in Art. 15 and Art. 17 of RTS 6 may include relevant controls, but it is important to remember that there could be other, more suitable controls not mentioned in Art. 15

or Art. 17 of RTS 6. Dependent on the algorithm's trading strategy and complexity, some controls may be more relevant than others. Market participants should carry out a separate assessment of each algorithm and decide which controls to implement. This assessment may differ from algorithm to algorithm.

In addition, an order-to-trade ratio rule, that is built directly into the algorithm, may be a beneficial safeguard. This could limit unintended trading activity by the algorithm, for example when interacting with another algorithm that follows a similar (or opposite) trading strategy.

Furthermore, each market participant should carefully assess what information or analytic input an algorithm is using and if any of the data could be considered inside information according to REMIT, e.g. maintenance data or data on unplanned outages.

The prohibition against insider trading relates to using inside information when trading. It is then natural to assume that if an algorithm does not take potential inside information into account, the information is not used in trading. Market participants should in any case assess how the measures to prevent insider trading (see chapter 3.1.3 above) have to be adjusted when introducing algorithmic trading.

In general, the following is recommended:

- Record clear documentation on what information the algorithm uses and what information it does not use.

- Define a standard approach on how to handle active trading algorithms when inside information reaches the trading floor, but not the algorithm. If the algorithm continues to trade, the market participant should be able to document that the algorithm did not use the inside information. The market participant should further document if the kill-functionality is enabled during such a situation. This might be necessary if the algorithm starts to deviate from the expected behaviour or starts to contribute to disorderly trading conditions during a trade stop for the trading desk.

- As stated above, each algorithm should be designed in a way that it does not use information or analytic input that could, at any point in time, contain inside information. In the case of unforeseen circumstances, it is, however, recommended to define a standard approach on how to handle situations when the input data to the algorithm does in effect contain inside information.

3.3.5. Test process

Art. 5:

(1) Prior to the development or substantial update of an algorithmic trading system, trading algorithm or algorithmic trading strategy, an investment firm shall establish clearly delineated methodologies to develop and test such systems, algorithms and strategies.

[…]

(4) […] 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*

Art. 6 (1):

An investment firm shall test the conformance of its algorithmic trading systems and trading algorithms with:

(a) The system of the trading venue […]

Art. 7 (1):

An investment firm shall ensure that testing […] is undertaken in an environment that is separated from its production environment and that is used specifically for the testing and development of algorithmic trading systems and trading algorithms.

Text box 20 with excerpts from RTS 6

Market participants should do two types of tests when developing new trading algorithms or making material changes to existing ones:

1) Conformance testing to ensure compatibility with the systems of the respective trading venue
2) Testing of trading activity to ensure that the algorithm behaves as intended.

Similar to the requirement in Article 7 of RTS 6, the testing should not be done in the actual trading system, but in a separate test environment.

It is considered best practice to follow a structured and formalised testing procedure and to document the results during that process, for example in the form of a final test result. It is further considered best practice to document deviations from the standard testing process and the reason for such deviations. It is up to each market participant to decide how extensively algorithms should be tested with regards to point 2 above.

The testing process should in general address the issues mentioned in Art. 5 (4) of RTS 6. Additionally, several potential test scenarios could be used, and each market participant should assess the necessity of these test scenarios:

- Test scenarios based on ACER's guidance: Could the algorithm be accused of breaching any of the market abuse types described in ACER's guidance?
- Interaction with another algorithm (that may follow a similar or opposing trading strategy)
- Interruptions of the continuous trading window on the intraday market due to maintenance breaks or intraday auctions
- Could the algorithm be tricked by another market participant, thereby causing a drastic price movement?
- Testing that the algorithm does not contribute to disorderly trading conditions (it does not multiply erroneous orders, it sends expected number of orders, reacts as expected to stressed market conditions, etc.)

3.3.6. Approval process

Art. 8:
Before deployment of a trading algorithm, an investment firm shall set predefined limits on:

(a) the number of financial instruments being traded;
(b) the price, value and number of orders;
(c) the strategy positions; and
(d) the number of trading venues to which orders are sent.

