REMIT Best Practice

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

3rd Edition

Updated: 13 April 2026

This document contains the 3rd edition of the REMIT Best Practice Report. The content of previous versions was updated with regard to the revised REMIT from May 2024 and the updated ACER Guidance on REMIT, version 6.1, from December 2024. New sections on monitoring requirements for persons professionally executing transactions and on erroneous orders were added. The publisher of this report is the Nord Pool Group ("Nord Pool"). The following participants have contributed to the 3rd edition of the report:

- *Å Energi AS*
- *Danske Commodities A/S*
- *E.ON SE*
- *Fortum Power and Heat Oy*
- *Hafslund AS*
- *Ignitis Group*
- *InCommodities*
- *Jämtkraft AB*
- *Lyse AS*
- *MFT Energy A/S*
- *Mind Energy A/S*
- *Nordic Association of Electricity Traders (NAET)*
- *Norlys Energy Trading A/S*
- *RWE AG*
- *Skagerak AS*
- *Statkraft AS*
- *Uniper Global Commodities SE*
- *UPM Energy Oy*
- *Vattenfall AB*
- *Ørsted A/S*
- *Nord Pool Group*

Disclaimer and rights

This 3rd 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 judgment 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	13 April 2026
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
13 April 2026	3rd edition REMIT Best Practice Report (updated with regard to Regulation (EU) 2024/1106 of 11 April 2024 (REMIT review), including new sections on PPET monitoring and on erroneous orders)	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, 13 April 2026

Camilla Berg
Project manager

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 and amended by Regulation (EU) 2024/1106 of 11 April 2024. While REMIT provides on the one hand a trustworthy level playing field for energy companies, it has on the other hand led 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 have 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 for ACER 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 thereby 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 3rd edition of the report is based on input and knowledge sharing from various market participants 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 have provided 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 can 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] *ACER 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*, 6.1st edition (18 December 2024)

[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 provide 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 serves as a guide on how to achieve this.

This third edition of the Best Practice Report is based on the REMIT revision from 11 April 2024 and the 6.1st edition[1] of the ACER Guidance on REMIT application. It includes best practices for Persons Professionally Executing Transactions (PPETs under REMIT Article 15(2)) and market participants employing algorithmic trading solutions (REMIT Article 5a).

Section 2 of this report focuses on how to develop and implement a compliance regime. The ACER Guidance, 6.1st edition, chapter 10 is used as a base to highlight the main elements of a compliance regime. Section 2.2 outlines a best practice for how PPETs can identify potential breaches of Articles 3, 4 and 5 of REMIT.

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 insider trading and how inside information should be published. Section 3.2 focuses on recommendations for measures to prevent market manipulation, both intentional and unintentional. Section 3.3 on algorithmic trading solutions discusses and recommends how to ensure compliance with Article 5a of REMIT. Section 3.4 outlines a best practice approach to prevent and mitigate risks of erroneous orders.

The target audience for this report is market participants covered by the REMIT regulation. Focus is primarily on electricity, but the concepts described can to a large extent be applied also to gas and hydrogen. 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 guidance, and each market participant must make its own assessment of how to ensure compliance. It is possible to achieve compliance without following the practices 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 MAR and 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, e.g., 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 document.

2 Compliance regime

REMIT does not set out specific requirements for a compliance regime for market participants outside of Article 5a[3]. The regulations describe requirements, prohibitions and sanctions, but not how to comply with the regulation. However, the ACER Guidance states the following:

> (520) 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 towards the other obligations and prohibitions of REMIT.
> (521) NRAs should consider the following best practice examples of such compliance regime for market participants, taking into account the market participant's size and trading capacity […]

Text box 1: ACER Guidance chapter 10 (520-521)

In addition to the recommendations from ACER, a compliance regime will support market participants in conforming to 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, other regulatory sanctions and potential civil law claims. It will also help avoid or minimise the risk of loss of reputation for instance due to bad press or poor 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 form the basis for prioritising the compliance work.

Ensuring compliance with REMIT is a complex task that requires the market participant to actively address and manage the risks involved considering 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.

[3] REMIT does set out requirements for having a compliance regime ("effective systems and risk controls", ACER Guidance (54)) for market participants falling under REMIT Article 5a, that is algorithmic traders and direct electronic access providers. See more information for algorithmic traders in section 3.3.

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 to and give examples of some compliance practices that have proven 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 prescribes a particular compliance regime or requirements in respect of a compliance regime. As stated above, it is essential 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 in a compliance regime for small and non-complex market participants compared to one for large and complex market participants.

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

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

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

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

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

v) Compliance programme; the identification of concrete actions to define compliant/non-compliant behaviour; see section 2.1.5.

vi) Communication; the communication of the rules and regulations to be observed, see section 2.1.6.:
- internal communication and training concept (raising the awareness of employees)
- external communication and reporting to the Agency/National Regulatory Authorities (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 section 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: ACER Guidance chapter 10 (521 point 2)

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

This report focuses on the market abuse prohibitions, namely insider trading, including not spreading inside information and publication of inside information, and market manipulation, and discusses additional requirements regarding algorithmic trading in chapter 3.3. 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: ACER Guidance chapter 10 (521 point 1)

The second element in a well-functioning compliance regime, as outlined in the ACER Guidance, is fostering a **corporate culture** committed to complying with REMIT. Note that a focus on compliance should be **embedded in management**. Without active support from management, there is a risk that efforts to establish a compliance culture will fall short.

Key aspects of a compliance culture include:

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

These elements will be explored further in the report. Each market participant must find its own relevant approach to foster 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:

i) 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 that would make the person unsuitable for the position. It is up to each market participant to decide how broad such a background check should be.

ii) 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 their 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: ACER Guidance chapter 10 (521 point 3)

The third element in a well-functioning compliance regime is a **properly organised and staffed** compliance function. There is no "one-size-fits-all", the setup should fit the market participant's needs and risk profile. However, some general principles are recommended:

i) **Clearly defined roles and responsibilities.** Depending 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.

ii) **Sufficient staffing and competence.** The compliance function should be staffed with sufficient people with sufficient business knowledge and competence and have sufficient resources in terms of e.g. IT support. It is advisable that compliance personnel have knowledge of the daily operation/trading activities in addition to in-depth knowledge of the REMIT requirements.

- Seating the compliance function close to operations/the trading desk encourages compliance personnel to be involved and learn about the trading activities whilst the traders may be more encouraged to ask questions and discuss relevant matters with compliance. 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.

iii) **Independence and separation of functions**. The compliance function should be **independent** from the business it advises, 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.
For PPAETs (Persons professionally arranging or executing transactions), REMIT explicitly stipulates the independency of their surveillance function in Articles 15 (1-2), stating that PPAETs must "guarantee that their employees carrying out surveillance activities […] are preserved from any conflict of interest and act in an independent manner".

iv) **Management support and authority.** The compliance function should have the **authority required** for such a function and the **support of management** to be able to perform its tasks. This e.g. includes the authority to implement procedures and report compliance failures.
It is important that focus on compliance is embedded in the management. Without active leadership support, there is a risk that the market participant will not succeed in creating a compliance culture. Management should communicate the importance of compliance both on a general level and by concrete messages, for instance clearly stating that insider trading and market manipulation are not tolerated.
Management can further demonstrate its commitment to compliance through concrete actions such as 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, evaluate and improve the effectiveness of the compliance regime.
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.

v) **Unlimited access to information.** 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.

vi) **Direct reporting to senior management.** 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.

vii) **Involvement in organizational changes.** 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.

viii) **Awareness of market and regulatory developments.** 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.

ix) **Documentation.** 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 (521 point 4)

The fourth element in a well-functioning compliance regime is to conduct **risk assessments** to prioritise the compliance efforts 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 of what compliance risks the market participant faces. Therefore, each market participant should perform a risk assessment. As there is no "one-size-fits-all", the risk assessment must be adjusted to fit the market participant's needs. Some general principles can be highlighted:

- The compliance function may on a regular basis carry out an assessment of the market participant's compliance areas and its risk exposure to
  - identify the relevant compliance areas (activities),
  - identify the main sources/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 conduct interviews with key stakeholders within the company
    - to acquire a description of the activities of the business unit,
    - using pre-structured questions, e.g. to identify the potential flow of inside information,
    - using 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 happening can be assessed together with the consequence of the risk occurring. 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.

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 to 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.

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 include an assessment of the different types of market abuse that may constitute Article 3, 4 or 5 breaches based on the expected risk of occurrence for the market participant. See the market abuse types described in chapter 9 in the ACER Guidance on REMIT as well as in the separate ACER Guidance Notes on specific market abuse types[2], and the obligation to publish inside information. In Appendix 2, 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.

2.1.5. Compliance programme

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

Text box 6: ACER Guidance chapter 10 (521 point 5)

The fifth element in a well-functioning compliance regime is the **compliance programme**. While the ACER Guidance describes this as the identification of concrete actions to define compliant/non-compliant behaviour, this report uses the term in a wider perspective. Based on the assessment of the identified compliance risks, 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 by a third party.

A compliance programme should cover three main pillars: prevention, detection and response. **Preventive** measures should be appropriate and proportionate and should be based on the results of the risk assessment and previous findings. For the **detection** of possible REMIT breaches, it is recommended to implement compliance activities and controls, monitoring and routines. To ensure effective compliance the market participant should ensure an adequate **response** to specific incidents or matters that may occur.

The compliance programme should address all three pillars, with emphasis on prevention. The annual compliance plan supports all three pillars. Further details on the points listed in Figure 1 are provided in other sections of this report.

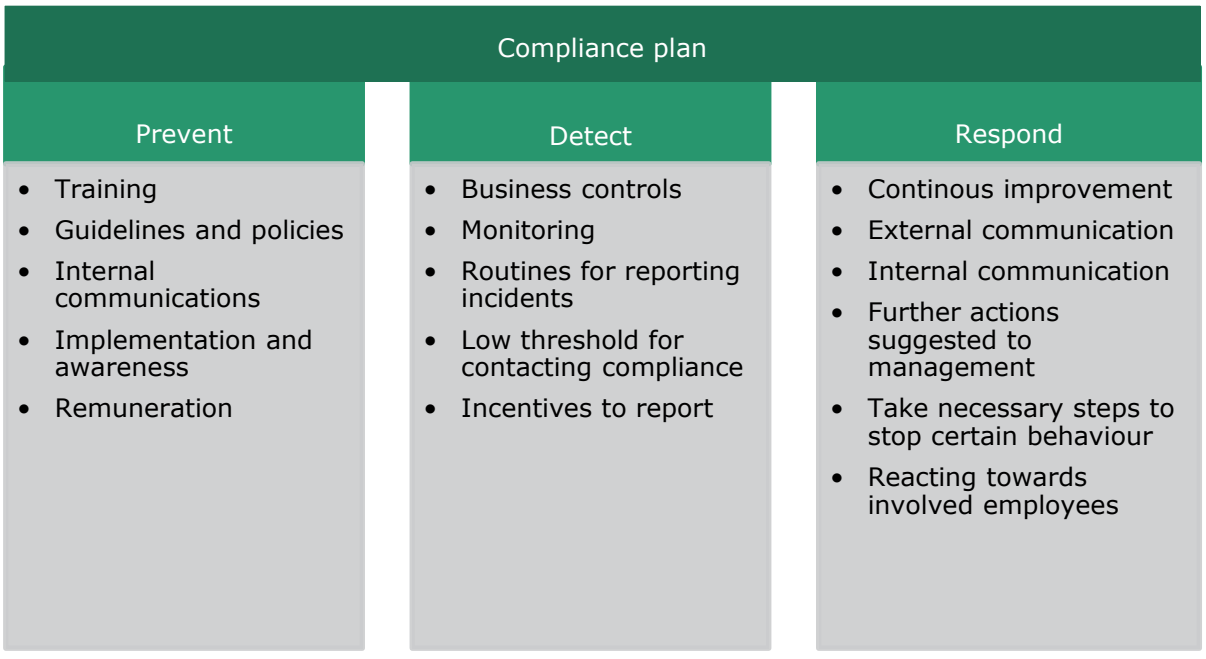

Figure 1: Prevent, detect and respond

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. The compliance plan is also a good place to include measures for continual improvement, ensuring the ongoing suitability, adequacy and effectiveness of the compliance regime.

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, e.g. contact person for OMP/NRAs
- Relevant market (different market rules or NRA approaches could lead to prioritisation or more frequent review)
- 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

Appendix 3 Sample contents of the Compliance Plan illustrate the bullet points above. The exact parameters to include can vary between market participants and compliance areas.

When there is 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 the concerns are, whether there have been any breaches, how many incidents occurred in the past year, and what has been achieved and not with the dedicated resources. In the end, it is 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: ACER Guidance chapter 10 (521 point 6)

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 on external consultations, if applicable
- 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 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&As, 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 to 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 the risk assessment.

Finally, 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 regularly distribute up-to-date guidelines, with all relevant employees signing to confirm they have read and understood the content, in addition to the possibility and encouragement to ask questions if anything is unclear.

An example of how to set up a tailored training programme is found in *Appendix 4 Training concept – example*.

