ACER

European Union Agency for the Cooperation of Energy Regulators



Guidance for IIPs and RRMs under REMIT Delegated Regulation (EU) 2026/255

Version 1.0

27 November 2026

Guidance for IIPs and RRMs under REMIT Delegated Regulation (EU) 2026/255

Version 1.0

27 November 2026

Please note that the present version of the Guidance for IIPs and RRMs under Commission Delegated Regulation (EU) 2026/255 provides guidance on the technical and procedural aspects specified in Article 9 of that regulation, with a view to facilitating compliance with the requirements applicable to IIPs and RRMs from 29 October 2027.

Find us at:

ACER

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

www.acer.europa.eu



© European Union Agency for the Cooperation of Energy Regulators
Reproduction is authorised provided the source is acknowledged.

Contents

1. Scope and purpose of the document 5
2. The application for authorisation 7
2.1. Transitional arrangements for already registered IIPs and RRMs 7
2.2. Principles of authorisation 7
2.3. When to apply for authorisation? 8
2.4. Authorisation process step-by-step 9
2.5. Material changes after authorisation 13
3. Testing phase 14
3.1. Reporting coverage and technical set-up 14
3.2. Connectivity, upload/download and validation 14
3.3. Success criteria and repetition of testing 15
3.4. Changes introduced after the authorisation that require testing 16
3.5. Testing process for already registered RRMs during the authorisation process 16
3.6. Testing process for already registered IIPs during the authorisation process 17
4. Security measures 18
4.1. Confidentiality 19
4.2. Integrity 22
4.3. Availability 24
4.4. Access control 26
4.5. Authenticity 28
4.6. Accountability 30
4.7. Reliability 32
5. Data validation and submission processes 35
5.1. Data integrity 36
5.2. Validity and consistency 36
5.3. Uniqueness 37
5.4. Reconciliation 38
5.5. Authentication 38
5.6. Timeliness 38
5.7. Traceability 39
5.8. Transparency 39
5.9. Pre-submission process 39
5.10. Register of invalid data 40
5.11. Post-submission processes 41
5.12. Client notification mechanisms and communication requirements 42
6. The flagging process for IIPs 43
6.1. Display of flags on the IIP website 44
7. Unplanned downtime or disruption 45

7.1. Disruption to the submission 46
7.2. Disruptions to the collection 46
7.3. Disruptions to the data quality 47
7.4. Security incident notification 47
7.5. Operational disruptions of the IIP's/RRM's systems 47
8. Annual report by RRMs 49
8.1. Timing and frequency 49
8.2. Content of the annual report 50
Annex I – Supporting documents as per Article 4 52
Annex II – Authorisation process workflow 54
Annex III – Operational guidance for security measures 56
Annex IV – Disruption report cardinality table 63
Annex V – REMIT validation rules document 65

1. Scope and purpose of the document

This document provides guidance pursuant to Article 9 of Commission Delegated Regulation (EU) 2026/255 of 30 January 2026 supplementing Regulation (EU) No 1227/2011 of the European Parliament and of the Council as regards the necessary details for the authorisation and supervision of inside information platforms and registered reporting mechanisms by the European Union Agency for the Cooperation of Energy Regulators (also referred to as the 'Delegated Regulation for the authorisation and supervision of IIPs and RRMs').

In accordance with Article 9 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, the European Union Agency for the Cooperation of Energy Regulators (ACER) is required to publish guidance by seven months from the entry into force of the regulation, following consultation with relevant stakeholders. The guidance covers the following key areas.

- Testing (Article 5(1))
- Application process (Article 8(1))
- Data validation (Article 12(1),(2))
- Security measures (Article 13(1)(d))
- Downtime and disruption reporting (Article 18(3))
- Flagging (Article 24(4))
- Data quality checks (Articles 23(1) and 27(1))
- Annual reporting (Article 33(1))

Table 1 below provides a high-level overview of the topics covered in this guidance, what they address, their relevance to different stakeholders, and when they apply. This guidance is primarily intended for entities which want to obtain the authorisation to provide registered reporting mechanism ('RRM') services or inside information platform ('IIP') services, and for already registered IIPs and RRMs.

Table 1: Overview of the guidance for IIPs and RRMs

Chapter	When is it relevant?	Who?	What is it about?	Relevant chapter
Application process	Authorisation	IIPs and RRMs	Applying for authorisation	2
Testing phase	Authorisation/ operations	IIPs and RRMs	Demonstrating ability to report/disclose	3
Security measures	Authorisation/ operations	IIPs and RRMs	Implementing security measures	4
Data validation and submission process	Authorisation/ operations	IIPs and RRMs	Setting up / operating validation systems and detecting issues before submission/publication	5
Flagging	Operations	IIPs	Flagging relevant information	6
Unplanned downtime or disruption	Operations, for incidents	IIPs and RRMs	Reporting disruptions to ACER	7
Annual reporting	Operations, annually	RRMs	Preparing the annual report	8

This guidance should be read in conjunction with the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, which sets out the relevant legal framework. Where a requirement or process is not further detailed in this guidance, the relevant provisions of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs are deemed to sufficiently cover the applicable requirements and procedural details and should thus be consulted directly.

Other requirements and processes established by the Delegated Regulation for the authorisation and supervision of IIPs and RRMs that are not specifically addressed by the mandate in Article 9, and as such are not further detailed in this guidance, include:

- the general application and authorisation of requirements and procedures;
- organisational and operational requirements not specifically referred to in Article 9;
- security incident management and notification;
- supervision and compliance processes;
- substantive annual reporting obligations beyond the prescribed format; and
- the procedures for the withdrawal of authorisation and orderly substitution, including related notifications and the involvement of national regulatory authorities (NRAs).

These matters may be referred to in this guidance where relevant for context or for the application of the matters covered by Article 9. Their applicable requirements and procedural details are set out in the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.

2. The application for authorisation

2.1. Transitional arrangements for already registered IIPs and RRMs

Pursuant to Article 9a(1) of Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency ('REMIT Regulation'), RRMs registered by ACER pursuant to Commission Implementing Regulation (EU) No 1348/2014 and included in ACER's list of RRMs ('already registered RRM') will be allowed to continue operating until ACER has taken a decision on their authorisation. The same approach applies to IIPs, as Article 4a(2) of Regulation (EU) No 1227/2011 states that IIPs registered by ACER pursuant to Commission Implementing Regulation (EU) No 1348/2014 and included in ACER's list of IIPs ('already registered IIP') will be allowed to continue operating until ACER has taken a decision on their authorisation.

> **Scenario.** An already registered IIP/RRM applies for the authorisation in March 2028; ACER confirms the completeness of the application in April 2028 and issues a positive authorisation decision in June 2028.
>
> **Explanation.** The IIP/RRM remains registered and can report until the decision is issued [June 2028] under its existing registration and by using the new electronic formats applicable at that time. As per the authorisation decision, the IIP/RRM is authorised and remains eligible to report data.

In the event of a decision to reject the authorisation (negative decision), the Delegated Regulation for the authorisation and supervision of IIPs and RRMs does not lay down a procedure for the orderly substitution of already registered IIPs or RRMs; such procedure is applicable only in relation to withdrawal of authorisation for the IIPs and RRMs.

However, in order to maintain consistency with Articles 9a(5) and 4a(7) of the REMIT Regulation, to ensure a smooth handover to new service providers and prevent disruptions to data reporting, ACER may consider it reasonable to allow already registered IIPs/RRMs that receive a negative decision to continue operations for at least six months following notification of the negative decision, or for a shorter period, if this compromises the ACER REMIT information system's (ARIS) stability[1]. Upon expiry of this period, ACER will remove the IIP or RRM concerned from the respective public list of registered RRMs or IIPs.

Already registered IIPs and RRMs that do not wish to apply for authorisation should notify ACER by having their RRM administrator complete the RRM registration termination form and follow the instructions provided therein. Such entities must also inform the market participants concerned without undue delay.

Already registered IIPs and RRMs that do not submit their applications for authorisation or the RRM registration termination form before 29 April 2028 will have their registrations terminated by ACER.

2.2. Principles of authorisation

The provision of Article 8(2) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs specifies that already registered IIPs and RRMs must provide ACER with the information referred to in Articles 3 to 7 of that Regulation, unless it was already provided in the framework of the registration process under Commission Implementing Regulation (EU) No 1348/2014.

Hence, the Delegated Regulation for the authorisation and supervision of IIPs and RRMs provides for a simplified authorisation process for the already registered IIPs and RRMs, as these entities are not required to provide information already submitted, insofar as such information conforms with the

[1] Already registered RRMs or IIPs that receive a negative decision on the authorisation will need to manage the transition according to the contractual arrangements with their respective clients.

requirements as laid down under Articles 3 to 7 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.

However, ACER may still request the resubmission of documentation already provided during the registration process, if necessary, to ensure compatibility with its IT systems, particularly in cases where technical updates are required.

ACER will automatically make existing information, documentation and any account-related settings and requirements used for the registration available for the application for authorisation. IIPs and RRMs can access their information and documentation at any time through the online authorisation tool and can update their information as needed. ACER will publish up-to-date information on the authorisation status of registered IIPs and RRMs, clearly indicating which entities are authorised and which are not.

Furthermore, simplified testing phase may apply to already registered RRMs. For further details, refer to Chapter 3 below.

The REMIT fees are charged as per Commission Decision (EU) 2025/1771, which has been in force since September 2025. The authorisation does not imply any additional fees for the RRMs already registered and that have paid the applicable REMIT fees for the year in which the authorisation is adopted.

The REMIT fees applicable to IIPs will be charged during the authorisation process, in accordance with Commission Decision (EU) 2025/1771.

2.3. When to apply for authorisation?

Article 8 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs establishes a process for the authorisation of already registered IIPs and RRMs. It applies to IIPs and RRMs that are already operating and registered with ACER, whether they are established inside or outside the EU, and requires them to undergo the new authorisation process, even if they were registered under the previous framework (according to Commission Implementing Regulation (EU) 1348/2014).

Article 8(1) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs establishes that already registered IIPs and RRMs are required to apply for an authorisation from ACER before 29 April 2028 (i.e. by 28 April 2028), following the requirements for authorisation set out in Articles 3 to 7 of the same regulation.

Accordingly, already registered IIPs and RRMs can submit their applications during a six-month period, from 29 October 2027 to 28 April 2028. During this six-month application window, already registered IIPs and RRMs are required to submit complete applications demonstrating compliance with all requirements specified in Articles 3 to 7[2] of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. Applications must be submitted electronically through ACER's online authorisation tool. Access to the tool will be made available on ACER's website before the opening of the application window.

The six-month period serves exclusively as the window for submitting authorisation applications by already registered IIPs and RRMs. For new applicants, there is no deadline, and they may apply for authorisation at any time from 29 October 2027 onwards[3]. For a better overview, please refer to Table 2 below.

[2] For further details on the step-by-step authorisation, please refer to Section 2.4 of this guidance.
[3] Further details are available in ACER's 'Open Letter on the implications of Commission Delegated Regulation (EU) 2026/255', 9 April 2026.

Table 2: Authorisation application timelines for IIPs and RRMs

Applicant type	When can they apply?	Application deadline	What does this mean?
Already registered IIPs/RRMs	During the **six-month application window (29 October 2027-28 April 2028)**	**28 April 2028**	This six-month period is the exclusive window for submitting their authorisation application.
New IIP/RRMIIP/RRM applicants	**From 29 October 2027 onwards**	**No deadline**	They may submit an application for authorisation at any time from this date onwards.

2.4. Authorisation process step-by-step

The authorisation process consists of two stages each comprising specific steps.

- **Stage 1.** Application submission by an IIP or RRM
- **Stage 2.** Assessment and decision by ACER

The submission of the complete application by the already registered IIP or RRM triggers the transition from Stage 1 (Application and submission) to Stage 2 (Assessment and decision).

For new applicants, the application and submission stage is expected to take approximately at least three to six months. For already registered IIPs and RRMs, this period is expected to be shorter, depending on the completeness and accuracy of the information already available to ACER and the extent to which it needs to be updated or supplemented.

Applicants may submit their applications and supporting documentation in any official language of the EU, in accordance with Article 44(1) of Regulation (EU) 2019/942. However, as English is ACER's internal working language, applicants are strongly encouraged to submit their documentation in English. Documents submitted in other official EU languages may require additional time for translation and, consequently, prolong the application assessment process.

Once ACER notifies the applicant that the application is complete, it has three months to issue a decision. Where more time is needed to adopt a decision, this period may be extended by up to two additional months.

The authorisation process is illustrated through workflow diagrams in Annex II to this document. Annex II provides step-by-step visual representations of the entire application journey for each entity type – IIPs and RRMs. Annex II also outlines the specific steps to be taken by already registered IIPs and RRMs.

1. Application submission stage

ACER will make available an online authorisation tool to enable applicants to prepare and submit their applications. A link to access the tool will be published on ACER's website before 29 October 2027.

For already registered RRMs, the tool will include the information submitted by the RRM applicant during the registration process[4], together with dedicated fields for any additional information required according to the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.

Already registered IIPs will be granted secure access to the ARIS test environment sufficiently in advance of the start of the authorisation process to allow them to verify the necessary technical set-up and familiarise themselves with the environment, ensuring they are ready to begin the authorisation process when it opens.

[4] This includes admin and user accounts, relevant certificates and virtual private network (VPN) connection, identification information, schema and interface selections and supporting documentation.

The application should include the following.

a. Identification and legal status of the applicant and access to ACER's data exchange systems as per Article 3 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs:

- the legal name and address of the applicant (for already registered RRMs the information will be sourced from the original registration, and applicants are asked to verify the original information before submitting their application);
- proof of the applicant's establishment in the European Union[5] (already registered IIP and RRMs will need to apply for authorisation and prove that they are established in the EU);
- legal entity form, including an excerpt from the relevant commercial or court register in the EU, or other forms of certified evidence of the place of incorporation, scope of business activity and the applicant's value added tax (VAT) identification number in the EU, valid on the application date (VAT certificate) (for already registered RRMs the information will be sourced from the original registration, and applicants are asked to verify the original information before submitting their application);
- the name and business contact details of the persons responsible for (i) compliance, and (ii) communication with ACER and with IIP clients and RRM clients (for already registered RRMs the information will be sourced from the original registration, and applicants are asked to verify the original information before submitting their application);
- the planned starting date for operating the IIP platform (not required for already registered IIPs);
- the planned starting date for the reporting of data records (not required for already registered RRMs).

b. Supporting documents as per Article 4 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs

The supporting documents must demonstrate compliance with the general organisational requirements for IIPs and RRMs set out in Articles 11 to 18 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, the specific requirements for IIPs laid down in Articles 19 to 25 or for RRMs laid down in Articles 26 to 29, as applicable, and the requirements for orderly substitution under Article 38. ACER will provide a template to applicants to support consistent and harmonised applications for authorisation. The completed template must be signed and uploaded to the online authorisation tool as part of the application. The template will be published on ACER's website before 29 October 2027.

Already registered RRMs can refer to Annex I to this guidance document, which provides an overview of supporting documents and indicates whether these requirements also existed for the RRM registration process under Commission Implementing Regulation (EU) 1348/2014. This overview assists already registered RRMs in mapping the requirements they needed to demonstrate during registration (as outlined in the RRM requirements document) against the new and enhanced requirements introduced by the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.

Already registered RRMs are required to complete the supporting documents template for all requirements set out in Article 4 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.

Where a requirement has already been addressed in documentation submitted during the initial registration process, RRMs may refer to that documentation by indicating only the name of the previously submitted document and the specific section in which the relevant requirement is addressed. In such cases, resubmission of the same information is not necessary.

In contrast, due to the nature of IIP registration and future data collection under Commission Implementing Regulation (EU) 2026/256 ('REMIT Implementing Regulation'), it is not feasible to provide the same overview as for RRMs. During the registration phase, IIPs were not required to submit attestation documents, making it impossible to reuse this information.

[5] The substantial activities of the IIP/RRM must be carried out in a Member State of the European Union on a stable and continuous basis.

Consequently, IIPs must complete the template to attest to their compliance with the requirements for the authorisation and supervision of IIPs and RRMs, and requirement mapping cannot be applied in their case.

Additionally, as per Article 4(5) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, IIPs and RRMs may demonstrate compliance with any of the requirements referred to in Article 4(2), (3 – the organisational chart of the IIP or RRM) and (4 – the programme of operations) through submission to ACER of a valid ISO/IEC 27000 standard series certificate on information security management systems or equivalent certifications.

ACER may ask the applicants for further clarifications regarding the certification provided, any missing information to demonstrate compliance with the requirements referred to in paragraphs 2, 3 and 4 and for an update of such certification after its expiration date.

Where such certification is relied upon, applicants must provide the valid ISO certificate, including the:

- certificate number;
- certification body;
- certification scope;
- date of issue; and
- validity/expiry date.

Applicants must also describe in the template which aspects relevant to the requirements of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs are covered by their ISO certification scope. Furthermore, in case of services being outsourced, applicants must provide supporting evidence for third-party service providers' adherence to the Delegated Regulation for the authorisation and supervision of IIPs and RRMs and, if applicable, the service providers' ISO 27001 certification. For an overview of which requirements under Article 4 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs are covered by the relevant ISO 27001 certification, please refer to Annex I to this document.

c. Testing phase as per Article 5 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs

The testing phase is a mandatory part of the application process and needs to be completed for an application to be considered complete.

To configure the testing phase, applicants must specify the types of data records they intend to report (for RRMs) or the inside information reports they intend to publish (for IIPs), selecting from ACER's predefined lists, as indicated in Annex V to this document. IIPs and RRMs must also identify the standard electronic formats they intend to use for reporting as established pursuant to Article 13(4) of the REMIT Implementing Regulation.

Applicants are required to demonstrate their systems' ability to report data through selected interfaces, ensuring full compliance with ACER's REMIT validation rules document, which defines the rules and their applicable date (please refer to Chapter 5 and Annex V). ACER will evaluate test results in the ARIS environment, assessing factors such as system performance and data accuracy.

The testing phase ensures that applicants demonstrate their readiness for operational reporting and that they can maintain consistent data quality standards.

Already registered IIPs and RRMs are exempt from further testing during the authorisation process, provided they have previously demonstrated their capability to correctly report their selected data types in the latest version of the electronic format through their chosen interfaces and where applicable, completed test cases for defined data types as detailed in Section 3.2. Previously performed tests will be considered during the authorisation process. The ability to correctly report and validate the selected data types in the latest version of the electronic format before the authorisation that commences on 29 October 2027 depends on both the RRM and IIP capability and the readiness of ACER's environments.

In cases where additional testing is required (e.g. if an IIP or RRM wishes to add a new data type to their selection or when they have not previously tested a data type in the correct electronic format), the testing will be limited to data types / electronic format versions that have not been tested before.

For more details about the testing process, please refer to Chapter 3 below regarding the testing phase.