Art. 11:
An investment firm shall ensure that any proposed material change to the production environment related to algorithmic trading is preceded by a review of that change by a person designated by senior management of the investment firm. The depth of the review shall be proportionate to the magnitude of the proposed change.

Text box 21 with excerpts from RTS 6

Before deployment, it is recommended to have a formalised approval process; both for new developments as well as for any material changes to an existing algorithm. Dependent on the size and complexity of the algorithmic trading activities, this could be organised in the form of a committee or one single person that gives the final approval before deployment. Ideally, the approval process involves the relevant key functions of a firm (senior management, risk, legal, compliance and IT). The approval and testing which aim to ensure the algorithm's robustness, must be documented and demonstrated to the satisfaction of the responsible persons.

It is then the members of the committee or the single person that bears the responsibility within the organisation for the proper deployment of the algorithm. The responsibility in case of a law breach is a matter of applicable national laws.

It is up to each market participant to decide on the exact design of the approval process, but it is considered best practice to assess the following:

- A thorough non-technical description in layman's terms of the algorithm or any changes to an existing algorithm, setting out what it intends to do, for which products, on which markets and how it works. This description can also be provided to a trading venue or the national regulatory authority in case of an inquiry.
- Risk assessment of how the trading strategy may impact the chosen market, how it may interact with other (algorithmic) trading strategies by the same market participant, how the algorithm may behave under stressed market conditions (e.g. low liquidity) and an assessment against ACER's guidance on different market abuse types.
- Final test report that includes what the algorithm was tested for, the test result(s) as well as red flags discovered and solved during the test process
- Version control: what are the changes compared to the previous version of the algorithm?
- Overview of the selected trade parameters (pre- and post-trade controls and, if applicable, the ones from Art. 8 in RTS 6) and their suggested limits. The limits could be approved as a range. This would give the trading desk the opportunity to adjust the trading activity of the algorithm without reiterating the entire approval process.
- A description on the usage of the kill functionality: under which circumstances will it be used, who will approve the use, who will trigger it and how do you introduce the algorithm back into the market?
- An assessment of which staff members should have access rights to deploy the algorithm and/or adjust the trade parameters of an algorithm.
- A description of how the algorithm will be followed up post-deployment.
- Monitoring arrangements, including assessment of whether the current monitoring arrangements (see point 3.3.8 below) are suitable for the new/updated algorithm.

3.3.7. Post-deployment management

Art. 2 (2):
An investment firm shall also ensure that compliance staff have, at all times, contact with the person or persons within the investment firm who have access to the functionality referred to [the kill functionality] or direct access to that kill functionality.

Art. 9 (1):
An investment firm shall annually perform a self-assessment and validation process and on the basis of that process issue a validation report.

Art. 17 (1):
An investment firm shall continuously operate the post-trade controls that it has in place. […]

Text box 22 with excerpts from RTS 6

The above-described governance approach covering the design, testing and approval process are meant to identify and solve potential issues prior to full deployment of the algorithm.

Market participants could additionally consider deploying an algorithm with a limited trading mandate in a limited period, e.g. the 100-10 rule: in the first 100 hours of deployment, the algorithm can only take positions within 10% of its intended trading mandate. The exact length of the period, whether to look at trading hours or trading days as well as the exact limitation of the trading mandate should be assessed on a case-by-case basis. This would limit the impact if the algorithm does not behave as intended in the production environment of the trading venue. It does, however, not replace the requirement to do adequate testing before deployment.

When deploying an algorithm, the market participant needs to be able to stop the trading activity at any time (kill functionality). It is vital that the market participant has remote access to the functionality and/or a robust back-up solution to be able to trigger the functionality under any circumstances (also during unexpected events such as loss of internet connectivity). The following needs to be assessed and documented:

- Under which circumstances should the kill functionality be used?
- Who has the responsibility to trigger it (e.g. the responsible trader)?
- Do you need approval by another function/a second person to trigger it?
- How do you make sure that the underlying issue, which motivated the use of the kill functionality, has been solved?
- How do you re-activate the algorithm after having used the kill functionality? Who approves it and who is responsible for re-introducing it into the market?

The responsibility for triggering the kill functionality needs to be clearly assigned to avoid a lengthy confirmation process during which the algorithm may continue to contribute to disorderly trading conditions.