TRAINING CONCEPT – KEY POINTS

- Set up a tailored training programme based on the company's needs and risk-groups of employees
- Training should consider 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,
- The compliance function should report the number of notifications received and their nature to management,

  Review of the notification handling procedures may be carried out regularly, for example through a self-assessment from the compliance function, 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 breaches of REMIT could be mitigating in case of an investigation. It **may** turn out to be positive to give the NRA an explanation of a potential breach before they potentially start an investigation. A proactive notification of a breach may have a positive impact on whether and which sanctions might be applied. In addition, a proactive approach could also improve 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. Note that MPs that are not PPETs under REMIT Art 15 (2) generally have no legal requirement to notify NRAs of breaches of REMIT, see section 2.2 for PPET monitoring requirements. The same approach could be considered in respect of the market surveillance departments of the affected PPAET(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, possibly 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 PPAET) 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 e.g. 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 the reception desk, the primary responsible, surveillance persons and IT-specialists. An example of such instruction is found in Appendix 5.

2.1.7. Monitoring improvements

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

Text box 8: ACER Guidance chapter 10 (521 point 7)

The seventh element of a well-functioning compliance regime is to have **monitoring procedures** in place and make improvements based on this monitoring. Continuous improvements are an important part of compliance systems. 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", see Figure 2. 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.

First line: Business operations and units	Second line: Compliance and risk control	Third line: Internal audit
• Business operations and units are the risk owners • Identify and assess risks • System (compliance workspace/tracking tools) • Internal controls • The control culture	• Provide oversight • Provide tools, systems and advice necessary to support the first line • Monitors and controls specific risks involving non-compliance with relevant laws, regulation and internal guidelines and procedures	• Independent assurance • That risks are managed by the business operations and units at an acceptable level • That business operations and units comply with guidelines and procedures • That compliance's oversight function works as desired

Figure 2: Three lines of defence

Monitoring of the business by the compliance function

Depending on the nature of the trading activities, it may be relevant or in the case of PPETs[4] mandatory to implement routines for monitoring 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", to 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, 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 guidance, but the measures implemented should be reasonable and proportionate for each individual market participant.

[4] For compliance of PPETs obliged to monitor under REMIT Art 15(2), see section 2.2.

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

2.2. Monitoring requirements for Persons Professionally Executing Transactions

REMIT obliges persons professionally executing transactions (PPETs) to notify ACER and regulatory authorities about any reasonable suspicion of breaches of Articles 3, 4 or 5[5].

> (2) **Any person professionally executing transactions** under Article 16 of Regulation (EU) No 596/2014 who also executes transactions in wholesale energy products that are not financial instruments, and **who reasonably suspects** that an order to trade or a transaction, including any cancellation or modification thereof, whether placed on or outside an OMP, could **breach Article 3, 4 or 5** of this Regulation, **shall notify** the Agency and the relevant national regulatory authority without further delay and in any event **no later than four weeks** from the day on which that person becomes aware of the suspicious event.

Text box 9: REMIT Article 15(2)

Section 9.4 of the ACER Guidance, "The duty to establish and maintain effective arrangements, systems and procedures", outlines the fundamental requirements for PPET monitoring. This best practice section aims to provide practical guidance to support the implementation of these requirements.

2.2.1. Who is required to monitor as a PPET?

Since 2024, the obligation to notify does not only apply to Persons Professionally Arranging Transactions (PPATs), but also on Persons Professionally Executing Transactions (PPETs).

Article 15(2) REMIT obligations apply to PPETs who have PPAET obligations under MAR Article 16[6] and who also execute orders in wholesale energy products that are not financial instruments (= wholesale energy products), see overview in Figure 3.

[5] These articles prohibit insider trading (Article 3), include the obligation to publish inside information (Article 4) and prohibit market manipulation (Article 5).

[6] This report does not provide best practices in the assessment of whether a company has obligations under MAR Article 16 or not. See for PPAET obligations under MAR e.g. ESMA70-145-111 MAR Q&A 6.1.

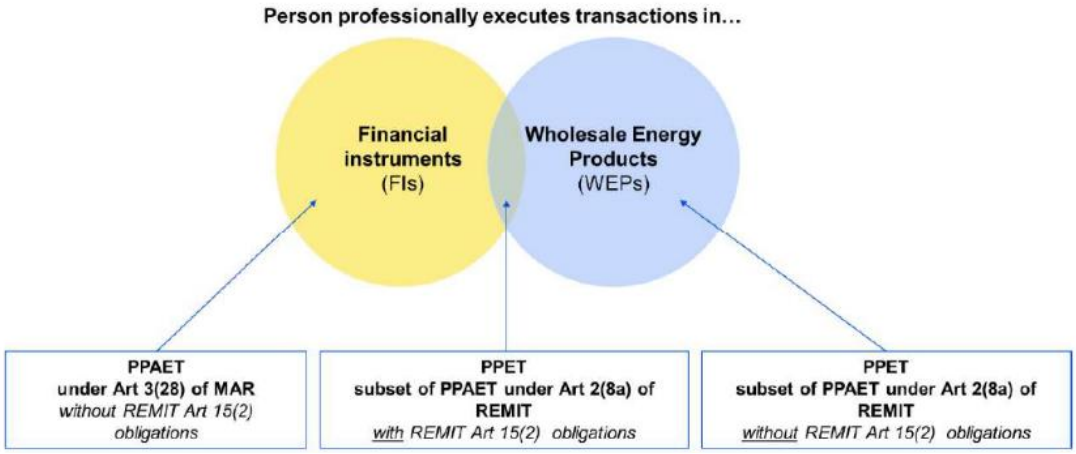

Figure 3: Overview on PPETs, taken from ACER Guidance, 6.1st edition (428)

According to REMIT Article 2(8), 'Person' is defined as a natural or legal person. 'Professionally' is interpreted by ACER as "engaged in a specific activity as part of one's normal and regular paid occupation"[7]. According to the ACER Guidance (424) understanding, 'execution' includes:

- execution of orders on behalf of a third party (either directly or in accordance with a discretionary mandate given by the third party), as well as
- trading on own account.

2.2.2. Setting up a PPET compliance regime

PPETs must establish and maintain effective internal arrangements, systems and procedures to fulfil their monitoring duties under REMIT Article 15(2). This requirement is described in REMIT Article 15(3).

> (3) The persons referred to in paragraphs 1 [PPATs] and 2 [PPETs] shall establish and maintain effective arrangements, systems and procedures to:
> (a) identify breaches of Article 3, 4 or 5;
> (b) guarantee that their employees carrying out surveillance activities for the purpose of this Article are preserved from any conflict of interest and act in an independent manner;
> (c) detect and report suspicious orders and transactions.

Text box 10: REMIT Article 15(3)

[7] See ACER's 3rd open letter, *Open letter on the designation of representatives by non-EU market participants and on the new obligations of persons professionally arranging or executing transactions (PPAETs), according to the revised REMIT* (25 September 2024)

Following ACER Guidance (472), these arrangements, systems and procedures can be established by extending the already existing ones under MAR Article 16(2) [8] to potential breaches of Articles 3, 4, and 5 of REMIT. Note that extending such arrangements requires an understanding of the differences between financial markets and wholesale energy markets, further outlined in this subchapter.

(472) Given that PPETs under Article 15(2) already need to comply with obligations under Article 16(2) of MAR and the relevant associated technical standards to *"establish and maintain effective arrangements, systems and procedures to detect and report suspicious orders and transactions (…)"* and notify *"Reasonable suspicions"* of *"insider dealing, market manipulation or attempted insider dealing or market manipulation"*, ACER understands that the relevant PPETs are already engaging in similar obligations than those prescribed under Article 15(2) of REMIT. **Consequently, the relevant PPETs should extend these already existing arrangements**, procedures and systems under MAR to potential breaches of Articles 3, 4, and 5 of REMIT, taking also into consideration the specific features of energy physical markets.

Text box 11: ACER Guidance chapter 9.4.2 (472)

The following sections break down how such **effective arrangements, procedures and systems** can look like for PPETs. We draw both directly on ACER Guidance for PPETs, and also look at guidance for PPATs, next to MAR and its Delegated Regulation[9]. Note that only REMIT is binding regarding PPET monitoring. Any Articles of MAR, the Delegated Regulation, and sections from the ACER Guidance in this section are for information only. Since PPATs are subject to stricter criteria in their compliance regime than PPETs, only selected excerpts from the ACER Guidance for PPATs that are deemed relevant for PPETs are included in this section.

We emphasize that **no "one-size-fits-all" solution** for PPETs exists and that the monitoring effort of any PPET should be reasonable and proportionate to its size as well as to the scale and complexity of the PPET's trading activities.

[8] "Any person professionally arranging or executing transactions shall establish and maintain effective arrangements, systems and procedures to detect and report suspicious orders and transactions. Where such a person has a reasonable suspicion that an order or transaction in any financial instrument, whether placed or executed on or outside a trading venue, could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation, the person shall notify the competent authority […] without delay." MAR Article 16(2)

[9] Commission Delegated Regulation (EU) 2016/957

2.2.3. Arrangements

The compliance function

The Delegated Regulation under MAR outlines general requirements for the compliance function[10] of PPETs in their capacity as a PPAET under MAR.

> (5) Persons professionally arranging or executing transactions, market operators and investment firms operating a trading venue shall ensure that the arrangements, systems and procedures referred to in paragraphs 1 and 3:
>
> (a) are **appropriate and proportionate** in relation to the scale, size and nature of their business activity;
>
> (b) are **regularly assessed**, at least through an annually conducted audit and internal review, and updated when necessary;
>
> (c) are **clearly documented** in writing, including any changes or updates to them, for the purposes of complying with this Regulation, and that the documented information is maintained for a period of five years.

Text box 12: Delegated Regulation Article 2(5)

In addition to the requirement that the compliance function must be *appropriate and proportionate*, further important aspects can be drawn from the ACER Guidance on PPAT arrangements[11]. In the context of PPATs fulfilling REMIT Article 15(3), ACER Guidance chapter 9.4.3 highlights aspects of governance, organisational setup, and a clear definition of the function as relevant arrangements. Some elements with relevance to PPET monitoring include:

- The trade surveillance function should have **adequate resources**, including staff, analytical tools and access to data and information to fulfil their monitoring duties.
- **No conflicts of interest.** The trade surveillance function should be preserved from any conflict of interest and act in an independent manner. For example, trade surveillance staff should not also work as or be closely tied to traders or the trading function. They should further not have short term commercial interests that are in conflict to fulfilling their trade surveillance function, see also section 2.1.2, on *the choice of remuneration system.*
- **Ensuring integrity and confidentiality / Information barriers.** Segregation measures for the trade surveillance team, such as information barriers are a good tool to ensure integrity and confidentiality. See more details on information barriers in section 3.1.2.

The purpose and work of the compliance function of a PPET should be clearly documented. A **trade surveillance strategy** can serve as a cornerstone document to the trade surveillance's work, and could include:

[10] While this section discusses arrangements for the compliance function, MPs who submit the PPET requirements in a market surveillance function can read market surveillance here instead.

[11] Note: to date, ACER Guidance does not have particular guidance for PPET arrangements.

- Legal requirements of the trade surveillance unit
- Obligations of the trade surveillance unit
- Defining routines, e.g. for monitoring, investigations, reporting suspicious transactions and orders
- How to handle conflicts of interest

Additionally, a **risk assessment** (see also section 2.1.4) can serve as documentation to identify high-risk areas and set priorities in the compliance function's work, e.g. which alerts and monitoring systems to set up. Any changes or updates to the documentation should be clearly documented.

Documentation and record-keeping

The Delegated Regulation under MAR sets requirements for PPETs in their capacity as a PPAET under MAR to keep documentation (Article 2(5)) and records on analyses carried out (Article 3(8)) for five years, and to provide them to competent authorities upon request.

(8) As part of the arrangements and procedures referred to in Article 2(1) and (3), persons professionally arranging or executing transactions […] **shall maintain for a period of five years the information documenting** the analysis carried out with regard to orders and transactions that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation which have been examined and the reasons for submitting or not submitting a STOR. That information shall be provided to the competent authority upon request.

Text box 13: Delegated Regulation Article 3(8)

Similarly, ACER guidance requests PPATs to keep records of their trade surveillance work for five years.

(512) All work carried out by the market surveillance team should be recorded whether in a dedicated case management system, a shared folder or in traceable email records, for a period of at least **five years**.

(515) NRAs should request PPATs to maintain for a period of at least **five years** the **information documenting the analysis carried out** with regard to a suspicious event/potential breach which have been examined and the reasons as to whether or not submitting a STR. This information shall be provided to the NRA upon request.

(516) **All processes and decisions** made by the market surveillance team should also be recorded. The PPAT should conduct internal audits or hire an external auditor to review their processes at least on a regular annual basis and in certain circumstances an NRA may wish to conduct a visit or audit.

Text box 14: ACER Guidance chapter 9.4.4.d (512, 515, 516)

As a best practice, PPETs should consider keeping documentation and records of their trade surveillance activities for five years. Such documentation and records can include:

- Documentation of arrangements, systems and procedures put in place to follow REMIT Article 15(2), and any changes or updates to them (see Delegated Regulation Article 2(5));
- Recording the trade surveillance work in a dedicated storage space like a shared case management system, shared folder or traceable email records (see ACER Guidance (512));
- Information on analyses carried out with regard to a suspicious event/potential breach of REMIT Articles 3, 4 and/or 5, including the reasons as to whether or not to submit a STOR (see ACER Guidance (515) and Delegated Regulation Article 3(8));
- Documentation of the trade surveillance processes and decisions (see ACER Guidance (516)).
- As a rule of thumb, PPETs should store all necessary data needed to trace the decisions of investigations.

