ACER

European Union Agency for the Cooperation of Energy Regulators

Market surveillance by persons professionally arranging or executing transactions

Arrangements, systems and procedures

8 May 2026

Market surveillance by persons professionally arranging or executing transactions

Arrangements, systems and procedures

8 May 2026

Find us at:

ACER

E press@acer.europa.eu
Trg republike 3
1000 Ljubljana
Slovenia

www.acer.europa.eu

Table of contents

Executive summary

Effective market surveillance is a key element for ensuring fair European energy markets. Energy exchanges, brokers and other persons professionally arranging transactions (PPATs) play an important role and also have a legal obligation to contribute to this goal.

This second annual European Union Agency for the Cooperation of Energy Regulators (ACER) report, building on the baseline established in the first edition published in May 2025, fulfils the obligation under Article 15(5)(a) of Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency (REMIT), which consists of assessing PPAT market surveillance arrangements, systems and procedures, as well as their effectiveness. The main conclusion of this report is that **while structural compliance is likely improving, more effort should be placed on effectiveness** to ensure fair, transparent, and well-functioning wholesale energy markets across the Union.

Compared to the first report, this edition broadens coverage by including **additional categories of PPATs**, most notably providers of direct electronic access (DEA) and trade matching systems, and introduces a **systematic assessment of surveillance arrangements, systems and procedures effectiveness**, complementing the established market surveillance capability assessment. This report, as the May 2025 one, focuses on PPATs.

The findings are primarily based on a structured survey conducted by ACER in November 2025 and aimed at collecting the necessary inputs from PPATs, therefore all percentages refer explicitly only to responding entities, complemented by ACER data on suspicious transaction and order reports (STORs). The survey covered governance arrangements, surveillance procedures, IT systems, and self-assessment of REMIT compliance. Respondents together arrange almost 91% of EU traded volumes on organised marketplaces (based on ACER 2025 data), ensuring high representativeness despite lower response rates.

Two distinct scoring frameworks were applied:

1. **surveillance capability score**, assessing the presence and robustness of arrangements, procedures and systems; and
2. **surveillance effectiveness score**, combining STOR quantity, completeness and thoroughness with declared proactive engagement through “know your customer” (KYC) and direct inquiries with clients.

Key findings:

A - Surveillance arrangements, procedures and systems

Governance and arrangements

- Most PPATs have a formal surveillance function, either as a dedicated unit or embedded in compliance or market monitoring functions.
- Survey results indicate that surveillance staff are largely independent in terms of methods and tools used and almost 90% of PPATs reported that their management cannot influence or block notifications to national regulatory authorities (NRAs) / ACER. However, in over one third of responding entities, surveillance staff may be relieved of duties without their consent. **It is essential to ensure that independence of market surveillance from potential conflicts of interest, in particular regarding surveillance operations, is effectively applied in practice**.
- Staffing levels and budgets are generally adequate, and conflict-of-interest declarations are widely in place.

Procedures

- Apart from four PPATs that declare having no surveillance procedures in place, all other responding PPATs confirmed that they have at least detection procedures in place and **90% of participating PPATs have fully formalised procedures covering three core components (“detect – analyse – notify”)**. About 60% have procedures covering also **deterrence**.

- The **ability of management to influence or block notifications** to NRAs or ACER is **reported by fewer than 10% of respondents**, a rate that is significantly lower compared to last year's responding entities.

Systems

- **Around 70% of responding PPATs use some form of surveillance system**. Only a minority rely on professional, third-party surveillance software.
- Many responding entities, particularly transmission system operators (TSOs), continue to use self-developed tools or general analytical software.
- Responding entities using professional systems report shorter notification timings, although system flexibility and independence can be more constrained.

B - Surveillance capability assessment

The **average surveillance capability score** across all respondents is **69%**, representing a **five percentage-point increase** compared to the previous year. Moreover, while variability is still high, it has decreased compared to last year's reporting entities. For example:

- **38%** of PPATs achieved a high score (>75%)
- **over 50%** fell into the moderate range (51–75%)
- **10%** exhibited low capability (<51%)

Energy exchanges and brokers have the highest scores, while TSOs, energy capacity platforms, and DEA providers show more mixed results, particularly in the Systems and Assessment dimensions. PPATs arranging trading in both electricity and natural gas demonstrate higher capability than those active in a single commodity.

Notably, longer market experience does not automatically translate into higher surveillance capability, although well-established entities tend to show more consistent performance.

C - Surveillance effectiveness assessment

This report introduces, for the first time, a **quantitative effectiveness assessment.**

Effectiveness refers to the extent to which something achieves its intended goal or produces the desired result. Given the large number of PPATs, it is not feasible at this point to conduct individual audits to assess the effectiveness of surveillance arrangements, systems, and procedures they declare, and how PPATs detect, analyse and confirm or dismiss suspicious behaviour. A measurable proxy was therefore identified as an initial approach, that may evolve in the future. It combines:

- **STOR effectiveness** (weighted at 65%, due to the importance of STORs in relation to effectiveness), based on STOR numbers, completeness and thoroughness; and
- **direct inquiry / KYC effectiveness** (weighted at 35%), reflecting proactive engagement with clients / market participants.

Key observations include the following findings:

- **65 PPATs responded that they have notification procedures in place, while only 30 PPATs submitted relevant STORs** during the assessment period (trading period 1 July 2024 – 30 June 2025), highlighting a discrepancy between self-assessed capabilities and actual STOR submissions, particularly among brokers and DEA providers.
- **Energy exchanges clearly outperform other PPAT types in effectiveness**, while **TSOs also perform relatively well given their specific market role**.
- PPATs handling **larger trade volumes tend to do better, on average**.

- **KYC practices are widespread but often static, as almost 70% of responding PPATs have a formalised KYC procedure in place**, yet only a small minority use ongoing KYC data updates for clients (market participants) as an active surveillance benchmark.

There is substantial variation in effectiveness score between assessed PPATs and the **average final effectiveness score** across all PPATs is below **25%**. **This shows a potential discrepancy compared to the results of the surveillance capability assessment**.

Conclusions and strategic implications

The report observes a **gradual strengthening of formal surveillance frameworks** across PPATs, with improvements in systems, procedures, and governance compared to the first reporting cycle. However, results need to be interpreted cautiously, since the comparison is between two distinct samples. To enhance the reliability and comparability of future assessments, **PPATs are encouraged to participate regularly in ACER's annual survey**, thereby reducing gaps in responses and limiting the risk of misleading conclusions.

This report includes a new assessment of surveillance arrangements, systems and procedures, based on a methodology that provides an indicator of effectiveness. This indicator highlights a **potential discrepancy between surveillance capability and its actual effectiveness.** Indeed, there is an inherent methodological limit of effectiveness assessment in focusing solely on direct inquiry / KYC and on STORs notifications without examining the upstream detection and analysis processes. However, the observed gap - particularly the wide variation in effectiveness scores among PPATs - may suggest an overestimation of surveillance capability in self-assessments, or that some PPATs apply STORs notification thresholds that are too high, leading to systematic under-reporting. Additionally, uncertainty about what constitutes a notifiable case, as well as operational or legal constraints, may discourage notifications even when suspicious behaviours are detected. It is possible that suspicious behaviour is reported through other means, nevertheless, **STOR notifications should go through ACER's Notification Platform**[1].

While there is no indication that the market is under-monitored or that significant breaches are being overlooked, PPATs are invited to review and where necessary improve surveillance arrangements, systems and procedures, working in particular on STOR completeness and thoroughness, as well as reporting timelines.

Key challenges remain, including:

- a need for greater functional independence and professionalisation of surveillance teams, including appropriate training;
- a high degree of reliance on basic monitoring tools;
- a need for improved and expanded coverage to monitoring of potential breaches of Articles 3 and 4, beside Article 5, which is reportedly covered quite well, along with a need to cover all markets / products at the same level;
- limited proactive engagement with market participants;
- asymmetric STOR reporting patterns across PPAT types raise questions on reporting completeness and suggest the need for sustained efforts to improve the detection-analysis-reporting lifecycle.

While PPATs are required to report any potential breach of Articles 3, 4 and 5 of REMIT, when they have reasonable grounds for suspicion, experience shows that reporting methodologies should ensure that STORs are sufficiently substantiated and contextualised, as described in the ACER REMIT Guidance[2]. Submitting multiple STORs based solely on automated alerts, without additional analysis, may generate a high volume of reports without providing commensurate added value for the NRAs'

[1] https://www.acer-remit.eu/np/home

[2] https://www.acer.europa.eu/remit-documents/guidance-remit-application

investigatory activities. PPATs are invited to focus on STOR thoroughness while respecting reporting timelines. In certain market situations the PPAT is not in a position to be able to provide a thorough analysis, for example due to not having access to relevant data. In such a case, PPATs are encouraged to report a STOR anyhow, precising the limitations of their assessment.

Overall, the report provides a quantified overview of the state of **PPAT market surveillance, which plays an important role in guaranteeing that REMIT is applied across the EU**. PPATs are particularly well placed to perform this function for their specific markets, due to their deeper knowledge and insight into operated markets, including the market participants that participate in those markets. While structural compliance is likely improving, **sustained efforts are needed to reinforce and sustain this role over time.**

1. Introduction

Regulation (EU) 2024/1106, adopted by the European Parliament and Council on 11 April 2024, amends Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency (REMIT). The revised REMIT, which entered into force on 7 May 2024, introduced several new provisions and obligations.

One significant change was made to Article 15 of the revised REMIT, broadening the scope of obligations of persons professionally arranging or executing transactions (PPAETs), as well as defining new obligations for the European Union Agency for the Cooperation of Energy Regulators (ACER) in the fifth paragraph of Article 15. According to this, ACER shall publish, in cooperation with national regulatory authorities (NRAs), an annual report on the implementation of Article 15 ("Obligations of persons professionally arranging or executing transactions") with aggregated information in compliance with applicable data protection law, excluding commercially sensitive information, on the implementation of this Article, in particular with regard to:

> (a) the arrangements, systems and procedures[3] referred to in paragraph 3 of Article 15 and their effectiveness[4]; and
>
> (b) the national regulatory authorities' analysis of suspicious transactions, response to poor quality reporting and non-reporting of suspicious transactions and related activities with regard to enforcement and penalties.

The present document covers point (a) above. This second report builds on the baseline established by the first report[5], published on 8 May 2025.

Similarly to the previous edition of the report, the present document focuses on persons professionally arranging transactions (PPATs) only. Still, there are some important differences compared to the first report. The PPAT list, which also serves as an invitation list for the survey, used by ACER to gather the necessary data, was expanded in cooperation between ACER and the NRAs, so as to include all PPAT types, now also taking stock of providers of the direct electronic access (DEA) and trade matching systems (TMS) – in line with the revised definition in REMIT. In this second report, an assessment of effectiveness, i.e. **the ability to produce the desired result or outcome**, which in the context of the methodology used in this report focuses on STOR numbers, completeness and thoroughness, as well as direct outreach to market participants, is included beside the surveillance capability assessment.

Point (b) of Article 15(5) is covered in a separate report[6] and aims to provide a qualitative and quantitative assessment on the quality of the STORs notified to the relevant NRAs and ACER through the Agency's Notification Platform, along with a comprehensive and in-depth statistical description of the STORs received.

1.1. Structure of the report

This report is structured as follows:

The remainder of Section 1 briefly touches upon the basic concepts relating to PPAETs.

---

[3] Any person professionally arranging or executing transactions shall establish and maintain effective arrangements, systems and procedures to: (i) identify potential breaches of Article 3, 4 or 5; (ii) 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.; (iii) detect and report suspicious orders and transactions.

[4] Article 1(18) of Regulation (EU) 2024/1106

[5] https://www.acer.europa.eu/sites/default/files/documents/Publications/ACER-Report-PPAETs-market-surveillance-2025.pdf

[6] https://www.acer.europa.eu/remit-documents

Section 2 covers the obligations of PPAETs regarding market surveillance and REMIT, and the duty to establish and maintain effective arrangements, systems and procedures.

Section 3 explains the methodology used in gathering the data, along with the analysis used to obtain results. It also touches upon the response rate.

Section 4 provides a comprehensive statistical analysis of survey responses. First, an overview of key findings from the preliminary analysis is presented, followed by a more in-depth exploration of the data for each of the four key survey sections: 'Arrangements', 'Procedures', 'Systems' and 'Assessment'. The section concludes with the surveillance capability assessment, analysed also by PPAT type, commodities covered and PPAT length of operation.

Section 5 provides the surveillance effectiveness assessment, along with an analysis of the interplay between surveillance capability and effectiveness for PPATs.

Section 6 gives structured recommendations, based on results from preceding sections.

Finally, details regarding the scoring methodology for the surveillance capability assessment are provided in the Annex.

1.2. Background of the report

REMIT established a sector-specific legal framework for identifying and penalizing insider trading and market manipulation in wholesale energy markets across Europe. The scope of REMIT was therefore specifically designed to accommodate the operational complexity of energy markets and specificities of the energy sector (electricity and natural gas) and to appropriately complement the market abuse legislation covering the financial sector.

The REMIT revision further aimed to align the scope of the regulation with evolving market dynamics. Key amendments include, among others, the expansion of the scope of data reporting (encompassing electricity balancing markets, coupled markets, and algorithmic trading), the extension of REMIT's market abuse provisions to wholesale energy products that are also financial instruments and the supervision of notifying entities.

1.3. Concept of PPAET, PPAT and PPET

Article 2(8a) of REMIT provides a definition of the PPAET concept. According to that definition, a **PPAET** is a *"(…) a person professionally engaged in the reception and transmission of order for, or in the execution of transactions in, wholesale energy products".* This concept is also included in Recitals (12)[7] and (18)[8] of Regulation 2024/1106, Article 8(4) of REMIT; and Article 2(4) of Commission Implementing Regulation (EU) No 1348/2014.

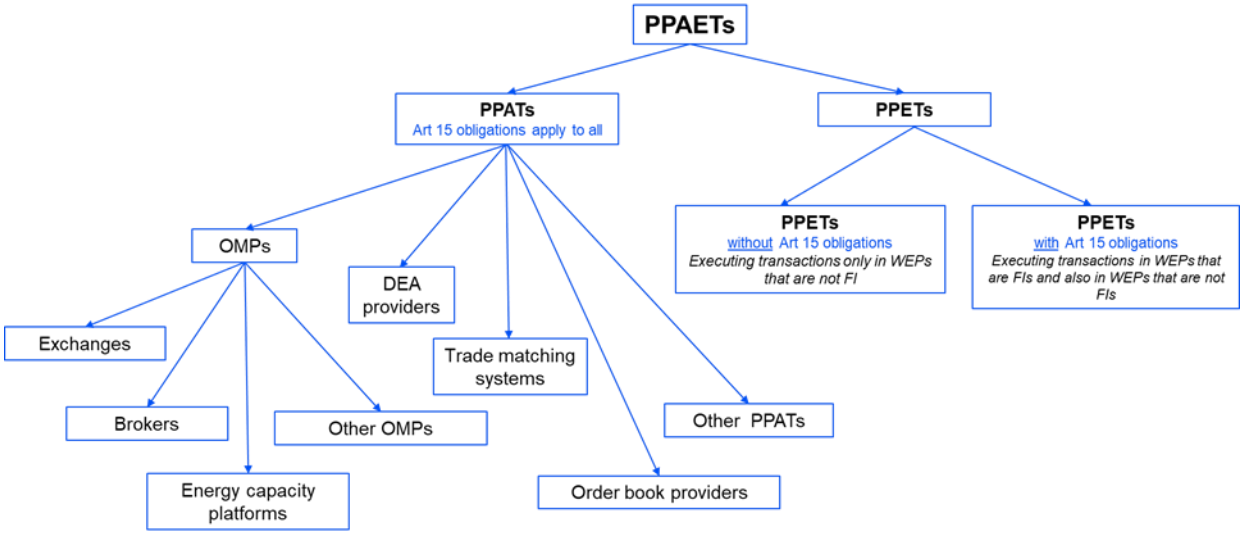
Moreover, Articles 15(1) and 15(2) of REMIT distinguish between PPATs and PPETs (persons professionally executing transactions) under Article 16 of Regulation (EU) No 596/2014 on market

[7] Recital 12: *"(…) order book providers should also be designated as persons professionally arranging transactions subject to the obligation to monitor and report suspected breaches of this Regulation".*

[8] Recital 18: *"Persons professionally arranging or executing transactions should have the obligation to report suspicious transactions in breach of Regulation (EU) No 1227/2011 with regard to insider trading and market manipulation and, in order to enhance the possibility of enforcement of such breaches, should also have the obligation to report suspicious orders and potential breaches of the obligation to publish inside information. Direct electronic access providers and order book providers are considered to be persons professionally arranging transactions.*

abuse (MAR[9]), where the latter also execute transactions in wholesale energy products that are not financial instruments. The overall classification of PPAETs is presented in Figure 1 below.

Figure 1: An illustrated overview of entities classified as PPAETs under REMIT[10]



The concept of '**PPAT**' is embedded in the broader concept of 'PPAET', which, under Article 2(8a) of REMIT, is defined as *"(…) a person professionally engaged in the reception and transmission of orders (…) in wholesale energy products."*.

In addition to the definition contained in Article 2(8a), the notion of PPAT also appears in other provisions of REMIT. For example, according to Article 8(4)(d) of REMIT, PPATs are responsible for the reporting of information for the purposes of Article 8(1), (1a) and (1)(b) of REMIT: *"For the purposes of paragraph 1, 1a and 1b information shall be provided by: (…) (d) an OMP [organised marketplace], a trade matching system or other persons professionally arranging or executing transactions"*.

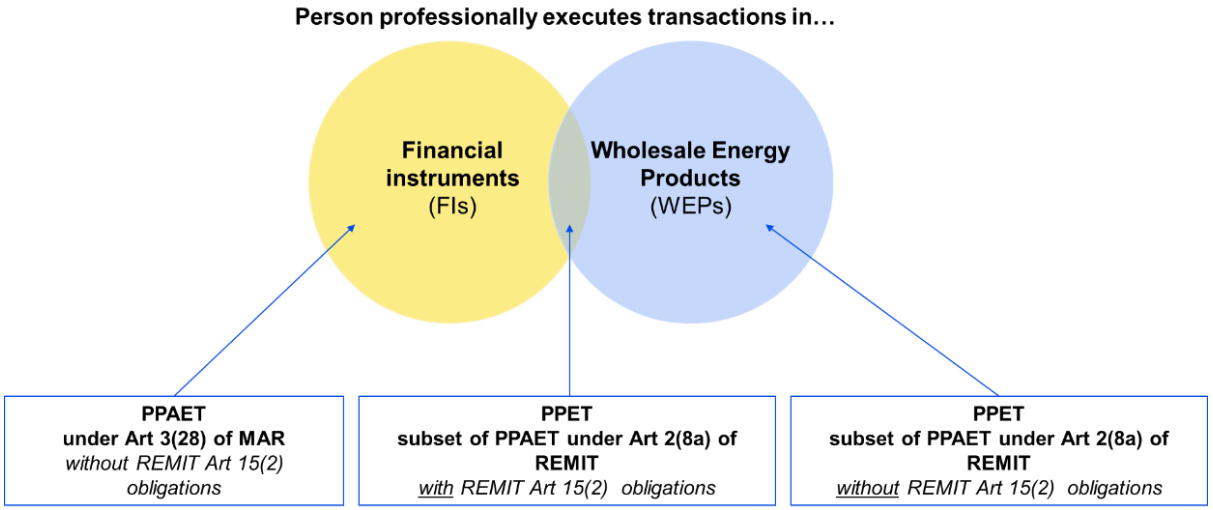
PPATs that are expressly referred to in REMIT can be aggregated in the following categories: OMPs, TMSs, order book providers, DEA providers and other PPATs.

Article 2(8a) of REMIT defines the concept of '**PPET**', which is embedded in the concept of PPAET, as *"(…) a person professionally engaged in (…) the execution of transactions in wholesale energy products"*. Under this provision, it is understood by the Agency that 'execution' should include trading on own account as well as execution of orders on behalf of a third party, either directly or in accordance with a discretionary mandate given by the third party. It should be noted that not all PPETs have obligations under Article 15 of REMIT. Article 15(2) of REMIT only includes obligations on PPAETs under Article 16 of MAR who also execute transactions in wholesale energy products that are not financial instruments, as shown in Figure 2.

[9] 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 2003/24/EC, 2003/125/EC and 2004/72/EC, OJ L 173, 12.6.2014, ELI: http://data.europa.eu/eli/reg/2014/596/oj.

[10] ACER's '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' (link).

Figure 2: PPETs with obligations under Article 15(2) of REMIT



The issue of PPAT identification and classification is discussed in the box to follow. For further information, refer to ACER's 6.1 edition of the REMIT Guidance[11].

PPAT IDENTIFICATION AND CLASSIFICATION

ACER acknowledges the recurrent issue of PPAT identification and classification. As already laid out in "Box 3" of last year's report and stemming also from this year's survey results, there seem to be different interpretations by entities in similar circumstances, especially regarding the distinction between the "Other OMP" and "Other PPAT" categories.