Additionally, market participants could consider implementing an operator presence control (also referred to as “dead-man’s switch”). The algorithm will, at regular intervals, send a message to the person responsible for monitoring the algorithm (for example in the form of a pop-up window). This message has to be confirmed before the algorithm continues trading. The intention is to avoid a scenario where an algorithm operates unattended for more than the pre-defined period.

Moreover, there are two additional requirements in RTS 6 that fall under the scope of this chapter. Article 17 requires firms to continuously operate the post-trade controls (i.e. market and credit risk) and Article 9 in RTS 6 requires an annual self-assessment to review the governance framework, routines and documentation related to algorithms.

It is considered best practice to regularly review the market risk based on the positions taken by algorithms and compare it to the market participant’s overall risk appetite. For the wholesale energy market, we do not consider credit risk a necessary risk matrix, as the positions are typically much smaller compared to financial trading and typically settled within a short timeframe.

It is furthermore considered best practice to regularly (and if necessary, on an ad-hoc basis) do a more extensive assessment of all routines and documentation related to algorithms. The extent of this assessment is dependent on the size and complexity of the algorithmic trading activities.

3.3.8. Monitoring

Art. 13:

1. *An investment firm shall monitor all trading activity that takes place through its trading systems, including that of its clients, for signs of potential market manipulation […]*
2. *For the purposes of paragraph 1, the investment firm shall establish and maintain an automated surveillance system which effectively monitors orders and transactions […]*
   […]
7. *Using a sufficiently detailed level of time granularity, the investment firm's automated surveillance system shall be able to read, replay and analyse order and transaction data on an ex-post basis […]*

Art. 16:

1. *An investment firm shall, during the hours it is sending orders to trading venues, monitor in real time all algorithmic trading activity that takes place under its trading code, including that of its clients, for signs of disorderly trading, including trading across markets, asset classes, or products […]*
2. *The real-time monitoring of algorithmic trading activity shall be undertaken by the trader in charge of the trading algorithm or algorithmic trading strategy, and by the risk management function*

Text box 23 with excerpts from RTS 6

Market participants should monitor whether the algorithm behaves as intended. Such monitoring should happen in real-time or close to real-time. To the extent that the complexity of the algorithm, the trading speed and the level of interaction with the market justifies automated monitoring, it is considered best practice to have an automated monitoring system/dashboard. As a starting point, we recommend that market participants receive an automated (and potentially audible) alarm if the algorithm exceeds any of the pre-defined trade parameters (e.g. price collars or order-to-trade ratio) or any other statistical metrics that the market participant deems reasonable to monitor in real-time.

Article 13 (1) of RTS 6 requires firms to also monitor for signs of potential market manipulation. REMIT, in its current form, does not have such a requirement; neither for human traders nor for algorithmic trading. As a result, we have chosen not to include a specific recommendation for algorithmic trading in this report.

It is important that the monitoring arrangements are at all times fit-for-purpose based on the size and complexity of the algorithmic trading activities. It is recommended to start the entire process with a risk assessment (please see Appendix 2 for an example) to identify the most suitable monitoring arrangements for each algorithm. The identified risks should be documented and appropriately addressed (for example by defining suitable statistical metrics that can be automatically monitored).

It is our opinion that it is sufficient that one function is monitoring for disorderly trading activity. It is up to each market participant to decide whether this is best

done by the trading desk or a separate risk/compliance function, but it is important that the chosen function can effectively address any unintended behaviour by the algorithm within a reasonable timeframe by, for example, activating the kill functionality.

It is considered best practice to have an adequate monitoring regime (with access to the kill-functionality) in place during the entire time that the algorithm is active in the market. Market participants may outsource the monitoring task to a third party (for example during night hours, if they do not have a trading desk that is staffed 24/7), but the market participant remains fully responsible for any trading activity of its algorithm(s) and the monitoring of that activity. It is up to each market participant to decide on the exact monitoring regime given the complexity of the algorithm, the trading speed and the level of interaction with the market.