PPETs do not necessarily need to store their orders and trades internally, but they remain responsible for the prompt access to the data (potentially via a 3rd party) for fulfilling their PPET obligations.

Training

The Delegated Regulation requires that trade surveillance staff and staff involved in processing orders and transactions receive effective and comprehensive training on both insider trading and market manipulation (Delegated Regulation Article 4(1)).

(1) Persons professionally arranging or executing transactions and market operators and investment firms operating a trading venue shall organise and provide **effective and comprehensive training to the staff involved in the monitoring, detection and identification of orders and transactions** that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation, including the staff involved in the processing of orders and transactions. Such training shall take place on a regular basis and shall be appropriate and proportionate in relation to the scale, size and nature of the business.

Text box 15: Delegated Regulation Article 4(1)

ACER Guidance for PPETs suggests extending this training with educational courses for staff on REMIT compliance (see ACER Guidance (point 473)).

(473) In addition to the already established processes and procedures under Article 16(2) of MAR, examples of arrangements, systems and procedures for PPETs under REMIT could include, but are not limited to:

- Adoption of internal procedures and educational **courses for staff on REMIT compliance**, including measures and systems to prevent and discover insider trading, market manipulation, and non-effective or non-timely disclosure of inside information

Text box 16: ACER Guidance chapter 9.4.2 (473)

Such REMIT courses for PPETs should particularly cover Articles 3, 4, and 5[5], and be given to trade surveillance staff and other staff where necessary. The trainings may be internal, external, or a combination of those. It is recommended to define the content, frequency, and audience of these trainings in the trade surveillance strategy. For guidance on developing and conducting internal training, refer to section 2.1.6.

2.2.4. Systems

PPETs with monitoring requirements under REMIT Article 15(2) already need to have systems and procedures set up for monitoring orders and transactions under MAR Article 16(2). For MAR monitoring, the Delegated Regulation details amongst others that:

- PPETs in their capacity as a PPAET under MAR shall ensure effective and ongoing monitoring of all orders and transactions (Delegated Regulation Article 2(1)).
- PPETs in their capacity as a PPAET under MAR must analyse all transactions and orders, and produce alerts indicating activities requiring further analysis, across all trading activities (Delegated Regulation Article 3(1)).

PPETs should apply similar rules for their monitoring systems for REMIT monitoring. There is no requirement in REMIT for PPET monitoring to be done on a real-time basis. Taking into account the specifics of wholesale energy markets, it is reasonable to opt for ex-post monitoring. However, it is important that the reporting deadlines specified in Article 15(2) shall be satisfied. See more on reporting deadlines in section 2.2.5 Procedures, subsection *"Writing and filing a Suspicious Transaction or Order Report".*

Extension of systems to monitor for REMIT breaches

The ACER Guidance advises PPETs to extend their MAR monitoring to comply with REMIT PPET requirements. To monitor orders and trades in wholesale energy markets for potential breaches of Articles 3, 4, and 5 of REMIT, one must consider specific characteristics of power markets, e.g.:

- Auction-based markets like SDAC operate differently from continuous financial markets and thus require different monitoring approaches. Auction-based matching results in a single price for multiple market participants – this increases the potential consequences of e.g. economic and physical capacity withholding as a type of market manipulation (REMIT Article 5).
- Types of market manipulation related to inefficient use of transmission capacity, e.g. transmission capacity hoarding.

- Continuous power trading, e.g. in continuous intraday market, is similarly to financial markets at risk of layering, spoofing, and wash trading (see also transmission capacity hoarding).
- Monitoring for insider trading (REMIT Article 3) in power markets shall take into account the special characteristics of inside information that is likely to occur in power markets and that it must be disclosed through Inside Information Platforms (IIP).
- There is no requirement for real-time monitoring under REMIT.

Automated alerts and thresholds

(3) Market operators and investment firms operating trading venues shall, to a degree which is appropriate and proportionate in relation to the scale, size and nature of their business activity, **employ software systems** and have in place procedures which **assist the prevention and detection** of insider dealing, market manipulation or attempted insider dealing or market manipulation.
[…]

(4) Persons professionally arranging or executing transactions and market operators and investment firms operating a trading venue shall put in place and maintain arrangements and procedures that ensure an **appropriate level of human analysis** in the monitoring, detection and identification of transactions and orders that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation.

Text box 17: Delegated Regulation Article 3(3), Article 3(4)

Once a PPAET reaches a certain level of activity, it is advisable to use **an automated surveillance system** to detect suspicious orders and transactions under MAR (similar to Delegated Regulation Article 3(3) for market operators and investment firms). Automated surveillance systems on their own are however not sufficient, and systems and procedures shall ensure an appropriate level of **human analysis** (Delegated Regulation Article 3(4)). There should always be an element of human analysis in the detection of orders and transactions that could constitute market abuse. The most effective form of surveillance will likely be a mix of both automated and human forms.

Similarly, for PPETs that are either sufficiently large or engage in sophisticated trading, e.g. algorithmic trading, REMIT-compliant monitoring systems should typically consist of an automated system that generates alerts regarding suspicious behaviour, which are then further analysed by a human analyst.

Automated alerts should be set up following the PPET's risk assessment (see section 2.2.3), and focus on the identified risk areas of breaches of REMIT Articles 3, 4 and 5. When such alerts operate based on set thresholds, these thresholds should be reviewed regularly and the rationale for changes should be documented.

PPETs who determine that their level of activity does not necessitate an automated alert system may introduce a more manual system, e.g. spot checks, to ensure compliance.

2.2.5. Procedures

ACER Guidance for PPETs names a range of procedures to be added for REMIT compliance of PPETs in addition to MAR procedures. The following sections will discuss best practices on how to set such procedures up.

(473) In addition to the already established processes and procedures under Article 16(2) of MAR, examples of arrangements, systems and procedures for PPETs under REMIT could include, but are not limited to:

- […]
- **Procedures** on how to conduct an **effective assessment** to determine a reasonable suspicion for potential breaches of Articles 3, 4, or 5 (the full decision-making process should be traceable and key decision points should be recorded; these provisions should cover also data storage);
- Internal handbooks and procedures on how to write adequate, complete and informative notifications; and
- Internal procedures on how to submit a notification via the Notification Platform to ACER and to the relevant NRA(s).

Text box 18: ACER Guidance chapter 9.4.2 (473)

Routine for monitoring and investigations

A PPET's monitoring routine should include the necessary "Procedures on how to conduct an effective assessment to determine a reasonable suspicion for potential breaches of Articles 3, 4, or 5" (ACER Guidance (473 pt. 2)). As a first step for such effective assessments, PPETs need to proactively monitor wholesale energy markets that they are involved in (ACER Guidance (465)).

(465) The provisions of Article 15(3) of REMIT set out the responsibility for PPAETs not only to notify whenever they have reasonable grounds to suspect a potential breach, but also to **proactively monitor the wholesale energy markets** in which they are involved. The provisions of Article 15(3) apply to a variety of entities and should be proportionate to the type, size, activities and information available to different PPAETs.

Text box 19: ACER Guidance chapter 9.4.1 (465)

According to the ACER Guidance, PPETs should focus their monitoring on behaviours observed i) in the course of the PPET's trading activities, and ii) in relation to information available to the PPET.

(471) ACER expects the monitoring activities of such PPETs to focus on reasonably suspicious breaches of Articles 3, 4, or 5 of REMIT, on behaviours observed (i) **in the course of their trading activities** and (ii) in relation to **information that is available to the PPET**. […]

Text box 20: ACER Guidance chapter 9.4.2 (471)

- We interpret "in the course of their trading activities" to include the PPET's own orders and transactions, as well as observations of other MPs in relation to the PPET's own trading.
- We interpret "their trading activities" to include both activities on the PPET's behalf and on behalf of third parties, executed by the PPET.
- Information available to the PPET should "not go beyond publicly available information and the data available to the PPAET, or data that can be obtained via third parties" (ACER Guidance chapter 9.4.1 (468)). We interpret that this available information does not include information from third parties stored behind a paywall, unless the information is otherwise already available to the PPET (e.g. purchased to be used for trading).
  Note that also suspicious behaviours detected by e.g. traders have to be reported based on this guidance.

The **monitoring routine** should be documented in the trade surveillance strategy, containing a description of the monitoring, and can include for example:

- Establishing responsibilities and segregating duties
- How to maintain records
- The use of alerts

If a PPET uses automatic alerts and a level of human analysis, the process of handling such automatic alerts could look as follows:

1. Automatic alerts are generated for a specified time period.
2. A human analyst reviews these alerts, discarding those that are not suspicious and identifying others for further investigation.
3. The analyst further investigates alerts that were not initially discarded. Such an investigation should follow a set **routine for investigations** to determine whether it is deemed a reasonable suspicion for potential breaches of Articles 3, 4, or 5. Points that can be considered when deciding whether to escalate an investigation to a potential breach include:
   - Criteria set out in REMIT regarding market manipulation, disclosure of inside information, and insider trading;
   - ACER Guidance[12];
   - Guidance by NRAs;
   - Published cases with and without sanction decisions[13];
   - Earlier experience.

[12] See overview of ACER REMIT Regulations documents.

[13] See ACER's overview of sanction decisions and the websites of the individual NRAs for more information.

4. Investigated cases are closed either as 'not reasonably suspicious' or 'reasonably suspicious for potential breaches of Articles 3, 4, or 5'.
5. For cases where the trade surveillance unit has reasonable suspicion of a breach of REMIT Articles 3, 4, or 5, they need to send a STOR.

For PPETs who do not use automatic alerts, but e.g. do spot checks, the trade surveillance process can be adapted to follow points 3 through 5 above as appropriate.

If a PPET's trade surveillance identifies a case that does not meet its internal threshold for 'reasonable suspicion' of a breach of Articles 3, 4 or 5, and therefore does not warrant submitting a STOR, the PPET may choose to send a tip-off to, for example, its OMP to alert the OMP's market surveillance team to the behaviour. Note that sending tip-offs does not satisfy the requirements of REMIT Article 15(2) if the PPET itself has a reasonable suspicion.

All investigations and decisions related to investigations should be documented, see also section 2.2.3 *Documentation and record-keeping*.

Writing and filing a Suspicious Transaction or Order Report

In case the trade surveillance of a PPET has reasonable suspicion of a breach of REMIT Articles 3, 4 or 5, it needs to

- **notify ACER** and the relevant **national regulatory authority,**
- without further delay and in any event **no later than four weeks,**
- from the day on which that person becomes aware of the suspicious event; see REMIT Article 15(2).

According to ACER Guidance, the four-week timeline starts once the suspicious quality of an event is established, not at the *occurrence* of the event or when an alert is generated. When e.g. using automatic alerts, this suspicious quality is typically established during the human analysis of the alert, and not already when the alert was triggered or the occurrence of the potentially manipulative event.

REMIT thus does not provide a deadline on the notification which relates to the *occurrence* of a potential manipulative event. However, as part of effective procedures as laid out in REMIT Article 15(3), it is best practice to establish internal targets for how long after the occurrence of an event the trade surveillance function should have notified a case to ACER and the relevant NRAs.

The procedures of a PPET should outline the necessary content of a *Suspicious Transaction or Order Report (STOR),* and how to report it to ACER and the relevant NRAs.
In a STOR, it is considered best practice to include the contents outlined in the ACER Guidance section 9.1.3, "What to notify". A template in line with section 9.1.3 can be

found in Appendix 6 of this document. Please also refer to ACER's Notification Platform Public User Guide[14].
For the submission of the STOR, one should utilize the ACER Notification Platform[15], which ensures secure communication of STORs to ACER and the relevant NRA(s), unless the relevant NRA has specified other means of communication on their website.

Delegating trade surveillance functions

PPATs under REMIT can delegate functions of their monitoring requirements or parts thereof. The ACER Guidance chapter 9.4.3a discusses the delegation of trade surveillance functions for PPATs.

Outsourced Surveillance Activity

[…] PPATs should be able to **outsource** a part of their surveillance activity, including the analysis of orders and transactions, alerts generation for the detection of suspicious events, as well as the identification of potential breaches of Articles 3, 4 and 5 of REMIT.

PPATs will remain fully responsible for the obligations stated in Article 15(1) and 15(3).

The PPATs should:

- **retain the expertise and resources** necessary for evaluating the quality of the services provided and the organisational adequacy of the providers, and for supervising the outsourced services effectively and managing the risks associated on an ongoing basis;
- **have direct access** to the relevant information related to the outsourced service;
- should still **be able to conduct any complementary analysis**; and
- define in a written agreement their rights and obligations and those of the providers. The outsourcing agreement should allow PPATs to terminate it.

Text box 21: ACER Guidance (480)

Although the excerpt above applies to PPATs, similar provisions can be assumed to be applicable for PPETs. Similar to the ACER Guidance, recital 4 of the Delegated Regulation for MAR states that PPAETs can delegate their trade surveillance tasks:

Persons that are professionally engaged in arranging or executing transactions **should be able to delegate the monitoring, detection and identification** of suspicious orders and transactions **within a group** or to **delegate the data analysis and the generation of alerts**, subject to appropriate conditions.