After completing the three steps described at points a. to c. above, applicants can submit their application through the online authorisation tool.

Already registered IIPs and RRMs should apply by 28 April 2028 to ensure continuity of their existing registration until ACER takes a decision on the authorisation.

Upon submission, entities will receive a confirmation email to acknowledge that their application has been received by ACER.

2. Assessment stage

a. Completeness check

As set out in Article 10 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, an application is considered complete when ACER has received all the information required under Articles 3 to 7 of the same Regulation. Once ACER deems the application complete, it will notify the applicant (via email) without undue delay.

At this stage, ACER performs a preliminary review of the application to verify that all required fields have been completed and all required documents and information have been submitted. ACER also reviews the testing results submitted by the applicant. If the testing has not been successfully completed, the applicant will be required to repeat the relevant tests. At this stage, ACER does not conduct an assessment on compliance with the requirements set out in Articles 11 to 29 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, along with the relevant requirements of the REMIT Regulation.

Where ACER finds that an application is incomplete, it will, in accordance with Article 8(3) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, notify the IIP or RRM applicant via email, specify the additional information required for the application to be considered complete, and set a deadline for its submission.

Where an applicant fails to communicate or provide the required information within three months following the incompleteness notification, ACER may consider the application withdrawn. The same applies where the applicant fails to communicate or provide the necessary information/explanations for more than three months following a request for clarification from ACER. At least two weeks before the expiry of the three-month period, ACER will notify the applicant of its inactive status and remind it of the consequences thereof.

Once the application is deemed complete, the IIP or RRM applicant will be notified via email, and ACER will proceed with the assessment. While the Delegated Regulation for the authorisation and supervision of IIPs and RRMs does not establish a specific deadline for ACER to perform the completeness check, ACER aims to perform this within six weeks from the date when the application was submitted. This indicative timeline may vary, depending on the quality of the application and the number of applications being processed concurrently.

b. Adoption of the decision on the authorisation

After the application is deemed complete, ACER assesses whether the applicant meets the requirements set out in Articles 3 to 7 and 11 to 29 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, along with the relevant requirements of the REMIT Regulation.

ACER must adopt a decision to grant or reject the authorisation within three months from the date of notification that the application is complete. If additional time is required, ACER may, before the expiry of the three-month period, inform the applicant that the deadline has been extended. Such extension will not exceed two additional months. Where ACER has concluded

that the applicable requirements are fulfilled, the authorisation is granted. Where the requirements are not fulfilled, the application is rejected.

If ACER does not adopt a decision within that additional time period, it must be deemed to have granted the authorisation. The IIP or RRM applicant will be informed about the decision via email.

All decisions are subject to procedural safeguards, including the right of applicants to receive reasons for a decision, present their views and challenge the decision. Applicants may appeal the agency's decision before the ACER Board of Appeal in accordance with Article 28 of Regulation (EU) 2019/942; following the conclusion of the appeal procedure, the decision may be challenged before the Court of Justice of the European Union in accordance with Article 29 of the same Regulation.

c. Notification of the decision on the authorisation

The decision will be notified to the applicant and the relevant NRA where the entity is established within five working days from its adoption.

d. Publication of the list of authorised IIPs and RRMs

In accordance with Articles 4a(1) and 9a(1) of the REMIT Regulation, ACER maintains publicly available registers of authorised IIPs and RRMs, including information on the services for which each IIP or RRM is authorised, on ACER's website. IIPs and RRMs are added to these registers immediately upon receiving authorisation from ACER.

2.5. Material changes after authorisation

IIPs and RRMs are required to keep their authorisation up to date. Where the IIP or RRM is no longer compliant with any of the requirements set out in the Delegated Regulation for the authorisation and supervision of IIPs and RRMs or in the REMIT Regulation as a result of a material change, ACER may adopt a decision pursuant to Article 34 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.

As per Article 31 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, when IIPs or RRMs or their IIP clients or RRM clients initiate material changes as referred to in Article 6(3), the IIPs or RRMs must notify ACER of such changes no later than ten working days after the change has taken place.

As per Article 6(3) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, a change will be considered material if it concerns any of the following:

- the manner in which the submission of inside information reports and the reporting of data records is carried out;
- the information contained in the supporting documents to be provided pursuant to Article 4;
- the types of data disclosed on IIP platforms or reported to the ACER by IIPs and RRMs;
- the relevant standard electronic formats in which data referred to in the above indent is reported.

The notification must describe the change in detail and be accompanied by the relevant supporting documents as referred to in Article 4, insofar as those documents have been amended.

RRMs must also notify ACER of any changes to the reported volumes, prior to their implementation. For the purpose of the notification, RRMs should consider whether the anticipated change in reporting volumes (e.g. number of records, number of files) is significant, taking into account in particular:

- the magnitude of the change compared with the current reporting volumes;
- whether the change is expected to be sustained rather than temporary;
- the underlying reasons for the change, including changes in the number of reporting clients.

ACER must respond to the IIP or RRM within 15 working days, informing them whether the change is in compliance with the requirements set out in the Delegated Regulation for the authorisation and supervision of IIPs and RRMs and in the REMIT Regulation, or whether any additional information or action is required.

3. Testing phase

To be able to undergo the testing phase and for the continued reporting of data to ACER, the applicants will be required to establish a VPN connection with ACER, have valid digital certificates and administrator and user accounts. The relevant details about how to establish all necessary technical set-ups will be provided to applicants after the signature of a non-disclosure agreement (NDA) with ACER.

All IIP and RRM applicants are required to undergo a testing phase to demonstrate their technical and operational compliance. The scope of testing is determined by the information (such as the identification of inside information reports and/or data records) the applicants intend to report. IIPs and RRMs registered pursuant to Commission Implementing Regulation (EU) No 1348/2014 will be eligible for a simplified testing procedure, as further described in Sections 3.5 and 3.6 below, reflecting their existing reporting activities and previously demonstrated technical capabilities.

The purpose of the testing phase is to verify the applicant's ability to report data records (RRMs) defined in the REMIT Implementing Regulation or types of inside information reports (IIPs) defined in Delegated Regulation for the authorisation and supervision of IIPs and RRMs and to demonstrate that the submitted content complies with the requirements established in the applicable reporting manuals and guidance for transaction data, exposure, fundamental data and inside information, along with technical manuals[6].

Data records and inside information reports must be reported using the relevant electronic formats as published by ACER and available on ACER's website.

The testing phase forms part of the application process and must be successfully completed before authorisation can be granted.

3.1. Reporting coverage and technical set-up

To configure the testing phase, the IIP or RRM applicant has to provide the following information:

(a) types of data records to be reported (RRM applicant) or types of inside information reports to be published on the platform and to be submitted to ACER (IIP applicant), based on a predefined list developed by ACER in line with the REMIT Implementing Regulation (refer to Annex V – REMIT validation rules document);

(b) identification of standard electronic formats in which such data records or inside information reports are to be reported to ACER, based on a predefined list of electronic formats as established by ACER as per the Article 13(4) of the REMIT Implementing Regulation;

(c) interface(s) used for the reporting.

Based on the selection made in points (a), (b) and (c), the authorisation tool will configure the relevant testing phase. The relevant testing materials, including test cases and test data, will be made available to the applicant.

IIP and RRM applicants may modify the pre-testing information provided under points (a), (b) and (c) above after its initial submission, provided that the testing phase has not yet been configured. Where such changes are made, the testing phase will be configured based on the updated information. Applicants must successfully complete all applicable tests before submitting their final application.

3.2. Connectivity, upload/download and validation

The IIP/RRM is required to complete at least five calendar days of conformance testing as part of the authorisation process. Testing should include the following activities.

[6] These include the *Transaction Reporting User Manual* (TRUM), the *Fundamental Data Reporting User Manual* (FRUM), the *Inside information Reporting User Manual* (IRUM), the 'Technical specification' document and the *Guidance for IIPs and RRMs*.

1. **Connectivity.** Perform connectivity and resiliency checks for the subscribed interfaces.
2. **Data upload of test data provided by ACER and validation (if available).** Validate and perform the upload of data based on a prescribed dataset and test cases, through the subscribed interfaces. IIP/RRM applicants must assign the relevant identification code (ID of the IIP or RRM / record ID / file ID / date and time) for the basic upload of the shared dataset. Please note that the test data may be available only for certain data types.
3. **Data download.** Perform a basic download of data receipts based on a prescribed dataset through the subscribed interfaces.
4. **Own data upload and validation.** Upload a set of data produced from the applicant's own data source and verify its successful validation through the subscribed interfaces. IIP/RRM applicants must indicate the record ID and file name of the submitted records. IIP applicants must generate inside information report(s) in XML format for the type(s) of inside information examples indicated prior to the testing.
5. **Invalid data receipt processing.** Download and process a set of negative receipts produced based on the data uploads as per point 2 above through the subscribed interfaces.
6. **Continual delivery.** The IIP/RRM applicant must submit a continuous set of data for a period of no less than five consecutive calendar days, up to a maximum of 10 consecutive calendar days, through the subscribed interfaces.

During testing, the automated validation rules are applied as specified in the REMIT validation rules document (refer to Annex V).

3.3. Success criteria and repetition of testing

To successfully pass the testing phase, the applicant needs to fulfil the following requirements.

- Test exactly the same type of data it has declared it will report/disclose.
- Test the same interface(s) it has declared it will use.
- Submit a minimum of 10 files per type of data over a minimum period of five calendar days but no more than ten calendar days (duration of the testing period):
  a. continuity of reporting must be ensured, and files with data records and/or inside information reports need to be sent for at least five calendar days in a row;
  b. the submitted files must be unique and must not contain duplicates (files and data records or inside information reports should be different among submissions simulating genuine reporting);
  c. each file needs to contain a meaningful sample of data records or inside information reports, not exceeding 100 records per file;
  d. the submitted files must fully comply with the relevant reporting manuals[7];
  e. the submitted files must fully comply with the field level validation defined in REMIT validation rules document (Annex V), which defines the rules and their applicable date (please refer to Chapter 5 below).
- Successfully complete the test cases.
- Submissions must comply with technical requirements defined in the documents received upon NDA signature.

ACER will inform the applicant of the outcome of the testing phase, indicating whether the required tests have been successfully completed. In the event of an unsuccessful testing attempt, ACER will notify the applicant about which specific testing criteria were not satisfied and for which data type. The applicant must repeat the part of the testing that was not completed successfully. A maximum of three

[7] Specifically, the TRUM, FRUM and IRUM.

testing attempts will be permitted. If the applicant does not successfully complete testing within three attempts, ACER may reject the application, and the applicant will be able to initiate the authorisation from the beginning should they wish to apply again for the authorisation.

If the applicant successfully tested one data type but failed in testing another data type, ACER will proceed with the assessment for the authorisation for the successfully tested data only.

3.4. Changes introduced after the authorisation that require testing

Where an authorised IIP or RRM requests changes to the selections made during the authorisation process (e.g. data types or interfaces), additional testing will be required only where the changes involve the addition of new data types, electronic formats or interfaces. Such testing will be limited to the modified scope of reporting and will complement the testing successfully completed during the initial authorisation process. Where the changes involve only the removal of previously authorised data types, electronic formats or interfaces, no additional testing will be required.

When an authorised IIP or RRM modifies its settings after authorisation has been granted, any testing required in relation to those changes is considered separate from the original authorisation process. The outcome of such testing does not affect the authorisation already granted. If the IIP or RRM fails the testing related to the proposed changes, it remains authorised to report the data types and records for which testing had previously been successfully completed. The new or modified data types and records may only be reported once the required testing has been successfully completed. For additional details, please also refer to Section 2.5 above.

3.5. Testing process for already registered RRMs during the authorisation process

To simplify the authorisation process for already registered RRMs, ACER intends to rely on the information and part of the tests already carried out before 29 October 2027 by such entities for the purpose of assessing the corresponding elements within the formal authorisation process.

When considering the testing, already registered RRMs will not be required to provide the reporting coverage, technical set-up or performance of connectivity tests described in Sections 3.1 and 3.2 unless they need to update or modify them compared to what they selected within the registration process and may continue to operate using the connectivity and communication arrangements in place when reporting as a registered RRM, such as a VPN, selected interfaces, digital certificates and other established technical configurations.

Already registered RRMs are, however, required to perform testing if introducing new/additional data types and/or electronic formats to their reporting coverage, including when new reporting obligations under the REMIT Implementing Regulation enter into force.

Article 17 of the REMIT Implementing Regulation defines a phased implementation (‘waves’) of the reporting obligations, with different entry-into-force dates (‘go-lives’) for different data types, which might have a direct impact on the authorisation (including the testing phase) of RRMs and corresponding obligations on ACER for the publication the relevant guidance documents and electronic formats.

The first wave of reporting becomes applicable on 29 October 2027, and ACER published the relevant guidance and electronic formats on 29 October 2026. For data types included in the first wave of reporting, RRMs do not need to perform any additional testing during the authorisation if the RRM had performed successful testing of these data types in the valid electronic format and is registered to report these data types in the correct electronic format in the context of the registration of RRMs. ACER may ask the registered RRM to perform testing of these data types during the authorisation process if the data is not compliant with the relevant reporting manuals or this guidance.

The second wave of reporting becomes applicable on 29 April 2028, and ACER should publish the relevant guidance and electronic formats by 29 April 2027. For data types included in the second wave of reporting, RRMs will need to undergo and complete the testing phase before 29 April 2028 as part of the authorisation process. ACER will review the testing results and if the tests have been successfully completed, the IIP or RRM may continue its reporting activities pending the adoption of a formal authorisation decision.

The data types included in the second wave will be reportable for the first time as of 29 April 2028; hence, they could not be tested and reported under the registration of RRMs.

Similarly, the third wave of reporting becomes applicable on 1 July 2028, and ACER should publish the relevant guidance and electronic formats by 29 October 2027. For data records included in the third wave of reporting, RRMs will need to undergo full testing as part of the authorisation or follow the procedure described in Section 3.4 if the RRM is already authorised.

3.6. Testing process for already registered IIPs during the authorisation process

Under the current framework, IIPs registered pursuant to Commission Implementing Regulation (EU) No 1348/2014 disclose inside information on behalf of market participants, while ACER collects the disclosed information from IIPs through web feeds.

Under the new framework, Article 13(2) of the REMIT Implementing Regulation provides that IIPs must, on the market participants' behalf, report the information disclosed on their platforms to ACER in an electronic format. The information reported must include the details set out in Annex II to the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. The reporting obligation in Article 13(2) of the REMIT Implementing Regulation becomes applicable on 29 April 2028.

For already registered IIPs, the testing phase cannot be simplified, as testing of reporting via electronic formats was not part of the previous IIP registration process. Consequently, as part of the authorisation process, already registered IIPs will be required to demonstrate their readiness to report the information disclosed on their platforms directly to ACER in the applicable electronic formats, replacing the current mechanism whereby ACER collects this information through IIP web feeds. The testing will cover the reporting functionalities and electronic formats that have not previously been tested and will be carried out in accordance with Sections 3.1 to 3.3.

The testing will verify that the IIP is able to generate and submit inside information reports in accordance with the applicable electronic formats, validation rules and relevant ACER manuals[8]. In particular, the testing will verify:

- the ability of the IIP's data validation system to perform the controls applicable to inside information reports, including:
  - the detection of duplicate disclosures;
  - the verification that the report contains the information required under Annex II to the Delegated Regulation for the authorisation and supervision of IIPs and RRMs and the applicable ACER manuals[9]; and
  - the detection of any data corruption caused by the IIP in processing the inside information report;
- the reporting of subsequent modifications to information already disclosed, as applicable.

The testing of the reporting to ACER is without prejudice to the assessment of compliance, as part of the authorisation process, with the other requirements applicable to IIPs under the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. In particular, the authorisation assessment will also cover the operation of the IIP platform required under Article 19, including the functionalities for filtering and downloading disclosed information, the availability of historical information and the linking of prior disclosures concerning the same event. These requirements will be assessed on the basis of supporting documentation submitted by the applicant and, where necessary, by requiring the applicant to demonstrate the relevant functionality.

[8] In this case, the IRUM.
[9] In this case, the IRUM.

4. Security measures

This section defines the policies, procedures, technical controls and organisational measures that IIPs and RRMs must establish and maintain under Article 13(1)(d) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs to protect their information systems, data and operations.

These measures are intended to support the confidentiality, integrity and availability of information processed, disclosed or reported in the context of wholesale energy market transparency and integrity. They also support, where appropriate, authenticity, accountability and reliability objectives depending on the risk profile of the system and data involved. Their implementation helps mitigate risks such as data breaches, unauthorised access, information leakage and physical threats to facilities, equipment and supporting infrastructure, thereby supporting market confidence and regulatory compliance. Controls must be monitored and periodically reviewed to ensure their ongoing effectiveness in response to evolving threats. IIPs and RRMs must maintain a documented information-security risk management process, covering systems, services, data and material dependencies within the scope of IIP/RRM activities. The process must identify and assess relevant risks, assign control owners, document risk treatment or acceptance decisions and be reviewed periodically and following material changes or significant incidents.

The security requirements in this guidance draw on internationally recognised cybersecurity and information security standards and good practices to promote consistency, interoperability and auditability. They consider ISO/IEC 27001:2022 and ISO/IEC 27002:2022, complemented where relevant by standards such as ISO/IEC 27005 (risk management), ISO/IEC 27035-1:2023 (incident management), ISO/IEC 27701 (privacy information management) and ISO/IEC 27017 (cloud security controls). IIPs and RRMs may also use other recognised frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, NIST SP 800-series publications, Centre for Internet Security (CIS) Critical Security Controls or equivalent standards, as appropriate to their risk profile and operational context. This approach supports alignment with Directive (EU) 2022/2555 (NIS2 Directive) and broader EU cybersecurity and resilience objectives. IIPs and RRMs may demonstrate compliance through relevant certifications or other supporting evidence covering applicable security measures, including physical security, access control, cryptographic protection, incident and vulnerability management, business continuity, backup and recovery, and third-party security assurance. Evidence may cover controls implemented by the entity or by cloud-based and managed service providers, provided it is relevant to the services and controls in scope. ACER may request additional information where necessary and proportionate to assess compliance, considering the protection of confidential, commercially sensitive and security-sensitive information. Reliance on third-party services does not transfer responsibility for compliance from the RRM or IIP.

The requirements in this guidance must be applied on a risk-based and proportionate basis, considering system criticality, data sensitivity, operational context, dependencies and regulatory impact. A critical system is a system for which its failure, compromise or unavailability would result in significant operational, financial, legal, safety or security impact. IIPs and RRMs must identify critical systems through a documented risk assessment, taking into account the nature and criticality of the services supported, relevant dependencies, regulatory obligations and the potential impact of disruption or compromise. The minimum requirements set out in Chapter 4 constitute the requirements against which ACER will assess IIPs and RRMs for the purposes of authorisation and supervision, in accordance with the applicable legal and regulatory framework. Best practices included in this guidance are optional and are intended to support IIPs and RRMs in strengthening their security posture beyond the minimum requirements, where appropriate. Annex III provides illustrative operational guidance on possible steps for implementing the minimum requirements and does not introduce or modify the obligations arising from them. IIPs and RRMs may implement equivalent alternative controls where these achieve the intended security objectives and meet applicable regulatory requirements. Where an alternative control replaces a stated minimum requirement, IIPs and RRMs must document the rationale, the control objective addressed, the alternative measure, the residual risk and identify who approved the alternative control. Such controls must be reviewed periodically on a risk-based basis, and the documented assessment and supporting evidence must be made available to ACER upon request, in accordance with applicable requirements.