3.3.9. Record keeping

Art. 5 (7):
An investment firm shall keep records of any material change made to the software used for algorithmic trading, allowing it to determine:
(a) when a change was made;
(b) the person that has made the change;
(c) the person that has approved the change;
(d) the nature of the change

Art. 17 (3):
An investment firm shall keep records of trade and account information, which are complete, accurate and consistent […]

Text box 24 with excerpts from RTS 6

Market participants should store relevant documentation to be able to answer any inquiry from a trading venue or the national regulatory authority as well as for internal purposes. Such documentation should cover, but is not limited to, the following:

- General methodology on how algorithms are designed, tested, approved and monitored
- Documentation of individual test processes and final test reports per algorithm
- Documentation of the approval per algorithm
- Description of the trading strategies, trade parameters, expected behaviour and information input per algorithm
- Change log which registers the updates made to an algorithm (Timing of the update? What was the update? Reason for the update? Who did the update? Who approved the update?)

It is up to the market participant to decide on the exact content and form of such documentation. It should, however, be detailed enough to be able to re-construct which version (trading parameters, trading strategy, information input, …) of the algorithm was active in the market at a given point in time and who approved the deployment.

Market participants should be able to access historical orders and transactions by algorithms. A log of orders and transactions may be accessible through the trading venue, in which case it may not be necessary for a market participant to keep a separate log.

It is considered best practice that market participants store such documentation for the period of at least five years. This mirrors the recommendation for PPATs in the ACER's guidance on the application of REMIT (last update: 16th July 2019).

3.3.10. Algorithms from third-party vendors

Art. 4:

(1) An investment firm shall remain fully responsible for its obligations under this Regulation where it outsources or procures software or hardware used in algorithmic trading activities.

(2) An investment firm shall have sufficient knowledge and the necessary documentation to ensure effective compliance with paragraph 1 in relation to any procured or outsourced hardware or software used in algorithmic trading.

Text box 25 with excerpts from RTS 6

Similar to Art. 4 in RTS 6, market participants remain fully responsible for the trading activity by algorithms from third-party vendors.

When purchasing trading algorithms from third-party vendors, the market participant should assess whether the testing procedures of the vendor are adequate. That means that the market participant needs to have sufficient staff members that have a thorough enough understanding of the third-party algorithm to be able to challenge the algorithm's compliance with specific requirements by the trading venue and applicable law, most notably the market abuse prohibitions in REMIT. The market participant has to assess whether the documentation by the third-party vendor is sufficient for that purpose or if in-house testing is required.

Each external trading solution should also be subject to the market participant's approval process.

This applies not only to new algorithms, but also to substantial updates of already-purchased algorithms.

Appendix 5 outlines some questions that can be used by market participants when purchasing algorithmic trading solutions from a third-party vendor. These questions may serve as a starting point and each market participant needs to assess whether they are sufficient to evaluate the governance model of the third-party vendor.

ALGORITHMIC TRADING – KEY POINTS

- Algorithmic trading is trading with limited or no human intervention that is based on a computer algorithm automatically determining individual parameters of orders.

- Algorithmic trading with wholesale energy products is – despite lack of specific regulation – subject to REMIT's general prohibitions against market abuse and any specific requirements imposed by relevant trading venues.

- The market participant should have a governance model, including a formalised approval procedure, for its algorithmic trading activity.

- The market participant needs to have the necessary skills and technical expertise to understand how its algorithms work.

- Independent functions such as Risk Management and Compliance must have a robust understanding of the market participant's algorithms.

- Algorithms should be thoroughly tested, in a separate test environment, before deployment.

- The market participant should monitor its algorithmic trading activity for disorderly trading activity in real-time or close to real-time and have access to the kill functionality at all times.

- Relevant documentation about the algorithm should be stored for at least five years.

4 Appendixes

4.1. Appendix 1 Abbreviations

Abbreviations	
ACER	Agency for the Cooperation of Energy Regulators
ESMA	European Securities and Markets Authority
IIP	Inside Information Platform
MAR	Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC
MiFID II	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU
MP	Market Participant
NRA	National Regulatory Agency
PPAT	Person Professionally Arranging Transactions
REMIT	Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency
RTS	Regulatory Technical Standard
RTS 6	Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organisational requirements of investment firms engaged in algorithmic trading

4.2. Appendix 2 Risk assessment

Below are **examples** on how a risk mapping could look like where each example from the ACER Guidance on market abuse is considered. The examples are fictitious, and there are many different approaches on how to design and conduct such a risk assessment. In the examples below, the likelihood for a breach to happen, together with the consequence if it happens, is graded from 0 to 3. Green, yellow and red colours are used to illustrate the risk level. The numbers representing the likelihood and consequence are only for illustration, and do not represent a real case.