[14] Link to the Public User Guide: https://www.acer-remit.eu/np/download-manual/np-user-manual

[15] Link to ACER Notification Platform: https://www.acer-remit.eu/np/str

Such delegation should make it possible to share resources, to centrally develop and maintain monitoring systems and to build expertise in the context of monitoring orders and transactions. Such delegation should not prevent the competent authorities from assessing, at any time, whether the systems, arrangements and procedures of the person to whom the functions are delegated are effective to comply with the obligation to monitor and detect market abuse.

The obligation to report as well as the responsibility to comply with this Regulation and with Article 16 of Regulation (EU) No 596/2014 should remain with the delegating person.

Text box 22: Delegated Regulation Recital 4

A key difference between the ACER Guidance and the Delegated Regulation for MAR when it comes to outsourcing, is that ACER Guidance explicitly mentions the retention of expertise and resources internally. Both references state that the responsibility remains at the PPAT or PPET in the case of outsourcing.

Thus, it is considered best practice to retain expertise and resources within the PPET to ensure the internal ability to evaluate the quality and organisational adequacy of the outsourced services, as well as to supervise these services effectively and manage associated risks on an ongoing basis.

CHECKLIST PPET

- PPETs who execute transactions in financial instruments **and** wholesale energy products must monitor for breaches of REMIT Articles 3, 4 and 5
- A PPET's monitoring effort should be reasonable and proportionate to its size, complexity and trading activities
- PPETs need to have effective arrangements, systems and procedures to fulfil their monitoring duties, including:
    - An independent market surveillance function
    - A market surveillance strategy and risk assessment
    - Comprehensive routines for monitoring and investigations
- Regular trainings on REMIT are required for relevant staff
- Market surveillance duties can be delegated to a third party, a certain level of expertise and responsibilities must remain in-house

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 section 3.3 when using algorithmic trading solutions. The aim of this section 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. As there is no "one-size-fits-all", each market participant must tailor their compliance regime accordingly. Regardless of the type, size and complexity 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 flow of potential inside information in case of an inquiry from NRAs or for their 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.

(1) '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.
For the purposes of this definition, 'information' means:

(a) information which is required to be made public in accordance with Regulation (EU) 2019/943 and (EC) No 715/2009, including guidelines and network codes adopted pursuant to those Regulations; information relating to the capacity and use of facilities for production, storage, consumption or transmission of electricity, hydrogen or natural gas or related to the capacity and use of LNG facilities, including planned or unplanned unavailability of these facilities;

(b) information which is required to be disclosed in accordance with legal or regulatory provisions at Union or national level, market rules, and contracts or customs on the relevant wholesale energy market, in so far as this information is likely to have a significant effect on the prices of wholesale energy products;

(ca) information which is conveyed by a market participant, or by other persons acting on the market participant's behalf, to a service provider trading on the market participant's behalf and relating to the market participant's pending orders in wholesale energy products, which is of a precise nature and relates directly or indirectly to one or more wholesale energy products; and

(c) other information that a reasonable market participant would be likely to use as part of the basis of its decision to enter into a transaction relating to, or to issue an order to trade in, a wholesale energy product.

Text box 23: REMIT Article 2(1)

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. Note that

- Steps in a lengthy process can be inside information (see REMIT Article 2(1)).
- Own plans and strategies are exempt from the requirement to publish inside information (see REMIT Recital 12).
- If clients convey inside information to a service provider who trades for them, both the client and the service provider are holding inside information and are liable as set out in REMIT, except when it pertains to own plans and strategies.

(i) Information shall be considered to be of a precise nature if it indicates a set of circumstances which exists or may reasonably be expected to come into existence, or an event which has occurred or may reasonably be expected to occur, and if it is specific enough to enable a conclusion to be drawn as to the possible effect of that set of circumstances or event on the prices of wholesale energy products. Information may be considered to be of a precise nature if it relates to a protracted process that is intended to bring about, or that results in, particular circumstances or a particular event, including future circumstances or future events, and also if it relates to the intermediate steps of that process which are connected with bringing about or resulting in those future circumstances or future events. An intermediate step in a protracted process shall be considered to be inside information if it, by itself, satisfies the criteria of inside information as referred to in the first subparagraph of this point.

Text box 24: REMIT Article 2(1)

(12) […] Information regarding the market participant's own plans and strategies for trading should not be considered as inside information

Text box 25: REMIT Recital 12

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, and REMIT Article 4 defines the obligation to publish inside information to the market.

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.

The use of inside information by cancelling or amending an order, or any other trading action concerning a wholesale energy product to which the information relates, where the order was placed before the person concerned possessed the inside information, shall also be considered to be insider trading.

Text box 26: REMIT Article 3(1)

"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.

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

i) Inside information is identified and information flows are mapped; section 3.1.1
ii) Inside information is protected; section 3.1.2
iii) Inside information is not used for market abuse; section 3.1.3
iv) Inside information is published; section 3.1.4

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, hydrogen or natural gas or related to the capacity and use of LNG facilities, including planned or unplanned unavailability of these facilities.

Market participants shall disclose the inside information through IIPs. The IIPs shall ensure that the inside information is made public in a manner which enables prompt access to that information, including through a website or a clear application programming interface, and a complete, correct and timely assessment of that information by the public.

Text box 27: REMIT Article 4(1)

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 – intentional and non-intentional
- Map information flows 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 third parties

Based on the above, each market participant should develop guidance on what kind of information may constitute inside information for the market participant. ACER Guidance Chapter 3.3. opens up for using appropriately tested thresholds[16] for assessing whether information qualifies as inside information. At the time of writing the report, there are indications that a threshold for the reporting of inside information pursuant to Article 4 might be established in the future by a regulatory act. Therefore, at the moment, specific thresholds may be defined, and these could be differentiated in situations with strained power balance.[17] Market participants may need to use informal thresholds for operational purposes so that personnel responsible for handling Urgent Market Messages (UMMs) can respond to situations quickly. 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.

[16] ACER Guidance (45) states that appropriately tested thresholds may include qualitative and quantitative analysis to test the likelihood of a significant price impact.

[17] See also Nord Pool's study on a Threshold for Publishing Inside Information here. Note that this study is provided for information purposes only, and does not constitute legal, technical, or professional advice of any nature and may not be relied upon as such.

It should be noted that while self-defined thresholds are a useful tool for handling information, exceeding the threshold does not automatically qualify the information as inside information.

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 on spreading inside information to any other person, unless it is made in the normal course of employment, profession or duties, and a specific prohibition on 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

Procedures are key when dealing with inside information. Market participants are recommended to make sure to have proper written procedures 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 of how to handle inside information
    - Internal communication process with definition of the point in time the information arises
    - That information is not spread to any unauthorised personnel prior to publication
    - No advice shall be given based on inside information
    - Inside information shall not be 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[18]

The above is a list of possible procedures that ensure 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 prevent inside information from reaching a hectic trading floor where the risk of unintentionally using inside information is higher.

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. See the section on Trade Stops below.

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.

[18] In prior editions of this report also called "Chinese walls".

If trading while holding inside information, the need for very robust processes, including documentation that trading is not and cannot be based on inside information, 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 barriers.

There is no clear definition of an information barrier 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. If such **third party inside information relates to the participant's own business**[19], it falls under the obligations of REMIT Article 4(1). For example, information of a third party's power plant that the market participant is trading on behalf of, or a power plant jointly owned by several market participants. In such cases, all market participants whose business the inside information relates to are responsible for ensuring publication under REMIT Article 4. This requires coordination between the involved parties to ensure that the inside information is only published once, and that the publication is timely and compliant with REMIT requirements. See section 3.1.4 on situations where multiple market participants are responsible for the publication of information.

A market participant could also receive **inside information unrelated to its own business**, but relating to a completely separate third party. For instance, information from a Transmission System Operator (TSO) that affects or could affect the market participant, or information from an upstream production unit. In this case, it is critical to assess if the information is correct, and whether it is truly not tied to the market participant's own business[19].

[19] 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(1)

If the information is inside information, but not related to the market participant's business, the following steps are recommended:

- Protect the information. In particular, prevent the 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.
    - If the information is not published by the owner, depending on the nature of the information and if the risk of disclosing imprecise/incorrect information is little, the market participant may consider publishing the information still, in order to get out of the insider position.

For traders acting on behalf of multiple market participants, we recommend implementing additional safeguards, so that inside information from one market participant is not used for trading for another market participant. Such additional safeguards can be information barriers, increased automation and/or use of algorithms, clearly defined trading mandates and rotating traders' work schedules.

Confidentiality agreements for external contractors

It is recommended to implement confidentiality agreements with external contractors when such contractors 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 they must 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), this inside information should not require any measures like e.g. a trade stop on the trading floor. 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 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 around the information flow,
- Establish periodic/systematic checks of 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 that an NRA or the market surveillance/trade surveillance department of a PPAET 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 barriers around traders

Creating information barriers 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 gain 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 is not 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 prevent traders from doing anything in the trading system whilst in an insider position or a potential inside position.

It is recommended that the routines for trade stop are documented, including when the alarm/lights go 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 28: REMIT Article 3(4)(b)

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 this 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 the use of the exemption 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 also the market surveillance department of the affected PPAET(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 from Article 3(4)(b) 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. Timely is interpreted by the ACER Guidance as "as soon as possible, but at the latest within one hour". For effective disclosure, REMIT Art 4(2)(2) states that "Market participants shall disclose the inside information through IIPs" (Inside information platforms"). For example, Nord Pool's UMM platform is a registered IIP. In ACER's registry of market participants[20], market participants shall disclose which IIP they are using.

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, and are recommended to be prepared for publishing information to the market. This implies having i.e. instructions or agreements, training and access to an IIP in place.

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 publication. 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.

[20] Link to ACER's registry of market participants: https://www.acer-remit.eu/portal/home

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.

Internal publication guidelines

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:
  - It is best practice to develop and use internal "templates" with standard wording to be used in various specified situations
  - Include at least information as stated in the ACER Guidance chapter 4.2.2. on the *Application of the obligation to disclose inside information:*
    - Published either in English only, or in the official language(s) of the relevant Member State and in English (ACER Guidance (126))
    - as concise and as specific as reasonably possible (ACER Guidance (128))
    - as precise and complete enough to allow a correct understanding of the underlying event(s) (ACER Guidance (128))
  - You can find guidance on how to publish inside information on Nord Pool's UMM platform in the REMIT UMM User Manual[21]

- It should state alternative procedures in case of any issues with the system used for publication
  - IIPs shall have redundancy, backup and/or fallback solutions (ACER Guidance (126)). Emergency procedures[22] are to be used in case an IIP is not available.

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

[21] Nord Pool. *REMIT UMM user manual*, version 1.6 (November 2024)

[22] See Nord Pool UMM Emergency procedures, as an example

- 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 publication 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 29: REMIT Article 4(2)

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 actionand 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 – where and 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
  - 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
  - May include routines for handling situations where a third party does not publish inside information affecting a market participants asset/business
  - 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 section 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 section 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, complexity 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 PPAET.

The definition of market manipulation is found in REMIT Article 2. In general terms, market manipulation can happen either through orders and transactions, through disseminating information in any way, including in relation to a benchmark, or by engaging in any other behaviour that could give false or misleading signals.

'market manipulation' means:

(a) entering into any transaction, or issuing, modifying or withdrawing any order to trade or engaging in any other behaviour relating to 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 is likely to secure, by a person, or persons acting in collaboration, the price of one or more 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 such transaction or order to trade conforms to accepted market practices on the wholesale energy market concerned; or
  (iii) employs 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;

(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;

[…]

or

(c) transmitting false or misleading information or providing false or misleading input in relation to a benchmark where the person who made the transmission or provided the input knew or ought to have known that it was false or

misleading, or engaging in any other behaviour which leads to the manipulation of the calculation of a benchmark.

Text box 30: REMIT Article 2(2)

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's prohibition of market manipulation 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.

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

Text box 31: REMIT Article 5

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 or input on benchmarks
  - Insufficient or wrong information or insufficient or wrong input on benchmarks

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; section 3.2.1
ii) Measures to prevent market manipulation through orders and transactions; section 3.2.2
iii) Measures to prevent market manipulation through spreading false or misleading information or input on benchmarks; section 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[2]. 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 PPAETs 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 PPAETs. 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.

Non-participation in the market, such as physical capacity withholding, can also be seen as market manipulation, see footnote 117 in the ACER Guidance. It is recommended to document a legitimate reason for not partaking in the market, which could be, e.g., due to available resources of expected associated costs.

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 **erroneous orders.** Erroneous orders can significantly impact the market and can in some cases qualify as inside information and constitute market manipulation. Market participants are therefore recommended to assess the risks of erroneous orders, and to have routines and procedures in place to prevent unintentional and negligent manipulation as well a clear process for handling erroneous orders should they occur. Measures to prevent and to handle erroneous orders are further discussed in section 3.4.

Specific issues to be aware of

It is recommended that the market participant develops a specific list of behavioural 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 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 / input on benchmarks

In addition to manipulating through orders and transactions, market manipulation can also happen through **spreading false or misleading information or input in relation to a benchmark**. 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.

Benchmark manipulation under REMIT concerns indexes which are used to determine the amount payable under a wholesale energy product or contract, or the value of a wholesale energy product, or indexes that can be used to measure the performance of products or markets (see full definition in ACER Guidance (303)). An example of a benchmark is Nord Pool's System Price. Transmitting false or misleading input in relation to a benchmark may be considered market manipulation, irrespective of the extent to which said benchmark is used by the market participant.