Organised marketplaces (OMPs) are a subset of PPATs, meaning that all OMPs are also considered PPATs, but this does not mean that all PPATs are OMPs. The definition of OMP in Article 2(20) of REMIT prescribes that an OMP is an energy exchange, an energy broker, an energy capacity platform or any other system or facility in which multiple third-party buying or selling interests in wholesale energy products interact in a manner that may result in a transaction. The last part of the definition is also what is sometimes referred to as 'Other OMPs' and which is further elaborated on in ACER's guidance on OMPs (https://www.acer.europa.eu/annex-ix).

The Annex contains four key cumulative criteria of an OMP: (1) operating as a system or facility, (2) includes multiple third-party buying or selling interests, (3) covers trading in wholesale energy products (as defined in REMIT), and, (4) the interactions (within the system or facility) have the potential to result in a transaction.

The Annex continues by providing specific examples of 'Other OMPs', one example being one-to-many platforms, such as TSO hosted platforms for the purpose of electricity balancing markets or for transmission capacity allocation, which when they fulfil the OMP criteria above are to be considered as OMPs for the scope of these activities. Within ACER's PPAT survey, these entities are thus expected to indicate the "Other OMP" category.

As mentioned, the scope of PPAT is broader than the scope of OMP. Consequently, if an entity fulfils the OMP requirements (either as an energy exchange, an energy broker, an energy capacity platform or as an 'Other OMP') it is also considered automatically as a PPAT, but it is also possible that an entity not qualifying as an OMP is recognised as a PPAT. As explained in ACER's REMIT Guidance, the three key cumulative criteria for an entity to be considered a PPAT are: (1) being a person, (2) acting professionally (i.e. part of one's normal and regular paid occupation), and, (3) arranging transactions. The key feature of the latter being the enabling or assisting third parties in a way that directly or indirectly brings about a wholesale energy transaction.

An entity fulfilling the PPAT criteria, and which are not an OMP, DEA provider, trade-matching system, or order book provider, should indicate the 'Other PPAT' category in ACER's PPAT survey.

Finally, if relevant activities are transferred to another legal entity, then this entity assumes the PPAT role and obligations, and are consequently the entity that should take part in this survey. In this regard, it should be stressed that the PPAT obligations also apply to the natural or legal persons that are responsible for an entity or a system that arranges transactions. I.e. in cases where an entity or system in itself does not have the form of a natural or legal person, it is the natural or legal person in control of the entity or system that assumes the PPAT status and thus should take part in this survey.

[11] https://www.acer.europa.eu/sites/default/files/documents/Other%20Documents/6.1st_Edition_ACER_Guidance.pdf.

2. Scope

This section briefly covers PPAET obligations under REMIT, along with the basic concepts regarding arrangements, procedures and systems, that need to be set up and maintained by PPAETs.

For more detailed information, refer to ACER's 6.1 edition of the REMIT guidance.

2.1. PPAET obligations under REMIT

In the context of this report the focus is on specific obligations of PPAETs based on the revised Article 15 of REMIT. According to this article, **PPAETs are responsible for identifying and notifying ACER and the relevant NRAs about any potential breaches of the prohibition of insider trading (Article 3), the obligation to publish inside information (Article 4) and the prohibition of market manipulation (Article 5)**. More precisely, *"any person [PPAT/PPET], 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, 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."*.

The obligation for PPATs under Article 15(1) has applied since 7 May 2024. However, obligations for PPETs under Article 15(2) are applicable from 8 November 2024 onwards.

Furthermore, Article 15(3) of REMIT obliges PPAETs to *"**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"*.

In general, it is also important to note the following regarding PPAET REMIT obligations:

- This scope extension for PPATs concerns:
    - wholesale energy products that are financial instruments (reflecting the changes in Article 1(2) of REMIT), in case they arrange transactions on these products;
    - new products categorised as wholesale energy products (e.g. contracts and derivatives relating to the storage of electricity or natural gas in the EU; contracts and derivatives for the supply of electricity that may result in delivery in the EU as a result of single day-ahead and intraday coupling reflecting the changes in Article 2(4)), in case they arrange transactions on these products.
    - the monitoring of Article 4 provisions, while Articles 3 and 5 were in scope (for PPATs) even before the REMIT revision.
- The REMIT revision explicitly identified certain categories of PPATs as new, either in the core text itself or in the recitals – for example, DEA providers and energy capacity platforms.
- Article 15 obligations for PPETs apply only to a subset of PPETs, as mentioned in Section 1.3.
- The REMIT revision introduces timelines for notification (*"[…] 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"*).

Both the 6.1 version of ACER's REMIT Guidance and ACER's open letter of 25 September 2024[12] address these obligations in further detail.

From the point of view of the final aim, it is important to note that PPAT and PPET market surveillance activities are important for guaranteeing an adequate level of supervision and therefore the integrity of electricity and gas markets. PPATs, in particular, are in a better position than other entities within their respective operated markets, due to their better knowledge of and insight into those markets, including market participants.

2.2. Arrangements, systems and procedures

According to Article 15(3) of REMIT, PPATs under Article 15(1) and PPETs under Article 15(2) *"shall establish and maintain effective arrangements, systems and procedures to*

(a) identify potential 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."*

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.

Arrangements and procedures in place shall establish the internal processes on **how to**:

- **determine** whether an event is suspicious;
- **notify** a potential breach to ACER and the relevant NRA(s) if there is a reasonable suspicion of breach(es) of Articles 3, 4 or 5 of REMIT; and
- **guarantee the independence** and preservation from conflict of interest of surveillance personnel.

ACER and NRAs expect PPAETs' notifications to be sufficiently substantiated and meaningful. PPAETs should produce timely, high-quality STORs, facilitating ACER's and NRAs' further review of the suspicious behaviour. ACER encourages PPAETs to also submit any relevant additional information that they may become aware of after fulfilling their notification obligations.

Finally, ACER expects alerts generated by systems to go through human screening and data quality control and to be complemented with circumstantial information and confirmation before being submitted as STORs to ACER and the relevant NRA(s). The thoroughness of the STOR is thus an important factor.

[12] https://www.acer.europa.eu/sites/default/files/REMIT/Guidance%20on%20REMIT%20Application/Open%20Letters%20on%20REMIT%20Policy/25092024_3rd_Open_Letter_Third_Countries_PPAETs.pdf

3. Methodology and response rate

This section explains the methodology underlying the report, explaining also the survey process and its structure, along with the scoring systems. Additionally, data acquisition and cleaning procedures are detailed, and the response rate is analysed for each PPAT type.

This report contains two distinct assessments. The first one relates to surveillance capability, which is assessed based on data collected through a survey among PPATs. It calculates a composite score for each participating PPAT, considering scores relating to four sections: 'Procedures', 'Arrangements', 'Systems' and 'Assessment'. It therefore stems directly from Article 15 of REMIT and the ACER REMIT guidance, which define these three key elements (procedures, arrangements and systems). The second assessment relates to effectiveness, and it is based partly on certain questions in the survey (relating to "know your customer" (KYC) procedures and direct inquiries with clients) and partly on an analysis of STORs that were sent to ACER.

3.1. Survey among PPATs

To collect the necessary information for this report, a survey among PPATs was conducted. There is no official, publicly available PPAT list to be used for the identification of survey participants. The only existing official list that covers some PPATs is ACER's 'List of organised market places (OMPs)'[13], though it represents only a subset of all PPATs. Hence, similarly to last year's survey, a dedicated list of companies already confirmed as PPATs or preliminarily considered as PPATs, based on available information, was compiled by ACER in collaboration with NRAs. For DEA providers, ACER's Centralised European Register of Energy Market Participants (CEREMP)[14] data was used.

The survey, done via the EU Survey tool[15], was distributed on 3 November 2025, with an initial closing date set for 17 November 2025. To address the low response rate at the deadline, the closing date was extended by one week. Alongside this extension, targeted measures were implemented: non-responding PPATs received direct email reminders and were contacted by ACER and NRAs to encourage participation. The survey was ultimately closed on 24 November 2025.

When comparing results to last year's, we thus need to be aware, that these are two distinct samples and also that the initial address list was expanded in 2025, in cooperation between ACER and the NRAs.

3.2. Survey structure and data cleaning

The survey contained 64 questions, mainly multiple-choice with a few free text answers, where not all fields were mandatory. It followed a similar structure to the survey from last year, enabling consistency in comparative analysis. Where necessary, questions were re-formulated taking into account feedback on last year's report. A few supplementary questions were added to allow for deeper insight, especially connected to KYC or direct inquiry procedures by PPATs.

The complete survey is included in the Annex.

The questions were divided into the following six sections:

[13] https://www.acer-remit.eu/portal/organised-marketplaces

[14] https://www.acer-remit.eu/portal/ceremp

[15] https://ec.europa.eu/eusurvey/home/welcome

- **Key information on respondents.** This section covers contact details and variables necessary for segmentation purposes, such as Member State coverage, duration of operation and type of markets and commodities covered.
- **Arrangements.** This section contains questions on surveillance governance, surveillance staff, influence of management on the surveillance function, training and budget availability etc.
- **Procedures.** This section includes questions on the implementation of the 'detect - analyse - notify – deter' principle, STOR notification procedures, notification timeline estimates, auditing, KYC procedures etc.
- **Systems.** This section addresses questions regarding the availability and type of surveillance software or system used by the PPAT.
- **Assessment.** This section contains self-assessment questions on PPATs' market surveillance, assessed also from a REMIT perspective.
- **Final comments.** This section allows PPATs to submit comments on the survey.

After the survey closed, a **plausibility and consistency check** was performed to spot potential mistakes in the responses. The obtained data contained inconsistencies, including internal contradictions, and non-plausible data. Particularly problematic areas included the responses of the DEA providers, the self-classification[16] of PPATs and the reported coverage of EU Member States and markets in terms of market surveillance.

For DEA providers, 17 answers were received from 157 addressed entities, and only ten answers were left in the analysis, while seven were removed. It was found out via direct communication with these seven entities, that they had mistakenly notified via CEREMP that they provide direct electronic access to an OMP. All of them were actually not DEA providers.

Inconsistent responses were verified and, if needed, adjusted through direct outreach via email to survey participants. Nine PPATs were contacted for additional clarifications. The data cleaning process was performed manually in order to improve accuracy, address missing information, and enhance consistency across the dataset. These efforts ensured a more reliable foundation for conducting a trustworthy analysis and deriving accurate results.

Missing values were not substituted. Throughout this report, the sample size is noted down next to the table or figure (e.g. *n* = *XX*).

3.3. Scoring systems

PPATs' surveillance capability and effectiveness were assessed using separate scorings. The **surveillance capability scoring** was conducted on mandatory questions similar to last year's report to ensure consistency and comparability. In case there was a change in any of the scored questions, its scoring was adjusted to closely align with last year's. The **surveillance effectiveness score** was a two-part score, based partly on STOR data and partly on responses regarding KYC / direct outreach procedures by PPATs.

Only mandatory questions were included in the scoring. Additional details on the scoring methodology are provided in the sections to follow and in the Annex.

3.3.1. Surveillance capability assessment

The survey included a total of 64 questions, 29 of which were used for the surveillance capability score. Since those questions are part of different sections, the surveillance capability score consists of **four weighted normalised partial scores**:

[16] Regarding the PPAT sub-type, i.e. exchanges, brokers, other OMP, other PPAT etc.

- arrangements score comprising 12 scored questions (60 points possible in total),
- procedures score comprising 9 scored questions (45 points possible in total),
- systems score comprising 6 scored questions (30 points possible in total),
- assessment score comprising 2 scored questions (11 points possible in total).

Weights of 0.3 for 'Arrangements', 'Procedures' and 'Systems' are chosen to ensure all three categories are treated equally, while the weight for 'Assessment' is 0.1, considering it is an additional section in comparison with the initial survey last year. **All partial scores, along with the final surveillance capability score, are normalised to scale from 0 to 100**[17].

3.3.2. Surveillance effectiveness assessment

The surveillance effectiveness score consists of **two parts**: the first part relates to **STORs**, sent to ACER by the PPAT, and the second to **KYC / direct inquiries scores**, resulting from the relevant questions in the survey. The STOR score's weight is 0.65 and the KYC / direct inquiries score weight is 0.35, reflecting the relative importance of each metric and thus prioritising the STOR score.

The prioritisation of the STOR score is also due to the potential self-report bias in the survey. However, some elements related to the processing of the STOR score also use qualitative criteria, as further explained in the continuation of this section.

Both partial scores are normalised to scale from 0 to 100. The final score is a weighted sum of both partial scores, resulting again in a minimum score of 0 and a maximum score of 100. PPATs that had either a STOR score (i.e. at least one relevant STOR) or a KYC / direct inquiry score (i.e. took part in the survey) were included in the analysis. The potentially missing part of the score is implicitly counted as 0.

The KYC / direct inquiry score is based on responses to specific questions, namely seven questions in the 'Procedures' section (for details see Annex). The selected questions reflect the effectiveness of communication between PPATs and their clients, specifically regarding KYC procedures and clarification requests submitted in the process of clarifying potential problematic behaviour. Those requests serve multiple purposes:

- they hint to the existence of monitoring or surveillance activity at the PPAT and may therefore have a deterrence effect; and
- the answers often have an educational effect, allowing improved monitoring, alerts recalibration and raising awareness about certain risks.

Therefore, such requests are considered a valuable input for the effectiveness assessment. KYC plays an important role in the process of conducting inquiries among market participants, especially when it entails important benchmark data for each specific market participant, against which a particular behaviour can be evaluated.

Effectiveness is to be understood as the degree to which something achieves its intended goal or produces the desired result. While REMIT points to the effectiveness of the entire setup, i.e. arrangements, systems and procedures, certain elements cannot be easily assessed. Given the large number of PPATs it is not feasible at this point to conduct individual audits. A measurable proxy was therefore identified as an initial approach, that may evolve in the future. This proxy is composed of STORs and the direct outreach / KYC.

The data on STORs from PPATs, relating to the trading period from 1 July 2024 to 30 June 2025, was sourced from ACER's Notification Platform. Since the Revised REMIT came into force in May 2024, the underlying of these STORs would already be bound by the new rules. STORs that were rejected by ACER, were sent by NRAs or had a low/poor ACER completeness rating, were removed from the

[17] The classic "Min-Max" normalisation method is used for all normalisations in this document, therefore each score is computed according to the following formula: *X_normalised = ((X_original - min(X)) / (max(X) - min(X)))*100*.

analysis. The core of the methodology is presented here, while more details regarding values / numbers are given in the relevant results section.

An **initial STOR count was prepared for each PPAT**. An **adjusted (lowered) count was prepared, to reflect the thoroughness of the STORs received from PPATs**. This adjusted count was then **multiplied by the completeness score, which is a value from 0 to 1**[18]. These values were used as an initial STOR score for each PPAT. For example, if 14 STORs for the relevant trading period were sent by the PPAT and were not rejected or classified as "poor quality", this number was reduced to 10 (taking into account thoroughness[19]). If then the average STOR completeness rating for relevant STORs was 0.9, then the initial nominal score for the PPAT would be 9.

Then, **two additional potential corrections of this score were applied**:

- Deduction for STORs by third parties: If, for the same trading period, relevant STORs were sent by third parties, addressing specific PPATs and similar behaviour was not notified by that PPAT, despite the PPAT being in a position to spot the said behaviour, a deduction of maximum one point was applied, again weighed by the STOR completeness assessment;
- Mark-down for ACER shared alerts: ACER alerts, shared with NRAs, relating to the same trading period (H2-2024 and H1-2025), were considered. Only PPATs, that had at least a 1% share within these alerts, were considered. If the alerts were not reflected somehow in the STORs, sent by relevant PPATs, a deduction of maximum 0.5 points was applied to the PPATs in question.

3.4. Response rate

From the 293 PPATs (157 DEA providers and 136 other PPAT entities) that received the survey, ACER received 72 responses for 74 entities[20] by the final deadline, yielding an **overall response rate of 25%**. **Excluding DEA providers**, which had an exceptionally low response rate, **this year's response rate is 47% (64 out of 136), which is 23 percentage points lower than last year**.

Putting DEA providers aside, 16 new entities were included in the initial list for the survey compared to 2024. There are 25 PPATs that replied in 2024, but not in 2025. Out of those that replied in 2025, 17 did not reply in 2024.

The PPATs were further categorised into six groups: energy exchanges, brokers, energy capacity platforms, TSOs, DEA providers and other PPATs. The **highest response rate of 100% was achieved among energy capacity platforms**. However, this group consisted of only five PPATs. For **exchanges, the response rate was 53%, followed by TSOs with 46% and brokers with 38%**. Out of 157 DEA providers, only 17 responded, but only ten responses can be considered valid, since seven were found out not to be DEA providers. This points to a potentially **substantial problem with incorrect notification via CEREMP regarding DEA provider status**. Three PPATs classified as "Other"[21] in Figure 3[22] did not respond at all. The years 2025 and 2024 in the legend correspond to the

[18] The approach regarding "completeness" is explained in detail in Section 3.2. of the Article 15(5)b report, available here: https://www.acer.europa.eu/sites/default/files/documents/Publications/ACER-Report-NRAs-activities-STORs-2025.pdf

[19] For example, rather than sending individual alerts or repeated STORs, doing the necessary assessment of repetition and other relevant circumstances within the same STOR.

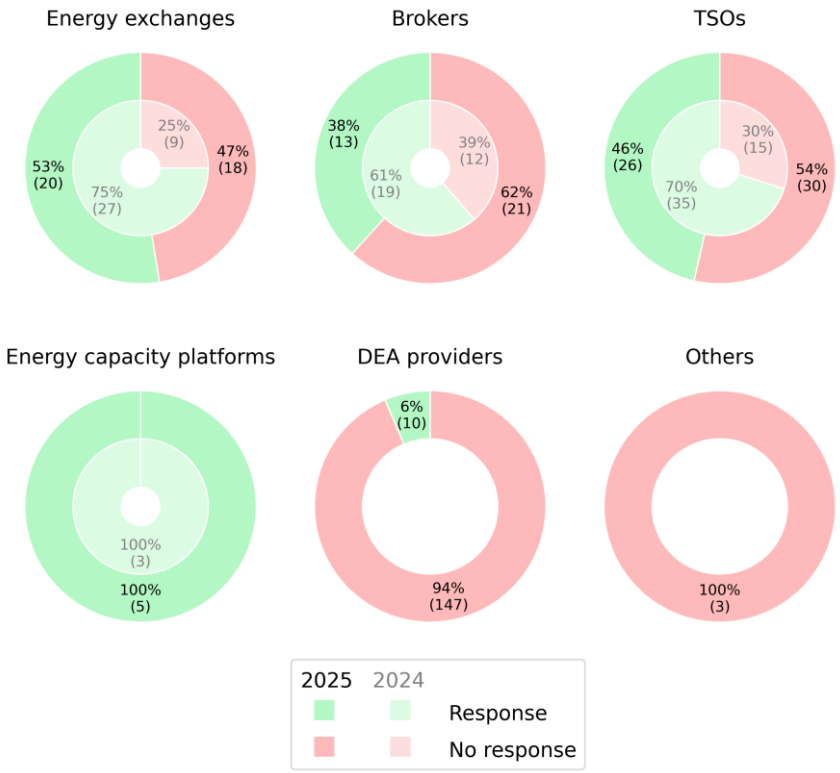
[20] The actual number of responses was 81, however seven were excluded from the analysis since it was found out by direct communication that they do not classify as PPATs. Furthermore, two responses were submitted for multiple entities, therefore the total count, relevant for the response rate, was 74. However, the analysis in the following sections is based on actual PPAT responses, which was 72.

[21] Comprising "Trade Matching System" and "Other PPAT" entities.

[22] Note: The absolute numbers of participants are given in brackets.

years of survey launch, meaning the time when the data was reported. The same approach is used in all following figures.

Figure 3: Response rate by PPAT type



All types of PPATs exhibited a decrease in the response rate compared to the previous year. The most significant drop was observed for the main three categories of PPATs, which are energy exchanges, brokers and TSOs, where the non-response almost doubled compared to the previous year. In addition, the PPATs, excluding DEA providers, **based outside of the EU achieved a low, 12% response rate**, while those based in the EU achieved a response rate of 54%.

When interpreting the results presented in the following sections, it is important to consider potential biases, namely non-response bias and reporting bias. Non-response bias may arise if the 75% of non-responding PPATs have systematically different characteristics from those who report. Reporting bias may occur if PPATs, aware of regulatory scrutiny, intentionally or unintentionally report higher levels or more favourable outcomes.

On the other hand, it is also important to note that – considering the data reported to ACER in 2025 as traded on OMPs – the **survey respondents cover slightly less than 91% of the traded quantities at the EU level**. This is also slightly lower than last year, when the percentage was slightly higher than 95%, but still high enough to give credibility to the results, despite the lower overall response rate. **Out of the 20 top volume ranked PPATs/OMPs, only five did not respond to the survey**.

Coming back to the overall response rate of 47% without DEA providers, it needs to be noted that although the response rate was much lower than last year (-23 percentage points), it **is still high considering the usual response rates for such surveys**. This did, however, require a lot of additional effort from both ACER and NRAs, at a level unsustainable when extended to PPETs.