4.1. Confidentiality

Confidentiality refers to the protection of sensitive information from unauthorised access or disclosure. It ensures that information is accessible only to authorised individuals or systems and prevents exposure to unintended parties. Maintaining confidentiality requires the implementation of appropriate technical and organisational measures, including access controls, encryption, secure communication mechanisms, network segmentation and trust zones, restriction of unnecessary services and interfaces, secure remote administrative access, protection of external-facing interfaces and documented review of material network-security rules and configurations.

For this guidance, 'sensitive' refers to any information that, if disclosed without authorisation, could result in regulatory breaches, market impact, reputational damage or harm to market participants. Data must be classified in accordance with a documented data classification framework implemented by the organisation. The data classification framework must identify the categories of information requiring protection, including REMIT data and other market-sensitive information. At a minimum, IIPs and RRMs must define classification levels (e.g. public, internal, sensitive, restricted) and apply them consistently across all systems and processes, as detailed in Annex III.

Where information is not explicitly classified, IIPs and RRMs must assess its confidentiality based on its content, context, regulatory relevance and the potential impact of unauthorised disclosure. Attention must be given to inside information and other market-sensitive data, where unauthorised disclosure could affect market integrity, transparency or regulatory compliance.

Minimum requirements and best practices

IIPs and RRMs must implement controls to prevent unauthorised access to or disclosure of sensitive information throughout its life cycle. These controls must ensure that sensitive data is accessible only to authorised users and systems and is protected against exposure, leakage or misuse, taking into account data sensitivity, regulatory obligations and potential market impact.

Access control

Minimum requirements

- IIPs and RRMs must implement access control mechanisms to restrict access to systems, applications and data to authorised users, systems and processes. Access control models must include role-based access control (RBAC), attribute-based access control (ABAC) or equivalent mechanisms suited to the organisation's architecture and risk profile, ensuring alignment with the access control requirements defined in Section 4.4. Access rights must be assigned and managed in accordance with the principle of least privilege and the organisation's data and system classification framework. Access controls must be defined using a risk-based approach and supported by the confidentiality assessment, including the need for enhanced access restrictions based on classification and regulatory impact, along with the type of user or entity involved (e.g. internal users, privileged users, external RRM clients, market participants interacting with IIPs or system accounts). Access control mechanisms must also address physical access to facilities, premises, equipment and supporting infrastructure hosting or providing access to systems and data, ensuring that such access is restricted to authorised individuals based on their roles and operational needs, in accordance with the applicable physical security requirements.

Best practices

- IIPs and RRMs may conduct more frequent or enhanced reviews beyond the risk-based minimum, to verify that access rights remain appropriate to the current roles and business needs and to identify unnecessary or inactive access.
- Privileged access management (PAM) solutions may be implemented to support centralised governance, monitoring and controlled use of privileged accounts and elevated access.
- Conditional or adaptive access controls may be applied based on contextual or risk-based factors such as user location, device posture, authentication context or assessed risk level, to reduce the likelihood of unauthorised access.

Encryption strategy

Minimum requirements

- IIPs and RRMs must implement cryptographic controls to protect data within the scope of the REMIT Regulation, in accordance with the organisation's data classification framework, excluding publicly available information. For data at rest, the application of encryption must be determined based on data classification, sensitivity and a documented risk assessment, taking into account applicable legal, regulatory and contractual obligations and business requirements. Data in transit must be protected using appropriate cryptographic controls, recognised industry-standard mechanisms and secure communication protocols to prevent unauthorised disclosure, interception or tampering. The scope and application of cryptographic controls must be proportionate to the identified risks, system criticality, operational context and performance requirements, considering the relevant stage of the data life cycle. Where encryption is not feasible, equivalent technical or organisational controls must be implemented based on the risk assessment. These requirements must apply from their date of entry into force and must not require retroactive encryption of legacy data, provided existing protections are documented as adequate in light of the current threat environment and applicable obligations. Where protection is inadequate, appropriate remediation or compensating controls must be implemented.

Best practices

- IIPs and RRMs may implement cryptographic key rotation at defined intervals to reduce risks associated with prolonged key exposure and support effective lifecycle management of cryptographic material.
- Hardware security modules (HSMs), managed key management services (KMS) or equivalent secure key protection mechanisms may be used to support the secure generation, storage, use, rotation and destruction of cryptographic keys while reducing the risk of unauthorised disclosure or compromise of key material.

Key management

Minimum requirements

- IIPs and RRMs must establish and maintain procedures for the secure lifecycle management of cryptographic keys, including generation, storage, distribution, rotation, recovery, archival and destruction. Key management controls must be defined using a risk-based approach, considering system criticality, data classification, operational environment and risk exposure, ensuring the confidentiality, integrity and availability of cryptographic operations. Key management processes must ensure that cryptographic keys are accessible only to authorised users, systems and processes and are protected against unauthorised disclosure, modification, loss or misuse.

Best practices

- Secure backup copies of cryptographic keys may be maintained in protected and, where appropriate, geographically separate locations to support resilience and recovery objectives.
- Documented key escrow and recovery procedures may be established and periodically tested to ensure continued access to encrypted information in the event of system failure, key loss or operational disruption.
- Automated key lifecycle management capabilities may be used, where operationally feasible, to support consistent generation, rotation, archival and destruction of cryptographic keys, reducing manual errors and improving operational efficiency, traceability and control effectiveness.

Data loss prevention

Minimum requirements

- IIPs and RRMs must implement technical, procedural and organisational controls to protect data classified in accordance with the organisation's data classification framework against unauthorised disclosure, transmission, loss or exposure. Controls must be defined based on

documented risk assessments, considering data classification, system criticality and regulatory relevance. Data leakage prevention measures must support the identification, detection and prevention of unauthorised disclosure events and must include controls depending on the operational environment and system architecture. Where automated data loss prevention (DLP) technologies are used, IIPs and RRMs must ensure they are appropriately configured, governed and monitored to support effective protection of sensitive information.

Best practices

- Automated alerting and escalation mechanisms may be implemented to support timely detection, prioritisation and response to suspected data leakage events or policy violations.
- DLP policies, rules and detection mechanisms may be reviewed and refined periodically based on operational experience, incident analysis, emerging threats and changes in the organisation's risk profile, helping to improve effectiveness while reducing false positives and unnecessary disruption.

Secure data disposal

Minimum requirements

- When data is no longer required, IIPs and RRMs must ensure its secure and irreversible disposal in accordance with the organisation's data classification framework and applicable legal, regulatory and contractual obligations. Disposal mechanisms must prevent unauthorised recovery, reconstruction or access to disposed information. Digital data disposal methods must include cryptographic erasure, secure overwriting or equivalent techniques appropriate to the storage technology and operational environment. Physical storage media containing data subject to disposal must be securely destroyed or sanitised using recognised methods such as shredding, degaussing, incineration or equivalent destruction techniques. IIPs and RRMs must establish and maintain documented procedures for secure data disposal and implement verification measures where appropriate to confirm that data cannot reasonably be recovered. Retention and disposal periods must comply with applicable legal, regulatory and contractual obligations and General Data Protection Regulation (GDPR) data minimisation principles. Relevant records must be retained for a minimum of five years, unless a longer retention period is required by applicable legal or regulatory obligations.

Best practices

- Certified or independently verified data destruction services may be used for disposal of highly sensitive information or media, including the use of certificates of destruction and verification that service providers comply with recognised security and disposal standards.
- Automated data lifecycle management capabilities may be implemented to support secure and timely deletion or disposal of data when retention periods expire, reducing manual errors and improving consistency of disposal practices.

Data minimisation

Minimum requirements

- IIPs and RRMs must apply data minimisation principles to ensure that only data necessary for defined business, operational and regulatory purposes is collected, processed, retained and shared. Data minimisation requirements must be defined based on a risk-based approach and aligned with the organisation's data classification framework and retention policies. IIPs and RRMs must avoid unnecessary collection or retention of data to reduce data exposure, limit the scope of processing and support compliance with applicable legal and regulatory obligations.

Best practices

- Data minimisation practices may be continuously refined based on operational experience, data usage analysis and changes in regulatory or business requirements to further reduce unnecessary data exposure and processing overhead.

Awareness training

Minimum requirements

- IIPs and RRMs must implement and maintain security awareness and training programmes appropriate to personnel roles and risk exposure. Training activities must ensure that personnel understand their responsibilities regarding the protection of sensitive information, the secure handling of regulated data, physical security and compliance with organisational security policies and procedures. This must include awareness of physical security risks, such as unauthorised access to premises, restricted areas, equipment and supporting infrastructure, and the procedures for reporting suspected security incidents. Role-specific training must be provided where appropriate for privileged users, operational personnel and users handling sensitive or regulated information. Training content and frequency must be defined and periodically reviewed based on risk, material changes, incident experience and relevant threat developments.

Annex III provides operational guidance on confidentiality, including a data classification scheme.

4.2. Integrity

Data integrity guarantees that information remains accurate, complete and unaltered except through authorised actions throughout its life cycle. It protects against accidental or deliberate data modification, deletion or corruption. Mechanisms such as digital signatures, cryptographic hashes, audit trails and validation processes are employed to verify data consistency and authenticity, thereby ensuring the reliability of information used for reporting and decision-making.

Minimum requirements and best practices

IIPs and RRMs must implement controls to ensure that data remains accurate, complete and consistent throughout its life cycle. These controls must prevent the unauthorised or unintended modification, corruption or deletion of data and ensure that any changes to data are properly authorised, recorded and traceable.

Change management process

Minimum requirements

- IIPs and RRMs must implement a formal change management process for modifications affecting data, systems, applications, infrastructure or security configurations. Changes must be documented, risk-assessed, authorised prior to implementation and tested before deployment to production environments. Appropriate rollback and recovery procedures must be defined and maintained to support restoration in case of failure, error or unintended impact. Change approvals must reflect the assessed risk and potential impact of each change, with higher-risk changes subject to appropriate review and oversight by the relevant stakeholders. Changes affecting system integrity are also subject to the vulnerability management and audit trail requirements set out in Sections 4.6 and 4.7, as applicable.

Best practices

- Structured governance mechanisms such as cross-functional review groups or designated approvers may be used to support review and oversight of higher-risk changes, ensuring consistent risk evaluation, accountability and coordination.
- Automated change management tools may be implemented to support the tracking of change requests, approvals, testing and deployment history, improving traceability, control and auditability.

Data integrity controls

Minimum requirements

- IIPs and RRMs must implement technical and procedural controls to ensure that REMIT data remains accurate, complete and consistent throughout its life cycle, in accordance with the applicable data classification framework. These controls must include mechanisms to prevent and detect the introduction or persistence of invalid, incomplete or inconsistent data within

systems and databases. Validation rules and integrity checks must be formally defined, documented and enforced through appropriate system controls. Integrity validation activities, detected discrepancies and corrective actions must be recorded to ensure traceability and auditability. Identified integrity issues must be investigated and corrected where necessary to maintain data accuracy and consistency. Further information on data validation principles and processes is provided in Section 5.

Best practices

- Integrity verification mechanisms such as cryptographic hashing (e.g. secure hash algorithm 256-bit (SHA-256) or stronger) may be used to detect any unauthorised modification of data. Integrity verification data may be stored separately from operational datasets and used for periodic comparison.
- Periodic reconciliation between systems may be performed based on an assessment of data classification, transaction frequency and regulatory relevance, with results documented for traceability.
- Advanced database or platform capabilities, such as stored procedures, views, roles, triggers, transactions or equivalent integrity enforcement mechanisms, may be implemented to support data consistency, enforce business rules, reduce processing errors and improve operational reliability.

Audit logging and monitoring

Minimum requirements

- IIPs and RRMs must ensure that changes to REMIT data and relevant system activities affecting its integrity are logged to support traceability, accountability and investigation activities. Audit logs must capture at minimum the identity of the user or system performing the activity, the timestamp and the nature of the event. Relevant, additional contextual information, such as affected data elements and activity outcomes, must be recorded to support investigation and analysis, in accordance with Section 4.6. Audit records relating to REMIT data changes, data validation and correction, regulatory submissions, authentication, digital signatures and other security-relevant activities affecting data integrity must be retained for five years, unless otherwise specified by applicable requirements or justified by the nature and risk of the data, in accordance with applicable legal, regulatory and contractual obligations and GDPR data minimisation principles. Audit logs must be protected against unauthorised access, modification and deletion. IIPs and RRMs must establish monitoring and review mechanisms proportionate to system criticality, data sensitivity and the potential impact of integrity failures. For critical systems where delayed detection could result in material data integrity issues or affect regulatory reporting, monitoring must support the timely detection of suspicious activities, unauthorised changes and integrity failures. Monitoring and review activities, identified issues, investigations, escalations and corrective actions must be documented.

Best practices

- Automated monitoring, correlation and alerting mechanisms may be implemented to support the detection of suspicious activities such as unusual access patterns, repeated authentication failures or unauthorised data changes.
- Structured audit log review procedures may be established to support consistent and risk-based monitoring activities across systems and processes. Where feasible, automated tools and analytics capabilities may be used to improve visibility, reduce manual effort and enhance the effectiveness of review and investigation activities.

Digital signatures

Minimum requirements

- IIPs and RRMs must implement cryptographic and authentication mechanisms to ensure the authenticity, integrity and non-repudiation of critical data exchanges and regulatory transactions detailed further in Section 4.5. The use of digital signatures or equivalent cryptographic assurance mechanisms must be based on a risk-based approach, considering the communication channel, system interaction type and associated risk profile. Where digital

signatures or certificate-based authentication are used, they must be applied at session or connection establishment to ensure the strong authentication of users or systems accessing IIP/RRM services. Once an authenticated and integrity-protected communication channel has been established, subsequent exchanges within the session are considered covered by the established trust context, provided that integrity controls remain active. Where applicable, signed data and related verification or authentication records must be retained for five years, unless otherwise specified by applicable requirements or justified by the nature and risk of the data, in accordance with applicable legal, regulatory and contractual obligations. Activities related to authentication, signature generation and verification must be logged to support traceability and accountability.

Best practices

- Qualified or advanced electronic signatures, as defined under Regulation (EU) No 910/2014 (e-IDAS), may be used for legally significant submissions or regulatory communications requiring enhanced assurance of signer identity and legal recognition across jurisdictions.

Annex III provides operational guidance on integrity.

4.3. Availability

Availability refers to the assurance that information and information systems are accessible and usable upon demand by authorised entities. It ensures that critical data and services remain operational and can be accessed by legitimate users and systems when needed, without undue delay or disruption. Maintaining availability involves implementing controls such as redundancy, backup procedures, disaster recovery planning and business continuity measures to protect against service interruptions caused by technical failures, natural disasters or malicious attacks.

Minimum requirements and best practices

IIPs and RRMs must implement controls to ensure that critical systems and data remain available and accessible when required. These controls must minimise the risk of service disruption and support the timely recovery of operations in the event of incidents, failures or external disruptions, considering system criticality and operational dependencies.

Backup strategy

Minimum requirements

- RRMs and IIPs must establish and maintain backup and recovery procedures to protect critical data and systems against loss resulting from technical failure, corruption, human error or malicious activity. Backup frequency, retention and recovery arrangements, including recovery point objectives (RPOs) and recovery time objectives (RTOs), must be defined based on data and system criticality, dependencies and the entity's operating model, business needs and applicable regulatory obligations. Procedures must define backup scope, scheduling, storage, retention and restoration responsibilities. Backup data must be protected against unauthorised access, modification or loss. Where justified by a documented risk assessment, backups must be stored in geographically separate or logically isolated environments. Backup and recovery processes must be tested periodically against defined recovery objectives. IIPs and RRMs must identify and manage security risks arising from third-party providers and supply-chain dependencies supporting critical or regulated services. Risk-based due diligence and ongoing assurance must address relevant security controls, incident notification, business continuity, data protection, sub-outsourcing and termination or exit arrangements. Appropriate evidence must be obtained to assess the adequacy of relevant third-party controls. Evidence must include ISO/IEC 27001 certification, independent audit reports, provider attestations, service level agreements (SLAs) and contractual commitments. The type and level of detail required must be proportionate to service criticality, associated risks and applicable requirements. Existing evidence must be reused where it is sufficiently current, reliable and relevant; supplementary evidence must be obtained where necessary to address gaps or limitations. Where certification or other assurance evidence is relied upon, IIPs and RRMs must verify its validity, scope and relevance to the services provided and retain evidence of the assessment. Evidence held by a third-party organisation operating a reporting platform must support an RRM's or IIP's assessment where it covers the relevant services and controls. Outsourcing or

reliance on third-party assurance must not transfer responsibility for compliance from the RRM or IIP.

Best practices

- Automated failover and resilience mechanisms may be implemented to support continuity of operations during system failures, including redundancy, replication or alternative processing environments.

Business continuity planning

Minimum requirements

- IIPs and RRMs must develop, implement and maintain business continuity and disaster recovery arrangements to ensure the continued operation and recovery of critical systems and processes during disruption events. Business continuity planning must identify critical services, systems, dependencies and recovery priorities, and define recovery strategies aligned with operational and regulatory obligations. Recovery objectives, including RTOs and RPOs, must be defined based on documented risk assessments and regulatory requirements. Business continuity arrangements must consider relevant disruption scenarios, including system failures, cyber incidents, natural disasters, human error, physical security incidents affecting premises, equipment or supporting infrastructure, loss of access to facilities, and third-party or supply chain failures. For critical or important outsourced dependencies, IIPs and RRMs must consider substitutability, concentration risk, loss of provider access, data or configuration portability and feasible exit or contingency arrangements. Recovery procedures, escalation paths, roles and responsibilities, communication arrangements and restoration activities must be documented and maintained. Business continuity and disaster recovery arrangements must be tested periodically to validate recovery capability and operational readiness. Testing scope and frequency must be defined based on documented risk assessment.

Best practices

- Business continuity exercises may include full-scale and tabletop exercises, failover testing or component-level recovery validation to identify weaknesses and improve recovery readiness.
- Capacity forecasting and resilience monitoring may be implemented to support operational preparedness, resource planning and continuity during disruption scenarios.
- Multiple independent communication channels may be established using different providers or network paths to support continued communication with ACER, market participants and internal stakeholders during disruption events.