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

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

3.3. Algorithmic trading solutions

Any algorithm deployed by a market participant in a wholesale energy market is subject to REMIT. This means that it has to follow the regulation's general prohibitions on market abuse, implicitly requiring that any algorithmic trading solution[23] is subject to robust governance such that it neither abuses the market nor creates disorderly conditions.

(1) A market participant that engages in algorithmic trading shall have in place effective systems and risk controls suitable to the business it operates to ensure that its trading systems

- are resilient and have sufficient capacity,
- are subject to appropriate trading thresholds and limits and
- prevent the sending of erroneous orders or
- otherwise function in a way that may create or contribute to a disorderly market.

The market participant shall also have in place effective systems and risk controls to ensure that the trading systems comply with this Regulation and with the rules of an OMP to which it is connected. The market participant shall have in place effective business continuity arrangements to deal with any failure of its trading systems and shall ensure that its systems are fully tested and properly monitored so that they meet the requirements laid down in this paragraph.

(2) A market participant that engages in algorithmic trading in a Member State shall notify that engagement to the national regulatory authority of the Member State where it is registered pursuant to Article 9(1) and to the Agency.
The national regulatory authority of the Member State where the market participant is registered pursuant to Article 9(1), may require the market participant to provide, on a regular or ad hoc basis, a description of the nature of its algorithmic trading strategies, details of the trading parameters or limits to which the trading system is subject, key compliance and risk controls that are in place to ensure that the requirements laid down in paragraph 1 of this Article are satisfied and details of the testing of its trading systems.
The market participant shall arrange for records to be kept for five years in relation to the matters referred to in this paragraph and shall ensure that those records are sufficient to enable the national regulatory authority of the Member State where the market participant is registered pursuant to Article 9(1) to monitor compliance with this Regulation.

(3) […]

(4) This Article is without prejudice to the obligations laid down in Directive 2014/65/EU.

Text box 32: REMIT Article 5a(1-2, 4)

[23] This section uses "algorithmic trading solution", "algorithmic trading" and "algorithm" interchangeably.

Moreover, REMIT includes additional obligations towards market participants who are engaged in algorithmic trading under Article 5a.

The aim of this section is to discuss and recommend a governance model and procedures around algorithmic trading of wholesale energy products to ensure compliance with REMIT. The section is organised according to the lifecycle of an algorithm, addressing relevant REMIT considerations and associated best practices at each stage. We look at the obligations of REMIT Article 5a, and recommend best practices for implementing algorithmic trading solutions in compliance with REMIT. Some of the best practices mentioned in this section are inspired by the financial regulation, such as MiFID and Regulatory Technical Standard (RTS) 6, but are judged to fit well with the power market. Please note that this section does not cover REMIT Article 5a(3) on direct electronic access.

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.

It is 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. Note that there is no "one-size-fits-all" approach.

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 section. 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.

This section on algorithmic trading solutions in wholesale energy markets first defines which algorithmic trading is subject to Article 5a in section 3.3.1, and then outlines the **best practice governance model to comply with REMIT** as an algorithmic trader under REMIT and for ensuring robust and effective operation of the trading solutions.

3.3.1. Definition of algorithmic trading

'Algorithmic trading' means
- trading, including high-frequency trading, in wholesale energy products
- where a computer algorithm automatically determines
  - individual parameters of orders to trade 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 human intervention or no such intervention at all,
- not including any system that is only used
  - for the purpose of routing orders to one or more organised marketplaces 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 33: REMIT Article 2(18)

The definition of algorithmic trading in wholesale energy markets of REMIT is very closely aligned with that of MiFID II Article 4(1)(39). ACER Guidance on REMIT includes guidance on which algorithms are in scope of the new notification obligation as regards algorithmic trading of REMIT Article 5a, see Table 1.

Table 1: ACER's distinction what is in scope and what is out-of-scope of REMIT Article 5a[24]

In-scope	Out-of-scope
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. Examples are execution and trading algorithms. 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. 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. An example for such an algorithm are signal generators.

[24] Refer to *ACER 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*, 6.1st edition (18 December 2024), p. 103-104.

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.[25] 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) 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 section 3.3.7 on "Post-deployment management").

3.3.2. General organisational requirements

REMIT Article 5a(2) requires market participants to notify the NRA of the Member State where they are registered about the usage of algorithms, similar to the obligations under financial regulation[26]. In its Guidance on REMIT, ACER states that this should be done via its Centralised European Register of Energy Market Participants system (CEREMP)[27]. ACER Guidance (347) states that market participants registered in Italy, Romania and Slovenia need to notify the NRA directly, and by doing so they will be considered to have also notified ACER.

Following REMIT Article 5a(2), algorithmic traders are to keep documentation, which can be required at any point in time by the NRA of the Member State where they are registered. See more on best practices for record keeping in section 3.3.8.

[25] At the time of writing this report, there are indications that a forthcoming regulatory act may introduce a requirement for reporting an algorithm ID for each transaction, expecting to allow the distinction among the different algorithmic strategies through its identification code components.

[26] MiFID II Article 17(2)

[27] Link to ACER's CEREMP: https://www.acer-remit.eu/portal/ceremp

(2) A market participant that engages in algorithmic trading in a Member State shall notify that engagement to the national regulatory authority of the Member State where it is registered pursuant to Article 9(1) and to the Agency.
The national regulatory authority of the Member State where the market participant is registered pursuant to Article 9(1), may require the market participant to provide, on a regular or ad hoc basis, a description of the nature of its algorithmic trading strategies, details of the trading parameters or limits to which the trading system is subject, key compliance and risk controls that are in place to ensure that the requirements laid down in paragraph 1 of this Article are satisfied and details of the testing of its trading systems.
The market participant shall arrange for records to be kept for five years in relation to the matters referred to in this paragraph and shall ensure that those records are sufficient to enable the national regulatory authority of the Member State where the market participant is registered pursuant to Article 9(1) to monitor compliance with this Regulation.

Text box 34: REMIT Article 5a(2)

Article 5a(1) requires algorithmic traders to have effective systems and risk controls for REMIT compliance. This refers to both technical and organisational arrangements, and can include:

- The hardware and software used for trading, order management and connectivity to OMPs, see considerations for the design of algorithms outlined in sections 3.3.3 and 3.3.9.
- Procedures and controls for monitoring trading activity, detecting errors or suspicious behaviour and ensuring compliance with regulatory requirements, see section 3.3.7.
- Processes for managing operational risks, such as system outages, cyber security threats or data integrity issues, see section 3.3.6.
- Risk controls may include a separation of responsibilities of trading desks and supporting functions, see section 2.1.3.

(1) […] The market participant shall also have in place **effective systems and risk controls** to ensure that the trading systems **comply with this Regulation** and with the rules of an OMP to which it is connected.

Text box 35: REMIT Article 5a(1)

Dependent on the size and complexity of the market participant's algorithmic trading activities, it is advisable to appoint a department or at least one person responsible for compliance with REMIT. This role may be combined with other tasks if sufficient independence is maintained.

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 section "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 section 3.3.7 on "Monitoring").

Each market participant is best suited to decide on the exact governance model. However, it is recommended to ensure that algorithmic trading solutions are fit-for-purpose at all times. As a minimum, this includes the ability to withdraw any algorithm from the market at any time (see further details regarding the "kill functionality" in section 3.3.6) and clear documentation of which persons have access rights to deploy or modify the coding or trade parameters of an algorithm.

3.3.3. Design recommendations[28]

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. Article 3 on insider trading and Article 5 on market manipulation). This can be ensured through appropriate training sessions on relevant market abuse types. Note that further, REMIT Article 5a(1) requires algorithmic traders to ensure that their operations prevent sending of erroneous orders or otherwise function in a way that may create or contribute to a disorderly market.

(1) A market participant that engages in algorithmic trading shall have in place effective systems and risk controls suitable to the business it operates to ensure that its trading systems

- are resilient and have sufficient capacity,
- are subject to appropriate **trading thresholds and limits** and
- **prevent** the sending of **erroneous orders** or otherwise function in a way that may create or contribute to **a disorderly market**.

Text box 36: REMIT Article 5a(1)

[28] This section discusses recommendations for in-house made algorithms. For recommendations regarding third-party vendor algorithms, see section 3.3.9.

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, it is advisable that market participants have the ability to immediately stop any trading activity by an algorithm as an emergency measure. See further details on such a kill functionality in section 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 trading thresholds and limits, one can draw inspiration from the financial regulation's RTS 6 (see also as mentioned in section 3.3). RTS 6 mentions pre-trade controls like price collars, maximum order values and maximum order volumes. For post-trade controls, see section 3.3.7 on monitoring. 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.

An order-to-trade ratio rule 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. Other useful pre-deployment parameters include predefined limits on the number of products traded, on the price, value and number of orders, on strategy positions, and on the number of trading venues to which orders are sent.

Furthermore, each market participant should carefully assess what information or analytic input an algorithm is using and whether 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 section 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
- 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 contains or potentially contains inside information.

3.3.4. Test process

> (1) […]
> The market participant shall […] have in place effective systems and risk controls to ensure that the trading systems comply with this Regulation and with the rules of an OMP to which it is connected. The market participant shall have in place effective business continuity arrangements to deal with any failure of its trading systems and **shall ensure that its systems are fully tested** and properly monitored so that they meet the requirements laid down in this paragraph.

Text box 37: REMIT Article 5a(1)

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 if the algorithm is directly connected without a trading venue-approved third party solution
2) Testing of trading activity to ensure that the algorithm behaves as intended.

Such 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 reasons 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 whether the algorithmic trading strategy:

- does not behave in an unintended manner
- complies with REMIT
- complies with the rules and systems of the OMP
- 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

Furthermore, several potential test scenarios could be used, and each market participant should assess the necessity of these test scenarios:

- Test scenarios based on ACER Guidance: Could the algorithm be accused of breaching any of the market abuse types described in ACER 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.)

3.3.5. Approval process

As part of the requirement for "effective systems and risk controls" in algorithmic trading, see REMIT Article 5a(1), it is recommended to have a formalised approval process before deployment. This is recommended 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 be able to be demonstrated to the satisfaction of the responsible persons.

It is then the members of the committee or the single person who bear the responsibility within the organisation for the proper deployment of the algorithm. The responsibility of a breach of REMIT 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.
- A 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 Guidance on different market abuse types.
- A 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?
- An overview of the selected trade parameters (pre- and post-trade controls and, if applicable, pre-deployment parameters mentioned in section 3.3.3) 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 of 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 an assessment of whether the current monitoring arrangements (see point 3.3.8 below) are suitable for the new/updated algorithm.

3.3.6. Post-deployment management

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.

(1) […]
The market participant shall […] have in place effective systems and risk controls to ensure that the trading systems comply with this Regulation and with the rules of an OMP to which it is connected. The market participant shall have in place **effective business continuity arrangements to deal with any failure** of its trading systems and shall ensure that its systems are fully tested and properly monitored so that they meet the requirements laid down in this paragraph.

Text box 38: REMIT Article 5a(1)

REMIT Article 5a(1)'s requires "effective business continuity arrangements to deal with any failure" of algorithmic trading systems. This refers to the plans and measures in place to ensure trading operations can continue, or be swiftly resumed, following a disruption or system failure. This can include:

- Procedures for responding to system failures, cyber incidents or other emergencies affecting trading activities
- Backup systems and data recovery processes to restore trading capability and protect critical information
- Regular testing of these arrangements to ensure they are effective and up to date
- Clear roles and responsibilities for staff during a disruption

A crucial aspect of business continuity is the inclusion of a **kill functionality**, that means that the market participant needs to be able to stop the algorithm's trading activity at any time. 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)?
- Is approval by another function/a second person required 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, taking examples from RTS 6, 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. These can also be relevant for algorithmic trading under REMIT.

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) perform 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.

3.3.7. Monitoring

> (1) […]
> The market participant shall […] have in place effective systems and risk controls to ensure that the trading systems comply with this Regulation and with the rules of an OMP to which it is connected. The market participant shall have in place effective business continuity arrangements to deal with any failure of its trading systems and **shall ensure that its systems are** fully tested and **properly monitored** so that they meet the requirements laid down in this paragraph.

Text box 39: REMIT Article 5a(1)

REMIT outlines that the trading systems shall be properly monitored to make sure they comply with REMIT and with the rules of the OMP. This is primarily understood as there should be monitoring for the technical functioning of the algorithm: It is important that the algorithm acts as intended and does not cause disruptions or technical issues. To the extent that the complexity of the algorithm, the trading speed and/or 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. Some elements of monitoring might not be time-critical and can be done ex-post, e.g. statistical analysis.

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.

Depending on the complexity of an algorithmic solution, one might also need to monitor for the algorithm's compliance with REMIT's prohibitions against market manipulation and insider trading. In most cases, such monitoring does not have to happen close to real time. For inspiration on monitoring systems, see also section 2.2.4 on systems used by PPETs for detection of suspicious activity.

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).

3.3.8. Record keeping

(2) […]
The national regulatory authority of the Member State where the market participant is registered […], may require the market participant to provide, **on a regular or ad hoc** basis,

- a description of the nature of its algorithmic trading strategies,
- details of the trading parameters or limits to which the trading system is subject,
- key compliance and risk controls that are in place to ensure that the requirements laid down in paragraph 1 of this Article are satisfied and
- details of the testing of its trading systems.