To enhance the reliability and comparability of future assessments, **PPATs are encouraged to participate regularly in ACER's annual survey**, thereby reducing gaps in responses and limiting the risk of bias and misleading conclusions.

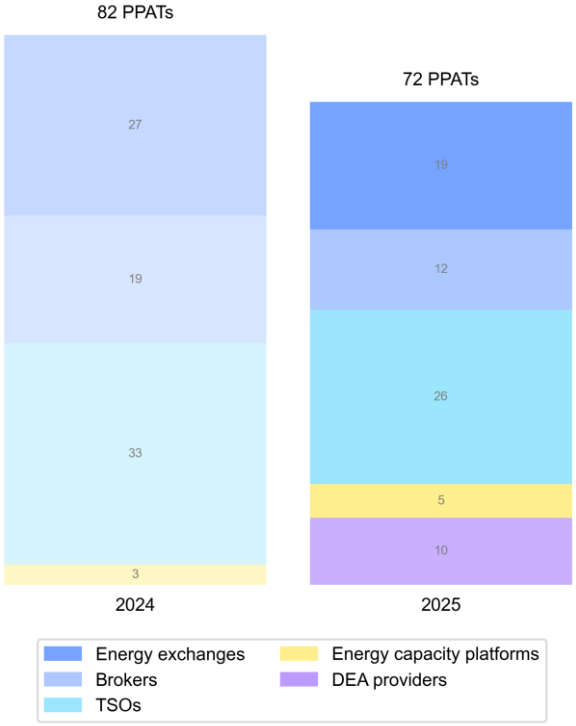
4. Survey results analysis

The analysis presented in the following sections is based on the collected survey responses. From this point onward, 72 responses are considered in the statistics. For clarity, the sample size or number of responses collected for each question, denoted as *n*, is provided next to each visualisation.

4.1. An overview of responding PPATs

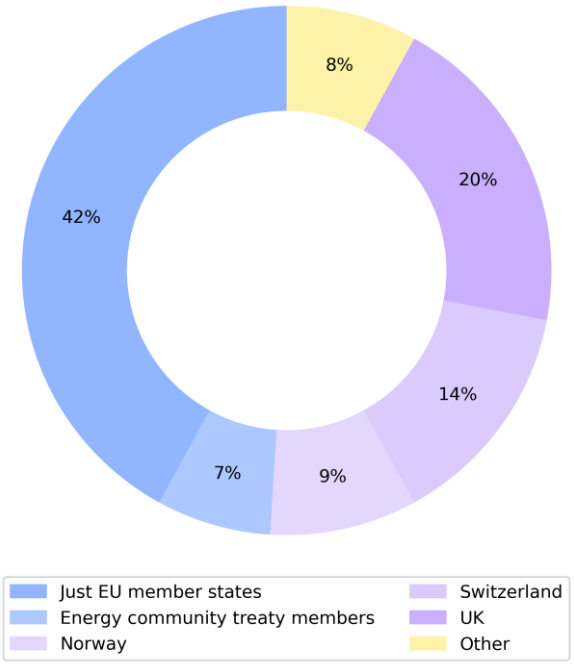
The largest group of PPATs consists of TSOs, accounting for more than one third of all participants. Energy exchanges form the second largest group, followed by brokers, DEA providers and energy capacity platforms. The proportions between different types of PPATs remain consistent compared to last year, as shown in Figure 4.

Figure 4: Types of PPATs



Note: for 2024 n = 82, for 2025 n = 72

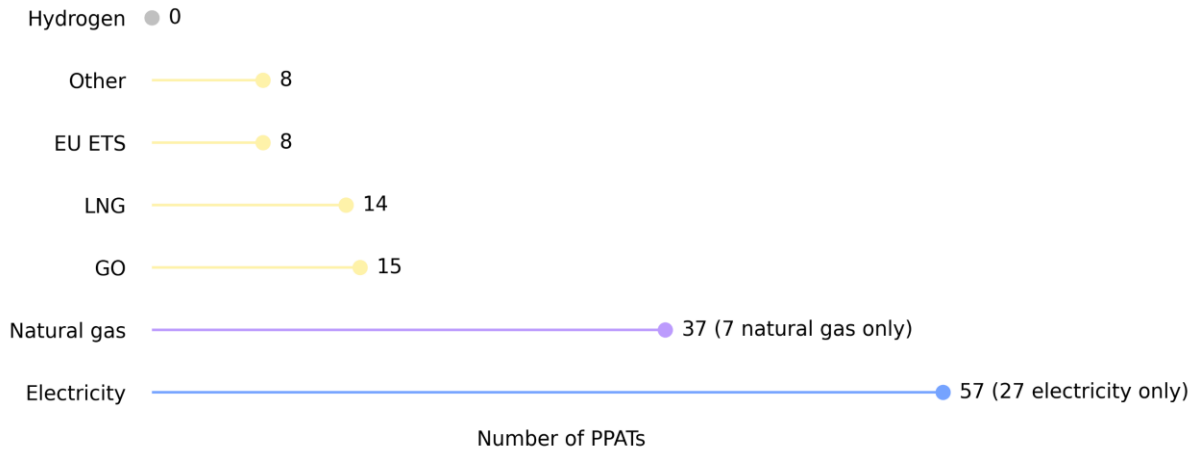
Figure 5: Arranging trading – delivery areas



Note: n = 72

More than half of all participants reported arranging trading not only for delivery areas in EU Member States, but also elsewhere. 20% of PPATs arrange trading also in the United Kingdom (UK), 14% in Switzerland and 9% in Norway, as presented in Figure 5. Companies arranging trading outside EU are predominately those reporting trading of liquified natural gas (LNG) products, including transportation and storage contracts, along with EU emission trading system (EU ETS) and guarantees of origin (GO). In general, **78% of PPATs reported arranging trading of electricity, while half reported natural gas**. One third of all respondents reported arranging trading of both electricity and natural gas, which mirrors last year's observations. Details are presented in Figure 6.

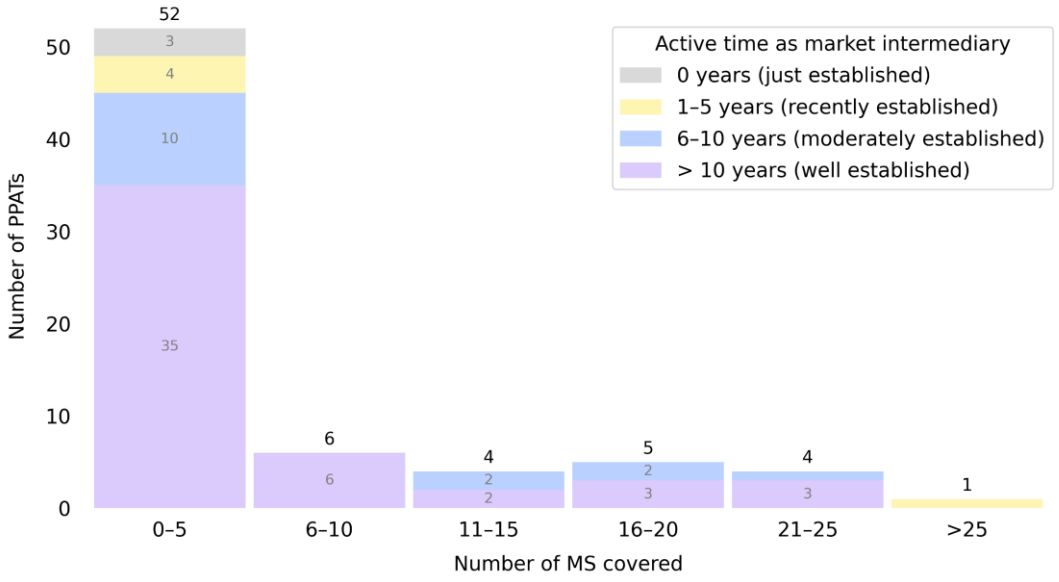
Figure 6: Commodities traded



Note: n = 72

Likewise, consistency with last year's results is observed in the reported times of PPATs operating as market intermediaries. The average active time reported this year being 14 years, compared to 15 years last year, indicating that respondents to the survey are mainly well experienced PPATs[23]. **More than 70% of these entities are covering less than six EU Member States in terms of delivery, with the majority covering only one Member State due to their TSO role**, as presented in Figure 7.

Figure 7: Number of Member States covered by traded products' delivery in relation to years as market intermediary



Note: n = 72

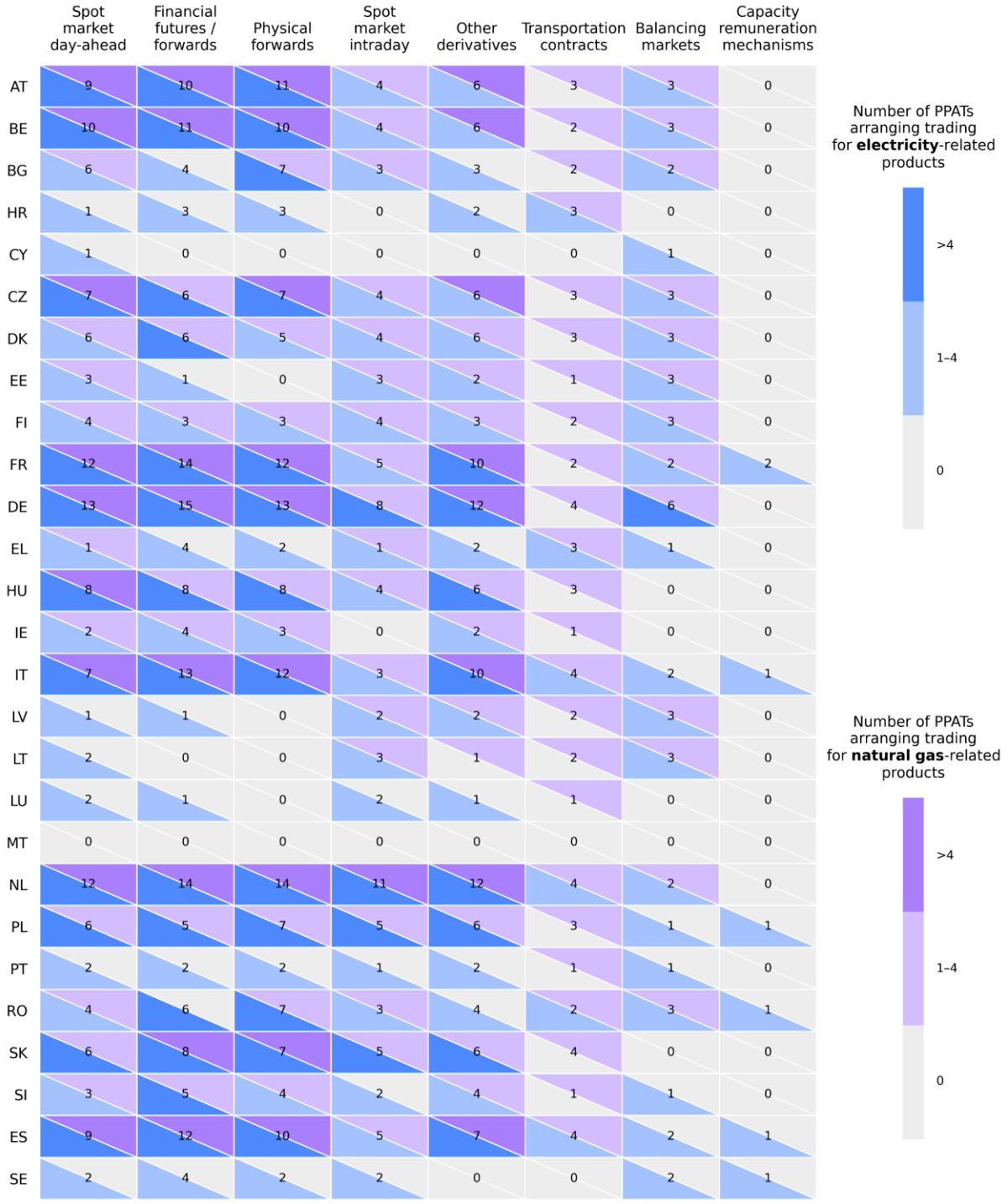
90% of participants are registered in Member States, most of them under German or Spanish jurisdictions. Beside EU Member States, entities registered in UK, Norway, Switzerland, Montenegro and the United States also participated.

The participants operate in a variety of wholesale energy markets. They are most active on spot day-ahead and physical markets regardless of the commodity traded. Other markets are more commodity

[23] Entities with lower reported active time are mostly TSOs, therefore this time does not necessarily correspond to the establishment of the legal entity, but rather to the start or perceived start of PPAT activities and obligations.

specific, namely financial futures / forwards and spot intraday markets are associated with electricity-related products. The least covered market segment is, as expected, capacity remuneration mechanisms. In terms of delivery, only a few PPATs operate in Cyprus and none in Malta. For details see Figure 8, which represents wholesale energy markets where PPATs arrange transactions, the number in each cell indicating the number of PPATs arranging trading in a specific market regardless of the commodity traded.

Figure 8: Wholesale energy markets where responding PPATs arrange transactions



Note: n = 72

4.2. Arrangements, procedures and systems in place at PPATs

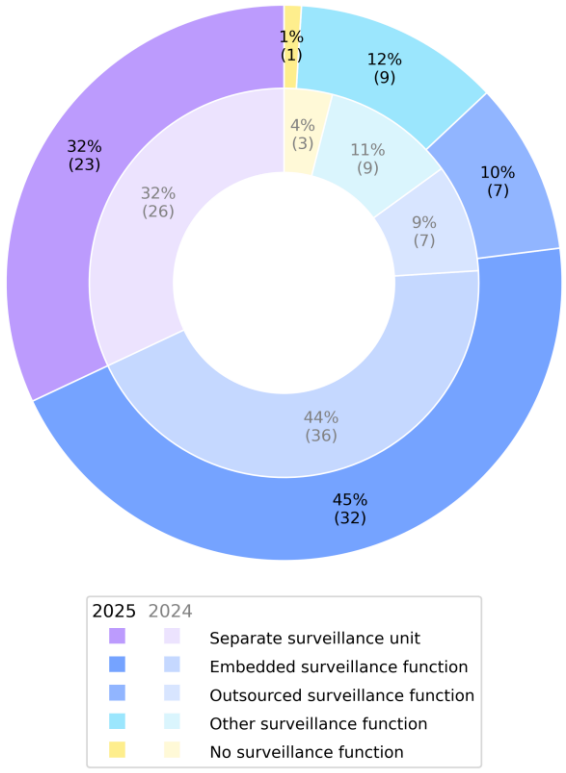
This section covers the main statistics on survey questions related to arrangements, procedures and systems that PPATs have in place to be able to effectively detect and notify potential breaches of Article 3, 4 and 5 of REMIT.

4.2.1. Arrangements

The first part of the survey offers detailed insight into how the surveillance function is structured within PPATs. It focuses on understanding the governance frameworks surrounding the surveillance function, including the roles and responsibilities of surveillance staff. By examining how these functions are integrated within the broader organisational structure, the survey aims to highlight best practices and potential gaps in the oversight mechanisms that govern market activities.

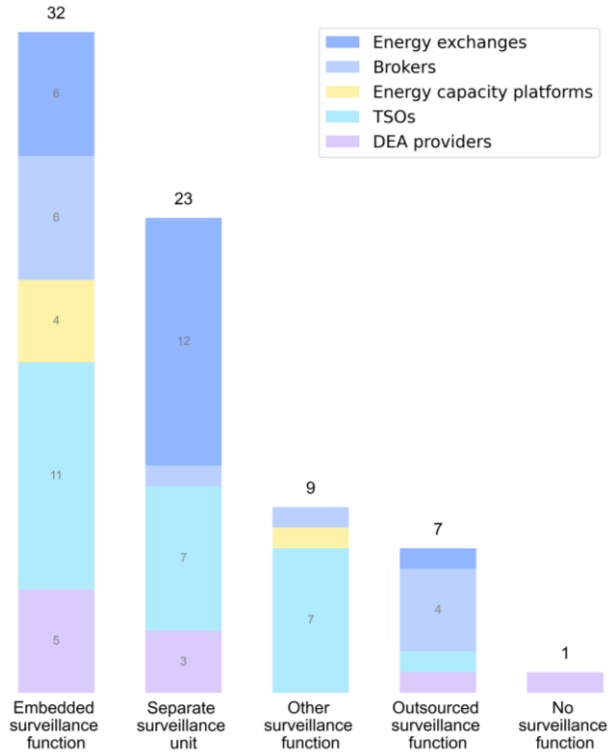
Approximately one third of PPATs have a separate surveillance unit or a similar structure. 45% have the surveillance function embedded in other functions, for example covered by the market monitoring or compliance departments. 22% outsource their surveillance function or arrange it differently, while **only 1% of PPATs, namely one entity, do not have a formal surveillance function in place at all**. The structure of the governance function reported this year closely aligns with last year's, as presented in Figure 9.

Figure 9: Governance of surveillance function



Note: for 2024 n = 81, for 2025 n = 72

Figure 10: Governance of surveillance function by PPAT type

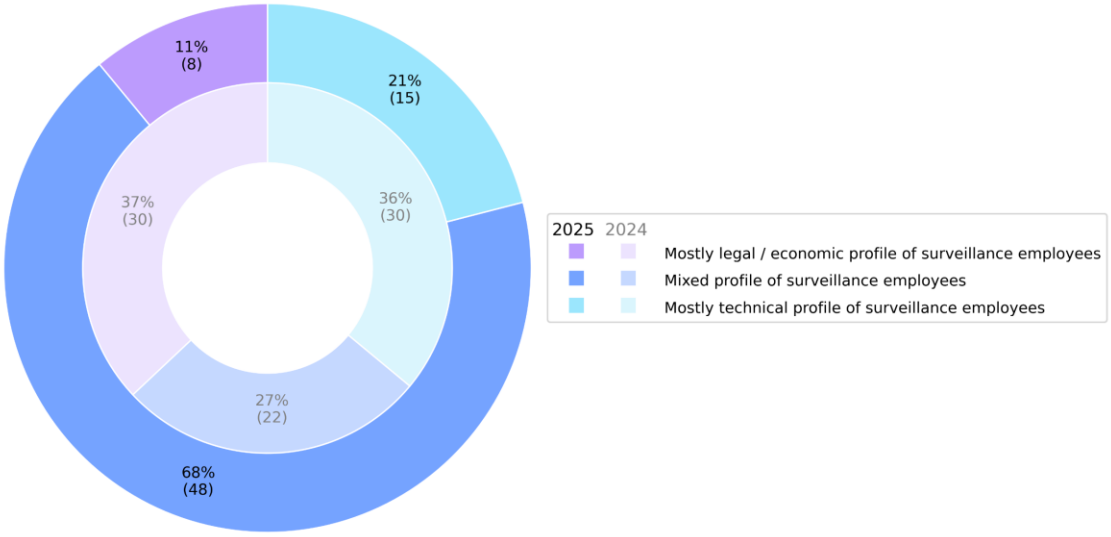


Note: n = 72

Energy exchanges predominately have separate surveillance units. In addition, the category of outsourced surveillance function consists mostly of brokers arranging trading of various delivery areas beyond EU Member States, specifically in the UK and Switzerland. This outsourcing can also be carried out with(in) the group. Similar observations were reported in last year's survey. For details, see Figure 10.

PPATs were also asked also to denote the **formal training of surveillance employees**. 68% of PPATs report having surveillance staff with mixed formal training, while 21% of PPATs report having a surveillance staff composed mostly of employees with engineering degrees and 11% of PPATs report employing mostly lawyers and economists. The latter two were commonly mentioned by PPATs that have the surveillance function embedded in other functions, while employees with **mixed profiles mainly correspond to separate surveillance units**. In comparison with the numbers reported last year, there is a significant difference in the structure of profiles, since in 2024 the three categories represented almost equal shares, while this year the mixed profiles predominate, as shown in Figure 11. In this respect it needs to be mentioned that this year's survey question was restructured to make it clearer, therefore the difference might be due to this fact.