System redundancy

Minimum requirements

- IIPs and RRMs must implement resilience and redundancy measures for critical systems and infrastructure to reduce the risk of service interruption due to component failures, infrastructure outages or operational disruptions. Redundancy measures must be defined based on system criticality, operational requirements and risk assessment outcomes. Redundancy mechanisms must include failover capabilities, redundant infrastructure components, load distribution, geographically separated environments or alternative processing arrangements to support continued operation or controlled degradation during disruption events. IIPs and RRMs must test redundancy and failover mechanisms periodically to confirm that continuity and recovery objectives are met and that critical services remain available under defined failure scenarios.

Best practices

- Service resilience and availability requirements may be defined through SLAs, operational agreements or equivalent arrangements with internal or external service providers, including availability targets, escalation procedures and recovery commitments.
- For IIPs and RRMs using primary and fallback systems, availability may be assessed at overall service level, including all active and fallback processing capabilities, to ensure continuous fulfilment of reporting and disclosure obligations.

- Availability metrics may be calculated based on unplanned service disruptions only. Duly planned and communicated maintenance activities are excluded from availability calculations where appropriately approved and managed.

Incident response and monitoring

Minimum requirements

- IIPs and RRMs must develop, implement and maintain formal procedures for detecting, managing and resolving incidents that impact system availability. Incident response procedures must cover the full life cycle of an availability incident, including detection, classification, impact assessment, containment, service restoration and post-incident review. Roles and responsibilities for incident response must be defined and assigned to appropriately qualified personnel or teams. Communication and escalation procedures must ensure timely notification of relevant internal stakeholders, affected clients and, where applicable, competent regulatory authorities. All incident response activities must be documented to support investigation, auditability and continuous improvement of operational resilience.

Best practices

- Beyond the continuous collection and risk-based analysis of monitoring data required under Section 4.7, IIPs and RRMs may use additional performance and availability metrics, predictive analysis or enhanced automated alerts to support earlier detection of degradation or disruption.
- Monitoring output may be used to support trend analysis, capacity planning and continuous improvement of resilience and availability controls.

Annex III provides operational guidance on availability.

4.4. Access control

Access control refers to the mechanisms and procedures that restrict access to information systems and data to authorised users and systems only. It ensures that individuals and systems can only access the information and resources necessary to perform their assigned functions, following the principle of least privilege. Maintaining effective access control involves implementing controls such as user authentication, authorisation mechanisms, access rights management and monitoring of access activities to prevent the unauthorised access and misuse of systems and data.

Minimum requirements and best practices

IIPs and RRMs must implement access control measures to ensure that only authorised users and systems can access sensitive information and critical systems. These measures must enforce the principle of least privilege, prevent unauthorised access and ensure that access rights are granted, reviewed and revoked in a controlled and traceable manner.

User authentication

Minimum requirements

- IIPs and RRMs must implement risk-based authentication mechanisms to verify the identity of users, systems and services before granting access to systems and data. Authentication controls must be selected based on a documented risk assessment, system classification, data sensitivity, system criticality and user type, including internal users, privileged users and external IIP/RRM clients. Authentication mechanisms must include secure password or passphrase policies proportionate to the identified risks, with controls to prevent the use of weak, default or compromised credentials. Multi-factor authentication (MFA) must be implemented for all user accounts accessing systems and data within the scope of IIP/RRM activities, including internal users, privileged users and external IIP/RRM clients. Authentication methods must be proportionate to the associated risks, taking into account system classification, data sensitivity, access privileges and access context. System-to-system and service authentication must use strong mechanisms appropriate to the architecture and risk, including certificate-based or other cryptographic credentials where suitable or required by applicable regulatory obligations or ACER technical specifications. Credentials, certificates and associated private keys must be protected against unauthorised disclosure, misuse and compromise throughout their life cycle. Default accounts must be disabled or securely

configured before deployment. Inactive or unnecessary accounts and credentials must be disabled, removed or revoked in a timely manner.

Best practices

- Adaptive or contextual authentication may be implemented using factors such as user location, device posture, access time and behavioural indicators to identify anomalous access attempts.
- Automated account protection mechanisms may be implemented to mitigate credential-based attacks, including controls for repeated failed authentication attempts and secure account recovery procedures.
- Session management controls may be implemented to reduce the risk of unauthorised access through inactive or compromised sessions, including session timeouts, secure token handling, session termination and restrictions on concurrent sessions, where appropriate.

Authorisation controls

Minimum requirements

- IIPs and RRMs must implement RBAC, ABAC or equivalent authorisation mechanisms to restrict access to systems, applications and information according to defined roles, responsibilities, contextual attributes and applicable regulatory functions. The authorisation model must be selected based on a risk assessment and system architecture. Access rights must be granted in accordance with the principle of least privilege, ensuring that users, systems and services are provided only with the minimum access necessary to perform their functions (e.g. read, write, execute, modify, approve). Access rights must be formally documented, including the business justification and approval authority. Privileged accounts, including administrator and system-level accounts, must be restricted to authorised personnel and used exclusively for administrative or other specifically authorised elevated functions. Such accounts must not be used for routine operational activities.

Best practices

- PAM solutions may be implemented to support centralised governance of privileged accounts, including the controlled elevation of privileges, just-in-time access provisioning, session monitoring and detailed audit logging of privileged activities. Such mechanisms may be adapted to the organisation’s technical architecture and risk exposure, ensuring proportionality and operational feasibility.

Access lifecycle management

Minimum requirements

- IIPs and RRMs must implement formal procedures to manage the full life cycle of user and non-human identities such as service accounts application identities used for automated processes, including provisioning, modification, review and revocation. Access provisioning must be based on documented requests specifying the user identity, required systems or data access, business justification and authorised approval. Access rights must be updated when users change roles, responsibilities or organisational functions and must be revoked without delay when access is no longer required or when users leave the organisation. IIPs and RRMs must perform periodic access reviews (e.g. quarterly) to verify that access rights remain appropriate and aligned with current authorised functions and responsibilities. The scope and frequency of access reviews must be defined through a documented risk assessment considering system criticality, data sensitivity, user population and rate of organisational or role changes, with privileged and higher-risk access reviewed more frequently where justified.

Best practices

- IIPs and RRMs may implement structured access recertification processes to continuously validate that user permissions remain appropriate to their current roles and responsibilities, supporting the principle of least privilege and preventing accumulation of excessive access rights over time.

- Automated identity and access management tools may be used to detect orphaned, excessive or inactive accounts and to support timely revocation of access rights following role changes or user departure.

Segregation of duties

Minimum requirements

- IIPs and RRMs must identify incompatible duties and implement controls to prevent or detect conflicts of interest where a single user could perform conflicting functions without appropriate oversight. Incompatible duties must include, but are not limited to, creation and approval of transactions, execution and authorisation of changes, data recording and reconciliation, or investigation and resolution of discrepancies. Segregation of duties must be implemented through role design, access control mechanisms, and procedural controls that prevent the concentration of conflicting responsibilities within a single individual. Where strict segregation is not feasible, including in smaller or self-reporting RRMs, IIPs and RRMs must implement appropriate compensating controls, such as enhanced logging, periodic independent access reviews and strengthened supervisory oversight, to ensure conflicts of interest are effectively managed.

Best practices

- IIPs and RRMs may implement dual approval mechanisms for critical activities, including significant transactions, system configuration changes or material data modifications, ensuring independent approval by appropriately authorised users with full traceability.

Access monitoring

Minimum requirements

- IIPs and RRMs must implement logging and monitoring mechanisms to record and oversee access to systems, applications and data, particularly where sensitive or regulated information is processed. Access logs must capture, at a minimum, the identity of the user or system, timestamp, accessed resource and whether the access attempt was successful or unsuccessful and in accordance with Section 4.6. Where relevant, logs must include key actions performed within the system. Access logs must be protected against unauthorised access, modification or deletion to preserve their integrity and evidential value. IIPs and RRMs must establish regular log review processes to identify unauthorised access attempts, abnormal usage patterns or indicators of suspicious activity, based on a risk assessment considering system criticality and data sensitivity. The frequency of reviews must be determined through a documented risk-based approach, considering system criticality, data sensitivity, privileged-access exposure, threat indicators and operational requirements.

Best practices

- IIPs and RRMs may implement automated alerting mechanisms to support timely detection of suspicious access activities, including unusual login patterns, repeated authentication failures and abnormal access behaviour, enabling faster investigation and response.
- IIPs and RRMs may implement enhanced monitoring for privileged users and access to sensitive systems, including tracking of application activity, system interactions and relevant system or network events to strengthen accountability and improve detection of insider threats, policy violations or abnormal behaviour patterns.

Annex III provides operational guidance on access control.

4.5. Authenticity

Authenticity refers to the assurance that information and communications are genuine and originate from the claimed source. Non-repudiation refers to the ability to prove that a specific action or transaction was performed by a specific user or system, preventing the user or system from later denying that they performed the action. Maintaining authenticity and non-repudiation involves implementing controls such as digital signatures, digital certificates and audit trails to verify the origin and integrity of information and to provide evidence of actions performed.

Minimum requirements and best practices

IIPs and RRMs must implement controls to ensure that information and communications are authentic and originate from trusted sources. These controls must enable verification of identity, support non-repudiation of actions and ensure that data and transactions can be reliably attributed to specific users or systems.

Digital signatures

Minimum requirements

- IIPs and RRMs must implement appropriate cryptographic mechanisms, including digital signatures or equivalent assurance techniques, to ensure the authenticity, integrity and traceability of critical data submissions, communications and approvals. Where required by applicable regulatory obligations or technical specifications, or justified by a documented risk assessment, digital signatures must comply with recognised standards and be verified before acceptance. The assessment must consider system architecture, communication channels and existing authentication, integrity and trust mechanisms to determine whether additional transaction-level signing is necessary. Signed records and verification evidence must be retained to support auditability and traceability.

Best practices

- Qualified or advanced electronic signatures may be used for legally significant submissions, in accordance with Regulation (EU) No 910/2014 (e-IDAS), to provide enhanced assurance of signer identity and support cross-jurisdictional legal recognition.
- Trusted timestamping services may be used to embed verifiable evidence of the time at which a transaction, approval or communication occurred, by obtaining timestamps from recognised timestamp authorities and incorporating them within digital signature frameworks or equivalent integrity mechanisms.

Certificate management

Minimum requirements

- IIPs and RRMs must establish and maintain procedures for the lifecycle management of digital certificates used for authentication, secure communications and digital signatures. Certificates must be issued by trusted certificate authorities (CAs). IIPs and RRMs are permitted to operate private public key infrastructure (PKI) environments or use externally managed or cloud-based certificate services, provided that appropriate security and governance controls are maintained. Private keys must be protected against unauthorised access, disclosure, modification or loss through appropriate technical and organisational controls. IIPs and RRMs must verify certificate validity and revocation status before relying on certificates for authentication or secure communications. Certificate lifecycle activities must be documented and periodically reviewed to support traceability, accountability and compliance with applicable security requirements.

Best practices

- IIPs and RRMs may implement certificate pinning or equivalent trust validation mechanisms for critical system-to-system communications to reduce the risk of impersonation or certificate substitution attacks.
- Periodic audits of certificate usage, validity and associated authentication mechanisms may be conducted to ensure certificates remain appropriately issued, correctly used and adequately protected, with findings documented and remediated in a timely manner.
- Certificate lifecycle management processes may be aligned with operational and technical requirements of issuing CAs and underlying infrastructure to ensure maintainability, scalability and operational feasibility.

User authentication

Minimum requirements

- IIPs and RRMs must implement authentication mechanisms to verify the identity of users and systems prior to granting access to systems, data or the execution of critical actions, detailed in Section 4.4. Authentication controls must be based on a risk assessment and system classification, to prevent impersonation and the unauthorised use of credentials, considering data sensitivity, system criticality and the impact of the action performed. Authentication mechanisms must include credential-based controls such as passwords or passphrases, defined and managed based on system classification and risk assessment. MFA must be implemented for all user accounts in accordance with the requirements set out in Section 4.4. Authentication must also be required before the execution of critical actions, including regulatory submissions, approvals and administrative changes. Authentication events, including failed attempts, must be logged to support detection of suspicious activity and potential misuse.

Audit trails

Minimum requirements

- IIPs and RRMs must maintain audit logs of authentication and identity-related events to ensure traceability and accountability and to support the investigation of potential misuse or security incidents, detailed in Section 4.6. Audit logs must capture, at a minimum, the identity of the user or system, timestamp, accessed system or service and outcome of the authentication attempt. Logging must distinguish between internal users (including staff, administrators and privileged accounts) and external IIP/RRM clients interacting through dedicated interfaces such as submission or reporting portals. For external clients, logging is must focus on authentication events, submission integrity and relevant transactional actions rather than full internal system activity. Audit logs must be protected against unauthorised modification or deletion and retained in accordance with regulatory and organisational requirements. Logs must be reviewed regularly based on risk, with emphasis on privileged access and high-impact system activities.

Best practices

- IIPs and RRMs may implement automated monitoring and analysis mechanisms to detect anomalous authentication behaviour, including repeated failed login attempts, access from unusual locations or devices, abnormal access times or indicators of compromised credentials.
- IIPs and RRMs may implement automated alerting capabilities to notify responsible personnel of suspected authentication anomalies, enabling timely investigation and response to potential security incidents.

Annex III provides operational guidance on authenticity.

4.6. Accountability

Accountability refers to the ability to hold individuals and systems responsible for their actions. It ensures that all actions performed on information systems and data can be traced to specific users or systems and that responsibility for those actions can be clearly established. Maintaining accountability requires the implementation of controls such as user identification, audit trails, access logging and incident investigation procedures, enabling IIPs and RRMs to provide reliable evidence of actions performed and to support investigations of security incidents and policy violations.

Minimum requirements and best practices

IIPs and RRMs must implement controls to ensure that all actions performed on systems and data can be traced to specific users or systems. These controls must support traceability, enable investigation of incidents, and ensure that responsibility for actions can be clearly established.

User identification

Minimum requirements

- IIPs and RRMs must ensure that users and systems are uniquely identifiable so that actions performed on systems and data can be reliably attributed to specific individuals or automated processes. User identifiers must be assigned in a manner that supports traceability across systems and processes, with a maintained and documented mapping between user identities and natural persons where applicable. Unique identification must be implemented based on risk, considering the type of user, including internal staff, privileged users and external IIP/RRM clients, as well as the nature of system access. For external users, identification must be implemented through dedicated accounts or controlled access mechanisms, provided that accountability for submissions and system actions is preserved. Shared or generic accounts are not permitted unless explicitly justified by operational necessity and are subject to formal approval and compensating controls, including enhanced logging, monitoring and periodic review. User accounts must be disabled or revoked without delay when access is no longer required, including role changes or termination.

Best practices

- Enhanced user activity monitoring may be implemented for privileged users and access to sensitive systems, including tracking of application usage, system interactions, file access and administrative activities to strengthen accountability and support detection of misuse or insider threats.
- Periodic identity and accountability assurance reviews may be conducted to verify the correct mapping between identities and users, the completeness of audit trails, the adequacy of logging and retention and the proper investigation and resolution of anomalies. Findings may be used to improve identity and access control effectiveness.

Audit trails

Minimum requirements

- IIPs and RRMs must maintain audit trails that record actions performed on critical systems and data to ensure traceability, accountability and support for investigation and regulatory oversight. Audit trails must capture sufficient information to enable the reconstruction of relevant events, including user or system identity, timestamp, type of action, affected systems or data and outcome of the action (success or failure). Audit records must be protected against unauthorised access, modification or deletion. Further information for audit logging and monitoring can be found in Section 4.2. Retention and disposal periods must comply with applicable legal, regulatory and contractual obligations and GDPR data minimisation principles. Relevant records must be retained for a minimum of five years, unless a longer retention period is required by applicable legal or regulatory obligations.

Best practices

- IIPs and RRMs may implement automated analysis and correlation mechanisms to support the detection of anomalous or suspicious behaviour within audit trails, including unusual access patterns, repeated authentication failures, unauthorised data modifications or policy violations.
- IIPs and RRMs may implement automated alerting capabilities to notify responsible personnel of potential security or compliance incidents, enabling timely investigation and response.
- IIPs and RRMs may leverage certified cloud-based service providers for identity, access management, and logging services where such platforms provide integrated authentication, authorisation and audit logging capabilities, provided that appropriate governance, oversight and validation controls are maintained.

Audit trail review

Minimum requirements

- IIPs and RRMs must establish and maintain processes for the regular review of audit trails to identify unauthorised actions, policy violations and suspicious or anomalous activity. Audit trail retention must comply with applicable regulatory requirements, including the five-year retention

period where applicable, taking into account system criticality, data sensitivity and a documented risk-based assessment. The scope and frequency of audit trail reviews must be defined through a documented risk-based approach considering system criticality, data sensitivity, transaction volumes, user population and regulatory impact. Audit trail reviews must detect indicators of risk, including unusual access patterns, repeated authentication failures, unauthorised data modifications and other deviations from expected behaviour or policy requirements. Findings from audit trail reviews must be documented, investigated where necessary and escalated to appropriate management levels. Corrective actions must be implemented without undue delay to address identified issues and reduce the likelihood of recurrence.

Best practices

- IIPs and RRMs may implement automated monitoring, correlation and analytics capabilities to enhance audit trail review effectiveness and support earlier detection of anomalous or suspicious behaviour.
- Review outcomes, investigations and corrective actions may be formally recorded in a consolidated record, with significant findings escalated promptly to management to support governance, oversight and the continuous improvement of control effectiveness.

Incident investigation

Minimum requirements

- IIPs and RRMs must establish and maintain formal procedures for the investigation of security incidents and policy violations to ensure consistent, structured and defensible handling of such events. Incident investigation procedures must cover the full life cycle of an incident, including detection, containment, evidence preservation, analysis, documentation of findings, implementation of corrective actions and reporting to internal management and, where applicable, competent regulatory authorities, in accordance with the notification obligations and timelines. Information disclosed to external parties must be relevant and proportionate to the purpose of the disclosure, while protecting sensitive details about affected systems, vulnerabilities and security measures. Incident investigations must be performed by appropriately trained and authorised personnel in accordance with documented procedures. Evidence handling must preserve the integrity and authenticity of relevant information to support investigative, operational and regulatory purposes. Investigation records must be retained in accordance with applicable legal, regulatory and contractual obligations and GDPR data minimisation principles.

Best practices

- IIPs and RRMs may establish dedicated or virtual incident response capabilities with clearly defined roles, responsibilities and escalation paths to support coordinated and efficient handling of security incidents.
- Regular training and awareness activities may be provided to personnel involved in incident handling and investigation to ensure the consistent application of procedures and improve investigative effectiveness.
- Periodic incident response exercises or simulations may be conducted to validate preparedness, improve coordination and enhance the organisation’s ability to respond effectively to security incidents.

Annex III provides operational guidance on accountability.