The market participant shall arrange for **records to be kept for five years** in relation to the matters referred to in this paragraph and shall ensure that those records are sufficient to enable the national regulatory authority […] to monitor compliance with this Regulation.

Text box 40: REMIT Article 5a(2)

Under REMIT Article 5a(2), NRAs may request information on algorithmic trading strategies from market participants at any time. See more details on this in section 3.3.8. which describes the record keeping for algorithmic trading solutions.

Market participants should store relevant documentation to be able to answer any inquiry from a trading venue or an NRA as well as for internal purposes.

The amended REMIT introduced specific record-keeping requirements for algorithmic trading in Article 5a, allowing NRAs to request documentation on a regular or ad-hoc basis. This documentation should cover, but is not limited to, the following (italics as mentioned in REMIT Article 5a, non-italics reflect our advised best practice approach):

- *Nature of Algorithmic Trading Strategies:* Description of the algorithmic trading strategies, expected behaviour and information input per algorithm and trading strategy as applicable
- *Trading Parameters and Limits:* Description of the trade parameters and limits.
- *Compliance and Risk Controls:* Description of effective compliance and risk control measures tailored to the specific algorithmic trading activities. This includes checking bids via automatic controls and thresholds and can also include further controls.
- *Testing and monitoring of algorithmic trading:*
  - 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 or trading strategy as applicable
  - Change log which registers updates made to an algorithm or trading strategy as applicable (Timing of the update? What was the update? Reason for the update? Who did the update? Who approved the update?)

Records must be kept for five years.

It is up to the market participant to decide on the exact content and form of such documentation. However, it should be detailed enough to be able to re-construct which version of the algorithm (trading parameters, trading strategy, information input, …) 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 made by algorithms and trading strategies as applicable. If a log of orders and transactions is accessible through the trading venue, it may not be necessary for the market participant to keep a separate log.

3.3.9. Algorithms from third-party vendors

Any third-party vendor algorithm engaged in markets regulated by REMIT needs to fulfil the requirements set out by REMIT Article 5a laid out in the prior sections. Market participants remain fully responsible for the trading activity generated by third-party vendors algorithms. This applies also to algorithmic trading providers that may have received technical approval from a power exchange - such approval does not imply automatic compliance with REMIT.

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 must assess whether the documentation provided by the third-party vendor of e.g. of functional specifications and testing procedures is sufficient for that purpose.

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 7 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 defined as trading with limited or no human intervention and is based on a computer algorithm automatically
    - determining individual parameters of orders, or
    - managing the order after its submission.

- Algorithmic trading with wholesale energy products is subject to REMIT's prohibition against market abuse and any specific requirements imposed by relevant trading venues.

- REMIT imposes specific obligations on algorithmic trading regarding effective systems and risk controls.

- Market participants engaged in algorithmic trading must notify the national regulatory authority.

- 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 and trading strategies work.

- Independent functions such as risk management and compliance must have a robust understanding of the market participant's algorithms and trading strategies.

- Algorithms and trading strategies 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.

- Algorithmic traders need to have effective systems in place to avoid breaches of REMIT.

- Relevant documentation about algorithms and trading strategies must be stored for at least five years.

3.4. Erroneous orders

3.4.1. Background

Erroneous orders are a risk for market participants trading in the wholesale energy market. Errors can have a significant impact on the market and can in certain cases qualify as inside information and/or constitute market manipulation.

Section 3.4 outlines a best practice approach for preventing and mitigating risks of erroneous orders, as well as for handling them should they occur. While the term "erroneous order" is used throughout the chapter, the suggested measures can be relevant for preventing other undesired situations related to bidding, as deemed relevant by market participants.

There is no "one-size-fits-all" when it comes to compliance measures, market participants should thus evaluate which measures are appropriate in the context of their business.

The recommendations in this section build upon earlier sections of the report, particularly section 3.1 on Inside Information and section 3.2 on Market Manipulation and should be reviewed in that context. The section also builds on guidance from regulatory authorities.[29]

3.4.2. Considerations around market manipulation and ACER's description of erroneous orders as market manipulation

Market manipulation is prohibited under REMIT Article 5. An erroneous order can qualify as market manipulation if it satisfies the definition of market manipulation as outlined in REMIT Article 2. This is because the erroneous order can send false or misleading signals as to the supply, demand, or price of wholesale energy product(s), or the prices can have been secured at artificial levels[30]. At the same time, not all erroneous orders are market manipulation.

ACER describes erroneous orders that satisfy the definition of market manipulation under REMIT Article 2 as:

---

[29] Autoriteit Consument & Markt (ACM). *Dealing with erroneous orders*. https://www.acm.nl/en/about-acm/remit-obligations/dealing-erroneous-orders
Autoriteit Consument & Markt (ACM). *Prevent, report, and follow up on erroneous orders*. https://www.acm.nl/en/prevent-report-and-follow-erroneous-orders#prevent-and-detect-mistakes
Commission de Régulation de l'Énergie (CRE). *Deliberation of Commission de Regulation de l'Énergie of April 14, 2022, relating to communication on the publication on of information relating to operational errors in the wholesale energy markets*. https://www.cre.fr/fileadmin/Documents/Deliberations/import/220414_2022-113_Communication_erreurs_operationnelles.pdf
Reguleringsmyndigheten for Energi (RME). *Erroneous orders in the day-ahead market may involve a breach of the prohibition on market manipulation*. https://www.nve.no/reguleringsmyndigheten/bransje/markedsovervakning/veiledning-til-aktoerer-markedsadferd-og-transparens/feilordre-i-doegnmarkedet-kan-innebaere-brudd-paa-forbudet-mot-markedsmanipulasjon/

[30] Notably, according to ACER, the definition does not require intent for the behaviour to be considered market manipulation. This is reflected in ACER Guidance Chapter 6.2, which notes that erroneous trading activity can be manipulative.

Erroneous orders as market manipulation
Unintentionally placing orders or entering into transactions that send false or misleading signals regarding supply, demand, or price of a wholesale energy product.

Text box 41: ACER Guidance chapter 6.1 (315 point L)

However, not all erroneous orders are manipulative. Consequently, ACER's description only applies to a subset of all erroneous orders. This relationship is illustrated in the figure below.

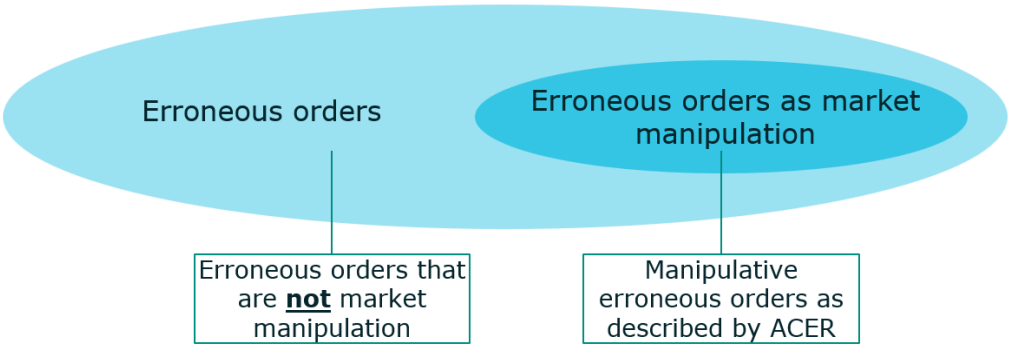

Figure 4: Relationship between erroneous orders and the subset of manipulative erroneous orders as described by ACER.

When the term "erroneous orders" is used in Section 3.4, it is reflecting all erroneous orders, including both those that may or may not be manipulative. The considerations and measures proposed in the following sections can also be relevant for other bidding-related incidents.
Market participants may use the measures proposed in this section to prevent erroneous orders and other bidding-related incidents to mitigate the risks related to those at their own discretion.

3.4.3. Publication of information about erroneous orders

If an erroneous order has occurred, it may be relevant to publish information about it through a UMM.
Publishing information on erroneous orders can serve at least two purposes within the REMIT framework:

- Firstly, if the erroneous order qualifies as inside information (see Section 3.4.4 for details) publication is required under **REMIT Article 4**. Such publication must be effective and timely, as described in section 3.1 on Inside Information of this report. This might also limit potential impact to the market of the error[31].

[31] In addition, in some countries such publication may also be relevant in determining the sanction. See example in Finland: https://www.finlex.fi/fi/lainsaadanto/2013/590#L4P20

- Secondly, if the erroneous order constitutes inside information, publishing information on the error allows the market participant to trade based on the disclosed information without breaching the prohibition of insider trading in **REMIT Article 3**. This might include trading to correct an erroneous position.

3.4.4. Considerations on erroneous orders and inside information

Inside information means information of a precise nature which, if it were made public, would be likely to significantly affect the prices of wholesale energy products. Further, information regarding the market participant's own plans and strategies for trading shall not be considered inside information. Based on this definition, information about an erroneous order in wholesale energy markets can qualify as inside information.
It is important to assess whether erroneous orders constitute inside information, as not all such orders meet the criteria. Important factors to consider may, for instance, include the size of the order, the price of the order, the market fundamentals, and to what extent and in which way and timeframe the erroneous order leads to trading that was not intended. Market participants may use internal thresholds for assessing whether erroneous orders shall be treated as inside information, as outlined in Section 3.4.5.
Following are two examples of erroneous orders. The first example illustrates a situation where information about the error is more likely to constitute inside information than in the second example.

Example

Situation: A market participant entered an order in the day-ahead market, offering 500 MW more for sale than intended in the relevant MTU at a price of €30/MWh. The market price cleared at €40/MWh in the relevant MTU, and the market participant became aware of the error only after the auction results were published. The market participant's willingness to trade was at prices higher than the realized market price.

Considerations: The order resulted in 500 MW erroneously traded volume in the relevant MTU. The market participant deems that the auction price might have been impacted, which in turn could potentially result in that information about the error can have a significant price impact on markets where trading opportunities are still open (such as the intraday and financial market).

The second example illustrates a situation where the erroneous order is less likely to constitute inside information.

Example

Situation: A market participant entered an order in the day-ahead market, offering 500 MW more for sale than intended at a price of €250/MWh. The market price cleared at €50/MWh, and the market participant became aware of the error only after the auction results were published.

Considerations: The order did not lead to any erroneously traded volumes in the relevant MTU, thus it is not likely that it had a significant impact on the realised market price and, therefore, on any other markets where trading opportunities are still open. Therefore, information about the order is not likely to constitute inside information.

When assessing whether an erroneous order is inside information the price impact of the erroneous order shall be considered in relation to subsequent markets and products that are still available for trading. That may include intraday, balancing markets, or financial products.

Notably, the erroneous orders illustrated in the examples above could be subject to different considerations regarding whether they constitute inside information, depending on e.g., the market conditions.

Erroneous orders are often detected after the order is placed to the market. The longer the delay in detection, the less likely the erroneous order is to constitute inside information. This is because the potential impact of publishing information about the error on the price of related wholesale energy products diminishes once those products can no longer be traded. For example, erroneous orders in the day-ahead market detected after a year are typically only relevant for a few financial products.

Regardless of whether the information constitutes inside information, the erroneous order may still qualify as market manipulation.

3.4.5. Threshold for disclosing information about an erroneous order

When an erroneous order occurs, the market participant should assess if information about the order constitutes inside information, as explained in the previous section. This involves assessing whether, under the case-specific circumstances, the information about the erroneous order is likely to significantly affect the prices of wholesale energy products if made public.

Such assessments can be complex, as erroneous orders may arise at any time, be identified in different parts of the organisation, and require careful handling by those possessing potential inside information. If deemed inside information, it must be disclosed in a timely manner, as detailed in section 3.1, which creates time pressure.

ACER Guidance Chapter 3.3 recommends best practice compliance rules including a framework for assessing whether information qualifies as inside information by using appropriately tested thresholds:

The best practices for internal compliance rules may include:
a framework for the assessment of whether the facts at hand can be qualified as inside information. This may include, for example, measures on how to identify inside information, appropriately tested thresholds[45], etc.

Text box 42: ACER Guidance's best practices for internal compliance rules

In a footnote, ACER Guidance states that appropriately tested thresholds may include qualitative and quantitative analysis to evaluate the likelihood of a significant price impact.

For example, qualitative and quantitative (econometrical) analysis to test the likelihood of a significant price effect.

Text box 43: ACER Guidance footnote 45

Thus, market participants may implement appropriately tested thresholds as a convenient practical measure for treating information about an erroneous order as inside information. The level of the threshold should take into account the specific nature of information regarding erroneous orders as compared to information on unavailability[32].
While thresholds can help streamline the handling of information on erroneous orders, exceeding the threshold does not automatically qualify the information as inside information. Furthermore, the potential price impact of an erroneous order may differ from that of an unavailability of the same scale, meaning that different considerations may apply in each case.