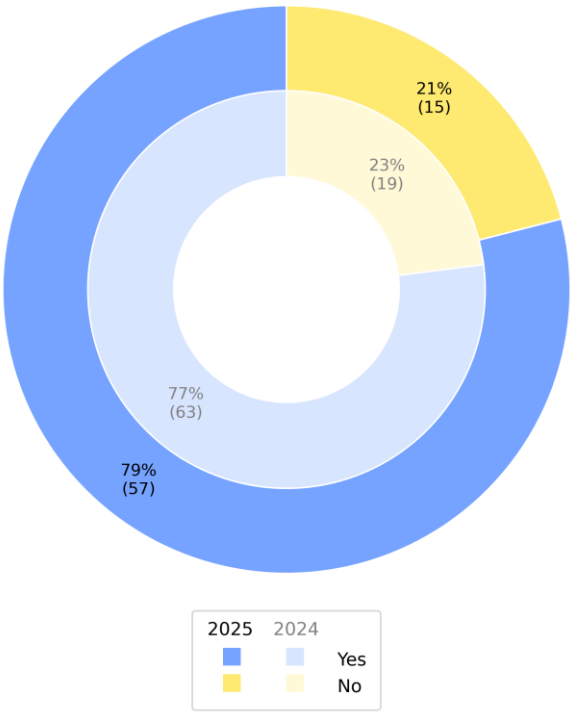
Figure 11: Profile of surveillance employees



Note: for 2024 n = 82, for 2025 n = 71

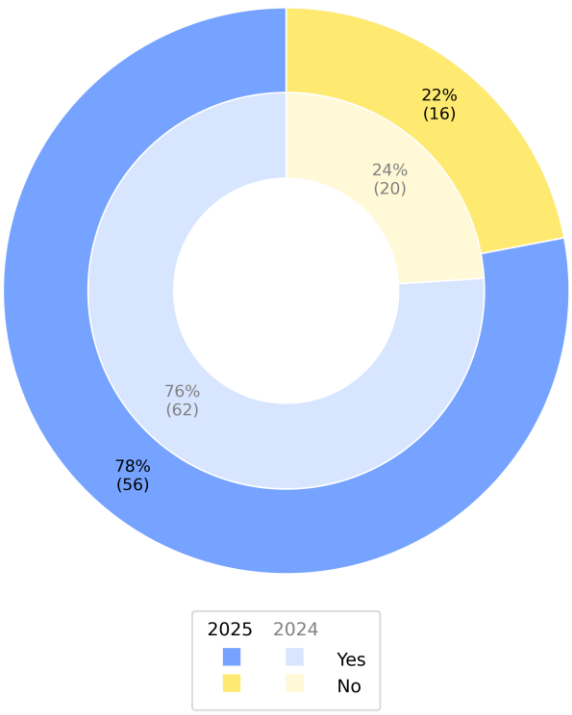
The survey results **confirmed that the majority of PPATs report having procedures in place to allow employees, who might have potential conflicts of interest, to report them. Most PPATs also report employing compliance officers.** Both measures improved by 2 percentage points compared to last year, suggesting a stable awareness of the importance of declaring potential conflicts of interests and maintaining good compliance practices. However, no pattern was identified among the entities without these procedures neither in relation to their market coverage or their activity time, nor in relation to the type of PPAT. For details refer to Figure 12 and Figure 13.

Figure 12: Employees declaring potential conflicts of interest



Note: for 2024 n = 82, for 2025 n = 72

Figure 13: Compliance officers employed at the company

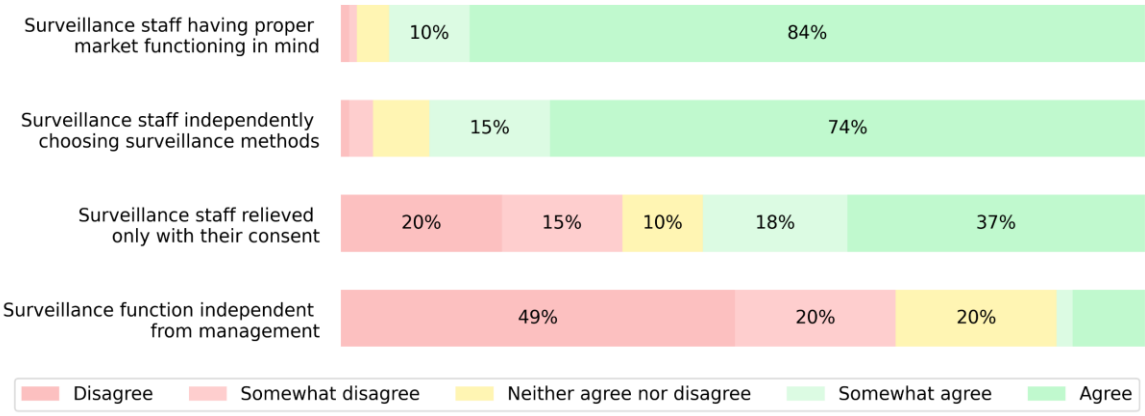


Note: for 2024 n = 82, for 2025 n = 72

Numerous respondents confirmed that their legal, national and company set-ups guarantee that surveillance staff have proper market functioning in mind when carrying out their duties. More than 90% reported that their surveillance staff choose methods for surveillance and thresholds for the detection independently, which has remained consistent since last year.

Nevertheless, there is room for improvement identified in relation to the dismissal of surveillance staff from their tasks. Namely, in more than one third of PPATs surveillance staff can be relieved without their consent, as presented in Figure 14. Besides, only 12% of PPATs' surveillance staff work exclusively on surveillance tasks, while the others work also on compliance tasks.

Figure 14: Autonomy and oversight of surveillance function

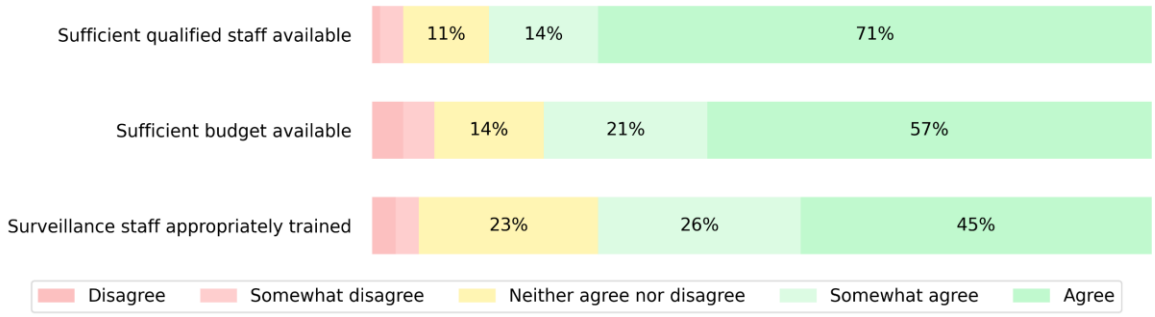


Note: for first n = 70, for second n = 67, for third n = 40, for fourth n = 66

The companies with the highest management influence are those that have their surveillance functions embedded in other functions, yet there are no specific types of PPATs (i.e. exchanges, brokers etc.) that would more commonly appear in this subsection.

The majority of PPATs report sufficiently qualified and appropriately trained staff and budget available to fulfil monitoring tasks, which aligns with last year's situation, as reflected in Figure 15.

Figure 15: Staff and budget availability



Note: for first n = 71, for second n = 72, for third n = 62

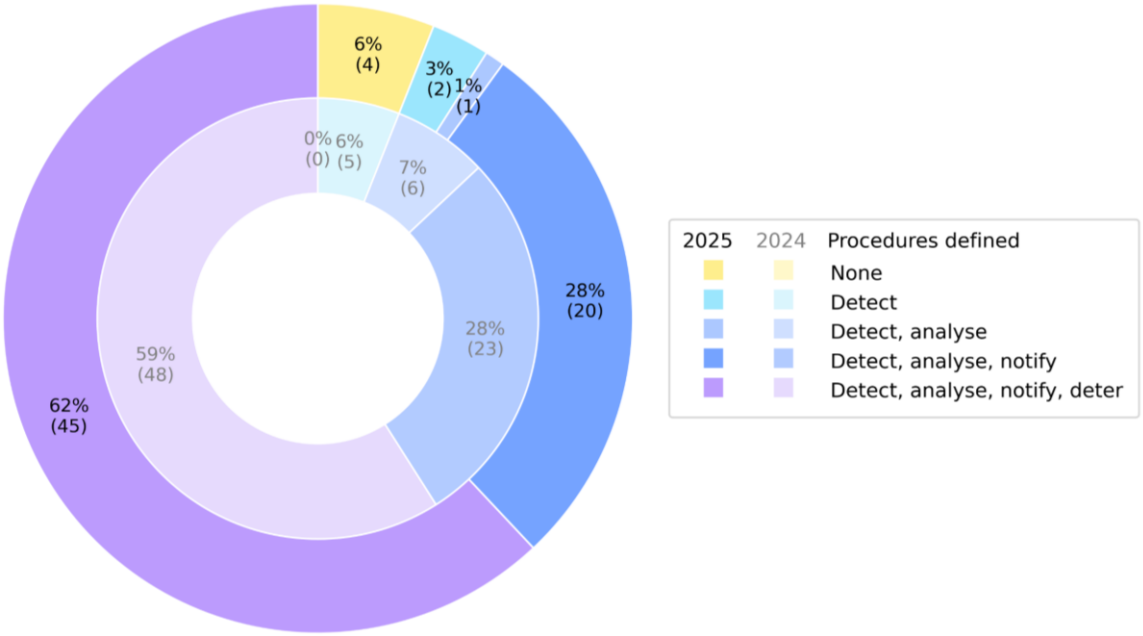
4.2.2. Procedures

The second part of the survey focuses on the procedures in place within PPATs, with particular emphasis on identifying formally defined procedures. It also assesses the timeliness of these procedures, specifically evaluating how quickly PPATs can detect suspicious activities. This section aims to gain insights into the robustness of the monitoring systems and the responsiveness of PPATs.

Apart from four PPATs that declare having no surveillance procedures in place, all other responding PPATs confirmed that they have at least detection procedures in place and **90% of participating PPATs have fully formalised procedures covering three core components ("detect – analyse – notify")**, while about 60% have procedures covering also **deterrence**. This aligns quite closely with last year's results, with the exception of reporting no procedures established, which was not detected last year, as demonstrated in Figure 16. This is likely due to the widening the PPAT reach, also including DEA providers.

65 PPATs responded that they have notification procedures in place, while only 30 PPATs submitted relevant STORs during the assessment period (trading period 1 July 2024 – 30 June 2025), highlighting a discrepancy between self-assessed detection capabilities and actual STOR submissions, particularly among brokers and DEA providers.

Figure 16: Procedures defined and formalised



Note: for 2024 n = 82, for 2025 n = 72

The survey explores the implementation of several individual procedures, including the auditing procedure. The **surveillance setup is audited in 40% of PPATs**, and the same proportion of PPATs are audited within a wider company context. All energy exchanges fall into one of these two categories. The remaining PPATs, namely a quarter of them, have never been audited. In comparison to last year, the latter category shrank.

Additionally, **one third of all PPATs do not have a policy in place that defines how to engage with clients under suspicion**. The biggest gap was detected among DEA providers[24].

When asked specifically regarding the STOR notification procedure, 80% of respondents confirmed having such a procedure defined, which is seven percentage points lower compared to last year's responding entities and also deviates from the data reported in Figure 16, related to the overall question on procedures. As reported by participating PPATs, this procedure is mainly formalised in an internal document, written in alignment with the relevant NRA and according to REMIT. Moreover, the **surveillance assessment[25] is part of the PPAT's internal procedures, such as onboarding or release of new tradable products for almost 70% of PPATs**, which is more than 10 percentage points higher as last year's responding entities.

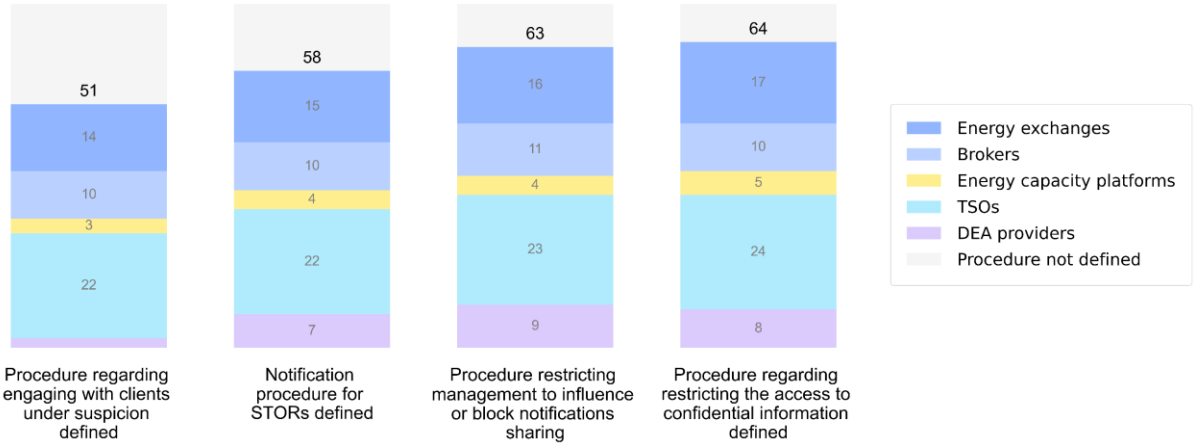
Furthermore, the **company management of almost 90% of PPATs cannot influence or block notifications to be shared with ACER and the responsible NRAs**, for example by requiring that management needs to formally approve the notification before it is sent. A significant increase of eight percentage points in comparison with last year's responding entities was detected in this regard. This result can be perceived as positive, considering the finding, that for almost 70% of participating PPATs surveillance is not judged as independent from management.

Moreover, in line with last year's results, surveillance teams in 90% of PPATs have adequate procedures and systems in place that restrict access to confidential information, as shown in Figure 17.

[24] Considering that DEA providers were only introduced as PPATs following the 2024 REMIT amendment, it is possible that they still experience some delays in implementing their obligations. However, such delays would be far less understandable next year.

[25] i.e. surveillance personnel are included in these processes

Figure 17: Procedures by PPAT types



Note: n = 72

One of the most representative indicators of the effectiveness of the procedures in place is the time between detection and notification of the suspicious event. Shorter times generally suggest that procedures are well established, maintained and functioning.

Article 15(1) of REMIT stipulates that notifications need to be submitted 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". The survey included two questions addressed to PPATs on this matter.

Firstly, PPATs were asked to provide the 'average time elapsed between the occurrence of the event (i.e. trading day) and the detection of its suspicious nature (i.e. establishing that the event should be looked at more closely)'.

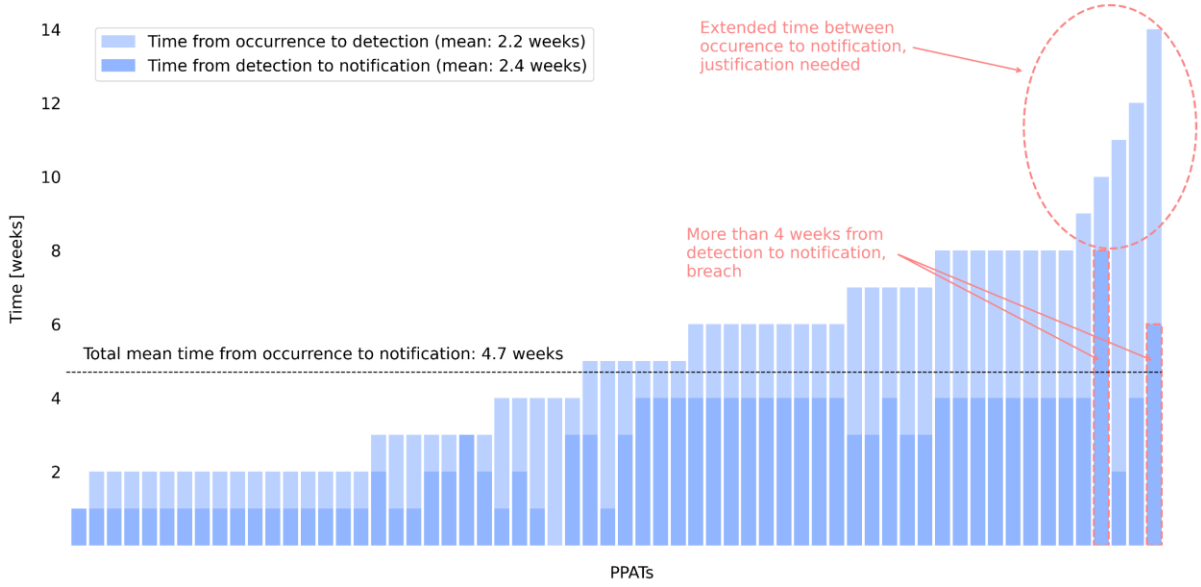
Secondly, they were requested to provide also the 'average time elapsed between the establishment of the suspicious nature of the event and the notification time (i.e. when the notification is sent to ACER / NRAs)'.

As already pointed out in ACER's open letter of 25 September 2024[26], contrary to the expected four weeks from the establishment of the suspicious nature to the STOR submission, the **time elapsed from the event and the awareness of the suspicious quality of the behaviour can vary but needs to be justified**.

The average time from the occurrence of the suspicious event to its detection, according to survey responses, is 2.2 weeks, while the average time from detection to notification is 2.4 weeks. The total mean time from occurrence to notification is 4.7 weeks, with the majority of PPATs reporting similar times for both procedures. Details are presented in Figure 18.

26 https://www.acer.europa.eu/sites/default/files/REMIT/Guidance%20on%20REMIT%20Application/Open%20Letters%20on%20REMIT%20Policy/25092024_3rd_Open_Letter_Third_Countries_PPAETs.pdf

Figure 18: Time of detection and notification

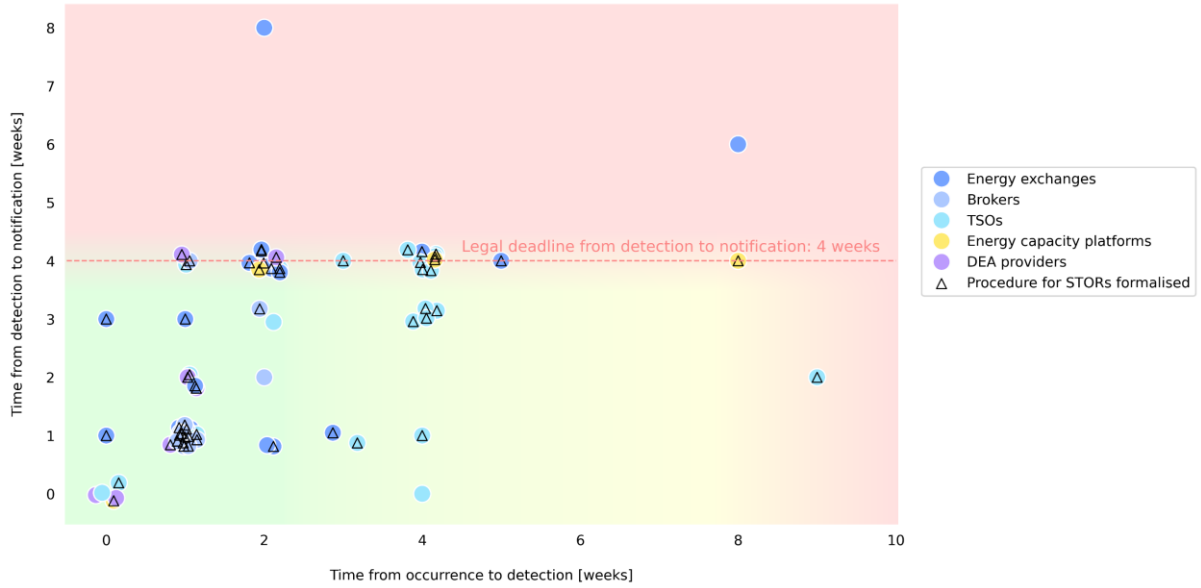


Note: n = 67

Brokers and DEA providers demonstrate the shortest detection to notification times with the lowest variability. The total time from occurrence to notification in this group is also approximately two weeks shorter than the mean time across all PPATs. **One practical consideration is that, while several PPATs report low detection to notification times in the survey, this is not reflected in the actual STORs delivered to ACER, as this is done by far fewer PPATs. This raises serious questions about the accuracy of the reported data.** Indeed, while no notification takes place, a detection to notification time cannot be calculated. It is possible, of course, that some reported detection to notification times taking into account STORs that are not part of the current sample, or notification paths not fully in line with REMIT.

As shown in Figure 19, the remaining PPAT groups show greater variability and report generally longer times. A positive correlation between detection and notification times was identified, whereby longer detection times go hand in hand with longer notification times.

Figure 19: Detection and notification times by PPAT type



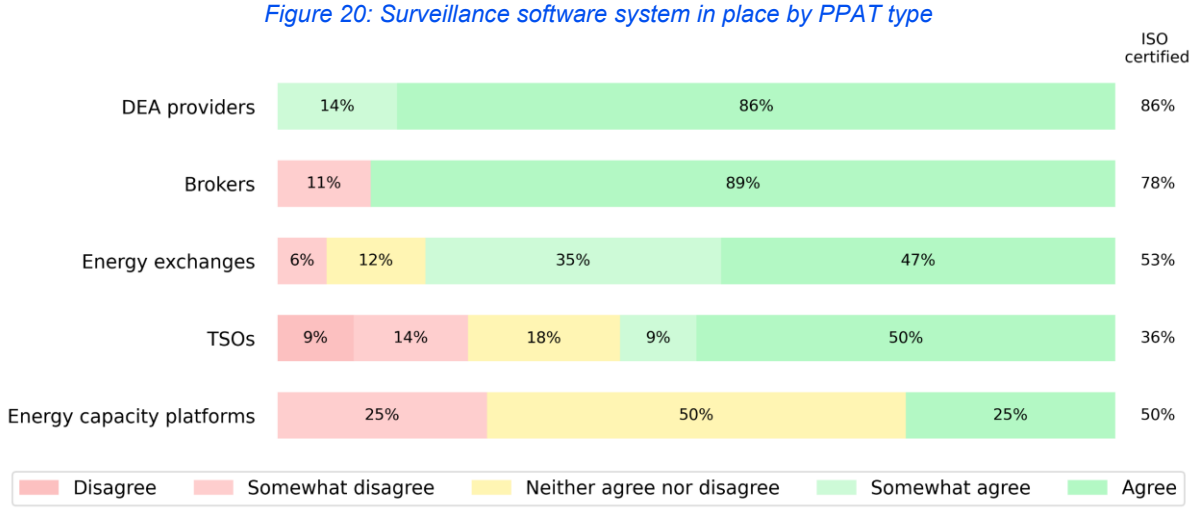
Note: n = 67

4.2.3. Systems

The Systems section investigates the software solutions used by PPATs to detect suspicious orders and transactions. This includes insight into how the systems function, the types of suspicious activities they identify, and the range of markets they monitor. Additionally, the survey addressed the issue of whether these systems are custom-built in-house or acquired from external providers.