4.7. Reliability

Reliability refers to the assurance that information systems and data remain consistent, accurate and available throughout their operational life cycle. It reflects the ability of systems to perform their intended functions correctly and consistently, including under adverse conditions. Maintaining reliability requires the implementation of controls such as system monitoring, performance management, vulnerability and configuration management, error detection and correction, malware detection and response and

continuous improvement processes to ensure that systems and data remain dependable and trustworthy.

Minimum requirements and best practices

IIPs and RRMs must implement controls to ensure that systems and data operate consistently, accurately and predictably throughout their life cycle. These controls must support stable system performance, reduce the likelihood of errors or failures and enable continuous improvement based on monitoring and analysis.

System monitoring

Minimum requirements

- IIPs and RRMs must implement monitoring mechanisms to track system performance, availability and health based on system criticality and operational risk. Monitoring must provide visibility into operational and security indicators, including system uptime, response times, resource utilisation, error conditions and security-related events. Monitoring data must be collected continuously and analysed using a documented risk-based approach. Mechanisms must be in place to ensure that responsible personnel are notified when predefined thresholds are breached or when abnormal behaviour, failures or anomalies requiring attention are detected. Monitoring data must be retained in accordance with applicable legal, regulatory and contractual obligations and GDPR data minimisation principles. Unless otherwise specified by applicable requirements or justified by the nature and risk of the data, relevant monitoring records must be retained for five years.

Best practices

- IIPs and RRMs may use automated alerting and remediation capabilities to support timely responses to monitoring events and predefined operational issues. Such capabilities may include notifying responsible personnel, restarting services, restoring baseline configurations or managing resource constraints. Automated actions should be logged and periodically reviewed to ensure transparency and control.
- Predictive analytics may be used to analyse historical performance trends, resource utilisation, error rates and security events to anticipate potential failures or degradation and support proactive risk mitigation.

Vulnerability management

Minimum requirements

- IIPs and RRMs must establish and maintain formal procedures to identify, assess, prioritise and remediate vulnerabilities across systems, applications and infrastructure, integrating security considerations throughout the secure development and change life cycle. Vulnerability assessments must include vulnerability scanning and, where appropriate, based on system criticality, exposure and risk, penetration testing to identify exploitable weaknesses and assessment of the effectiveness of security controls. The scope and frequency of these activities must be determined through a documented risk-based approach and following significant changes to systems or infrastructure, where appropriate. Identified vulnerabilities must be prioritised according to their severity and potential impact and addressed within risk-based remediation targets or equivalent internal deadlines. Remediation must include patching, configuration changes, upgrades or compensating controls where immediate remediation is not feasible. Where remediation cannot be completed within the applicable target, the residual risk must be formally assessed and accepted by an authorised person, with documented justification, a defined validity period and appropriate compensating controls. Risk acceptance must be reviewed before expiry and whenever there is a material change in the risk. Remediation actions must be verified and documented to confirm that vulnerabilities have been effectively mitigated or resolved.

Best practices

- IIPs and RRMs may implement continuous or near real-time vulnerability scanning capabilities to detect emerging vulnerabilities promptly and reduce exposure to threats.

Configuration management

Minimum requirements

- IIPs and RRMs must implement configuration management procedures to ensure systems are securely and consistently configured throughout their life cycle. Configuration management must be applied based on system classification, data sensitivity and operational impact. Configuration baselines must be defined, approved, documented and maintained for in-scope systems, particularly for critical systems. Systems must be monitored to detect configuration drift, and any unauthorised or unintended configuration changes must be identified and remediated without delay. All configuration changes must be managed through the formal change management process detailed in Section 4.2, including appropriate testing prior to deployment into production environments. Configuration documentation must be maintained and kept up to date to support operational stability, troubleshooting, auditability and compliance.

Best practices

- IIPs and RRMs may implement automated configuration management tools to enforce secure baselines, detect configuration drift continuously and support-controlled remediation of deviations.

Error detection and correction

Minimum requirements

- IIPs and RRMs must implement mechanisms to detect, log, analyse and correct errors affecting systems, applications and data throughout their operational lifecycle. Error detection is required across data processing activities, data transmission and system operations based on system criticality and data classification. Detected errors must be recorded and analysed to identify trends, recurring issues and potential root causes. Where errors are identified as systemic or recurring, they must be addressed through appropriate corrective actions, including technical fixes, process adjustments or compensating controls where necessary. Verification activities must confirm that identified errors have been resolved and do not reoccur, and outcomes must be documented.

Best practices

- IIPs and RRMs may conduct formal root cause analysis for significant or recurring errors to identify underlying systemic issues and implement preventive measures to reduce recurrence and improve system resilience and reliability.

Capacity planning

Minimum requirements

- IIPs and RRMs must establish and maintain capacity planning procedures to ensure systems are provisioned with sufficient resources to meet current and anticipated operational demand. Capacity planning must be based on system and data classification and service criticality. Capacity planning must consider factors such as data growth, user volumes, transaction throughput, processing requirements and infrastructure constraints. Capacity review frequency must be defined through a documented risk-based approach considering system criticality, historical trends and changes in demand or usage. Where capacity risks are identified, resource scaling or optimisation measures must be implemented to prevent performance degradation, service disruption or reduced system reliability.

Best practices

- IIPs and RRMs may establish continuous improvement processes to assess system performance and capacity metrics to identify bottlenecks and optimisation opportunities.
- Findings from capacity analysis may be used to implement improvements and support ongoing enhancement of system performance, resilience and scalability.

Annex III provides operational guidance on reliability.

5. Data validation and submission processes

According to Article 12 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, IIPs must have data validation systems in place to comply with the principles and follow the processes set out in Articles 22, 23 and 24, while RRMs must have data validation systems in place to comply with the principles and follow the processes set out in Articles 26, 27 and 29.

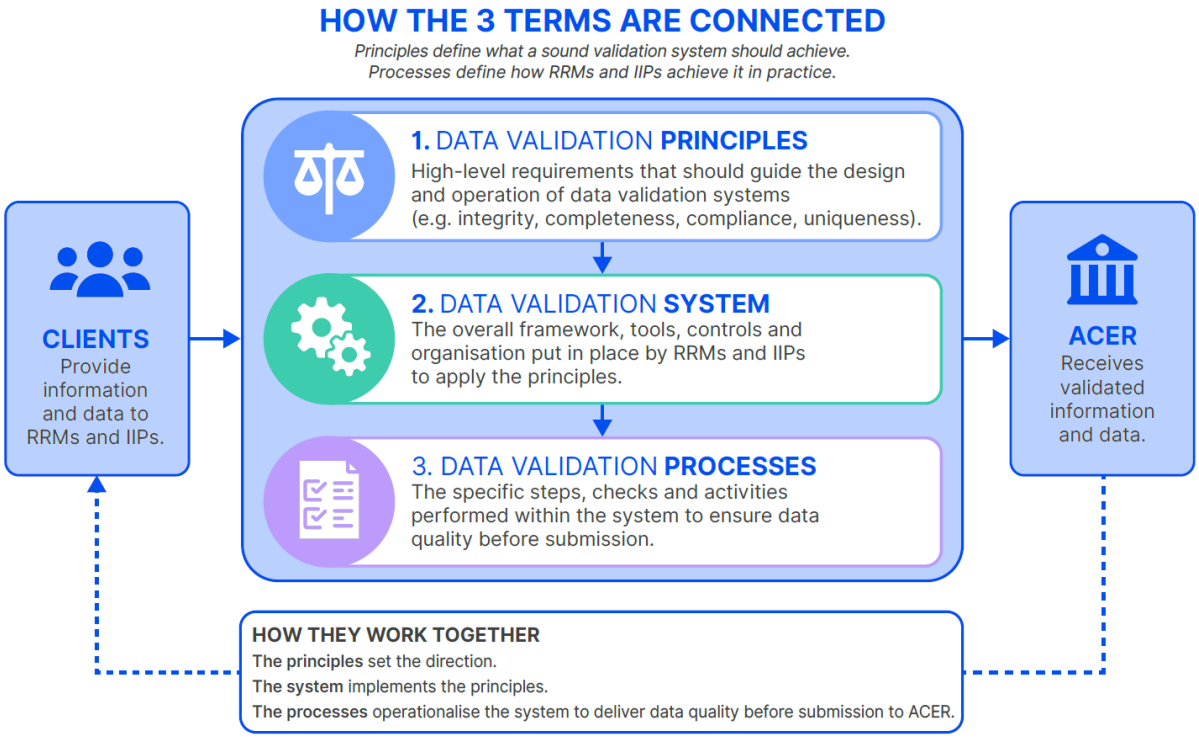
This chapter details the data validation systems that IIPs and RRMs need to have in place to comply with the principles and processes set out in the mentioned articles. First, the principles and validation processes to which IIPs and RRMs must adhere are explained. This is followed by the pre-submission section that provides a step-by-step guide on how to detect and handle invalid data before it is sent to ACER. Finally, the post-submission obligations and client notification requirements are explained.

Data validation principles. Refer to high-level requirements that should guide the design and operation of the IIPs'/RRMs' data validation systems.

Data validation processes. Refer to checks and steps that IIPs and RRMs should perform to apply the data validation principles in practice. IIPs and RRMs must implement processes to detect, communicate and correct errors attributable to their own processes, facilitate the correction and resubmission of data by the responsible clients, and register invalid data prior to submission to ACER in accordance with Articles 23 and 27 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. These processes must ensure that all inside information reports to be published on the platform and submitted to ACER and data records to be reported to ACER are accurate, complete and traceable, while facilitating timely feedback to clients and supporting efficient correction and resubmission. Automated systems should be used wherever feasible to facilitate detection and notification of errors, minimise delays and maintain full auditability for regulatory oversight.

Figure 1 explains the three terms (data validation principles, systems and processes) and their dependency.

Figure 1. Data validation principles, systems and processes



Validation systems and processes are required to be implemented during the pre-submission of inside information reports and data records to ACER and need to be applied consistently across all IIPs/RRMs

clients. IIPs and RRMs must ensure that validation processes are documented, transparent, and applied in a non-discriminatory manner.

The objective of data validation is to ensure that information reported to ACER and published on IIPs is accurate, complete, consistent, unique and compliant with the reporting manuals.

5.1. Data integrity

Inside information reports and data records should remain complete and accurate throughout the validation and submission process. IIPs and RRMs should ensure that any transformation is authorised by the relevant client, controlled and traceable and does not result in unintended alteration, omission or corruption.

Validation process to ensure data integrity

IIPs and RRMs are required to implement controls to ensure that the inside information reports or data records submitted by clients are not unintentionally altered, omitted or corrupted and that their integrity is maintained throughout the processing and submissions of inside information reports or data records to ACER. These controls are defined in Chapter 4 of this guidance.

5.2. Validity and consistency

Validity means that the reported data meet the requirements that ACER defined in the technical manuals while consistency ensures alignment with requirements set in the reporting manuals.

All required data fields must be populated correctly and must comply with the applicable electronic formats and reporting manuals. Where feasible, IIPs and RRMs must prevent the submission of duplicated inside information reports or data records to ACER.

Validation processes to ensure validity and consistency

Before submitting data to ACER, IIPs and RRMs are required to carry out data quality checks to ensure that all reportable inside information report or data record comply with the following.

- **Technical validation.** To comply with the principle, IIPs and RRMs need to comply with the requirements set out in ACER's technical manuals, which are provided by ACER upon signature of an NDA. Examples of these requirements include:
  - electronic formats compliance;
  - file naming convention validation;
  - signature and encryption validation;
  - data formats, file contents and file size.
- **Field level validation.** Defined in Annex V to this guidance (REMIT validation rules document), IIPs and RRMs are required to implement validation rules for data for which they are authorised to report.

  Field-level data quality validation refers to more in-depth validation checks performed on the data to ensure its internal consistency and logical coherence. These checks go beyond verifying the presence or format of individual fields and assess whether the relationships between fields are correct according to reporting manuals and whether the data, as a whole, is meaningful, consistent and verifies the relevant content against the European Register of Market Participants and other lists published by ACER. IIPs and RRMs can refer to the REMIT validation rules document (Annex V to this guidance) to identify the validation checks to be performed before submitting inside information records or data records to ACER and before publishing inside information records.

  The REMIT validation rules document is a living document that is maintained and updated on an ongoing basis by ACER. Updates may include the addition, removal and activation/deactivation of specific rules, the refinement of validation logic, including exceptions or conditional checks, and the clarification or correction of rule definitions and implementation specifications.

  In the event a validation rule is eligible for IIPs or RRMs to implement in their systems, ACER will set a deadline that will depend on the complexity of the rule and that must not exceed one year upon ACER's notification, unless duly justified. IIPs and RRMs should ensure that validation rules

are implemented in an appropriate way depending on the overall design of their systems and the data type they are reporting. While the method of implementation is at their discretion, they must ensure that data quality issues are properly detected, notified to their clients and, where needed, stored in the register of invalid data.

Additionally, IIPs and RRMs must implement automated duplicate detection mechanisms to identify and prevent a double report or record submission. Such mechanisms are based on unique identifiers and key data fields that define specific validation rules stated in the REMIT validation rules document.

IIPs and RRMs may implement additional validation rules in their systems beyond those included in the REMIT validation rules document, provided they align with ACER's manuals and REMIT regulatory requirements. ACER encourages IIPs and RRMs to develop validation rules at their own initiative, as part of continuous efforts to improve data quality.

- **Validation requested by ACER for individual RRMs** (e.g. where an identified data quality issue is specific to a particular organised marketplace (OMP)).

  Unlike rules described in the REMIT validation rules document that are common for all RRMs reporting the same or similar data in the electronic format, additional rules may be identified based on the content of data that is specific to one RRM or based on the style of reporting of that RRM.

- **Detection of anomalies**

  Where feasible and appropriate, RRMs are encouraged to implement systematic monitoring mechanisms to detect significant anomalies in data submissions, particularly when there is a clear and consistent expectation of reporting by the client. Such monitoring helps ensure data completeness. For example, if an RRM consistently receives approximately 10 000 records per day from a given client, a sudden and unexplained absence of data should warrant further investigation.

  When an anomaly is detected, notifying the client about the absence of data can help clarify the situation, while internal checks should also be conducted to rule out system-related causes.

  This monitoring applies to RRMs reporting on behalf of third parties for which a predictable reporting pattern exists. Monitoring efforts should remain proportionate, focusing on significant deviations rather than routine fluctuations and should only be applied when practical and justified by the circumstances.

5.3. Uniqueness

IIPs and RRMs must prevent reporting of duplicated inside information reports and data records originating from clients' IIPs/RRMs.

Validation processes to ensure the uniqueness of an inside information report

IIPs' validation systems must detect whether the inside information to be disclosed has already been published by the same IIP, as per Article 22(a) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. It is worth noting that once the inside information has been disclosed by a market participant and published on an IIP, it is then considered public information and does not meet the criteria of 'inside information' defined in Article 2(1) of the REMIT Regulation.

At the same time, the duplication check should be carefully designed so as not to inadvertently prevent market participants from disclosing inside information relating to events that may share similar or identical characteristics with previously published messages. In this context, ACER considers that a proportionate approach is to define duplication based on a 'unique event key', composed of a specific combination of data fields, ensuring that genuinely new disclosures are not blocked while still preventing exact duplicates. IIPs should refer to the REMIT validation rules document to implement the required rules in order to detect duplicated inside information reports.

Validation processes to ensure the uniqueness of a data record

RRMs' validation systems are required to detect duplicated data records before submission to ACER, irrespective of whether the duplicates originate from their own clients or systems, but are not responsible for duplicates submitted via other RRMs. Additionally, clients should receive clear feedback if a submission is rejected due to duplication, including references to the original record, and should be guided on how to amend their submission if necessary.

RRMs should refer to the REMIT validation rules document to implement the required rules in order to detect duplicated data records.

5.4. Reconciliation

This chapter refers to the obligation of RRMs to reconcile the data records received from their clients that are related to transactions other than orders to trade in the wholesale energy market and **that are concluded or executed on an OMP**. RRMs need to verify and ensure that corresponding records from both counterpart transactions are available prior to reporting, as a measure to ensure the completeness of the order book reported information. Bilateral transactions are thus excluded from the reconciliation obligation.

RRMs have to reconcile transactions as per Article 3 of the REMIT Implementing Regulation but excluding transactions concluded as a result of single intraday coupling, an auction or primary capacity allocations.

RRMs do not need to reconcile data records that have been categorised as erroneous by the RRM client.

Validation processes to ensure reconciliation

The reconciliation must be carried out by verifying whether RRMs have received a corresponding data record related to the other party to the transaction.

If the reconciliation was not successful, RRMs are required to request to the OMP to provide the missing corresponding data records from the other party to the transaction, as stated under Article 28(3) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. Prior to submitting the data record to the Agency, RRMs are also required to provide the OMP with the unique transaction identifier, the ID of the market participant or the counterparty and the transaction timestamp of the relevant transaction, as stated under Article 28(2).

5.5. Authentication

The source of information must be verifiable, confirming the identity of the IIP or RRM client submitting the inside information report or data record or the identity of any other person submitting information on behalf of the IIP or RRM client.

Validation process to ensure authentication

All submissions to ACER must originate from authenticated and authorised sources to ensure data integrity and prevent unauthorised or fraudulent submissions. IIPs and RRMs are responsible for maintaining full traceability of the information back to the responsible client. A unique identifier, preferably the ACER or EIC code, should be used to link the information to its source.

Authentication and identity verification checks must comply with the minimum requirements set under Chapter 4 of this Guidance. Upon request, ACER may contact the IIP or RRM to verify the source of the submitted data.

Note that this validation process does not apply where an RRM and its clients belong to the same legal entity, as indicated in Article 26(c) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.

5.6. Timeliness

RRMs should report data records to ACER as soon as technically possible and always within the timelines set out in the REMIT Implementing Regulation. IIPs should report inside information reports to ACER within no later than one day following the publication of the inside information in their platforms, as stated in Article 20 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.

Validation process to ensure timeliness

To avoid disruptions to the process and reporting deadlines, IIPs and RRMs should design appropriate corrective mechanisms and technical arrangements, provided that the necessary data is received from

clients without delay. Systems should be configured to flag potential delays and fallback mechanisms to address technical failures without breaching deadlines.

Where possible, RRM clients should be instructed to provide data with sufficient lead time to allow for validation, while pre-validation checks should minimise last-minute corrections.

IIPs or RRMs must notify ACER of systematic or material delays (e.g. recurring late submissions, technical failures) via disruption reports (please refer to Chapter 7 below).

5.7. Traceability

A register of invalid data must be maintained for 18 months from the date of submission to the IIP or RRM, and accessible by ACER as per Articles 23 and 27 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. If the invalid data was corrected and successfully resubmitted to ACER, it may be removed from the register. Note that corrections are considered valid for submission to ACER and should therefore be kept for a period of five years (Article 17(3)(f) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs).