3.4.6. How to publish information about erroneous orders

If an erroneous order constitutes inside information, the market participant must publish information about the erroneous order to comply with disclosure requirements set out in REMIT Article 4, and to avoid the risk of insider trading, which is prohibited under REMIT Article 3. The inside information shall be published on a certified inside information platform (IIP), such as the Nord Pool REMIT UMM platform.
When publishing the information on an IIP, it is considered best practice to use the "Remarks-field" (or similar) to inform the market of

- the realised volumes that were erroneously offered and whether they were sold or bought
- which market the order was placed on
- the affected timeframes

To ensure timely and effective publication, it is best practice to establish a procedure for handling erroneous orders and create a template for publishing information about

[32] In 2022, Nord Pool published a report suggesting 100 MW as an appropriately tested threshold for inside information in the Nordic and Baltic wholesale electricity market. However, the market participant may assess if the threshold suggested in the report is relevant also for erroneous orders.

erroneous trades. See Section 3.4.13 for processes for handling erroneous orders, and Section 3.4.7 for UMM template examples to publish information on Nord Pool's platform. When using other platforms, procedures should be tailored to those platforms.
REMIT Recital 12 states that *"information regarding a market participant's own plans and strategies for trading should not be considered as inside information"*. Thus, market participants are not required to publish details on how erroneous orders are handled. Nor are they required to publish details about the order beyond the information on what was erroneously traded. This is important to avoid potential collusion between market participants.

3.4.7. Publishing information about erroneous orders on an IIP

When publishing a UMM for an erroneous order via the Nord Pool IIP, one should use the message type "Other Market Information". Similar message types are available on other IIPs. It is recommended to prepare a template for the UMM text that includes the necessary details about the erroneous order, which can be filled in the Remarks field. The template should be easily accessible to relevant personnel, allowing them to quickly retrieve and use it when needed. Below are two examples of UMM templates.
The first UMM template is to be used when it is possible to simplify the information, while keeping it sufficiently precise, e.g., when the volume range of the erroneous order is close to its average:

UMM TEMPLATE EXAMPLE:
GENERAL

"Incorrect bids for delivery date [*insert date*] were submitted to the [*insert market*] in [*insert bidding zone*]. These incorrect bids led to a volume of [*insert average volume of error*] MW on average between MTU [*insert first MTU affected*] and [*insert last MTU affected*] [*insert time zone*] with a minimum of [*insert minimum volume of error*] MW and a maximum of [*insert maximum volume of error*] MW [*being/not being*] [*sold/bought*]."

UMM TEMPLATE EXAMPLE:
SEVERAL SINGLE MTU ERRORS

"Incorrect bids for delivery date [*insert date*] were submitted to the [*insert market*] in [*insert bidding zone*]. These incorrect bids led to a volume of [*insert volume of error*] MW in MTU [*insert MTU affected*] [*insert time zone*], [*insert volume of error*] MW in MTU [*insert MTU affected*], and [*insert volume of error*] MW in MTU [*insert MTU affected*] [*being/not being*][*sold/bought*] compared to what was intended."

3.4.8. Informing Regulatory Authorities

Publishing information about erroneous orders makes it publicly available, including to NRAs, so that further notification is generally not needed.
However, market participants classified as PPAETs under REMIT Article 15 are required to notify the relevant NRA if they reasonably suspect that the erroneous order constitutes a breach of REMIT Articles 3, 4 or 5. This is done by submitting a Suspicious Transaction and Order Report (STOR).

3.4.9. Informing the exchange

Publication of information about erroneous orders on an IIP makes the information publicly available. Notifying the exchange of the error in addition, should not be necessary. However, some exchanges might have specific provisions requiring this information to be communicated to them directly.

3.4.10. Risk areas relevant to erroneous orders

Section 2.1.4 on compliance risks emphasizes the need for market participants to conduct a risk assessment to establish an effective compliance regime with the right measures.
The following section highlights potential risk areas that may be relevant to consider when evaluating the risk of erroneous orders. Please note that the list is not exhaustive, and other factors specific to the organisation of the market participant may also play a role.

System errors

The availability of critical systems in the trading process can affect a market participant's risk of erroneous orders. For example, internal IT issues may cause system downtime, disrupting the trading process and preventing the submission of correct bids before gate closure, e.g., in the day-ahead market. Similarly, an external network error could disrupt a market participant's connectivity to the exchange's trading platform. Such a system error could prevent access to the trading platform, either directly or through an API solution, thus hindering the market participant's ability to submit correct bids.

Example

A market participant is in the process of submitting both curve and block orders to the day-ahead market. However, due to a system error, only the block orders are successfully submitted. As a result, the market participant offers only a portion of their intended volume, effectively selling less to the day-ahead market than planned.

Third party errors

Market participants' risk of erroneous orders can be affected by factors attributable to third parties. For example, market participants may rely on input in the trading process from a forecast provider, or from clients. If the input is delayed or erroneous, it could lead to the market participant placing orders that are based on the wrong assumptions.
It is recommended to introduce measures for controlling, to the extent possible, that the orders placed by market participants are correct.

Process errors

The risk of erroneous orders may be negatively influenced by process issues in the trading process. For example, inadequate workflow controls may cause deviations in the trading process from the defined procedures, potentially leading to missed steps.
Another example involves manual processing of data, for example, copying data from one tool into another, such as forecasts into planning and trading tools. This introduces vulnerability to copy-and-paste errors, potentially leading to erroneous orders being submitted to the market. Automating such steps can reduce the risk of such errors occurring.

Human errors

Human errors, such as manual data entry mistakes, are a common cause of erroneous orders. Traders may, for example, accidentally enter the wrong price or volume for an order, mix up the values for price and volume, confuse the purchase and sales data, or

Example

Due to a stressful situation a trader makes a mistake and places a sell order to the day-ahead market with a volume of 300 MW instead of the intended volume of 200 MW.

enter volume and price data from the wrong day. These erroneous orders, though likely unintentional, can distort the market outcome, and may qualify as inside information and/or market manipulation.

Human errors often arise from process errors, as insufficient processes can increase the likelihood of mistakes. The following section outlines approaches to reduce the risk of erroneous orders and enhance the robustness of the market participants' processes.

3.4.11. Approaches to prevent and mitigate the risks of erroneous orders

To reduce the risk of erroneous orders, it is recommended to implement appropriate preventive and mitigating measures.
There is no "one-size-fits-all" in terms of compliance measures, and market participants should evaluate which measures are most appropriate and effective for their specific business context. For example, a market participant trading larger volumes in the day-ahead market may require different measures than one trading smaller volumes in continuous markets.
The following sections provide practical measures that market participants may consider implementing to reduce the risks of erroneous orders. However, it is important to note that while these measures can mitigate the risks, they cannot eliminate them entirely.
Some of the measures recommended below may also contribute to fulfilling requirements set out under REMIT Article 5a on algorithmic trading.

Limiting manual steps in the trading process

Manual steps in the trading process carry a risk of errors, which can lead to erroneous orders. Automating these steps can reduce the risk of human mistakes but may introduce new risks, such as system and process errors. To address this, market participants should carefully consider automation, in order to limit manual steps in the trading process.
An example of automation is to automate solutions for flowing source data into internal planning and bidding tools as this could reduce the likelihood of data corruption during the transferring process and wrong data selection such as e.g., importing data from the wrong day. It is important to note that automation does not eliminate the risk entirely, and market participants are recommended to implement control measures and periodically review the automated solutions.
For market participants trading on behalf of clients, it could be relevant to consider automating the process for importing external data such as client nominations.
Automation of manual steps can be combined with other mitigating measures. These measures could include alert functions in internal bidding and trading tools, along with testing of tools and source data, as outlined below. Such strategies can help market participants balance the different risks associated with manual and automated processes.

Pre-trade limits

By implementing a pre-trade limit tool, market participants can set minimum and maximum limits for offered volumes and prices. The tool could be set to flag orders that exceed these limits and to require manual confirmation before allowing the trader to proceed. If relevant, the tool could be designed to set different limits for different production units, bidding areas etc.
Market participants should assess all flagged orders and confirm that they are correct before gate-closure time as both offering excessive or too little volume, or incorrect prices should be avoided.

Example

Situation: A trader mistypes the bid volume for a production unit with an installed production capacity of 20 MW and offers 200 MW instead of the 20 MW for the unit.
Considerations: If the pre-trade limit in the example is set to the level of the maximum installed capacity of the production unit (20 MW), the order would be flagged in the pre-trade limit tool and should be corrected by the market participant before the gate closure time of the auction.

Testing and monitoring of tools and source data

Tools and source data that market participants rely on during the trading process may be subject to errors, which can increase the risk of erroneous orders. For example., tools may contain software bugs or other vulnerabilities, while source data could be incorrectly formatted or become corrupted during transfer or processing.
To mitigate these risks, market participants are advised to appropriately test the tools in a testing environment before deployment. This can help to identify potential software bugs and other errors or vulnerabilities, so that they can be corrected.
Similarly, market participants are advised to implement measures to validate source data before use, for example, by checking for issues such as incompleteness, inaccuracies, or formatting problems in the data. The purpose is to ensure that the data is accurate, consistent, and properly formatted before it is applied to the trading process.
After deployment, source data should be continuously monitored, both in terms of format and consistency, to reduce the risk of errors.

Alert functions in internal bidding and trading tools

Alert functions can be integrated into internal bidding and trading systems to identify and notify market participants of potential errors. For example, an alert can be designed to notify when there is a mismatch between the source data, such as a production unit's available capacity, and related abnormal data entered into the bidding and trading tools. When implementing such alerts, it is important to ensure that inside information is not used for trading, i.e., availability data must not include data on outages that have not yet been publicly disclosed. Another example of an alert is one that highlights discrepancies between real-time production and the production plan with a certain threshold.

Example

Situation: Real-time production of a market participant falls below the planned production by 102 MW.
Considerations: If the market participant has defined a 100 MW threshold for the deviation between real-time and planned production, the alert should notify the traders, who in turn can make sure to not overcommit by placing orders they cannot fulfil. However, it is important that market participants assess if information provided by such alerts constitutes inside information, and if so, follow internal procedures for handling inside information.

Preventing erroneous orders by algorithms

To mitigate the risk of erroneous orders in algorithmic trading, it is recommended that market participants implement a robust governance model as described in section 3.3 on Algorithmic trading solutions and comply with the requirements in REMIT Article 5a. This could involve appropriate controls, such as limits on order volume, price, frequency, and real-time monitoring to detect potential malfunctions in the algorithmic trading solution.

Back-up solution

Market participants may experience an IT system outage, reducing the support from technical tools in the bidding process. In such cases, they have to rely more heavily on manual solutions, as well as the training and competence of their personnel.
To mitigate this risk, it is recommended that market participants establish routines for submitting and updating safety bids[33] to the relevant auction in advance. Submitting bids in advance provides a safety net, reducing potential market impact resulting from system failures.
It is also recommended that market participants that submit bids through an API solution ensure that relevant personnel are familiar with how to log in and navigate in any trading user interface used for backup, should issues arise with submitting bids through the API. To achieve this, it is recommended to arrange regular training on backup solutions for relevant personnel.

Reasonability check tool

Some power exchanges have implemented reasonability checks in the exchanges' day-ahead auction system. One example is the Nord Pool reasonability check, which is an on-

[33] *Safety bid* refers to an approximate bid entered well before the auction's gate closure, and which is updated closer to gate closure.

a-best-effort service where submitted curve orders are compared with previous trading days. A substantial deviation based on the reference day price will flag the submitted curve order.
Typically, market participants trading with a power exchange have access to the platform's trading user interface. When an order is flagged in a reasonability check, it may be highlighted and accessible to the market participant through the trading user interface. Market participants are advised to keep reasonability check tools enabled in the trading user interface, and to review all flagged orders. Any incorrect orders should be adjusted before gate closure.
Reasonability check tools may be built into the market participant's internal planning and bidding tools. In such cases, it is recommended to ensure that the tool highlights flagged data clearly, such as through colour-coded matrices, to capture the trader's attention.
Market participants should provide appropriate training to traders and relevant personnel who handle reasonability check results, to ensure that they are able to accurately interpret and respond to the results.

Checklist for essential steps in the trading process

There may be many essential steps to a market participant's trading process. To ensure a thorough, controlled and error-minimised process, market participants are advised to design and implement relevant checklists covering all relevant steps of their processes. An example could be to implement a checklist that includes all operative steps in the process of bid submission to the market. Such a checklist could for instance include elements such as bid preparation, bid creation, internal review (e.g., the four-eyes principle), bid submission, post-submission validation, and ongoing monitoring and adjustments.

Four-eyes principle in bidding

The four-eye principle entails review and validation by a second, independent, and competent person. This can help minimise errors and reduce the risk of erroneous orders. It is therefore recommended to implement this principle in bidding routines, such as reviewing the final bids submitted to the market, to reduce the risk of errors. This is especially relevant for the markets where reviewing bids can be effectively incorporated in the bidding process, such as the day-ahead and intraday auctions (IDAs).

Technical unavailability and active UMMs

As a part of the bidding process, it may be relevant for market participants to make a comparison of technical unavailability in the internal outage system with lists of UMMs. The purpose is to ensure that the information from the UMMs is included in the bids to the market.
It may also be relevant to establish routines to keep an overview of active UMMs that are considered relevant by the market participant, to ensure that the intended information is

taken into account when placing bids to the market. For example, if a UMM that the market participant deems relevant expires and the trading desk is unaware of it, traders may overlook this information when planning and placing bids. This oversight could lead to offers being placed without considering the available information.