Surveillance software systems are in place at approximately 70% of all respondents. DEA providers, brokers and energy exchanges stand out in this aspect. Slightly more than half of TSOs have surveillance software systems in place, whereas only a quarter of energy capacity platforms have them. Entities with professional systems are typically ISO-certified. Details are provided in Figure 20.

Figure 20: Surveillance software system in place by PPAT type

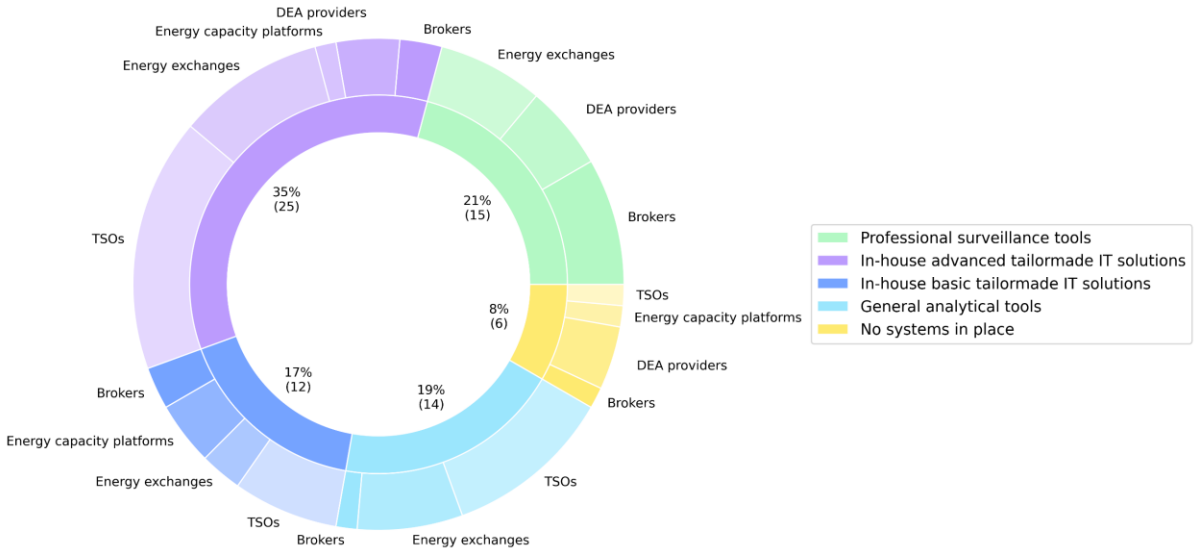


Note: n = 63

To detect suspicious orders and transactions, **only 21% of PPATs use a professional surveillance software system, while approximately half of PPATs report the use of self-developed tailor-made IT solutions**. Among those, most of them report using advanced solutions. Half of them are TSOs. 19% use general analytical tools, such as Microsoft Office, while the rest have no systems in place.

Those using professional surveillance systems also report shorter detection and notification times than those using self-developed solutions, potentially reflecting optimised and standardised protocols. It is worth mentioning that a correlation can be found, but a causal relation cannot be confirmed. Potential other causes could for example be better staffing, better training of the staff or less administrative burdens in the notification process. In general, there is no specific pattern in relation to the type of PPAT and the solutions it has in place - see Figure 21.

Figure 21: Surveillance systems PPATs rely most on

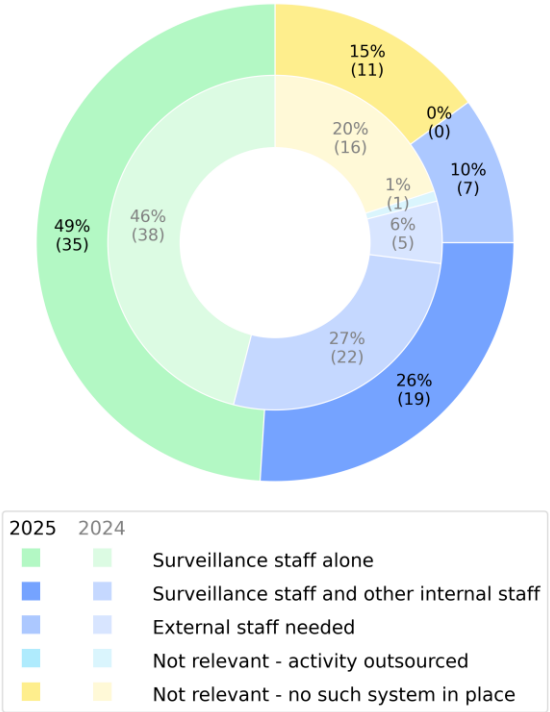


Note: n = 72

Half of the participants stated that surveillance system parameters can be changed by surveillance staff alone, meaning that there is no need for the involvement of others, either internals or externals. About a quarter of respondents require validation by other internal staff, while 10% require external staff support. Overall, the independence of surveillance staff in modifying system parameters has improved compared to last year (for details, see Figure 22).

Notably, the change of surveillance parameters depends significantly on the type of surveillance system in place. **In-house developed solutions allow surveillance staff greater independence, whereas professional software systems require external assistance for most of the changes**. Regardless of the system in place, PPATs ensure that every change of surveillance parameters is statistically justified and tested before its final implementation. **Most PPATs do a periodic review of surveillance parameters, ensuring that systems are continuously updated and effectively calibrated to respond to current market dynamics**.

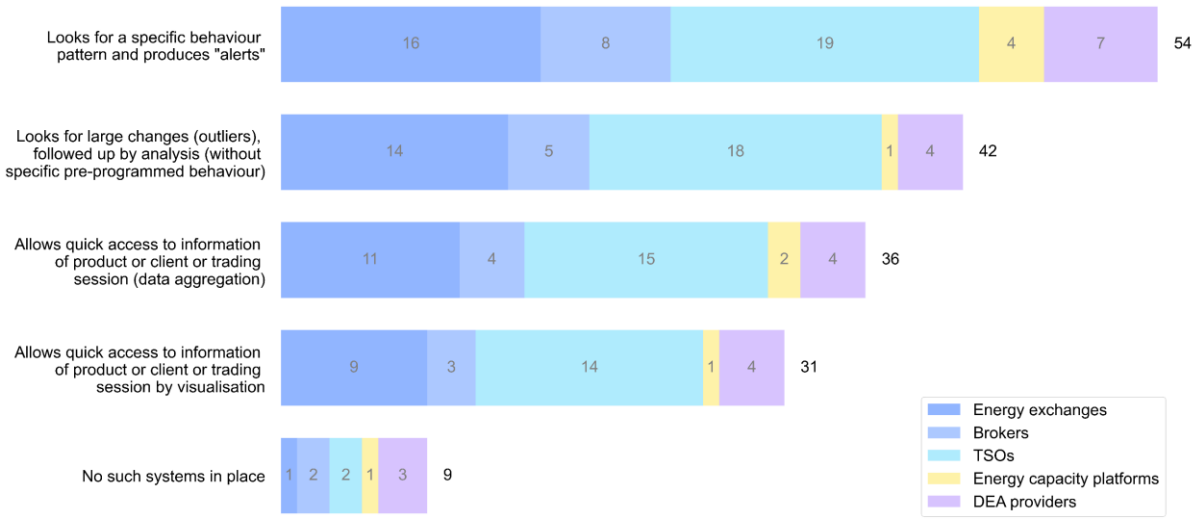
Figure 22: Change of surveillance parameters



Note: for 2024 n = 82, for 2025 n = 72

A large proportion of surveillance systems in place at PPATs look for specific behaviour patterns and produce alerts and also identify large changes or outliers that are followed up by analysis without specific pre-programmed behaviour. The surveillance systems of more than 40% of the respondents allow quick access to information regarding the product, client or trading session, accompanied by visualisations, which is in line with last year's findings. No significant difference between different PPAT types can be identified, as shown in Figure 23.

Figure 23: Work of surveillance systems in general, by PPAT type



Note: n = 72

4.3. Assessment of PPAT surveillance capability

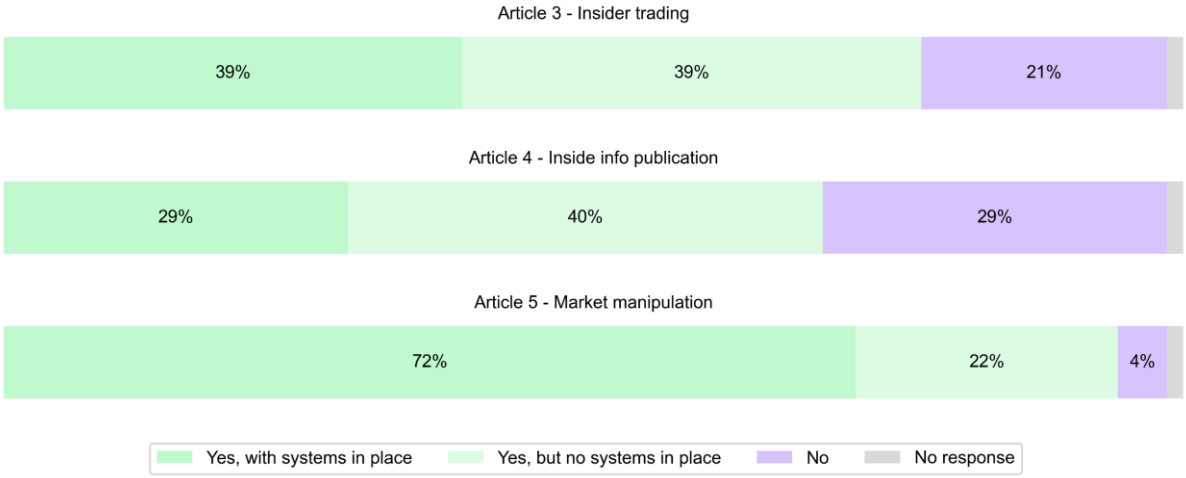
4.3.1. Detection capability

Similarly to the previous edition of this report, the survey covered PPATs' self-assessment detection capabilities. This year, this section was **complemented with a self-assessment on the ability to cover breaches of different REMIT articles, different operated markets and specific behaviours**.

The ability to detect REMIT breaches is explored separately for Articles 3 (insider trading), 4 (publication of inside information), and 5 (market manipulation). **Article 5 breaches are reported to be detectable by more than 90% of all PPATs**. The majority use surveillance systems for detection. **Slightly lower is the ability to detect breaches of Article 3, while one third of PPATs are completely unable to detect breaches of Article 4**. Besides, no discernible pattern between different types of PPATs can be identified. For details, refer to Figure 24.

In addition, **60% of PPATs report covering all markets at the same level** in terms of market surveillance, with the majority having detection abilities for all the previously mentioned REMIT articles. Approximately a quarter of participating PPATs cover all markets, but at different levels, whereas 10% only cover some of the markets they operate in.

Figure 24: Ability to detect REMIT breaches – self-assessment



Note: n = 71

The assessment section of the survey also gathered information on the capacity of PPATs to detect market manipulation by specific behaviour. On average, brokers and DEA providers reported the highest detection capacities. **It is to be noted, however, that this self-assessment is not supported by the number of STORs submitted by these entity types, compared to those submitted by others**. Slightly more limited are the self-assessed detection capacities of energy exchanges, followed by TSOs. Energy capacity platforms stand out significantly as they lack operational surveillance for many behaviours, yet this should be interpreted in an appropriate context, since only five energy capacity platforms participated in the survey. Moreover, not all behaviours are relevant for all markets.

Detection capacities are highest for erroneous orders, misleading signals, layering, spoofing, abusive squeeze, and orders placed with no intention to execute, and are lowest for front running, capacity withholding, dissemination of false or misleading information, non-effective disclosure of inside information, and double printing. Overall, the variability of detection capacities across behaviours is low.

For a detailed breakdown see Figure 25, in which the number in each cell represents the average detection capacity for a pair of behaviour and PPAT type.

Figure 25: Capacity to detect market manipulation by behaviour type

	Brokers	DEA providers	Energy exchanges	TSOs	Energy capacity platforms	Average
Erroneous orders	2.2	2.5	2.1	1.9	1.3	2.0
Giving, being likely to give or attempting to give false or misleading signals	2.4	2.1	2.2	2.0	1.0	1.9
Layering / Spoofing	2.5	2.6	2.4	1.0	1.0	1.9
Abusive squeeze	2.2	2.4	1.8	1.6	1.0	1.8
Placing orders with no intent to execute	2.4	2.6	2.2	1.6	0.0	1.8
Wash trades	2.5	2.6	2.5	1.0	0.5	1.8
Insider trading	2.3	2.2	1.6	1.3	1.2	1.7
Advancing the bid	1.9	2.6	1.9	1.2	1.0	1.7
Pre-arranged trading	2.2	2.6	2.2	0.9	0.5	1.7
Quote stuffing	2.2	2.6	2.0	1.1	0.0	1.6
Cross-product manipulation	1.9	1.7	1.8	1.2	1.0	1.5
Distort costs	2.2	1.5	1.1	1.3	1.3	1.5
Creating a floor or ceiling	2.2	2.5	1.6	1.4	0.0	1.5
Marking the reference period	2.3	2.6	1.7	0.7	0.0	1.5
Momentum ignition	2.5	2.6	1.8	0.8	0.0	1.5
Smoking	2.2	2.4	1.7	0.6	0.0	1.4
Painting the tape	2.2	2.6	1.8	0.5	0.0	1.4
Transmission capacity hoarding	1.7	0.6	1.2	1.6	2.0	1.4
Trash and cash / Pump and dump	2.4	2.2	1.8	0.4	0.0	1.4
Phishing	1.7	2.1	1.8	0.6	1.0	1.4
Front running or prepositioning	2.1	2.2	1.4	0.9	0.0	1.3
Capacity withholding	1.6	0.6	1.2	2.0	1.3	1.3
Dissemination of false or misleading information	2.1	2.0	1.3	0.9	0.0	1.3
Non effective publication of inside information	1.6	1.1	1.1	1.3	1.0	1.2
Double printing	1.6	1.2	1.2	0.8	0.0	1.0
Average	2.1	2.1	1.7	1.1	0.6	

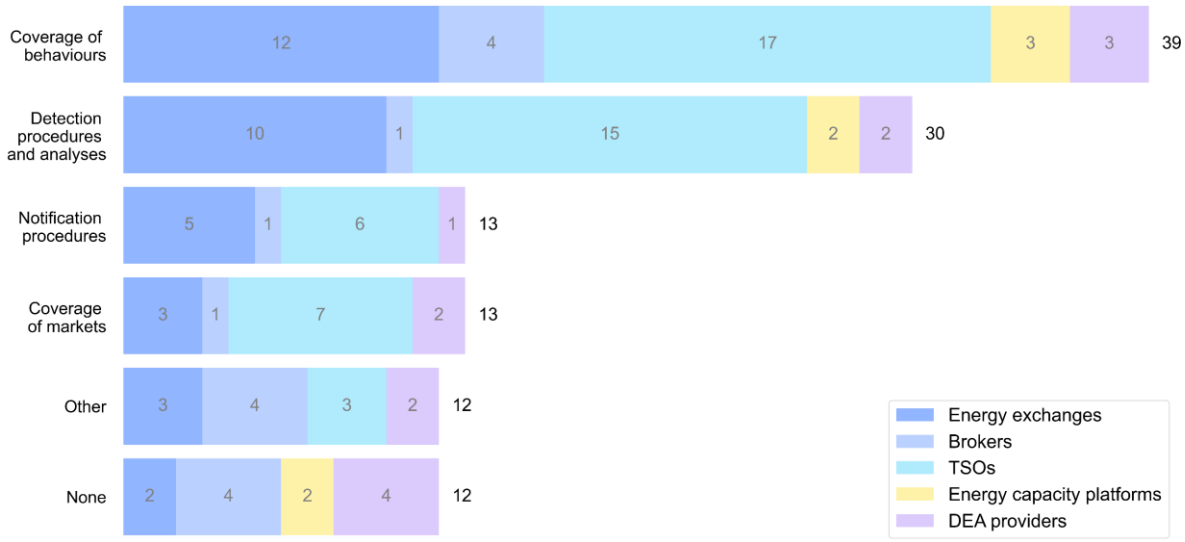
0 - No operational surveillance
1 - Limited detection capacity
2 - Medium detection capacity
3 - High detection capacity

Note: n = 62

4.3.2. Needs for improvement

The final section of the survey focuses on a general self-assessment, aiming to foster reflection about the overall effectiveness of PPAT's surveillance set-up, helping participants recognise strengths and areas for growth. The results reveal that **more than 40% of PPATs desire to improve detection procedures, analyses and coverage of manipulative behaviours**, highlighting the importance of more robust and wider monitoring systems, which was already stressed in the previous year. For details, refer to Figure 26.

Figure 26: Surveillance set-up elements to be improved by PPAT type

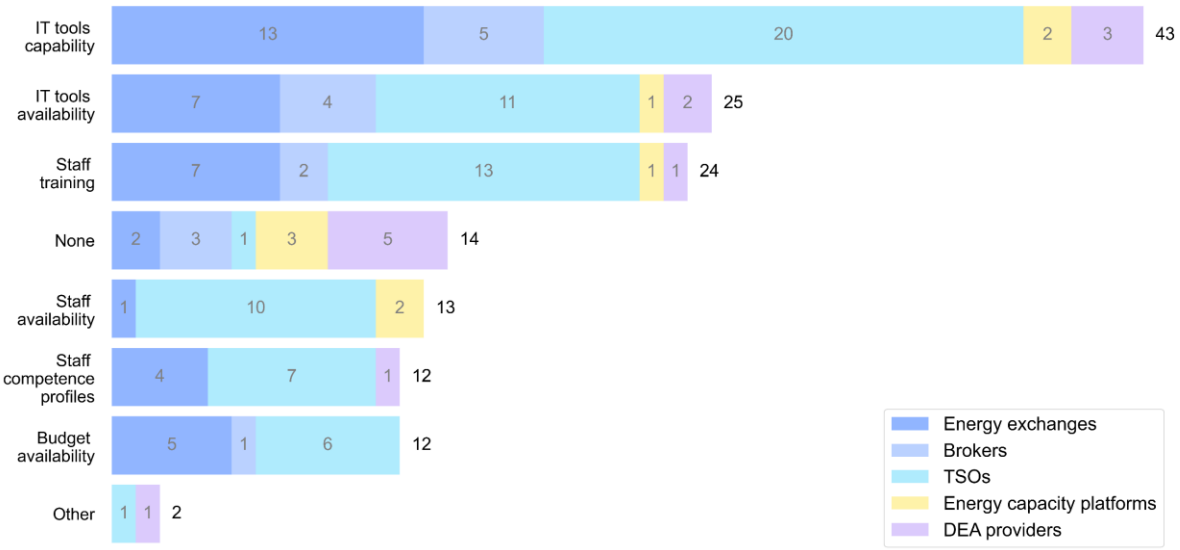


Note: n = 72

Additionally, PPATs expressed a **wish to improve a variety of surveillance conditions**. The most reported ones are **IT tools capability, IT tools availability and staff training**. Of particular importance, as already noted last year, are the need for enhancement of IT tools availability and capability, highlighting the critical role of reliable, efficient, and accessible technology in supporting effective surveillance operations.

The need for improvement in staff training aligns with the fact that for more than half of PPATs, surveillance staff is judged not to be receiving appropriate training and guidance on REMIT, in particular regarding the application of Article 15 of REMIT (e.g. in the form of in-house or outside training, conferences or similar). For details and a breakdown per PPAT type, see Figure 27.