Validation process to ensure traceability

A register must be maintained to log all invalid data received from clients or identified during validation, with each entry timestamped and retained for at least 18 months from the date of submission, as stipulated in Articles 23 and 27 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. IIPs and RRMs should refer to Section 5.10 of this guidance for further details on the content of such a register.

5.8. Transparency

IIPs and RRMs must either provide each client with secure access to, or directly transmit to them, all information regarding their own submitted data. When errors are detected, IIPs and RRMs must notify the affected clients and provide the necessary tools and information to resolve their reporting issues.

Validation process to ensure transparency

IIP and RRM systems should be designed to provide clients with secure access to their submitted inside information reports or data records. In cases where invalid data is detected, IIPs and RRMs are required to provide their clients with detailed information regarding the validation results and request them to resubmit the inside information report or data record to the IIP or RRM with the necessary corrections or missing data.

After receiving such corrections, the IIPs or RRMs are required to submit them to ACER as soon as technically possible.

5.9. Pre-submission process

While the principles and processes outlined above specify what validations must be performed, they must be executed in a structured, multi-stage order to be effective. This section provides a step-by-step guide focusing on a core subset of principles to illustrate the mandatory sequence for detecting and handling invalid data prior to their submission to ACER.

Data is considered invalid when it fails to comply with the core principles and processes of data integrity: validity, consistency, uniqueness and authentication. Invalid data must not be submitted to ACER nor published on an IIP.

Examples include:

- a data record or inside information report that does not comply with ACER's electronic formats, for example, due to missing mandatory fields or values not technically supported by design;
- a data record or inside information report that fails one of the field-level validation rules defined in the REMIT validation rules document;
- unregistered or unauthorised clients that manage to submit data to the IIP or RRM, indicating a potential security breach;

- the duplication of inside information reports or data records.

When invalid data is detected, IIPs and RRMs must interact with their clients to:

1. notify them promptly and without undue delay, indicating the specific data reports or inside information records that have been detected as invalid;
2. provide them with the reasons the data was detected as invalid; feedback needs to be communicated in a manner that allows clients to take corrective action efficiently;
3. request that they correct the invalid data and provide them with instructions on how to submit a new data record or inside information report or correct the one that failed validation, and the IIPs and RRMs should grant access to support channels for exceptional cases requiring further clarification.

Upon receiving the required corrections from their clients, RRMs need to submit the data record to ACER as soon as technically possible, as per Articles 23(1) and 27(1) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. This ensures timely compliance and minimises the risk of delayed submissions. In the case of IIPs, once an inside information report has been corrected, it must be published on the IIP as soon as possible and submitted to ACER within one day following its publication.

Note that there might be cases in which an inside information report or data record that is stored in the register of invalid data does not need correction (e.g. a duplicated record or unauthorised submission). In that case, such an inside information report or data record may be kept in such a register for 18 months.

The aforementioned provisions regarding interactions with clients do not apply when the RRM and its clients belong to the same legal entity. However, validation processes remain applicable, and any necessary corrections must be submitted to ACER as soon as technically possible and within the deadlines stipulated by the REMIT Implementing Regulation.

In addition, when invalid data is detected, IIPs and RRMs are required to retain it in the register of invalid data until the client provides the corrected inside information report or data record. The following section describes such a register in further detail.

5.10. Register of invalid data

The register of invalid data applies to all pre-submissions that have been received by an IIP or RRM but subsequently identified as invalid and therefore not reported to ACER nor published on an IIP. RRMs must include the data record in the register of invalid data only when the applicable deadline for reporting as per the REMIT Implementing Regulation has elapsed. In accordance with the requirements set out in Articles 23(2) and 27(2), IIPs and RRMs must maintain a register of such invalid data, which must include at a minimum:

- the data type intended to be reported to ACER and, where technically possible, the invalid data itself, in the electronic formats defined by ACER;
- the identity of the source of information or the client, except in cases where the data has been identified as incorrect because its source could not be authenticated;
- the specific reason(s) for invalidation;
- the date of detection of the invalid data and the resubmission status.

The register of invalid data must ensure that all subsequent corrections related to the same submission are clearly linked and traceable through the IIPs' or RRMs' processes. This should allow for full transparency of the correction process, from initial rejection to final acceptance of the data.

Registers should be maintained for at least 18 months and be accessible to ACER, which may notify the relevant NRAs of instances in which IIP or RRM clients submitted invalid data, along with the identity of such clients. ACER may request, on ad hoc basis, a set of data under such a register via the established communication channels. In such cases, the IIP or RRM is required to provide the requested data within two weeks. This timeline may be extended in duly justified cases, depending on the volume of the impacted data.

Once invalid data has been corrected and successfully resubmitted to ACER without any errors, the invalid data entry in the register may be removed. The corrected submission – now considered valid – is then subject to the five-year retention requirement under Article 17(3)(f) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. There is no obligation for the IIP or RRM to retain the original invalid data after this point.

It should be noted that, where pre-submission validation checks deployed by IIPs or RRMs (e.g. built-in validation within the interface with clients) inhibit the successful submission of an inside information report to the IIP or data record to the RRM – thereby preventing the creation or retention of any record – such instances must not be captured within the register of invalid data.

5.11. Post-submission processes

Articles 24 and 29 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs set out the post-submission obligations of IIPs and RRMs. This section describes the processing of the receipt issued by ACER after the inside information reports or data records are submitted, how to manage and correct rejections and how to notify clients following the issuance of ACER's receipt. In addition to these post-submission processes, IIPs and RRMs are subject to a record-keeping obligation (five years) under Article 17(3)(f) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.

Following submission, ACER processes the received inside information report or data record and provides the submitting IIP or RRM with a receipt. Such receipt contains, inter alia, information whether the submission was accepted or rejected and, where applicable, the reason(s) for rejection. Note that the receipt is the only formal confirmation that ACER has successfully received and processed the submission.

IIPs and RRMs are responsible for ensuring that the receipt is accurately processed and the inside information report or data record linked to the corresponding submission.

In cases where ACER issues a receipt indicating a rejection, IIPs and RRMs are expected to establish and maintain procedures to address errors identified in their submission and, where needed, resubmit the corrected inside information report or data record to ACER. IIPs and RRMs should always take corrective measures to try to resubmit the data successfully in cases where they have received a rejection from ACER or explicit instructions to do so (e.g. after opening a support ticket if no receipt is issued within 24 hours).

IIPs and RRMs are responsible for determining whether the error originated from their own systems or processes or from the inside information report or data record provided by their clients.

Where an error is attributable to the IIP or RRM, they are responsible for correcting the report or data record and submitting it to ACER within five working days from the date of the receipt issuance by ACER, as per Articles 24(2) and 29(2) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. Where compliance within this time frame is not possible, a disruption report (see Chapter 7 of this guidance) needs to be produced, providing a justification for the delay and, if considered duly justified by the IIP/RRM, a request to extend the timeline. ACER will then assess the request and determine whether an extension may be granted in duly justified cases (e.g. due to a disruption as described in Chapter 7).

Where an error is attributable to the client, the IIP or RRM needs to provide appropriate guidance to their clients on the necessary corrections and request that the amended data be resubmitted without undue delay. The IIP or RRM is then responsible for resubmitting the amended data to ACER as soon as it is received from the client, and in any case within 10 working days from the date of the receipt issuance by ACER, as per Articles 24(3) and 29(3) of the Delegated Regulation for the authorisation of IIPs and RRMs. Where compliance within this time frame is not possible, the client can, in duly justified cases, request an extension from ACER through its IIP/RRM providing a justification for the delay. ACER will then assess the request and determine whether an extension may be granted in duly justified cases. If a client fails to correct data within 10 working days, the RRM is not required to create a disruption report.

Note that there may be instances where ARIS issues a rejection receipt, but, after assessment by the IIP or RRM, no resubmission is required. This includes cases such as the erroneous resubmission of a record previously accepted without errors, where ARIS identifies the submission as duplicate.

To submit corrected inside information reports or data records that were previously submitted and rejected by ACER's system, IIPs and RRMs must follow the procedures set out in ACER's technical manuals.

Lastly, in cases where the inside information report is flagged in accordance with Article 24(4) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, IIPs must refer to Chapter 6 of this guidance.

5.12. Client notification mechanisms and communication requirements

This section of the guidance is not applicable to RRMs that do not have clients and report data records to ACER solely on their own behalf.

IIPs and RRMs must implement automated notification systems to ensure timely communication with their clients following interaction with ACER. These systems should, at a minimum, notify clients when the inside information report or data record has been rejected by ACER and the error is attributable to the client.

For both accepted and rejected records, IIPs and RRMs must provide clients with:

- a copy of the inside information report or data record as submitted to ACER;
- the content of the receipt issued by ARIS in a readable format;
- access to pre-validation and ARIS validation results.

Additionally, for rejected records, if the error is attributable to the client, IIPs and RRMs must also comply with the requirements set out in Section 5.9 of this guidance.

RRMs reporting liquified natural gas (LNG) market data must **provide** their clients with the above as soon as possible.

IIPs and RRMs must act as the primary point of contact between ACER and their clients, ensuring that clients are duly informed of any errors, non-compliance or required corrections. Appropriate communication channels should be established to facilitate efficient information exchange.

Where necessary, and in accordance with Article 29(5) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, ACER may contact clients directly for clarification purposes, particularly in relation to LNG market data.

6. The flagging process for IIPs

The timely and effective disclosure of inside information is an obligation under Article 4(1) of the REMIT Regulation. While Article 12(3) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs generally requires that IIPs submit only fully validated reports to ACER, Article 24(4) introduces a derogation to ensure that the inside information is published without undue delay – even when certain details may require further clarification.

This chapter outlines the flagging process, a mechanism that allows IIPs to publish and submit inside information reports that may require further clarifications from the IIP client following ACER's indication and in collaboration with their clients.

An inside information report that is flagged refers to a report that may require further clarifications, provided that the content in the reports is relevant for market participants' trading choices according to the REMIT Regulation. The published inside information report should be flagged, where applicable, in accordance with the logic defined in the REMIT validation rules document**.**

Flagged reports only concern reports requiring further clarification **on the client side**. A report that is flagged needs to be published on an IIP as close to real time as possible and submitted to ACER no later than one day (i.e. 24 hours) following the disclosure.

Flagged reports are not considered invalid, and no error notification is sent to the IIP after submission to ACER. ACER has defined a list of minimum requirements that defines when an inside information report is invalid (and hence cannot be published and submitted) in Chapter 5 of this guidance.

The following principles apply.

- Rejection rules detecting invalid data must take precedence over flagging rules. That is, only reports that successfully pass all rejection validations can be published on the IIP and submitted to ACER with a flag (if applicable), specifying the reason(s) for flagging.
- The existence of a flag does not exempt IIPs or their clients from providing further clarifications, if relevant. After the inside information report has been published, corrections cannot be made on the same inside information report, but only in subsequent publications (versions) relating to the same event.
- The field-level validation rules defined by ACER represent minimum requirements. As part of their service offering to clients, IIPs may implement flagging rules as rejections in their systems, unless explicitly communicated by ACER, provided that such rules are supported by the applicable manuals and that clients are sufficiently informed that these rules form part of the IIP's service offering. Such rules may be applied where they contribute to higher data quality standards. Additionally, an IIP must not apply a rule as a flag if ACER has defined it as a rejection.
- IIPs should notify clients of flagged reports. Where possible, this notification should occur during the submission process (e.g. pop-up warning for manual submissions), allowing clients to correct the report before publication. In all cases, clients have to be informed of the flag immediately after publication of the inside information report on the IIP, including the reason for flagging.

Table 3 provides an overview of the differences between a rejection (invalid data) and a flag.

Table 3: Differences between rejection and flag

	Rejection	Flag
Validation outcome	Validation failed	Validation flagged
Publication by the IIP	No	Yes
Submission to ACER	No	Yes

Legal basis	Article 12 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs	Article 24(4) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs
Inclusion in the register of invalid data	Yes	No
Client follow-up	Client should correct and resubmit the information to the IIP.	Provide relevant clarification or confirmation that the flagged report is correct to the IIP, upon ACER's request issued to the IIP. Corrections may also be made upon client's initiative.
IIP Follow-up	IIP is required to inform its clients and request that they resubmit the information.	Provide information to the client that the report is flagged and the reason(s) for flagging. In the event the information needs to be corrected following ACER's indication, IIPs must collaborate with their clients to correct it.

6.1. Display of flags on the IIP website

IIPs are required to make flagged inside information reports clearly visible to users of their platforms. The following requirements must apply.

- When an inside information report is published as a flagged urgent market message (UMM), a visible indicator (e.g. a visual flag with the flagging message displayed when users hover over the corresponding visual flag) needs to be displayed and easily identifiable by users. IIPs should additionally make sure that the flag does not create uncertainty for IIP users (e.g. by introducing a disclaimer stating that the UMM remains valid under the REMIT Regulation).
- IIPs must allow users to filter and download events that are flagged on their platforms. Such functionality must be provided free of charge, as established by Article 19(4) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.
- The indicator needs to clearly distinguish the flagged UMMs from non-flagged UMMs both in the IIP and when the information is exported to any other format. In case of exported UMMs, an indicator (Yes/No) should reflect whether the UMM is flagged, and, where applicable, the corresponding flagging codes and flagging messages must be reflected.
- The applicable flagging message, as defined in the REMIT validation rules document**,** must be publicly available to users to easily identify the reasons for the flag. Where a report is flagged for multiple conditions, all applicable warning messages need to be displayed in a consolidated manner (e.g. as a list under the visual indicator).
- Any subsequent update or correction of a flagged UMM would be published as a new version of the existing event and would therefore be validated again by the IIP. The flag on the previous UMM needs to remain published.

7. Unplanned downtime or disruption

This chapter clarifies under which circumstances IIPs and RRMs should notify ACER of unplanned downtime or disruptions, along with the format and content of these notifications.

IIPs and RRMs should also note that the guidance provided below does not address their obligation under Article 18(1) and 18(2) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs to establish and implement processes for the notification to their clients of any planned maintenance, unplanned downtime or other disruptions affecting their services.

In accordance with Articles 11 to 29 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, IIPs and RRMs must implement and maintain policies, contingency plans and arrangements to ensure the completeness, accuracy and timeliness of their reporting and to ensure transparency about their governance structure, compliance policies and measures to prevent conflicts of interest.

In the context of this guidance, unplanned downtime or disruption refers to any event, internal or external, that limits or prevents the IIP or RRM from complying with the requirements laid down in Articles 11 to 29 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. This includes any unplanned situation that compromises, totally or partially, the completeness, uniqueness, compliance, timeliness, traceability, availability, authenticity, quality, integrity or confidentiality of stored, transmitted or processed inside information reports and data records, or of the services offered by, or accessible via, the IIP and RRM systems.

If unplanned downtime or disruptions of their compliance as laid out in these articles occur, IIPs and RRMs should, as per Article 18(3) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs:

- **notify ACER within 24 hours of becoming aware of the event (disruption information);**
- **within one month of becoming aware of the event**, **IIPs and RRMs should also submit a report to ACER detailing the causes and the actions taken to prevent any reoccurrence.**

IIPs should note that ACER will use the disruption information as part of its IIP's assessment of compliance with the availability requirements laid down in Article 17(7) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, and that it falls within the IIP's compliance obligation to report such unplanned downtime or disruptions whenever the conditions of Article 18(3) are met, irrespective of whether the disruption results in the breach of the 99.5 % minimum availability level.

To enable harmonised reporting of notification obligations in accordance with Article 18(3) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, ACER is mandated by Article 9(e) to provide guidance on the format of the report on unplanned downtime or disruption.

For this reason, it developed the disruption report form, which distinguishes several disruption scenarios:

1. disruption to the submission of an inside information report or data record to ACER and/or disclosure of inside information;
2. disruption to the collection of inside information reports or data records from clients;
3. disruption to the data quality of submitted inside information reports or data records;
4. security incident notifications;
5. operational disruptions of the IIP/RRM's platform.

The content of notifications submitted via the disruption report form is presented in Annex IV to this guidance.

The disruption report form should not be used to inquire about or request support regarding the usage of ARIS, such as:

- the application's functionality;
- data transmission and receipts;
- interfaces and schemas / data types;
- connectivity;
- user account;

- certificates; and
- other technical aspects of reporting.

If IIPs and RRMs experience issues with ARIS and require support from ACER, they should contact the ARIS Service Desk.

If ARIS prevents RRMs and/or IIPs from submitting (partially or completely) inside information reports or data records to ACER, they should determine whether the issue originates from their own systems or processes. If the issue is confirmed to be on the RRM's or IIP's side within 24 hours of becoming aware of the disruption, they must notify ACER via the Disruption Report Form. If the issue is confirmed to originate on ACER's side or cannot be confirmed to originate from the RRM's or IIP's systems or processes within 24 hours of becoming aware of the disruption, they should contact the ARIS Service Desk for further assistance, and they do not need to notify ACER via the disruption report form. The different disruption scenarios are described in more detail below, including the circumstances in which each scenario should be used and the types of events it covers.

7.1. Disruption to the submission

If IIPs or RRMs encounter a total or partial disruption affecting the submission of inside information reports or data records to ACER and/or, in the case of IIPs, the disclosure of inside information to the public, while remaining able to collect the relevant information from their clients, they should open a disruption through ACER's disruption report form, selecting Scenario 1.

For IIPs, the use of the backup infrastructure (or external provider) forms part of the contingency arrangements required under Article 17 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs and, by itself, does not constitute a reportable disruption. As long as the backup infrastructure (or external provider) ensures the continued disclosure of inside information and the submission of inside information reports to ACER, the IIP remains compliant with the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, and no disruption notification is required.

During the downtime, the IIP or RRM should take appropriate measures to properly secure the data it will collect and store, which should be properly disclosed and/or submitted to ACER after the downtime period is over. A proper sequence of submissions should be preserved.

Nevertheless, in instances where an IIP client has disclosed inside information on another IIP in accordance with Article 17(8) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, ACER understands that the client should not publish the same information again on its primary IIP, as this would lead to duplicated publications of the same inside information on two platforms. If the client instead disclosed the information on its own website, the primary IIP should, upon restoration of its services, publish the information on its platform as soon as technically possible, in accordance with Article 17(9). In respect to Article 17(9), ACER understands that the IIP clients should provide the necessary information to the IIP after the services are restored.

This scenario may apply to disruptions affecting, among other things, the requirements laid down in Articles 17, 19, 24 and 29 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, depending on the nature and cause of the disruption.

7.2. Disruptions to the collection

If IIPs or RRMs encounter a disruption affecting their ability to collect inside information reports or data records from their clients, they should report the incident using Scenario 2 of ACER's disruption report form. This scenario applies when the entity is unable, partially or entirely, to receive or retrieve the inside information report or data record that is required for subsequent disclosure or submission to ACER.

IIPs or RRMs should inform their clients that they have to preserve and store the inside information reports or data records themselves, preferably in the standards and electronic formats defined by ACER. Notwithstanding the IIP clients' obligation to publish inside information on their own website or use another IIP to disclose it, during an IIP and its backup unavailability.