Relevant personnel accessible

Having relevant personnel available pre- and post-trade can be important to reduce the likelihood of erroneous orders and mitigate their potential impact. For instance, it is recommended that relevant personnel (e.g., the responsible trader or trading team) are reachable if the exchange's trading desk spots abnormal orders placed to the day-ahead auction during reasonability checks. The exchange's trading desk may call the market participant to validate the order or advise the market participant to correct it before gate closure. If the relevant personnel are unavailable, the auction may run with the abnormal order.
Some market participants have different teams responsible for orders across different portfolios. It is recommended to ensure that the correct contact information is available to the exchange, so that the correct team is contacted if an abnormality is spotted. Having the right contact details available, especially close to gate closure, helps reduce the stress for both the exchange's trading desk and the relevant personnel at the market participant.
Erroneous orders may be identified at any time of day. When an erroneous order is identified, it may need to be discussed with other relevant personnel, such as a lead trader, responsible manager, or a compliance officer. Therefore, it is recommended to establish a suitable routine for the traders to be able to access relevant personnel, based on the needs, requirements, and general trading operation of the market participant.

Trainings

As outlined in section 3.2.1, the key measure to prevent market manipulation is to ensure that employees are aware of behaviours that could be manipulative. Therefore, all market participants should provide mandatory training for traders and other relevant personnel involved in the trading process. This training should cover specific scenarios related to market manipulation, such as scenarios related to erroneous orders.

3.4.12. Incident investigation for erroneous orders

Once an erroneous order is identified, it is recommended to initiate a standard incident handling process to address it. The process could include an investigation with the following steps:

- Assessing the facts of the situation, documented in a course of events document
- Legal assessment
- Root cause analysis
- Identification of mitigating actions
- Internal reporting

- Potentially sending a STOR

After investigating the incident, it is recommended to document it in an incident report, which for example can be shared with senior management on an ad-hoc or regular basis. Based on the report, the management may consider additional measures to enhance operational robustness and prevent similar errors.
The above process is a general recommendation and should be adapted to the market participants' processes, procedures and business. Furthermore, the list is not exhaustive, and other relevant steps may also be considered.

3.4.13. Process for handling erroneous orders in auction and continuous markets

Market participants are recommended to establish clear processes for handling erroneous orders. The processes may vary depending on the products being traded, e.g., the approach to auction markets like the day-ahead and intraday auctions may differ from the approach used in continuous markets like the intraday market. Furthermore, there is no "one-size-fits-all," so market participants should tailor the approach to the context of their business.
Below are two examples of processes for handling erroneous orders. The first is for auction markets, while the second is for continuous markets.

PROCESS FOR HANDLING ERRONEOUS ORDERS IN AUCTION MARKETS

1. Erroneous order is identified
2. If the order is identified before Gate Closure Time, correct the order[34]
3. Activate trade stop, if relevant
4. Assess if information about the erroneous order shall be treated as inside information under REMIT
5. If not, deactivate trade stop and resume trading
6. If the error requires publication, publish a UMM to the Inside Information Platform
7. Assess if erroneous order constitutes potential market manipulation (case-by-case assessment). Include the compliance and/or legal department if necessary or required
8. Inform the compliance and/or legal department about the error, if not already done
9. Perform incident investigation
10. Potentially notify the NRA through a STOR

ACM's regulatory guidance[34] states that an erroneous order should be cancelled promptly to minimize its potential consequences. This is particularly relevant for continuous markets, when the order has not been executed, or only partially executed. Based on this regulatory guidance, it is recommended that such an erroneous order is cancelled or corrected immediately when detected.

PROCESS FOR HANDLING ERRONEOUS ORDERS IN CONTINUOUS MARKETS

1. Erroneous order is identified
2. If the order is not yet (fully) executed, cancel order[34]
3. Activate trade stop, if relevant
4. Assess if information about the order shall be treated as inside information under REMIT
5. If not, deactivate trade stop and resume trading
6. If the error requires publication, publish a UMM to the Inside Information Platform and resume trading
7. Assess if erroneous order constitutes potential market manipulation (case-by-case assessment). Include the compliance and/or legal department if necessary or required
8. Inform the compliance and/or legal department about the error, if not already done
9. Perform incident investigation
10. Potentially notify the NRA through a STOR

[34] On its website, the Dutch NRA (ACM) states that if you place an erroneous order, "you must limit the consequences of the erroneous order as much as possible. You must cancel the order as quickly as possible […] in order to eliminate a possibly false or misleading signal to the market."

4. Appendixes

4.1. Appendix 1 Glossary

ACER	Agency for the Cooperation of Energy Regulators
Delegated Regulation	Commission Delegated Regulation (EU) 2016/957
ESMA	European Securities and Markets Authority
IDA	Intraday auction
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
MTU	Market Time Unit
NRA	National Regulatory Agency
OMP	Organized Market Place
PPAET	Person Professionally Arranging or Executing Transactions
PPAT	Person Professionally Arranging Transactions
PPET	Person Professionally Executing 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, amended by Regulation (EU) 2024/1106 of the European Parliament and of the Council of 11 April 2024
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
STOR	Suspicious Transaction or Order Report
TSO	Transmission System Operator
UMM	Urgent Market Message

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 to 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 2: 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
					2
Medium	2	(2). 1 + Reputational risk	2	Manage the risk	3
					4
High	3	(3). 2 + Personal Sanctions or heightened reputational risk	3	Mitigate and reduce the risk	6
					9

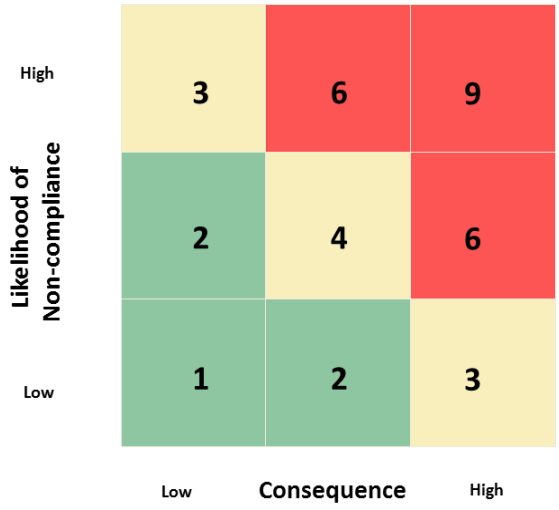

Figure 5: Example of risk mapping and prioritisation

Table 3: Example Risk mapping and prioritisation

				Market 1		
REMIT			**ACER Guidance**	**Likelihood**	**Consequence**	**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 Sample contents of the Compliance Plan

	Example area for compliance plan	
	Compliance with the obligation to publish inside information	*Documentation of an approved algorithm / trading strategy*
Assessment of activity	Compliance with guidelines for publication of inside information	Compliance with algorithm governance and guidelines and procedures
Compliance risk	Effective and timely publication	Unapproved algorithms / trading strategies, inadequate governance and compliance around algorithms / trading strategies
Relevant department	The monitoring & control centre	Short term power desk? Could also be a desk trading commodity derivatives using algorithms /trading strategies
Relevant person responsible, e.g. contact person for OMP/NRAs	Head of monitoring & control centre	Head of the relevant desk or person responsible for algorithms deployed
Relevant market	-	SIDC
The source for compliance (e.g. guidelines, interviews or samples of Urgent Market Messages)	Guidelines and procedures for publication of inside information and samples of UMMs and logs (and may be interview of persons involved in process)	-
Type of control	E.g., spot checks of a number of UMMs	Control of documentation and governance against guidelines and procedures (including REMIT requirements)
Conclusion	Conclusion as to whether the UMMs were timely and effective	Conclusion as to whether an algorithm / trading strategy has been approved and adequately documented
Completion	In case of detection of non-compliance incidents assessment of root cause and mitigation actions	In case detection of non-compliance incidents assessment of root cause and mitigation actions of

4.4. Appendix 4 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**

4.5. Appendix 5 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.

4.6. Appendix 6 Template for Filing a Suspicious Transaction or Order Report

The template below is set up in a way that any text written *in italics* needs to be amended by the PPAET's market or trade surveillance function. It is closely following the ACER Guidance on REMIT, see chapter 9.3.1. 'What to notify?'.

SUSPICION OF BREACH OF REMIT ARTICLE *[chose 3, 4 and/or 5]*

Name of the notifying party,
Organisation,
Position and contact details

Notification date and time

Market participant involved in the potential breach:	
ACER Code:[35]	
Affected Markets:	

Sub-category of REMIT breach
[delete all options but the one(s) applicable to the case reported]

Insider Trading (choose one or several below):

- *Using inside information to trade/try to trade*
  - *Trading based on inside information*
  - *Front running*
- *Disclosing inside information to third parties*
- *Recommending third parties to trade based on inside information*

Disclosure of inside information obligation (choose one or several below):

- *Obligation to disclose in an effective and timely manner*
  - *Inside information not published*
  - *Inside information not published properly*
  - *Other*
- *Reporting of delay to publish inside information*
  - *Delay not reported to ACER and the NRA*
  - *Delay improperly reported*
  - *Other*

Market manipulation (choose one or several below):

- *False/misleading signals; Artificial Price; Deception*

[35] You can find this code here: https://www.acer-remit.eu/portal/european-register

- *Wash trades*
    - *Wash trades A to A*
    - *Wash trades A to B to A*
    - *Wash trades A to B + A from C*
    - *Pre-arranged trades*
- *Placing orders with no intention to execute them*
    - *Trash and cash (order based)*
    - *Pump and dump (order based)*
    - *Layering/spoofing*
    - *Quote stuffing*
    - *Smoking*
    - *Other strategies to paint the tape (Momentum ignition)*
- *Creating a floor or a ceiling in the price pattern*
- *Marking the close or other relevant reference periods*
    - *Marking the opening*
    - *Marking the close*
    - *Marking other reference period*
- *Market cornering*
- *Capacity withholding*
    - *Economic withholding*
    - *Physical withholding*
- *Phishing*
- *Transmission capacity hoarding*
- *Opening a position and closing it immediately after its public disclosure*
- *Creating a misperception through specific actions*
- *Misleading research or recommendation*
- *Other types of NON-intentional behaviours*
    - *Erroneous orders*
- *Combining with other potentially unlawful behaviours*
    - *Tax fraud*
    - *Money laundering/transfer; P&L rearrangement*
    - *Breach of market rules*

▪ *Dissemination of false/misleading information*
- *Trash and cash (info based)*
- *Pump and dump (info based)*
- *Art. 5 -A Other*

Description of the potential breach

Describe the transaction(s)/order(s)/behaviour(s)/disclosure of inside information as well as absence of disclosure):

- *description of the order(s)/transaction(s)/behaviour(s): product(s) involved, product delivery location, product delivery date (start and end, orders/transactions timestamps, time period when the potential breach occurred), load type, contract ID(s), transaction ID(s), transactions/orders, other details;*
- *description of the inside information related to the potential breach of Article 3 and Article 4: date of disclosure of inside information, asset concerned, start date and*

time, end date and time, content disclosed remarks on the inside information disclosure, installed and unavailable capacity;
- *information on the potentially affected parties and products; and*
- *identification of the PPAET(s) involved (other than the notifying party – if applicable): PPAET name, additional PPAET identification details.*

Reasons for suspecting a breach of REMIT
[delete all options but the one(s) applicable to the case reported]

- *Insider trading:*
  It has to be considered if and when the information about […] constituted inside information as set out in REMIT Article 2(1) and whether […] has breached the prohibition against insider trading according to REMIT Article 3.
- *Requirement to disclose inside information:*
  It has to be considered if the disclosure of inside information done in relation to the observed behaviour constitute a breach of the requirement to disclose inside information as set out in REMIT Article 4.

- *Market manipulation:*
  It has to be considered whether the observed behaviour could constitute market manipulation as set out in REMIT Article 2(2)(a)(i) and (ii), and whether the behaviour could be a breach of the prohibition against market manipulation as set out in REMIT Article 5.

Describe your reasons for suspecting that the order(s)/transaction(s)/ behaviour(s) might constitute insider trading/market manipulation/ disclosure requirements.

The notified parties
This case is sent to ACER as well as the *[…]* NRA. ACER Guidance stipulates that both the NRA in the Member State of the delivery of the wholesale energy product *(…)* and the NRA in the Member State in which the Market Participant involved in the potential breach has registered *(…)*, should be notified.

Should you have any questions to the above, please do not hesitate to contact Market / Trade Surveillance at *[…]*.

You can add a disclaimer here.

Appendices
Further information which may be of significance:
- analysis of the behaviour;
- spreadsheet analysing the relevant transaction(s)/order(s)/behaviour(s);
- copy of the communications with the market participant or other entities on the event;
- any kind of other action already undertaken by the PPAET;

- estimation of the impact of the event on the market prices;
- estimation of the benefit from the potential breach for the market participant;
- Member State(s) affected and any related supporting evidence;
- any other information which the PPAET considers relevant (e.g. information on events which may lead to a potential breach of another REMIT provision).

4.7. Appendix 7 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? Note that the parameter ranges should be well-defined and the effect of setting parameter values at the boundaries of the permissible parameter set should be well understood.

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?

6. If the algorithm is running on vendor infrastructure (e.g. co-location):
    a. How is it ensured that client data remains confidential and segregated with regards to other client data and towards the vendor?

    b. Who from the vendor has access to the algorithmic trading server?

    c. Are accesses and changes to the algorithmic trading server logged?

7. Logging:
    a. Does the vendor store logs containing the algorithm version, the parametrization, and the algorithm states for the retention time prescribed by REMIT?

    b. Does the market participant have access to the log data? If not, can the data be provided to the Market Participant within 24 hours in a workable format?