Figure 27: Surveillance conditions to be improved by PPAT type



Note: n = 72

4.4. Surveillance capability analysis

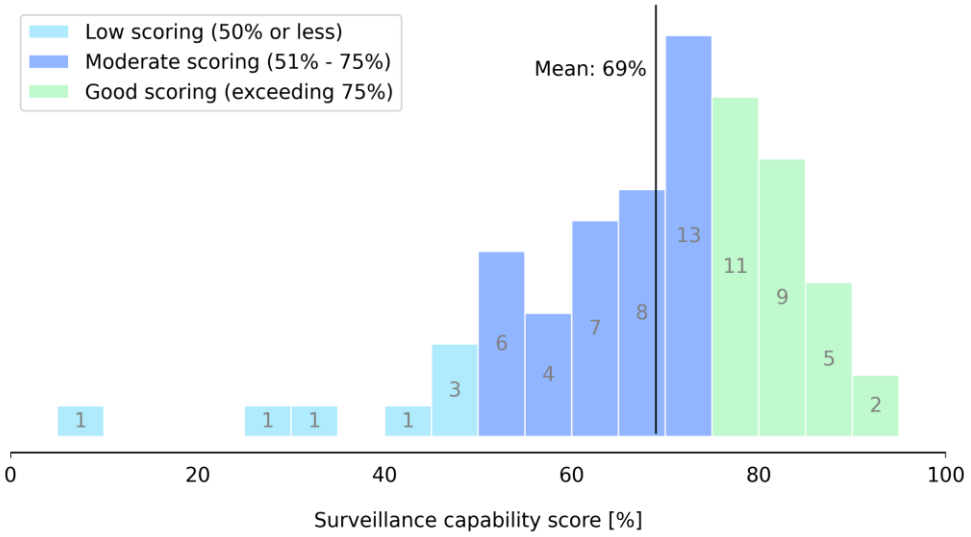
In this section we present a synthetic assessment of PPAT surveillance capability, based on specific questions from the four sections of the survey: Arrangements, Procedures, Systems, and Assessment. Details regarding scoring are available in the Annex.

4.4.1. Key findings

The average total weighted surveillance capability score across all respondents is 69%, which is five percentage points higher than last year.

The lowest score recorded is 8%, indicating that some participants meet very few of the criteria, and the highest score achieved is 91%, reflecting the strongest performance within the dataset. The standard deviation of 15 percentage points reveals a relatively high degree of variability in the scores, yet lower than in the previous year, resulting in the higher average score. The interquartile range of 19 percentage points indicates that the middle 50% of the scores fell within a 19 percentage-point range, showing a moderate level of consistency in the central scores while reflecting the spread in higher and lower scores. The score distribution is presented in Figure 28.

Figure 28: Distribution of surveillance capability scores



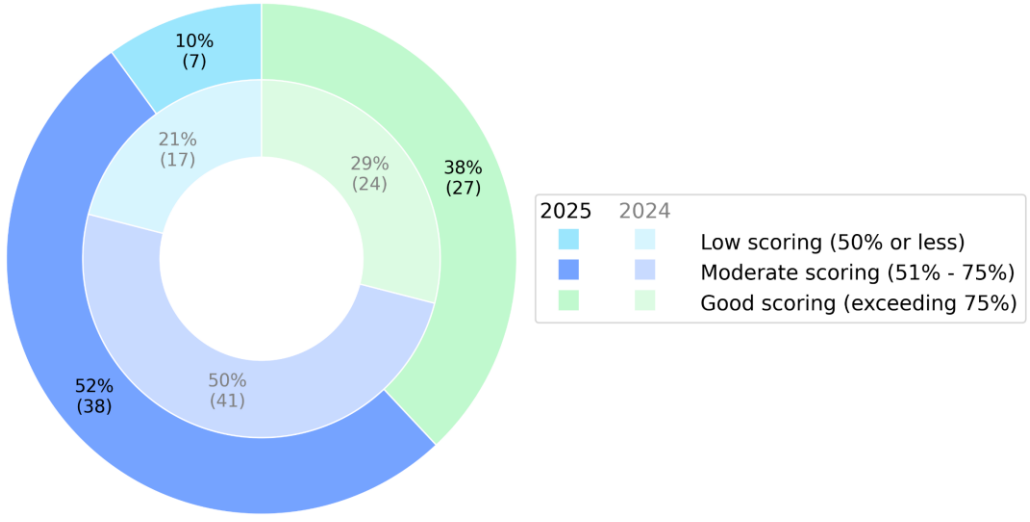
Note: n = 72

For illustration purposes, PPATs can be **categorised into three groups based on their surveillance capability score**:

- 50% or less – low scoring, substantial room for improvement identified;
- between 51% and 75% – moderate scoring, partial room for improvement identified;
- exceeding 75% – good scoring, room for improvement regarding less critical issues identified.

27 PPATs (38% of participants) achieved a good score, 38 PPATs (more than half of participants) a moderate one, while the remaining seven PPATs (10%) were ranked as low. An overall improvement is detected, since the proportion of PPATs achieving a low score has almost halved compared to last year. Nonetheless, it is important to emphasise that this year's sample, containing ten fewer responding entities than the previous year despite the much larger number of addressees, may not be a representative sample of all PPATs. Therefore, the surveillance capability scores could be overestimating the real situation. See Figure 29 for details.

Figure 29: Surveillance capability scores

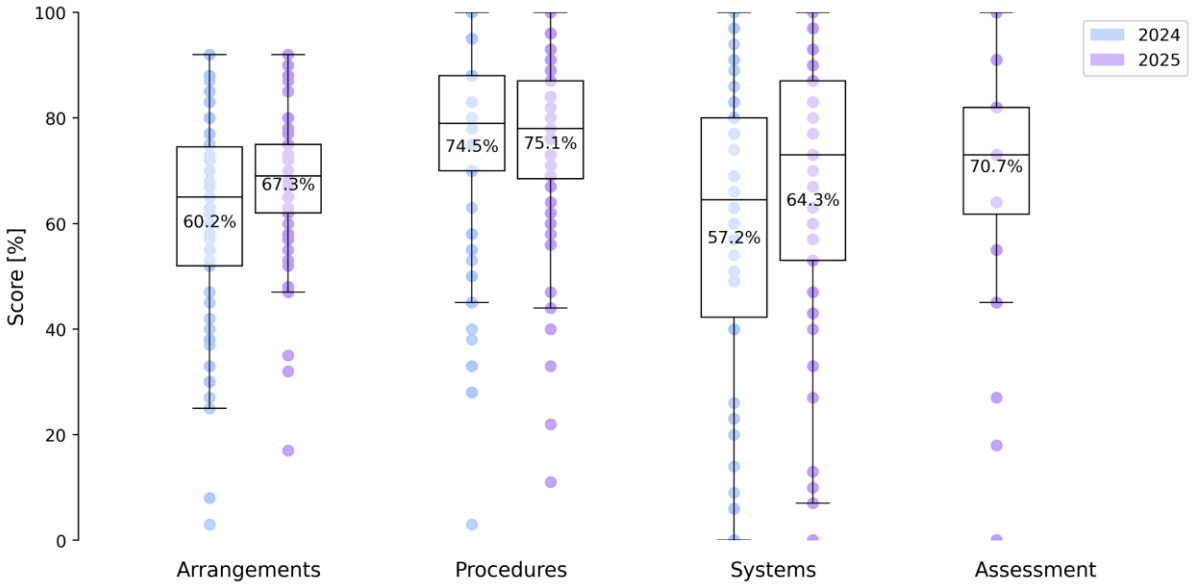


Note: for 2024 n = 82, for 2025 n = 72

Beside the sampling bias, the ratings are a result of the methodology selected for the evaluation of the survey results. An above average rating does not necessarily relate to the timely notification of above average STORs, similarly, a low score is not necessarily associated with below average STORs. This aspect is evaluated separately in the surveillance effectiveness assessment presented in the following section.

The analysis of the surveillance capability scores for Arrangements, Procedures, Systems and Assessment reveals small differences in scores across the four areas. The area with the **highest score is Procedures**, achieving an average score of 75%. It is followed by Assessment, with an average score of 71%. Arrangements and Systems follow with 67% and 64% respectively. The **greatest variability in scores can be detected in Systems**, as indicated by the wider spread of the results. The results closely align with last year's results. The most significant improvement was observed in the Systems section. For details, refer to the box plot in Figure 30.

Figure 30: Partial surveillance capability scores by section



Note[27]: for 2024 n = 82, for 2025 n = 72

The scores are further analysed by categorising participants based on their type, relevant commodities, and years of operation as market intermediaries. The results for each group are presented in the following sections.

4.4.2. Scores by types of PPAT

First, the surveillance capability scores were examined across different types of PPATs: energy exchanges, brokers, TSOs, energy capacity platforms, and DEA providers. A summary of the scores by PPAT type is provided in Table 1. Next to each category, the number of PPATs in that specific category is indicated in brackets. A similar approach is used in all subsequent tables.

[27] A box plot is a graphical representation of a dataset that summarises its distribution. The box represents the interquartile range, which contains the middle 50% of the data. The lower bar of the box indicates the first quartile (Q1), meaning that 25% of the data lies below this value. The bar in the middle of the box is the median value (Q2), representing the mid-point of the dataset. The bar at the top of the box indicates the third quartile (Q3), meaning that 75% of the data lies below this value. The interquartile range is equal to Q3 – Q1. The box plot also contains whiskers, which extend from Q1 to the minimum and from Q3 to the maximum, excluding outliers. Additionally, the number displayed inside the box represents the mean.

Table 1: Surveillance capability scores by section and PPAT type

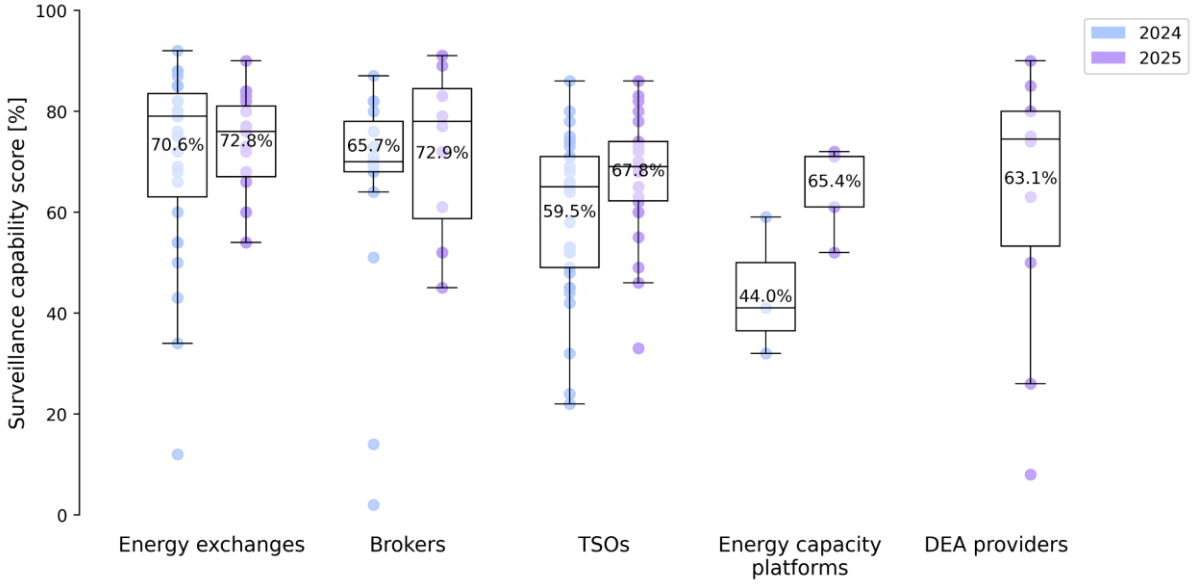
	Arrangements	Procedures	Systems	Assessment	**Total**
Energy exchanges (19)	70%	78%	70%	71%	73%
Brokers (12)	65%	84%	66%	84%	73%
TSOs (26)	66%	71%	64%	72%	68%
Energy capacity platforms (5)	72%	72%	54%	58%	65%
DEA providers (10)	64%	69%	58%	58%	63%

Note: n = 72

The **highest scoring is observed among energy exchanges and brokers**, with an average total score of 73%, representing an increase relative to their performance last year. In addition, the variability of scores among PPATs in those two groups is significantly lower than last year. The distribution of scores across different sections is even in the case of energy exchanges, but varies more in the case of brokers, as already identified last year. In the Arrangements and Systems sections, the lowest scores are achieved by brokers, suggesting that there may be room for improvement in this area. On the other hand, brokers excelled in the Procedures and Assessment sections, achieving an average score of 84%.

The average score for TSOs is 68%, indicating moderate adherence to expected standards. **The most significant gap is identified in the Systems section, which was to be expected given certain TSO specifics**. TSOs are followed by energy capacity platforms, which achieved an average score of 65%, and DEA providers, which scored two percentage points lower. Notably, the biggest gap in their performance is observed in the Systems and Assessment section. In addition to these observations, further details on the distribution of scores across all groups are presented in Figure 31.

Figure 31: Surveillance capability scores by PPAT type



Note: for 2024 n = 82, for 2025 n = 72

4.4.3. Scores by commodities

The analysis also examines whether there are significant differences in the scores of PPATs arranging trading of different commodities, where not only energy is considered, but also storage and transportation capacity. To explore this, PPATs can be categorized into three groups: those arranging trading of electricity-related products only, those arranging trading of gas-related products only, and those arranging trading of both.

The findings show that **PPATs involved in arranging trading of both electricity and gas-related products achieved the highest surveillance capability scores**, with an average total score of 75%, which is three percentage points higher than last year. In contrast, PPATs involved in arranging trading of only one type of commodity, either gas or electricity, have marginally lower average scores. PPATs arranging trading of only gas-related products achieved 71%, while those arranging trading of only electricity-related products achieved 65%. It is noteworthy that the group of PPATs arranging trading of only electricity-related products is more than two times larger than the group of PPATs arranging trading of only gas-related products. Besides, two DEA providers reported not arranging trading of either electricity or gas-related products[28]. The results are summarised in Table 2.

Table 2: Surveillance capability scores by section and traded commodities

	Arrangements	Procedures	Systems	Assessment	**Total**
Electricity and gas (24)[29]	68%	78%	77%	74%	75%
Electricity only (33)	67%	71%	57%	57%	65%
Gas only (13)	66%	81%	64%	70%	71%
Neither electricity nor gas (2)	71%	76%	37%	69%	62%

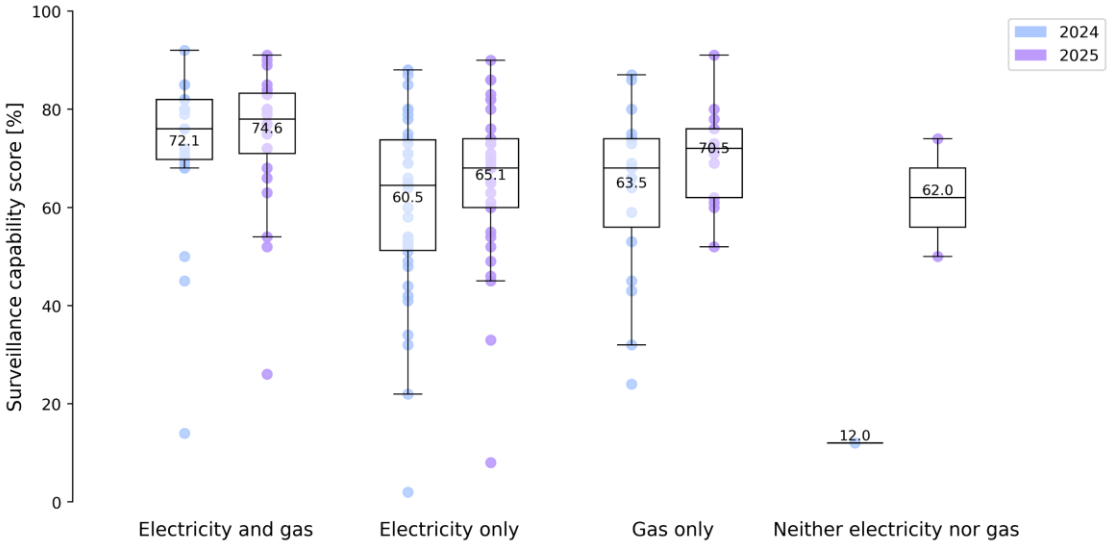
Note: n = 72

The highest variability in scores is observed among PPATs arranging trading of only electricity-related products. However, some outliers are identified among PPATs arranging trading of both commodities. In comparison with last year's scores, the variability among PPATs trading solely one commodity is substantially lower, reflecting a more homogenous dataset. Figure 32 presents the details.

[28] The status and role of these DEA providers has to be clarified later.

[29] The number in brackets next to the group represents the number of respondents for each commodity type, two PPATs are excluded since they are not arranging trading of neither electricity nor gas.

Figure 32: Surveillance capability scores by traded commodities



Note: for 2024 n = 82, for 2025 n = 72

4.4.4. Scores by active years

Surveillance capability is also assessed according to the PPATs' experience as market intermediaries and the number of Member States covered. PPATs are categorised according to their years of activity as market intermediaries in three groups: recently established (less than 5 years), moderately established (5 to 20 years), and well-established (more than 20 years), with average scores of 68%, 70% and 69%, respectively, as presented in Table 3.

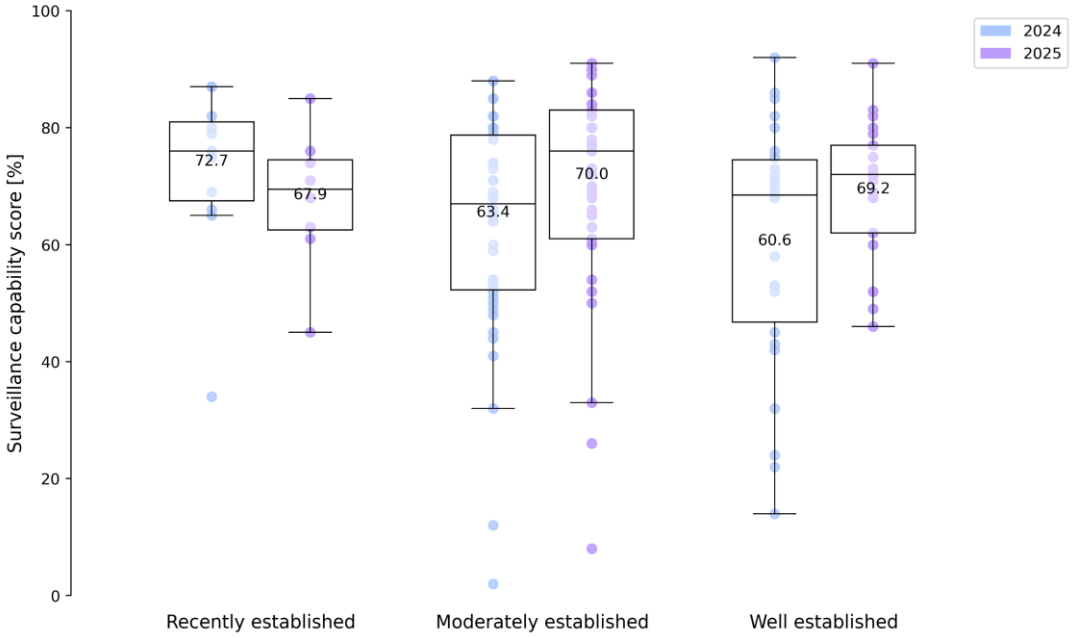
Table 3: Surveillance capability scores by section and active time as market intermediary

	Arrangements	Procedures	Systems	Assessment	**Total**
Recently established (8)	65%	71%	67%	66%	68%
Moderately established (39)	66%	74%	69%	70%	70%
Well established (25)	71%	77%	58%	74%	69%

Note: n = 72

In general, similar conclusions to those observed last year apply. **Longer established PPATs, namely moderately and well-established ones, generally tend to achieve slightly higher surveillance capability scores** in comparison with recently established entities, yet the identified correlation is not as strong as the one detected last year, possibly due to the smaller sample size. In addition, the variation of results in the group of well-established PPATs is significantly lower than in the other two groups, suggesting a more consistent performance of well-established entities (see Figure 33).

Figure 33: Surveillance capability scores by active time as market intermediary



Note: for 2024 n = 82, for 2025 n = 72

5. Surveillance effectiveness analysis

Surveillance effectiveness was evaluated based on PPATs' responses to the survey, including newly introduced questions compared to 2024, along with ACER's analysis of STOR data.