This scenario may apply to disruptions affecting, among other things, the requirements laid down in Article 15 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, depending on the nature and cause of the disruption.

7.3. Disruptions to the data quality

Scenario 3 applies to data quality issues identified **after** the inside information reports or data records have been disclosed and/or submitted to ACER. Where an IIP or RRM becomes aware that an inside information report or data record already disclosed or submitted does not comply with one or more of the data quality requirements laid down in the Delegated Regulation for the authorisation and supervision of IIPs and RRMs (e.g. completeness, accuracy, validity, consistency or absence of data corruption), the IIP or RRM should notify ACER using Scenario 3 of ACER's disruption report form.

By contrast, where data quality issues are identified **before** submission to ACER, IIPs and RRMs should follow the data validation principles and processes described in Chapter 5, 'Data validation principles and submission processes', of this guidance. Accordingly, invalid data should not be submitted to ACER, and no disruption notification is required when the data quality issue is identified prior to submission, as the relevant information should be corrected before submission. **The only data quality issue that needs to be notified via the disruption report prior to the submissions of data records or inside information reports is a timeliness breach attributable to the IIP or RRM**, as the applicable reporting deadline cannot be rectified before submission.

Following the notification of a disruption under this scenario, the IIP or RRM is expected to identify and resolve the root cause of the issue and, where necessary, coordinate with ACER on any corrective actions, including the need for the resubmission of the affected inside information report or data record.

This scenario may apply to disruptions affecting, among other things, the requirements laid down in Articles 11, 20, 22, 24, 26, 28 and 29 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, depending on the nature and cause of the disruption.

7.4. Security incident notification

If IIPs or RRMs experience a security incident, they should report it using Scenario 4 of the disruption report form. This scenario applies in cases such as cyberattacks, unauthorised access, data breaches or other events compromising information security, regardless of whether reporting or disclosure services remain operational.

IIPs and RRMs should keep in mind that the reporting timeline for security incidents differs from the general disruption notification timeline described in this chapter of the guidance and set out in Article 18(3) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. Pursuant to Article 14(2), IIPs and RRMs must:

- notify ACER within 24 hours of becoming aware of the incident;
- notify affected IIP or RRM clients, where applicable, within 48 hours of becoming aware of the incident;
- provide ACER with the initial assessment within 72 hours of becoming aware of the incident; and
- submit a detailed incident report to ACER within one month of becoming aware of the incident, outlining the nature of the incident, the remedial measures taken and the actions implemented to prevent recurrence.

This scenario may apply to disruptions affecting, among other things, the requirements laid down in Articles 13 and 14 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, depending on the nature and cause of the disruption.

7.5. Operational disruptions of the IIP's/RRM's systems

If IIPs or RRMs are able to disclose and/or submit inside information reports or data records to ACER but are not meeting one or more operational or system-related requirements governing the functioning of their system or reporting infrastructure, as outlined in the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, they must report the situation using Scenario 5 of the disruption report form. This scenario applies where deficiencies affect the proper operation, controls or functionalities of the system, such as source authentication, automated alert systems, communication channels with clients, filtering and download functionalities for disclosed information, consistency of the information made available through different access channels, or the linking of related disclosures, even if the reporting or disclosure of information continues.

In such cases, the IIP or RRM should continue to disclose and/or submit the inside information report or data record unless this represents significant risks to information security or unless ACER requests that they temporarily stop doing so.

Where an RRM and its clients belong to the same legal entity (self-reporting RRMs), the RRM should note that Scenario 5 does not apply to them. The Delegated Regulation for the authorisation and supervision of IIPs and RRMs exempts this type of RRM from the obligations covered by this scenario, and, consequently, disruptions affecting those obligations do not require notifying ACER.

This scenario may apply to disruptions affecting, among other things, the requirements laid down in Articles 19, 22, 23, 24, 26, 27 and 29 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, depending on the nature and cause of the disruption.

8. Annual report by RRMs

The purpose of this chapter is to detail the format, content and timing of the annual report that RRMs are required to submit to ACER, in order to support the supervision of their activities. The high-level requirements of this report are set out in Article 33 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs.

In accordance with Article 33(4) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, where ACER considers that the annual report does not comply with the requirements set out in Article 33, ACER may request that the RRM amend and resubmit the annual report, including any clarification or corrected information considered necessary. The RRM must submit the amended annual report within 30 working days from receipt of ACER's request.

Where, during the relevant reporting period, an RRM did not identify any invalid data records requiring follow-up with its RRM client(s) for correction or did not report any bilateral trades on behalf of a non-client market participant, the corresponding sheet(s) of the annual reporting template may be left empty. Likewise, where an RRM and its clients belong to the same legal entity (self-reporting RRMs), the RRM should note that it is not required to report the number of corrected invalid data records or their non-client counterparties in bilateral trades.

Beyond supporting compliance with Article 33 of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs, the annual report provides ACER with a structured overview of RRMs' validation and reporting activities and improves ACER's visibility over recurring reporting issues affecting market participants. This information supports a more targeted supervisory approach by enabling ACER to identify market participants with persistent reporting deficiencies and to focus follow-up activities where they are most needed, thereby contributing to the overall effectiveness of the REMIT reporting framework.

8.1. Timing and frequency

The annual report must cover RRM activities during a full calendar year, understood as the period from 1 January to 31 December (the 'reference year'). The first reportable year is the first complete calendar year following the date on which the RRM receives confirmation of its authorisation from ACER under the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. As a result, a partial year, i.e. the period between the date of authorisation and 31 December of that same year, is not considered a reportable period and is therefore excluded from the annual report.

The annual report must be submitted to ACER no later than 31 March of the year following the reference year. In practice, this means that submission can take place at any point from 1 January up to and including 31 March of that year.

The table below further aims to clarify the timeline for the submission of the annual report by RRMs depending on the date of authorisation.

Table 4: Timeline examples

Authorisation date	First reference year	Submission deadline	Period covered in 1st report
17 February 2028	2029	31 March 2030	1 Jan–31 Dec 2029
8 December 2028	2029	31 March 2030	1 Jan–31 Dec 2029
1 January 2029	2029	31 March 2030	1 Jan–31 Dec 2029
2 January 2029	2030	31 March 2031	1 Jan–31 Dec 2030

8.2. Content of the annual report

Article 33(2) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs defines the content of the annual report while this guidance further details the format for each of the reportable information. The annual report has to contain the following for each market participant and data type:

1. the number of invalid data records that remained uncorrected and therefore were not submitted to ACER by the end of the relevant reporting period (snapshot from the register of invalid records representing the status on 31 December of the respective year);
2. the number of invalid data records that were subsequently corrected following the RRM's follow-up with its client, after the applicable reporting deadline had elapsed; RRMs should count all initially detected invalid records during the reference period that were subsequently corrected on or before 31 December of the reference year;
3. reporting of non-client counterparties in bilateral trades.

As Table 5 exemplifies, the information for points 1 and 2 can be combined into one format since both are to be reported per market participant. RRMs should provide the required information separately for each market participant and data type for which at least one invalid data record was identified during the relevant reporting period, including the fields showcased in Table 5 below. Data records should be counted as per the definition of Article 2(5) of the Delegated Regulation for the authorisation and supervision of IIPs and RRMs. The market participant must be identified using one of the unique identification codes registered with its NRA and available in the Centralised European Register of Energy Market Participants (CEREMP) (ACER code, legal entity identifier (LEI), bank identifier code (BIC), energy identification code (EIC) or global location number (GLN) / Global Standards One (GS1) code). The ACER code is the preferred identifier and should be used whenever available.

Table 5: Format example for the annual report of corrected and uncorrected invalid records

Market Participant Name	MP ID code	Number of uncorrected invalid data records	Number of corrected invalid data records	Data type as per the authorisation
				Example 1: Table 1 Example 2: Fundamental data – Electricity nominations Example 3: Exposure

Regarding point 3, the annual report must also contain information on market participants that are not clients of the RRM but are reported by the RRM as the counterparty in one leg and as the market participant in the other leg of a bilateral transaction reported to ACER. This covers transactions concerning non-standard contracts across the relevant data types, including where such contracts are reported as secondary transactions. It must not include cases in which an RRM client reports a bilateral transaction with a non-client counterparty, as the RRM is only reporting the transaction on behalf of its client.

Table 6 provides the format for the reporting of non-client counterparties in bilateral trades. RRMs must report one row per unique non-client market participant identified during the relevant reference year, irrespective of the number of bilateral trades reported involving that market participant. The market participant must be identified using one of the unique codes registered with its NRA and available in CEREMP (ACER code, LEI, BIC, EIC, GLN/GS1 code). The ACER code is the preferred identifier and should be used whenever available.

Table 6: Format example for the annual report of non-client counterparties in bilateral trades

ID of the counterparty (not a client of the RRM)

Annex I – Supporting documents as per Article 4

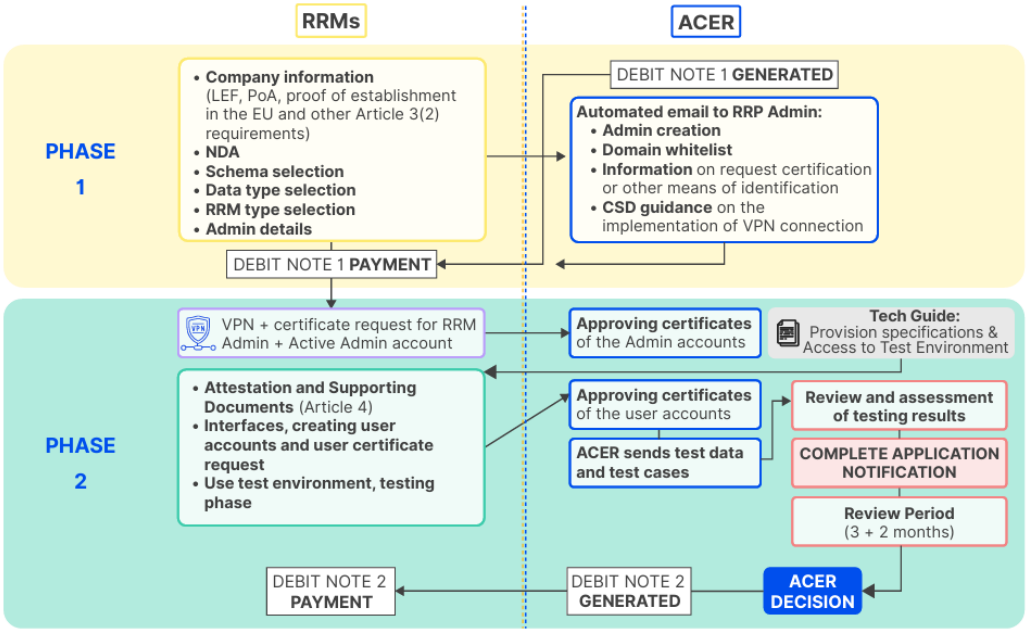
DR provision	What must be provided	Current RRM requirement	Gap / difference	Action	Can the valid ISO/IEC 27000-series certificate be used?
4(1)	**Supporting documents** showing compliance with Arts. 11–18 and orderly substitution under Art. 38; plus Art. 19–25 for IIPs and 26–29 for RRMs.	Current RRM **5.2–5.11** cover many operational/ security/ validation topics.	Major structuring gap. DR article-by-article evidence required; orderly substitution is new.	**Expansion**	/
4(2)(a)	**Timing policies, contingency plans** and **arrangements for disclosure/ submission/reporting** under Art. 11.	**5.3** Timely Transmission of Data	Mostly covered; update to new DA/REMIT IR timing framework.	**Update**	**Yes, partially**
4(2)(b)	**Data validation system** checking accuracy and completeness under Art. 12.	**5.4** Validation of Input + **5.7** Validation of Output	Covered in principle; broaden validation evidence.	**Enhance**	**Yes, ISO can support the security, integrity, change control, access control and operational controls surrounding data validation**
4(2)(c)	**Security arrangements** demonstrating compliance with Art. 13.	**5.2** Secure Transmission + **5.11** Security Breaches	Current RRM focus is narrower; broader security compliance needed.	**Enhance**	**Yes**
4(2)(d)	**Organisational chart for relevant REMIT activities:** group structure, ownership links, activities, legal names/addresses, responsible persons, tasks and contacts.	Partial overlap with **5.8** Governance and **5.12** Communication with Agency	Formal organisational chart required.	**New**	**Yes partially**
4(2)(e)	**Programme of operations:** operational framework, business model, services/products, outsourcing, internal controls, governance, risk management, monitoring and mitigation.	Partial overlap with **5.8** Governance / outsourcing / Governance and **5.9** Operational Reliability.	New standalone document.	**New**	**Yes partially**
4(2)(f)	**Arrangements preventing conflicts of interest and discrimination** under Art. 16.	Partial overlap with **5.8** Governance	Explicit conflicts/non-discrimination framework needed.	**New / expand**	/

DR provision	What must be provided	Current RRM requirement	Gap / difference	Action	Can the valid ISO/IEC 27000-series certificate be used?
4(2)(g)	**Resources and backup facilities** to maintain services under Art. 17.	**5.3** Timely Transmission + **5.9** Operational Reliability	Clearer evidence of resources and backup facilities.	**Enhance**	**Yes**
4(2)(h)	**Implementation of technical standards**, including updates, for secure and efficient data collection/ reporting.	**5.5** Output Format + **5.6** Output Content	Add technical standards governance and update process.	**Enhance**	**Yes**
4(6) – IIP only	IIPs must provide **the time needed to disclose validated information** and **explain how IIP client fees are set** under Article 25.	Not applicable to current RRM requirement mapping.	IIP-specific requirement.	**IIP only, new**	/
4(7) – RRM only	RRMs must provide **supporting documents regarding the information systems** they have in place to ensure data transfers from other systems or platforms in accordance with Article 15. RRM applicants shall indicate the **name of such systems or platform (RRM systems)**, and of **any user facilities generating reportable data** to the technical solution implemented by the RRM **(systems that generate data that RRMs will report, e.g. trading and market infrastructure platforms)**	Partial overlap with **5.4** Technical Solution Description.	Additional RRM-specific documentation required.	**RRM only, Expansion**	/

NB: DR = Delegated Regulation for the authorisation and supervision of IIPs and RRMs, IR = REMIT Implementing Regulation

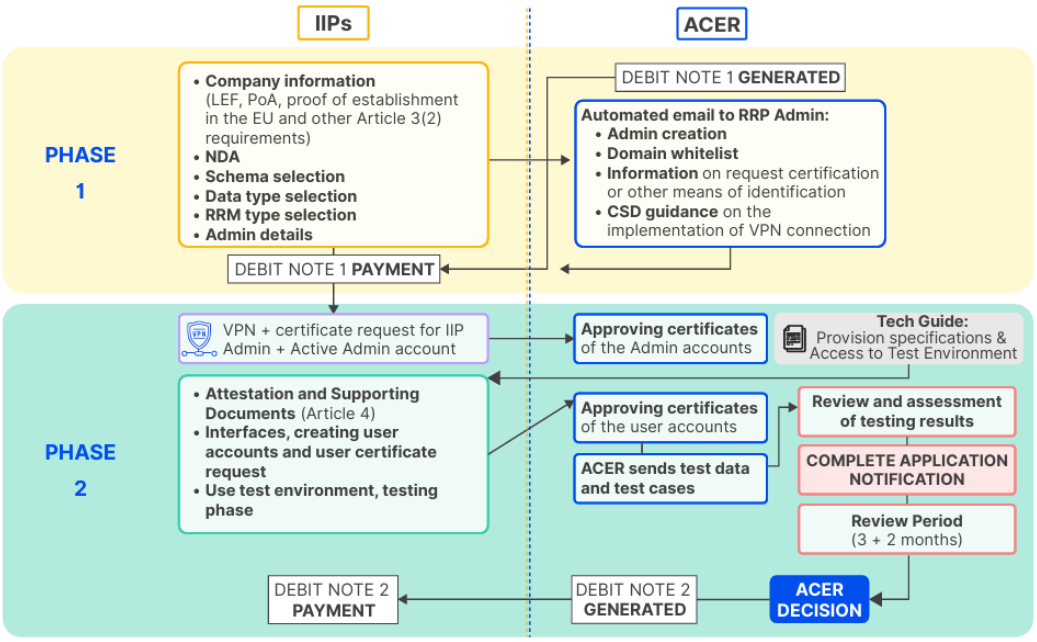
Annex II – Authorisation process workflow

Authorisation process workflow for RRMs:



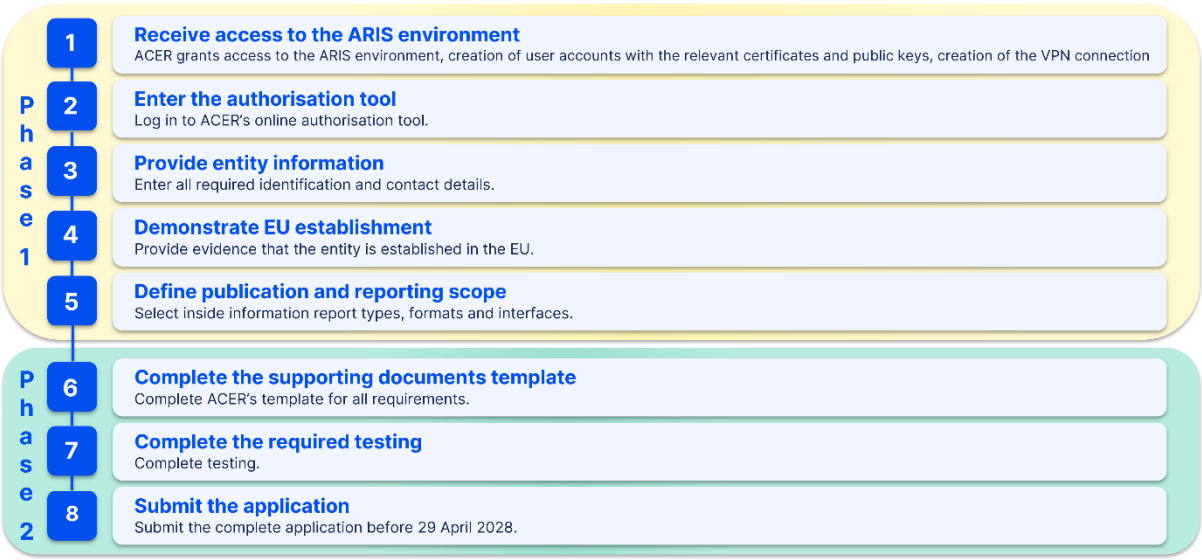
NB: LEF = Legal Entity Form; PoA = Power of Attorney, CSD = ARIS Central Service Desk

Authorisation process workflow for IIPs:

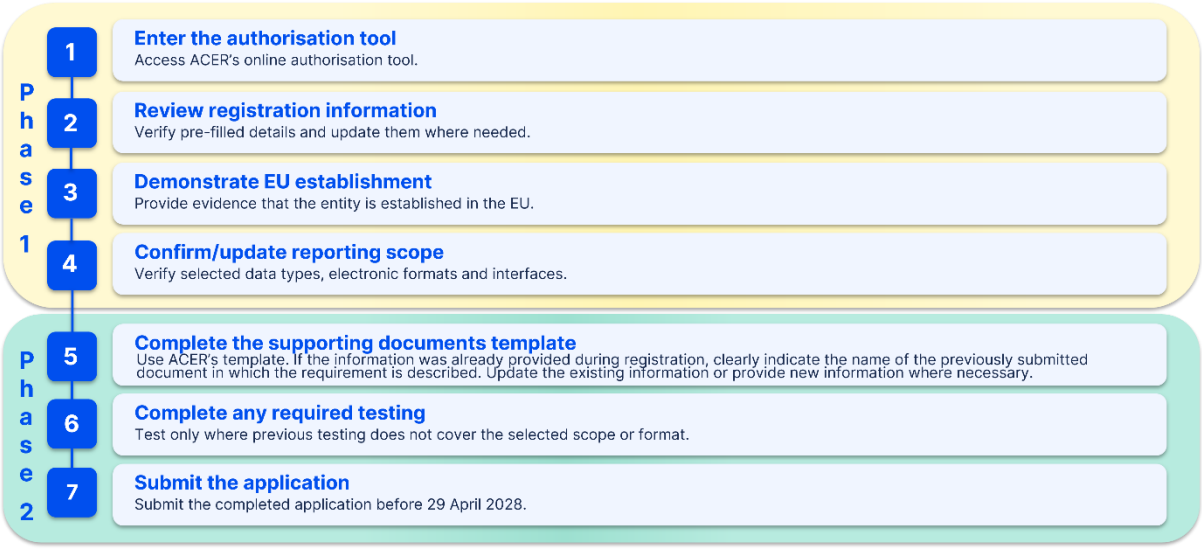


NB: LEF = Legal Entity Form; PoA = Power of Attorney, CSD = ARIS Central Service Desk

Already registered IIPs – transition to authorisation:



Already registered RRMs – transition to authorisation:



Annex III – Operational guidance for security measures

Operational guidance for confidentiality

Step 1: Data inventory and mapping

IIPs and RRMs may maintain an inventory of information systems, applications, databases and data repositories involved in the processing, storage, transmission or reporting of regulated or sensitive information. The inventory may identify data types, system and service owners, storage locations and key internal and external interfaces. Data flows between systems, external stakeholders, service providers and regulatory interfaces may be documented where relevant to support risk assessment, access management, incident response and business continuity activities. The level of detail may support a risk-based approach and reflect operational needs and system criticality. For example, an RRM may document transaction reporting systems, client submission interfaces, communication platforms and supporting infrastructure used for regulatory reporting.