Table 1 Example of risk mapping and prioritisation

Likelihood		Consequence		Likelihood x Consequence = Risk	
N/A	0	N/A	0	Acceptable risk	0
Low	1	(1). Company sanction	1		1
Medium	2	(2). 1 + Reputational risk	2		2
High	3	(3). 2 + Personal Sanctions or heightened reputational risk	3	Manage the risk	3
					4
				Mitigate and reduce the risk	6
					9

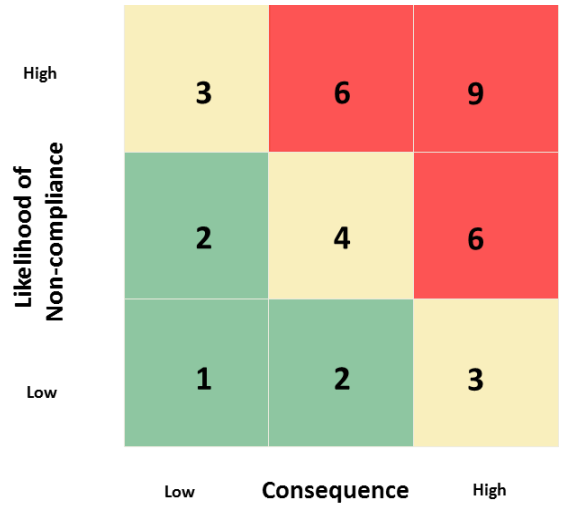

Figure 3 Example of risk mapping and prioritisation

Table 2 Example Risk mapping and prioritisation

	REMIT		ACER Guidance	Market 1 Likelihood	Market 1 Consequence	Market 1 Risk
Prohibition of Insider trading	Possess inside information	(a) Use the information		2	3	6
		(b) Disclose the information		2	2	4
		(c`) Recommend or induce		1	2	2
Obligation to publish inside information	Disclose in an effective and timely manner			2	2	4
Prohibition of market manipulation	Orders/ transactions	False or misleading signals	Wash trades	2	3	6
			Improper matched orders	2	2	4
			Placing orders with no intention of executing them	1	2	2
		Secures the price at an artificial level	Marking the close	2	3	6
			Abusive squeeze/market cornering	2	3	6
			Cross-market-manipulation	2	3	6
			Physical withholding	1	2	2
		Fictitious device/deception/ contrivance - false/misleading signals	Scalping	1	3	3
			Pump and dump	2	3	6
			Circular trading	2	2	2
			Pre-arranged trading	1	2	2
	Information	Disseminating information - false/misleading signals	Spreading false/misleading signals through the media	1	3	3
			Other behaviour spreading false or misleading information	3	2	6

In the example above, a number of the risks are marked as red, meaning that mitigating measures should be implemented in order to reduce the risks.

4.3. Appendix 3 Training concept – example

- **Clustering of employees in risk-groups**
  - Group 1: traders, dispatchers, originators, managers
  - Group 2: power plant personnel
  - Group 3: back office, middle office etc.

- **Choosing the right training**
  - Group 1: professional training with focus on market abuse
  - Group 2: training with focus on inside information and insider trading
  - Group 3: training with focus on reporting compliance incidents and not spreading inside information

- **Regular update trainings to keep awareness high**
  - Recommended for Group 1 and 2: regular in-class training
  - In addition, and for Group 3: also possible via web-based trainings
  - Recurring meetings with relevant target groups to exchange information about new regulatory and market developments and lessons learned from compliance incidents etc.

- **Ad-hoc trainings in case of new developments**

- **Training for new employees**

4.4. Appendix 4 Dawn Raid Manual – example of instructions

Below is an example of such instruction**. Please be aware that different rules may apply in different jurisdictions that may affect the content of such a manual**.