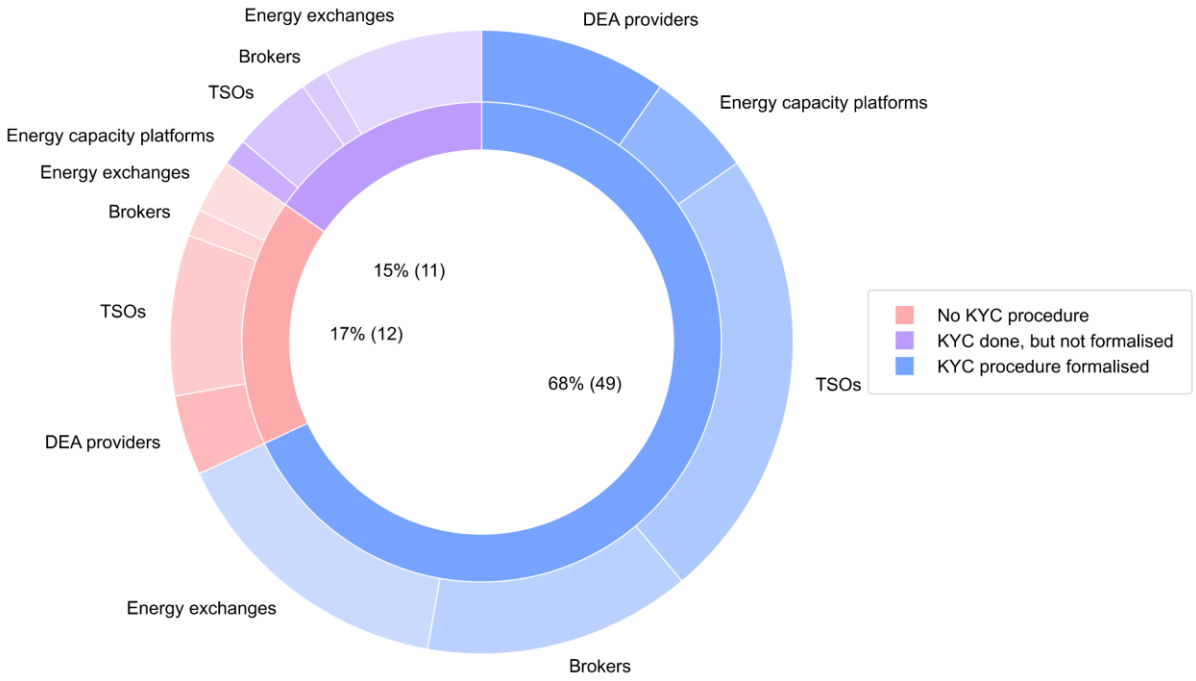
As already described in Section 3.3.2, the score consists of two partial scores – a direct inquiries / KYC score and a STOR score.[30]

5.1. Direct inquiries and KYC

Almost 70% of PPATs have KYC procedures formalised within the company to admit members or clients. KYC procedures are used, but not formalised, by 15% of responding PPATs. The remaining 17% declare having no KYC procedure at all. The limited performance of this last group of PPATs is identified also in the surveillance capability analysis, where they score more than 10 percentage points lower than the average. There are no significant differences between different types of PPATs in relation to the KYC procedure formalisation, apart from brokers exhibiting a high level of KYC implementation with more than 80% of them having KYC procedures formalised. For a detailed breakdown per PPAT type, refer to Figure 34.

Furthermore, **43% of PPATs issue educational communications or offer training courses to clients or members in relation to REMIT or REMIT breaches**. Half of these prepare both communications and courses.

Figure 34: KYC procedure formalised to admit members

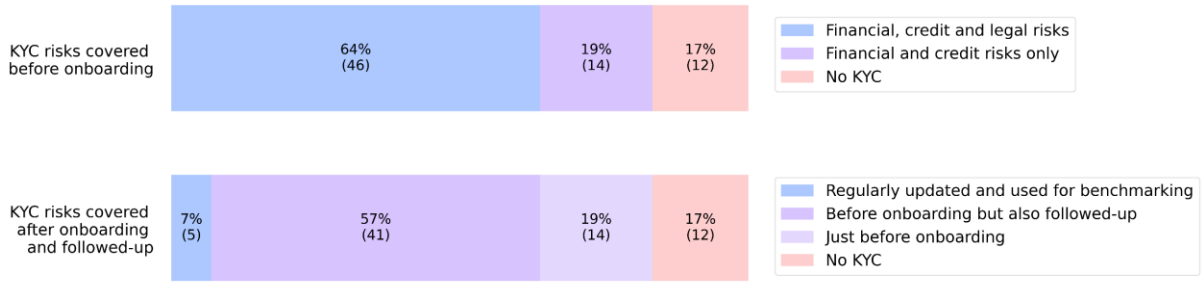


Note: n = 72

[30] The direct inquiries score contains information from PPATs gathered by the survey regarding their direct inquiries with market participants, coupled with KYC processes. It is based on responses to specific questions, specifically 7 questions in the Procedures section. For details, see the complete questionnaire in the Annex.

64% of KYC procedures before onboarding a new member or client cover financial, credit and legal risks, including also REMIT related risks, for example checks for previous sanctions, notifications for the legal entity in question or connected entities and lack of compliance measures. Approximately one fifth of procedures cover only financial and credit risks. **Only 7% also regularly conduct updates in the context of their KYC procedures – more precisely on data relating to the member – after the member has already been active for some time and use them for benchmarking when assessing potentially manipulative behaviour**. This category consists of well-established PPATs, arranging trading for delivery areas beyond Member States, with an average surveillance capability score 12 percentage points higher than the mean. Besides, more than half report following up the procedures with updated data, while a quarter perform the procedure only before onboarding, see Figure 35.

Figure 35: KYC procedure before versus after onboarding

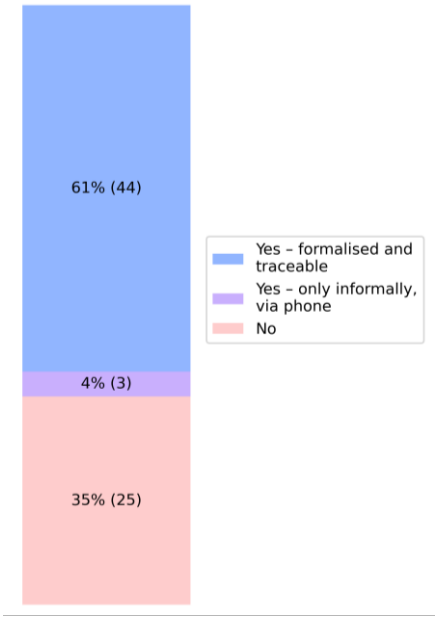


Note: n = 72

In cases of REMIT-related suspicion, **65% of PPATs contact the relevant client or member in a traceable manner to obtain clarifications, with the majority using a formalised approach**. The remaining 35% do not contact the relevant members; these are mainly PPATs the surveillance function of which is embedded in other functions and that arrange trading only for delivery areas in Member States. In addition, no specific type of PPATs can be identified among those not contacting the members. See Figure 36 for details.

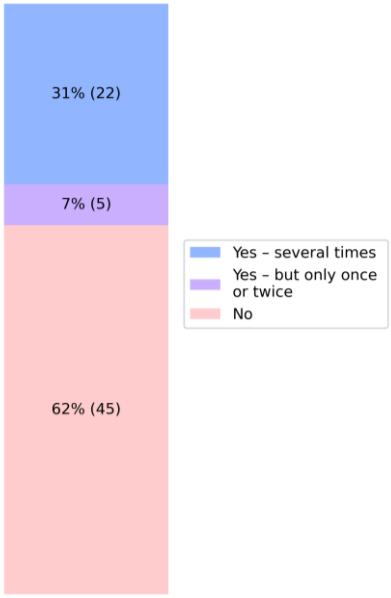
More than a third of PPATs contacted a member in the past year regarding a potential REMIT breach. These are mainly PPATs with a moderate surveillance capability score, on average 4 percentage points above the mean (see Figure 37). In cases, where a member does not respond to a clarification request, one third of PPATs have a formalised follow-up procedure in place.

Figure 36: Contacting relevant members in case of REMIT-related suspicions



Note: n = 72

Figure 37: Contacting relevant members regarding a potential REMIT breach in 2024



Note: n = 72

Additionally, 25% of PPATs – mostly energy exchanges and energy capacity platforms – report having removed a market participant, for whichever reason, from their market or having terminated a client in the past three years. The same proportion of PPATs reported that no removal took place despite situations potentially requiring such action. One PPAT initiated a removal procedure, but it did not result in an actual removal. The remaining 44% have never removed a market participant, as no situation requiring such action has arisen.

As regards the **scoring**, survey questions C12 to C17 were used as an input for the final effectiveness score. The maximum achievable score was 21 points. Further details on scoring methodology are provided in the Annex. Table 4 presents the (normalised) results by PPAT type. While there is high variability in all categories, **exchanges score higher than other PPAT types, on average**. For the purposes of this analysis, and for the STOR score analysis in the following section, cross-border capacity platforms are included in the TSO category, due to their low numbers. The overall KYC normalised score average is 50.1.

Table 4: Direct inquiry / KYC normalised scores by PPAT type

PPAT type	Average	Maximum	Minimum
Exchange	59.1	100	10
Broker	49.8	81	14
TSO	47.2	90	0
DEA provider	40.9	90	0

Note: n = 72

5.2. STOR effectiveness

The methodology is explained in Section 3.3.2. In this section, key results are presented to give some context to the final scores:

1. **STORs.** 168 STORs from 30 PPATs for the assessment period. Individual numbers ranged from 1 to 40.
2. **Adjusted STOR count.** The adjusted total count was 88 STORs, when accounting for thoroughness, then discounted to 72.8 STORs when multiplying by the ACER completeness score (which ranges from 0 to 1). As mentioned, "thoroughness" reflects the in-depth analysis and contextualization of the suspected breach. Individual PPAT scores, i.e. adjusted STOR count multiplied with the average STOR completeness for the PPAT, ranged from 0.6 to 8.6.
3. **Third-party report parameter.** A deduction ranging from 0.2 to 0.8 was applied for 14 PPATs if
    - the PPAT in question did not submit a STOR, and
    - the alleged behaviour could have been noticed by the PPAT.
4. **ACER alert parameter.** A deduction ranging from 0.25 to 0.5 was applied for four PPATs, if
    - several (NRA-shared) ACER alerts[31] exist without corresponding PPAT STORs. It should be noted that these shared alerts might correspond to cases that are in fact examined by the PPATs and subsequently dismissed. Therefore, this reduction was applied parsimoniously.
5. **Final scores.** The final scores ranged from -0.7 to 8.6 for 36 PPATs and were then normalised to a scale from 0 to 100.

While ACER and NRAs value all STORs that allow to detect potential REMIT breaches, the STOR thoroughness allows the scoring to positively reflect the PPAT's additional efforts to contextualise the suspicion.

5.3. Final effectiveness score

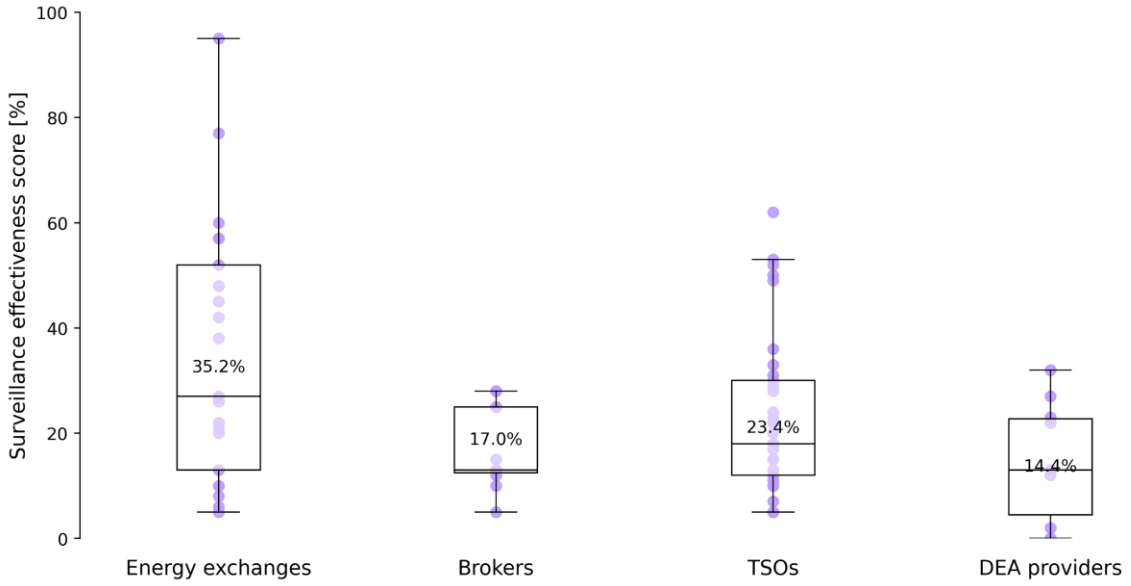
The **final effectiveness score was computed for PPATs, that had a direct inquiry / KYC score, a STOR score, or both**. Out of the 75 PPATs assessed, 31 had both scores, 39 did not have the STOR score (i.e. no relevant STORs or deductions) and five did not have the direct inquiry / KYC score (i.e. they did not reply to the survey). Regarding the link to the survey, out of 72 responses, one was removed because the PPAT ceased operation in 2025, while two responses were merged since the two entities from the same group fully merge surveillance activities, thereby bringing the total to 70. Since 5 entities only had the STOR part of the score, this brings the total number of assessed entities to 75.

It is also important to stress, that in the overall, final ranking the missing part (STOR or direct inquiry) was implicitly counted as 0.

The final scores by PPAT type are presented in Figure 38 and Table 5.

[31] These are ACER alerts that are screened by ACER Surveillance analysts, judged relevant and therefore shared with the relevant NRAs.

Figure 38: Final effectiveness score by PPAT type



Note: n = 75

Table 5: Final effectiveness score by PPAT type and score completeness

PPAT type	Both elements	STOR score only	Inquiry score only	Grand total
Exchange	41.4 %	10 %	19 %	35.2 %
Broker	28 %		15.9 %	17 %
TSO	35.6 %	10.7 %	15.2 %	23.4 %
DEA provider			14.4 %	14.4 %
Grand total	38.3 %	10.4 %	15.5 %	24.6 %

Note: n = 75

The following **conclusions** can be made:

- There is very **high variability** overall, and within particular categories.
- On average, **energy exchanges show a better score compared to other PPAT types**.
- **TSOs show quite a good score on average**, especially when considering that arranging transactions is not their core activity. TSO's role is of relevance for overall market surveillance effectiveness due to the fact, that balancing markets data was not reported continuously under REMIT I, which would have enabled ACER and NRAs to develop market surveillance similarly as for other markets (e.g. day-ahead).
- Since the **DEA provider** sample size is quite modest, comprising also some entities with very specific arrangements, no definitive conclusion can be made, apart from the fact that the **general awareness of REMIT obligations seems to be rather low**.
- **Brokers show the lowest score in this assessment**, particularly in the STOR score segment.

5.3.1. Interplay between capability and effectiveness

A cross-check was performed also regarding the **interplay between the capability score and the final effectiveness score**. A subset of PPATs, which have **submitted two or more STORs relevant for the same trading period (second half of 2024 and first half of 2025) was considered**, i.e. the same sub-set of STORs as in the effectiveness assessment was used. The average capability score of these PPATs in higher, albeit slightly, than that of the overall average. On the contrary, their average effectiveness score is, as expected, more than double the average for all PPATs. Details are presented in Table 6.

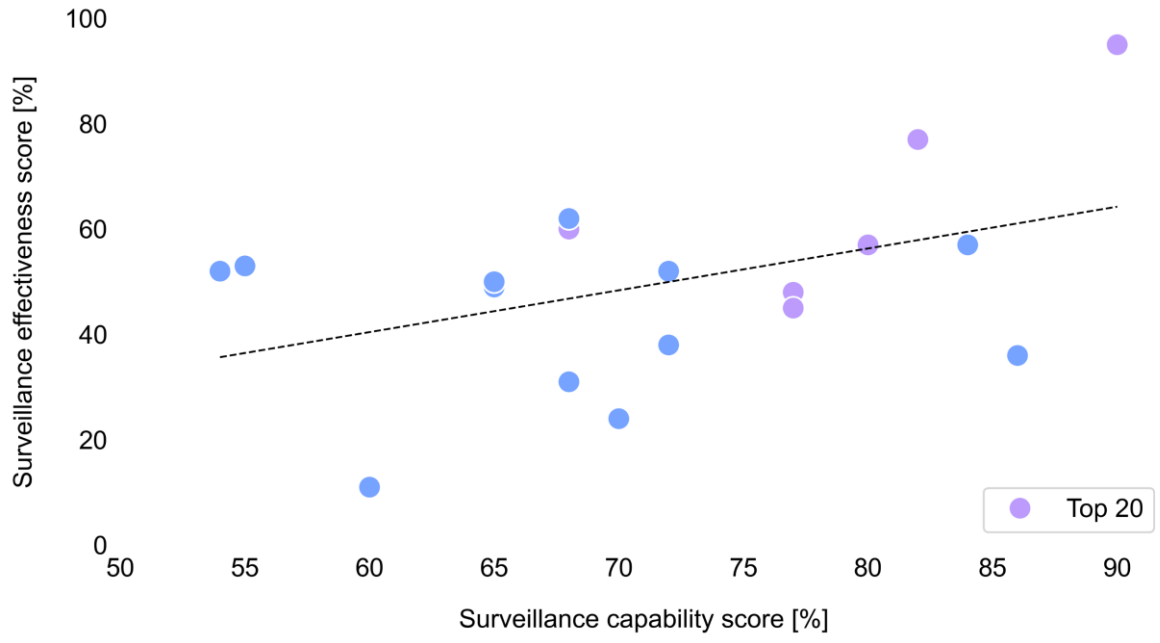
Table 6: Average score and STOR submission

PPAT type	Capability score	Effectiveness score
PPATs with 2 or more STORs (n=18)	71.8	49.8
All PPATs	69 (n=72)	24.6 (n=75)

As shown in Figure 39, there is a **positive correlation between capability and effectiveness, although the association is not very strong**.

Furthermore, PPATs that were in the top 20 in 2025 regarding volumes are marked on the graph. We can see that **high volume PPATs have on average a better score for both capability and effectiveness**, while the association between capability and effectiveness shows a pattern similar to that of the overall sample.

Figure 39: Interplay between capability and effectiveness



Note: n = 18

6. Recommendations

In summary, the survey and associated analyses provide insights into PPATs surveillance capability and effectiveness under REMIT, identifying strengths and areas for improvement. They highlight the need for continued development of surveillance systems, particularly IT tools optimisation. Based on the report results, ACER recommends the following to PPATs.

Arrangements

1. As also outlined last year, PPATs **should focus on ensuring the autonomy of the surveillance function**. Greater specialisation and professionalisation of staff, along with the use of appropriate tools to prevent potential conflicts of interest, can contribute to improving compliance. This recommendation is particularly relevant for approximately half of responding PPATs, that reported having the surveillance function embedded in other functions (e.g. market operations). At the same time, **this does not imply that the surveillance function should be isolated**; on the contrary, it should remain sufficiently well informed of all relevant developments and integrated in relevant processes, such as member onboarding or listing of new products.
2. The aforementioned autonomy also needs to extend to the **relationship between PPAT management and the surveillance function**. Survey results do indicate that surveillance staff are largely independent in terms of methods and tools used. A key aspect in this regard is the freedom to notify authorities. Almost 90% of PPATs reported that **PPAT management cannot influence or block notifications to NRAs/ACER**, it is essential to ensure that this independence is effectively applied in practice.
3. While there was a slight improvement compared to last year, PPAT **human resources policies need to progress further in protecting surveillance staff from potential conflicts of interest**.

Procedures

1. **The 'detect – analyse – notify – deter' procedures should be clearly defined and formalised**. Apart from four PPATs that declare having no surveillance procedures in place, all other responding PPATs confirmed that they have at least detection procedures in place and 90% of participating PPATs have fully formalised procedures covering three core components ("detect – analyse – notify"), while about 60% have procedures covering also deterrence. Clearly defined and formalised procedures facilitate market surveillance work.
2. The formalisation should be extended to **policies to deal with clients under suspicion**. The **communication between PPATs and market participants**, also in the scope of market surveillance, is a very important aspect. PPATs should **proactively contact market participants in case of suspicion or unclear circumstances**. 35% of respondents do not contact relevant clients at all. **Formalised KYC procedures, with periodic updates of data relating to clients, should be in place**. Furthermore, only 43% of PPATs issue educational communications or offer training courses to clients or members in relation to REMIT in general or REMIT breaches. This is also a critical area for potential development, particularly given its deterrent effect on market participants more broadly.
3. Although the survey-reported **detection and notification times** are largely in line with REMIT requirements, this is **in practice not reflected in actual STORs sent to ACER**. In other words, the number of PPATs that send STORs is much lower than the number of those that report notification times. While it is possible that suspicious behaviours are reported through other means, STOR notification should go through ACER's Notification Platform. The **emphasis should be on the time between the detection of the suspicious nature to its notification**, since the detection of the suspicious nature may require, in some cases, more prolonged, statistics-based information.

Systems:

1. About 8% of respondents reported having no system in place at all. **Not having systems in place constitutes a breach of REMIT**. As mentioned already in last year's report, the **use of professional and certified systems or advanced in-house solutions to detect and notify suspicious behaviour is encouraged, provided it is available for the specific needs of the PPAT**. General analytical tools may be insufficient to produce reliable surveillance coverage. A mixture of professional tools and tailor-made solutions is likely to achieve the best results in terms of surveillance capabilities. Based on some top-performer examples from among both PPATs and NRAs, another possible avenue is to build a sophisticated system in-house. Nevertheless, this also requires time and effort. It is expected that the evolution of systems goes hand in hand with other surveillance elements, in particular sufficient and well-trained staff.
2. The **coverage of existing surveillance systems needs to be expanded to cover all tradable products**. Only if this is achieved, manipulative behaviour across products or asset classes can be detected in a sufficiently reliable manner.
3. Regarding systems, surveillance functions at PPATs **need to be more independent from other departments within PPATs and from external providers**, to flexibly adjust alert parameters, and to uphold deterrence through the effective protection of surveillance methods and thresholds. Having advanced in-house developed systems means lower dependence on external contractors.