Instructions for reception desk

- Ask for identification papers from all representatives from the authorities, make copies of the identification papers or note down name and authority they represent
- Immediately notify the person they request to meet and the primary responsible person
- Ask the authorities to wait in the reception until the responsible person arrives. If they disapprove of waiting, do not hinder them from commencing with the inspection
- If the inspectors disapprove of informing the responsible manager, inform that the company's routines oblige you to contact the responsible legal counsel or compliance officer. Immediately contact this person.

Instructions for primary responsible person

- Check ID and decision/authorisation (legal basis) issued by the relevant authority
- Check whether you are under inspection or approached as witness
- Request that the inspectors wait to commence the inspection until the attorneys have arrived. Typically, they accept waiting for some time before commencing the inspection. If they disapprove of waiting, do not hinder them from commencing with the inspection.
- Inform all concerned managers
- Make sure secretarial assistance, meeting rooms and copying facilities are made available for the inspectors
- Instruct everyone concerned by the investigation neither to delete nor destroy any documents, nor to communicate with anyone outside the company regarding the ongoing inspection and to fully cooperate with the inspectors
- Ensure that legally privileged documentation (correspondence with external legal advisors) is kept away from the inspectors until a legal advisor is present and can make an assessment
- Do not let the inspectors walk around unattended
- Ask for a copy of the inspectors' list of documents. If necessary, make your own list, with the assistance of the owner of the office and a secretary.
- The duty to explain only applies to specific and concrete information. If you are uncertain or do not remember certain facts, it is important to make this clear to the inspectors. Avoid speculations, assessments and assumptions, negligently providing incorrect information may be a criminal offence.
- If you understand that an answer will reveal an illegal action, you should, after conferring with your legal advisor, point out the principle of self-incrimination (no-one is obliged to contribute to his/her own incrimination), and state that this

is a self-incriminating question and that there is no duty to answer. The inspectors will then usually relinquish the question. Should they insist on it, request that it is noted in the protocol that you answer on request and under the threat of criminal prosecution. This may influence the value for the authorities of the deposition for subsequent handling of the case.

- Do not sign the protocol of the deposition before it has been carefully reviewed with your legal advisor. If points are missing or it does not give a correct and accurate picture, request amendments or corrections.

4.5. Appendix 5 Third-party vendors of algorithmic trading solutions

The following questions can be used by market participants when purchasing algorithmic trading solutions from a third-party vendor. These questions may serve as a starting point and each market participant needs to assess whether they are sufficient to evaluate the governance model of the third-party vendor.

1. Please provide a general description on your governance model for the development of an algorithm. This should cover the following:
    a. Do your staff members receive regular training on applicable market abuse prohibitions?

    b. What is your process when updating an already sold algorithm? Do you provide a description of the update itself and the reason for it? What are your procedures to test this update (including conformance testing with the relevant trading venues)?

    c. Do you regularly do a more extensive assessment of all your routines and documentation related to algorithms?

    d. Please provide an overview of your business continuity arrangements and cybersecurity measures.

2. Please provide a thorough non-technical description in layman's terms of the algorithm, setting out what it intends to do, for which products, on which markets and how it in general works. This description should also cover the following:
    a. An assessment on how the proposed trading strategy will affect the market.

    b. An assessment on how the algorithm behaves when interacting with an identical/similar algorithm in the market.

    c. An assessment on how the algorithm behaves under stressed and/or extraordinary market conditions (e.g. large volumes added to/removed from the order book, low/no liquidity, rapid price movements, maintenance break on the trading platform, etc.)

3. Please provide a thorough non-technical description of how you test the algorithm (including a general description of the testing process and a list of the different test scenarios).

4. Questions related to the design of the algorithm:
    a. Do you have a built-in kill functionality?

    b. What trade parameters/pre-trade controls are coded directly into the algorithm and can be adjusted by us?

c. What information or analytic input does the algorithm use/can the algorithm be connected to?

5. Questions related to the day-to-day working of the algorithm:
    a. Will the algorithm be deployed from your servers? What happens if you encounter technical problems (e.g. loss of internet connectivity)?

    b. Who, how and when can we contact you if we have an urgent question/issue?