Assessment:

1. Breaches of Article 5, i.e. market manipulation, are reported to be detectable by more than 90% of all PPATs. Slightly lower is the ability to detect breaches of Article 3, which relates to insider trading, while one third of PPATs are completely unable to detect breaches of Article 4, which relates to inside information publication. Therefore, the **focus should be on expanding coverage to detection and notification as concerns Articles 3 and 4**.
2. 60% of PPATs report covering all markets, where they provide their services, at the same level in terms of market surveillance. Approximately a quarter of participating PPATs cover all markets, but at different levels, whereas 10% only cover some of the markets they operate in. **PPATs should strive to cover all markets (and relevant behaviours) at the same level**.
3. Despite the relatively solid reported detection-analysis-notification capacities, this does not seem to always translate into thorough and detailed STORs, which is part of the effectiveness assessment. This is also quite likely the reason for the somewhat loose statistical relationship between the assessed capability and the final effectiveness. **Effectiveness of all arrangements, systems and procedures should be the final aim of PPATs' activities under Article 15 of REMIT**.

Most of the above-mentioned recommendations seem to **overlap with the results of the self-evaluation concluded by the PPATs surveillance staff**: **IT systems and tools**, along with **staff training**, are the greatest concern in terms of their availability, flexibility and capability to deal with the very specific requirements of energy markets.

ACER again encourages all PPATs to verify their surveillance capabilities paying particular attention to the following cases, that **need to be avoided**:

- **no surveillance function in place** or not de facto in place;
- employees **not declaring potential conflicts of interest according to a well-defined procedure**;
- '**detect - analyse - notify - deter' procedures not defined and formalised**;
- **no surveillance system in place**;

- **PPAT management influencing content or blocking notifications** (STORs) to be shared with ACER and the responsible NRAs.

In general, all PPATs that identify the situations listed above, should take immediate action to address them.

Overall, the report provides a quantified overview of the state of **PPAT market surveillance, which plays an important role in guaranteeing that REMIT is applied across the EU**. PPATs are particularly well placed to perform this function for their specific markets, due to their deeper knowledge and insight into operated markets, including the market participants that participate in those markets. While structural compliance is likely improving, **sustained efforts are needed to reinforce and sustain this over time.**

Annex

This Annex contains further details on the scoring methodology, along with all the questions in the survey with added scores for possible answers. The scoring methodology might be further developed in future editions of the report.

Question number	Question text	Min score	Max score	Scoring	Score
***A1**	What is the full name of your entity/company?	0	0	Not scored	
***A2**	Please provide the full name and role of the person, responsible for filling out the questionnaire	0	0	Not scored	
***A3**	Please provide the e-mail contact of the person, responsible for filling out the questionnaire	0	0	Not scored	
***A4**	How many EU Member States are covered by the market you operate, in terms of delivery?	0	0	Not scored	
***A5**	Which type of person professionally arranging transactions (PPAT) are you?	0	0	Not scored	
***A6**	Do you arrange trading for electricity-related products?	0	0	Not scored	
A6a	Electricity - which products for which delivery area?	0	0	Not scored	

***A7**	Do you arrange trading for natural gas-related products?	0	0	Not scored	
A7a	Natural gas - which products for which delivery area?	0	0	Not scored	
***A8**	Do you arrange trading for some other product, beside electricity and / or natural gas?	0	0	Not scored	
***A9**	Do you arrange trading for some other delivery area, outside of the EU?	0	0	Not scored	
***A10**	How many years has the entity/company been active as an intermediary on the market?	0	0	Not scored	
***B1**	What is the governance structure of the surveillance function?	0	5	Five possible answers: - no surveillance function: 0 - outsourced: 5 - embedded within other functions: 3 - separate surveillance unit or similar: 5 - other: 1	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**
***B1a**	Any further comments on the governance structure of the surveillance function? - If the governance structure was "other", please describe - If “outsourced”, please explain whether to an affiliated company (same group) or other -	0	0	Not scored	

	If you offer surveillance as a service,				
***B1b**	Does the legal set-up guarantee that surveillance staff is carrying out their duties only with proper market functioning in mind?	0	5	Slider: - No - 1: 0 - 2: 2 - 3: 3 - 4: 4 - Yes - 5: 5	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**
***B1c**	Is surveillance staff exclusively working on surveillance tasks?	0	5	Two possible answers: - yes: 5 - no: 0	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**
B1c2	If surveillance staff are assigned to other tasks, is there a protocol or specific procedure in place to prevent conflicts of interest at the individual and/or the corporate level? Please briefly describe the tasks and the protocol, if there is one.	0	0	Not scored	
***B2**	To what degree can the company management interfere in the work of the surveillance function?	0	5	Slider: - Low - 1: 5 - 2: 4 - 3: 3 - 4: 2 - High - 5: 0	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**
***B3**	Can surveillance staff be relieved of their	0	5	Slider: - No - 1: 5	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**

	duties without their consent?			- 2: 4 - 3: 3 - 4: 2 - Yes - 5: 0	
*B4	Can surveillance staff choose methods for surveillance and thresholds for the detection work?	0	5	Slider: - No - 1: 0 - 2: 2 - 3: 3 - 4: 4 - Yes - 5: 5	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**
*B5	Is there sufficient budget available to fulfil monitoring tasks?	0	5	Slider: - No - 1: 0 - 2: 2 - 3: 3 - 4: 4 - Yes - 5: 5	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**
*B6	Is there sufficient qualified staff available to fulfil monitoring tasks?	0	5	Slider: - No - 1: 0 - 2: 2 - 3: 3 - 4: 4 - Yes - 5: 5	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**
*B7	What is the profile of the employees, working on market surveillance tasks?	0	5	Multiple choice answers: - no market surveillance: 0	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**

				- mostly technical (engineers, mathematicians, quantitative analysis etc.): 4 - mostly legal / economists: 3 - mixed: 5	
***B8**	Are Monitoring/Surveillance Team members given appropriate training (e.g. 5 days p.a.; in-house or outside trainings, conferences and similar) and guidance on REMIT and the practical considerations for the application of Article 15 of REMIT?	0	5	Slider: - No - 1: 0 - 2: 2 - 3: 3 - 4: 4 - Yes - 5: 5	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**
B8a	Please briefly describe further the level or education / training as well as arrangements for training Surveillance staff	0	0	Not scored	
***B9**	Are employees declaring potential interests that they may have in companies active in the wholesale energy markets (e.g. shareholdings, close family relationships …) or other potential conflicts of interest?	0	5	Two possible answers: - yes: 5 - no: 0	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**
***B10**	Are there compliance officers employed at the company (PPAT)?	0	5	Two possible answers: - yes: 5 - no: 0	**SURVEILLANCE CAPABILITY SCORE - ARRANGEMENTS**

***C1**	Relating to the 'detect - analyse - notify – deter' principle, for which parts are procedures defined and formalised?	0	5	Multiple choice answers: - 0 procedures: 0 - 1 procedure: 1 - 2 procedures: 2 - 3 procedures: 3 - 4 procedures: 5	**SURVEILLANCE CAPABILITY SCORE - PROCEDURES**
C1a	Do you have any additional comments regarding the formal definition of 'detect - analyse - notify – deter' procedures?	0	0	Not scored	
***C2**	Is the notification procedure for STORs (suspicious transactions and orders reports) defined / formalised?	0	5	Two possible answers: - yes: 5 - no: 0	**SURVEILLANCE CAPABILITY SCORE - PROCEDURES**
C2a	How is the notification procedure for STORs formalised?	0	0	Not scored	
***C3**	From your past experience, what is your estimate (in weeks) of the average time elapsed between the OCCURENCE of the event (i.e. trading day) and the detection of its SUSPICIOUS nature (i.e. establishing that this event should be looked at more closely)?	0	5	Written answer (answers rounded to integers): - 1 week: 5 - 2 weeks: 4 - 3 weeks: 3 - 4 weeks: 2 - 5 weeks: 1 - more than 5 weeks: 0	**SURVEILLANCE CAPABILITY SCORE - PROCEDURES**
***C4**	From your past experience, what is your estimate (in weeks) of the average	0	5	Written answer (answers rounded to integers):	**SURVEILLANCE CAPABILITY SCORE - PROCEDURES**

	time elapsed between the ESTABLISHMENT OF THE SUSPICIOUS nature of an event (i.e. establishing that this event should be looked at more closely) and the NOTIFICATION TIME (i.e. when the notification is sent to ACER / NRAs)?			- 1 week: 5 - 2 weeks: 4 - 3 weeks: 3 - 4 weeks: 2 - 5 weeks: 1 - more than 5 weeks: 0	
***C5**	Is surveillance assessment part of relevant company internal procedures, such as onboarding or the release of new tradable products?	0	5	Two possible answers: - yes: 5 - no: 0	**SURVEILLANCE CAPABILITY SCORE - PROCEDURES**
***C6**	Has the surveillance setup ever been audited (e.g. also in the context of a general company audit)?	0	5	Three possible answers: - yes – specific for surveillance: 5 - yes – in a wider company audit context: 3 - no: 0	**SURVEILLANCE CAPABILITY SCORE - PROCEDURES**
***C7**	Do you have a policy in place that defines how to engage with clients under suspicion?	0	5	Two possible answers: - yes: 5 - no: 0	**SURVEILLANCE CAPABILITY SCORE - PROCEDURES**
***C8**	Can the company management influence or block notifications (STORs) to be shared with ACER and the responsible NRAs (e.g. by requiring that the management needs to formally approve the STOR before it is sent)?	0	5	Two possible answers: - yes: 0 - no: 5	**SURVEILLANCE CAPABILITY SCORE - PROCEDURES**
C9	Do you have any further comments on	0	0	Not scored	

	the influence of company management on notification procedures (or the reason for absence thereof)?				
***C10**	Does the surveillance team have adequate procedures and systems in place that restrict the access to confidential information and its know-how?	0	5	Two possible answers: - yes: 5 - no: 0	**SURVEILLANCE CAPABILITY SCORE – PROCEDURES**
C11	How do you assure data security, non-proliferation of sensitive information and segregation from commercial interests?	0	0	Not scored	
***C12**	Do you have a "know your customer" (KYC) procedure formalised within your company to admit members / clients?	0	3	Three possible answers: - no: 0 - KYC done, but not formalised: 1 - yes: 3	**SURVEILLANCE EFFECTIVENESS SCORE – DIRECT INQUIRES**
***C13**	Which potential risks does the KYC procedure cover before onboarding a new client / member?	0	3	Three possible answers: - no KYC: 0 - just financial and credit risks: 1 - financial and credit risks, but also REMIT related risks: 3	**SURVEILLANCE EFFECTIVENESS SCORE – DIRECT INQUIRES**
***C14**	Is KYC performed just before onboarding or also followed-up with updated data, after the client/member has already been active for some time?	0	3	Four possible answers: - no KYC: 0 - just before onboarding (1): 1 - before onboarding but also followed-up: 2	**SURVEILLANCE EFFECTIVENESS SCORE – DIRECT INQUIRES**

				- regularly updated and used for benchmarking when assessing potentially manipulative behaviour: 3	
***C14a**	Do you issue educational communications or offer training courses to clients/members in relation to REMIT in general and/or REMIT breaches?	0	3	Four possible answers: - No: 0 - Communications: 1 - Trainings: 2 - Both: 3	**SURVEILLANCE EFFECTIVENESS SCORE – DIRECT INQUIRES**
***C15**	In case of REMIT-related suspicions, do you contact the relevant client/member in a traceable manner (e. g. formal mail or email) in order to obtain explanations / clarifications?	0	3	Three possible answers: - no: 0 - yes - only informally, via phone: 1 - yes - formalised and traceable: 3	**SURVEILLANCE EFFECTIVENESS SCORE – DIRECT INQUIRES**
***C16**	Have you directly contacted your client / member within the past 12 months in order to obtain clarifications / information, regarding a potential REMIT breach?	0	3	Three possible answers: - no: 0 - yes, but only once or twice: 1 - yes, several times: 3	**SURVEILLANCE EFFECTIVENESS SCORE – DIRECT INQUIRES**
***C17**	Do you have a formalised procedure in case your client does not respond to your clarification request?	0	3	Two possible answers: - yes: 3 - no: 0	**SURVEILLANCE EFFECTIVENESS SCORE – DIRECT INQUIRES**
C18	Was a participant removed from your market or a client terminated in the past 3 years?	0	0	Not scored	

***D1**	Is there a surveillance software system in place in order to detect suspicious orders and transactions?	0	5	Slider: - No - 1: 0 - 2: 2 - 3: 3 - 4: 4 - Yes - 5: 5	**SURVEILLANCE CAPABILITY SCORE - SYSTEMS**
***D2**	Which systems does surveillance work MOSTLY rely on?	0	5	Five possible answers: - professional surveillance tools: 5 - in-house advanced tailormade IT solutions: 4 - in-house basic tailormade IT solutions: 3 - general analytical tools, such as MS Office: 2 - no systems in place: 0	**SURVEILLANCE CAPABILITY SCORE - SYSTEMS**
***D3**	Can surveillance systems parameters usually be changed by surveillance staff or does it need the involvement of others (internal/external)?	0	5	Five possible answers: - surveillance staff alone: 5 - surveillance staff and other internal staff: 4 - external staff needed: 3 - not relevant – activity outsourced: 1 - not relevant – no such systems in place: 0	**SURVEILLANCE CAPABILITY SCORE - SYSTEMS**
D3a	Please briefly describe how surveillance	0	0	Not scored	

	systems' parameter values are set and their values changed. Is the change statistically motivated?				
***D4**	Are surveillance systems / procedures / information security certified through ISO or similar standards?	0	5	Two possible answers: - yes: 5 - no: 0	**SURVEILLANCE CAPABILITY SCORE - SYSTEMS**
***D5**	Which markets are covered by the professional surveillance system (and tailor-made IT solutions)?	0	5	Three possible answers: - all operated markets: 5 - part of operated markets: 3 - no such system in place: 0	**SURVEILLANCE CAPABILITY SCORE - SYSTEMS**
***D6**	How does the surveillance system work in general?	0	5	Multiple choice with five possible answers – points sum up: - looks for a specific behaviour pattern and produces "alerts": 2 - looks for large changes (outliers), followed up by analysis (without specific pre-programmed behaviour): 1 - allows quick access to information of product or client or trading session (data aggregation): 1 - allows quick access to information of product or client or trading session by visualisation: 1 - no such system in place: 0	**SURVEILLANCE CAPABILITY SCORE - SYSTEMS**
***E1**	Which potential REMIT breaches are you able to detect on your markets?	0	6	For every REMIT article (3,4,5) – 1 point if yes, but no systems in place and 2 points if yes, with systems in place	**SURVEILLANCE CAPABILITY SCORE - ASSESSMENT**
***E2**	How does market surveillance cover	0	5	Single choice: - No market surveillance in place: 0	**SURVEILLANCE CAPABILITY SCORE - ASSESSMENT**

	different markets, you operate?			- Only some markets covered: 1 - All markets covered, but at different levels: 3 - All markets covered at same level: 5	
E2a	Please explain, which markets are not covered or are covered at a lower level	0	0	Not scored	
E3	What is your capacity to detect market manipulation by behaviour type?	0	0	Not scored	
***E4**	Which elements would you like to improve in your surveillance set-up?	0	0	Not scored	
E4a	Do you have any further comments on possible improvements of surveillance elements? If you selected "other", please briefly explain.	0	0	Not scored	
***E5**	Which surveillance conditions would you like to improve in your case?	0	0	Not scored	
F1	Do you have any further comments on possible improvements of surveillance conditions / capabilities?	0	0	Not scored	
F2	Do you have any other comments / clarifications regarding this survey?	0	0	Not scored	

Survey questions labelled with * were mandatory. The survey invitation was sent to the following entities (in alphabetical order), excluding DEA providers, identified by ACER and the NRAs as PPAT or potential PPATs:

AB Amber Grid, AGCS Gas Clearing and Settlement AG, Amprion GmbH (Amprion), AS Augstsprieguma tīkls, Aurel BGC SAS, Austrian Power Grid AG (APG), Balkan Gas Hub EAD, BBL Company V.O.F., BGC BROKERS L.P., BioEx, Braemar Securities Limited, BritNed, BSP d.o.o., Bulgarian Energy Trading Platform AD (BETP AD), BURSA ROMANA DE MARFURI SA ROMANIAN COMMODITIES EXCHANGE, C.N. Transelectrica S.A. (Transelectrica), Cavendish Energy Markets LTD, Cavendish Markets B.V., CEEGEX Ltd., ČEPS a.s. (ČEPS), CME Europe Limited, Coordinated Auction Office in South East Europe, Corretaje e Información Monetaria y de Divisas Sociedad de Valores SOCIEDAD ANONIMA, CIMD SV (OTF), Creos Luxembourg S.A., Croatian Power Exchange Ltd., Cyprus Transmission System Operator (Cyprus TSO), Deutsche Boerse AG, EirGrid plc (EIRGRID), Electroenergien Sistemen Operator EAD (ESO), Elering AS, ELES, d.o.o., Elia System Operator SA (ELIA), Enagás GTS, EnCoHub OTC Marketplace, Energinet, ENGNSOL SAS, Enmacc GmbH, Enterprise Commodity Services Limited, EPEX SPOT SE, ETPA B.V., Euronext Amsterdam N.V., European Energy Exchange AG, eustream, a.s., Evolution Markets Limited, EXAA Abwicklungsstelle für Energieprodukte AG, FGSZ Földgázszállító Zártkörűen Működő Részvénytársaság, FGSZ Kereskedési Platform Kft, Fingrid Oyj (Fingrid), Fluxys Belgium S.A., Gas Networks Ireland, Gasgrid Finland Oy, Gasunie Transport Services B.V., GAZ-SYSTEM S.A., Gestore dei mercati energetici SpA (GME), GFI EU, a trading name of Aurel BGC, GFI Securities Ltd, GMG Europe BV, GNI UK, Griffin Markets Europe SAS, Hellenic Gas Transmision System Operator S.A. (DEFSA), HENEX SA, HOPS d.o.o. (HOPS), HROTE, Hungarian Derivatives Energy Exchange, HUPX Ltd., ICAP Energy AS, ICAP Energy Limited, ICAP Energy LLC, ICE Endex Gas Spot Ltd., ICE Endex Markets BV, ICE Futures Europe, ICGB AD, Independent Bulgarian Energy Exchange (IBEX), Independent Power Transmission Operator S.A.(IPTO), Interconnector (UK) Limited, JAO, JSC Conexus Baltic Grid, Litgrid AB, Marex SA, Marex Spectron Europe Limited, MAVIR Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság (MAVIR), MIBGAS DERIVATIVES S.A., MIBGAS, S.A., N2EX/Nord Pool Spot AS, Nasdaq OMX Oslo ASA, Nasdaq Stockholm AB, NET4GAS, s.r.o., New York Mercantile Exchange, Inc. (NYMEX), Nord Pool AS, OB Group Energy Limited, OKTE, a.s., OMIP - Pólo Português, S.G.M.R., S.A., OMI-Polo Español S.A. (OMIE), OPERATORUL PIETEI DE ENERGIE ELECTRICA SI DE GAZE NATURALE “OPCOM” SA, OTE, a.s., Plinacro, Plinovodi, d.o.o., Polskie Sieci Elektroenergetyczne S.A. (PSE S.A.), Power Deriva Oy, Power Exchange Central Europe, PXE a.s., Power Sprinter GmbH, Premier Transmission Limited, PRISMA European Capacity Platform GmbH, PVM Oil Futures Ltd, Red Eléctrica de España S.A. (REE), Rede Eléctrica Nacional, S.A. (REN), REN - Gasodutos, S.A., RENTA4 BANCO, Réseau de Transport d'Electricité (RTE), SEMOpx, Shard Capital Partners LLP, Single Electricity Market Operator, SEMO, Slovenská elektrizačná prenosová sústava, a.s. (SEPS), SPX, s.r.o., Storengy, SVENSK KRAFTMÄKLING AB, Svenska Kraftnät, Swedegas AB, System Operator for Northern Ireland Ltd (SONI), TenneT TSO B.V. (TenneT NL), TenneT TSO GmbH (TenneT DE), TERÉGA, Terna - Rete Elettrica Nazionale SpA (Terna), Towarowa Giełda Energii S.A., TP Icap (Europe) S.A, TP ICAP E&C Limited, Tradition Financial Services Espana Sociedad De Valores SA, Tradition Financial Services Ltd, TRANSGAZ S.A., TransnetBW GmbH (TransnetBW), Trayport, TSAF OTC, Tullett Prebon Americas Corp., UAB GET Baltic, 42 Financial Services, 50Hertz Transmission GmbH (50Herz)