Step 2: Data classification and validation

IIPs and RRMs subject to REMIT obligations may establish and maintain a data classification framework as part of their information security management system to support the consistent protection of information throughout its life cycle. IIPs and RRMs may classify information according to sensitivity, regulatory relevance, business impact and operational criticality. Classification may support the application of appropriate controls relating to access management, encryption, monitoring, retention, disposal and incident handling. Classification approaches may align with recognised standards such as ISO/IEC 27001:2022 and ISO/IEC 27002:2022, and with applicable requirements under Directive (EU) 2022/2555 (NIS2 Directive), where applicable. IIPs and RRMs may review classifications periodically to ensure they remain accurate in response to changes in systems, data usage or regulatory obligations.

Data classification

Level	Classification	Typical IIP/RRM examples	Protection expectation
1	Public	Published inside information; public market information; publicly available documentation	No confidentiality restriction, but integrity/authenticity should still be protected
2	Internal	Internal procedures; non-sensitive operational information; general system documentation	Access limited to authorised personnel/parties
3	Sensitive	REMIT transaction/reporting data; exposure data; fundamental data before public disclosure; commercially sensitive information; non-public market information	Enhanced access control, encryption, monitoring and controlled disclosure
4	Restricted	Inside information prior to authorised disclosure; credentials/cryptographic keys; security configurations; privileged access information; highly sensitive personal data	Strict need-to-know access, enhanced security controls and tightly controlled disclosure

Step 3: Access control implementation and maintenance

IIPs and RRMs may implement access controls to ensure that systems and data are accessible only to authorised users, systems and processes. Access rights may be assigned based on roles, responsibilities, business needs and the sensitivity or criticality of the information being accessed. Accessing management processes may include provisioning, modification, periodic review (e.g. quarterly) and timely revocation when access is no longer required, including role changes, contract

termination or user departure. Authentication and access controls may be defined based on a risk-based approach and system criticality, in accordance with the requirements set out in Section 4.4 of this guidance. Additional safeguards for privileged access or access to sensitive systems may be applied where appropriate. Default, inactive or unnecessary accounts and credentials may be disabled or removed without delay. For example, when a user changes role or leaves the organisation, access rights associated with the previous role may be reviewed and revoked where no longer required.

Step 4: Encryption enablement and verification

IIPs and RRMs may identify systems and data requiring cryptographic protection based on classification, sensitivity, regulatory relevance and documented risk assessments. Appropriate cryptographic controls may be implemented to protect data at rest and in transit using recognised industry standards and secure communication protocols. Encryption key management may include secure procedures for the generation, storage, distribution, recovery, archival and destruction of keys. Secure key management mechanisms such as hardware security modules (HSMs), key management services (KMS), or equivalent solutions may be used where appropriate for the operational environment and risk considerations. Encryption scope and key management practices may be defined based on a risk-based approach considering system criticality, operational performance, processing requirements and resilience needs. Cryptographic controls may be reviewed periodically to ensure continued effectiveness. Documentation of encryption and key management activities may be maintained to support auditability and compliance. For example, an IIP may encrypt sensitive data and secure communications using recognised cryptographic protocols, with periodic review based on operational and regulatory risk.

Operational guidance for integrity

Step 1: Establish a change control process

IIPs and RRMs may establish and maintain a formal change management process governing modifications to systems, applications, databases, infrastructure, configurations and data-processing rules that may affect security, integrity, availability or regulatory reporting activities. Changes may be documented, assessed based on risk and potential impact, approved prior to implementation and tested before deployment, where applicable. Changes may be categorised according to risk (e.g. standard, normal, emergency), with controls applied based on the assessed risk level. Emergency changes addressing urgent operational or security issues may follow expedited approval and testing procedures, provided that the change, rationale and authorisation are documented and the change is subject to timely post-implementation review. Rollback and recovery procedures may be defined for significant changes to support restoration in case of failure or unintended impact. Governance structures such as change review groups or change advisory boards may be implemented where relevant to operational complexity and risk environment. All change activities, approvals, testing outcomes and implementation results may be documented to ensure traceability and auditability. For example, an RRM may apply this process before deploying changes to transaction validation or reporting logic.

Step 2: Implement data integrity controls

IIPs and RRMs may identify data and processing activities requiring integrity protection based on classification, regulatory relevance, and operational criticality. Technical and organisational controls may ensure that data remains accurate, complete, consistent and protected against unauthorised or unintended modification throughout its life cycle. Integrity controls may include validation rules, database constraints, format checks, uniqueness controls, referential integrity, reconciliation processes or equivalent mechanisms appropriate to system design. Integrity rules may be documented and consistently enforced to support reliable processing and reporting. Where appropriate, cryptographic techniques such as hashing, checksums or digital signatures may be used to support detection of unauthorised modification and verification of data integrity. Integrity controls may be tested and reviewed regularly to ensure continued effectiveness. For example, an IIP may apply validation rules and reconciliation checks to ensure the accuracy of regulated data.

Step 3: Enable audit logging

IIPs and RRMs may implement logging mechanisms capable of recording actions affecting critical systems, regulated data and security-relevant activities. Audit logs may capture sufficient information to support traceability, accountability, monitoring and investigation activities, including user or system identity, timestamps, activity type, affected data or systems and outcome. Where appropriate, additional

contextual information such as change details may be recorded. Audit logs may be protected against unauthorised access, modification and deletion to preserve integrity and evidential value. Logs may be retained in accordance with documented retention policies and applicable legal or regulatory requirements, with retention periods aligned to a minimum of five years unless longer retention is required. Logging retention and processing practices may consider data minimisation principles and avoid the unnecessary retention of information. Backup and resilience mechanisms may be implemented to ensure the availability of critical logs. Logging configurations may be documented and reviewed regularly. For example, an RRM may log changes to reporting configurations and access rights for audit and investigation purposes.

Step 4: Conduct regular reviews

IIPs and RRMs may establish risk-based procedures for reviewing audit logs, integrity controls and related monitoring output to identify unauthorised activities, anomalies, errors or control weaknesses. The frequency and scope of reviews may be defined based on documented risk assessments considering system criticality, data sensitivity, transaction volumes, user population, operational complexity and regulatory impact. Systems processing regulated or sensitive data may require more frequent or automated review mechanisms, while lower-risk systems may apply less frequent review cycles based on documented risk assessment. Review schedules and methodologies may be reassessed periodically to ensure continued effectiveness. Findings from reviews may be documented and addressed through corrective actions where necessary.

Operational guidance for availability

Step 1: Identify critical systems and data

IIPs and RRMs may identify systems, services, processes, and data critical to operational activities, regulatory obligations, and business continuity through documented risk assessment and business impact analysis. The assessment may consider operational, financial, legal, regulatory and reputational impacts associated with disruption, degradation or unavailability. IIPs and RRMs may identify dependencies, including supporting infrastructure, external service providers, communication channels and upstream or downstream system interfaces relevant to critical operations. For critical systems and processes, recovery objectives including RTO and RPO may be defined based on operational and regulatory requirements. The level of analysis and documentation may reflect a risk-based approach and the nature of the systems in scope. For example, an IIP may identify its inside information platform, publication system and communication interfaces as critical services supporting regulatory obligations.

Step 2: Develop a backup strategy

IIPs and RRMs may establish and maintain backup and recovery procedures for systems, configurations, applications, and data identified as critical through risk assessment and business impact analysis. Backup design may be defined based on recovery objectives, data classification, system criticality, and operational requirements. Backup procedures may define scope, frequency, retention, storage locations, protection measures, and recovery responsibilities. Backup data may be protected against unauthorised access, corruption, loss, or destruction using appropriate technical and organisational controls, including encryption and logically or physically separated storage where appropriate. IIPs and RRMs may implement mechanisms to verify backup integrity and test restoration procedures periodically to confirm that recovery objectives can be achieved. Backup and retention practices may comply with applicable legal, regulatory, and data minimisation obligations. For example, an IIP may implement full and incremental backups for critical reporting systems based on defined recovery needs.

Step 3: Establish a business continuity plan

IIPs and RRMs may establish and maintain business continuity and disaster recovery arrangements to support continued operation or timely restoration of critical systems, processes and regulatory reporting activities following disruption events. Business continuity arrangements may identify critical services, dependencies, recovery priorities, communication procedures and roles and responsibilities. Recovery strategies may include failover mechanisms, alternative processing arrangements, backup infrastructure or manual workarounds appropriate to the operational environment and risk profile. For critical or important outsourced dependencies, IIPs and RRMs may consider substitutability, concentration risk, loss of provider access, data or configuration portability, and feasible exit or contingency arrangements. Business continuity and recovery procedures may be reviewed and tested

periodically using risk-based testing approaches. Testing activities may include technical recovery tests, simulations or full-scale recovery exercises. The scope and frequency of testing may be defined based on documented risk assessments and operational requirements. For example, an RRM may perform periodic recovery simulations and failover testing to validate readiness for regulatory submission activities.

Step 4: Implement monitoring and alerting

IIPs and RRMs may implement monitoring and alerting mechanisms to support the detection of conditions that may affect system availability, reliability, integrity or regulatory reporting obligations. Monitoring activities may include relevant metrics such as system availability, response times, resource utilisation, capacity thresholds, processing errors or security-related events, depending on the system and operational context. Automated alerting mechanisms may be implemented to notify responsible personnel when defined thresholds or abnormal conditions are detected. Monitoring configurations, thresholds, escalation procedures and review activities may be documented and periodically reviewed to ensure continued effectiveness, in accordance with the requirements set out in Section 4.7.1 of this guidance. For example, an IIP may monitor systems supporting inside information publication and trigger alerts when availability or performance thresholds are breached.

Operational guidance for access control

Step 1: Define roles and access requirements

IIPs and RRMs may define and maintain a structured set of roles reflecting business functions, operational responsibilities and system usage requirements. For each role, IIPs and RRMs may document associated access requirements, including the systems, applications and data required to perform assigned duties, along with permitted functions and access scope. Role definitions may be justified based on business needs and aligned with the principle of least privilege. Where relevant, contextual restrictions such as time-based, location-based or conditional access constraints may be defined based on risk considerations. For example, an RRM may define roles such as trade data submitter, data validator or system administrator, each with clearly defined access requirements.

Step 2: Implement role-based access control or equivalent mechanisms

IIPs and RRMs may implement role-based access control (RBAC) or equivalent mechanisms to enforce defined roles and associated access requirements within systems. Access permissions may be assigned to roles rather than to individual users wherever possible, and users may be assigned to roles based on their job responsibilities. RBAC configurations may be documented, maintained and periodically tested to ensure that access controls operate as intended and enforce defined restrictions effectively. For example, an IIP may implement roles such as disclosure creator, compliance officer or system administrator with clearly defined permissions for regulatory reporting and system administration activities.

Step 3: Provide and manage user access

IIPs and RRMs may establish and maintain procedures for the provisioning, modification and removal of user access in accordance with defined roles and business requirements. Access provisioning may be based on documented requests specifying user identity, required role or access level, and business justification. Requests may be reviewed and approved by authorised personnel prior to implementation. Access rights may be granted in accordance with approved role assignments and may be updated promptly when users change roles or responsibilities. Access may be revoked without delay when no longer required. For example, when a new analyst joins an organisation, access may be provisioned based on an approved request and assigned to the appropriate role in accordance with defined access policies.

Step 4: Conduct regular access reviews

IIPs and RRMs may conduct periodic reviews of user access rights to ensure that access remains appropriate, necessary and aligned with current roles and responsibilities. Access reviews may be performed based on a risk-based schedule considering system criticality, data sensitivity and organisational changes such as role changes, transfers or departures. Reviews may include verification of assigned roles and permissions, identification of excessive or unnecessary access and removal or adjustment of access where required. The review process and outcomes may be documented, and identified issues may be remediated in a timely manner through appropriate corrective actions. For

example, an RRM may review user access to regulatory submission systems quarterly to ensure alignment with current responsibilities.

Operational guidance for authenticity

Step 1: Obtain digital certificates

IIPs and RRMs may obtain digital certificates from trusted certification authorities or equivalent trusted mechanisms for authentication, integrity protection and digital signature purposes where cryptographic assurance is required. Certificate issuance may be based on defined purposes such as authentication, signing or encryption, following a risk-based approach aligned with system criticality, data sensitivity and communication context. Where interoperability with ACER or other regulatory systems is required, certificates may be issued by recognised authorities within the applicable regulatory trust framework. In other contexts, IIPs and RRMs may use certificates issued by internal or external certification mechanisms, including privately managed PKI environments, provided that appropriate trust and governance controls are in place. Certificates may be securely deployed, and their purpose, ownership and validity may be documented.

Step 2: Implement digital signature procedures

IIPs and RRMs may implement integrity and authenticity controls for critical data submissions, transactions or communications where assurance of non-repudiation or tamper detection is required based on risk assessment or regulatory obligations. Digital signatures may be used as a technical mechanism where appropriate. Where implemented, IIPs and RRMs may define the scope of signed transactions, the systems involved and validation requirements prior to acceptance or processing. Signature application may be protected against modification after signing, and signature verification may be performed prior to acceptance of externally received signed data where applicable. Where equivalent system-level integrity controls, authenticated APIs or secure communication channels provide sufficient assurance, additional signing steps may not be required. Signature-related activities may be logged where relevant to support oversight and investigation.

Step 3: Manage certificate life cycle

IIPs and RRMs may implement lifecycle management procedures for digital certificates used in authentication and integrity protection to support continued validity and operational continuity. This may include monitoring validity, renewal before expiration, revocation upon compromise or decommissioning, and maintaining an up-to-date certificate inventory. Certificate lifecycle management may align with risk assessment, operational requirements and the policies of the issuing trust framework. IIPs and RRMs may ensure timely renewal to help prevent service disruption. Certificate management activities may be documented and reviewed periodically.

Step 4: Verify signatures and authenticity

IIPs and RRMs may implement verification mechanisms to support the integrity and authenticity of received data, transactions or communications where assurance is required based on risk-based, regulatory or operational needs. Verification controls may include the validation of digital signatures, certificate trust status, revocation status and data integrity checks. Where timestamps are used, verification may include the validation of time assertions to support integrity and auditability. Verification may not be required where equivalent assurance is provided through secure communication channels, authenticated APIs or system-level integrity controls and is adequately documented. Verification outcomes may be recorded where relevant for audit and investigative purposes.

Operational guidance for accountability

Step 1: Establish user identification procedures

IIPs and RRMs may ensure that users are uniquely identifiable so that actions performed within systems can be attributed to specific individuals or automated processes. A user identity registry may be maintained, linking user identifiers to individuals, roles and responsibilities, and kept accurate throughout the user life cycle. System, service and automated-process identities may be linked to an accountable owner, defined purpose and approved access scope. Shared or generic accounts may be used where formally justified and approved, subject to appropriate compensating controls, including enhanced logging, monitoring and periodic review. For example, an IIP may assign unique user identifiers to employees and maintain a registry linking each identity to role and department. Shared

accounts may only be used in controlled administrative scenarios under enhanced monitoring and logging.

Step 2: Configure audit logging

IIPs and RRMs may implement audit logging for systems and processes handling critical, regulated or sensitive data to support the traceability of relevant actions. Audit logs may capture, where applicable, user or system identity, timestamp, action performed, affected data or system, and outcome of the action. Audit logs may be protected against unauthorised access, modification or deletion and retained in accordance with a risk-based retention policy aligned with regulatory, legal and operational requirements, as set out in Section 4.6.1 and the retention principles in Section 4.2.1 of this guidance. For example, an RRM may configure its reporting system to log submission events, user identity, timestamps, validation results and processing outcomes. Logs may be protected and retained in accordance with defined retention rules.

Step 3: Establish audit trail review procedures

IIPs and RRMs may define and maintain risk-based procedures for the review of audit logs, including scope, frequency, responsibilities and escalation processes. Audit trail reviews may focus on identifying anomalies, including unauthorised access, unusual patterns and policy violations. The frequency and scope of reviews may be based on system criticality, data sensitivity, transaction volume and threat exposure and may be reviewed periodically. Findings may be documented, investigated where necessary and escalated for corrective action. For example, an IIP may review audit logs for its information disclosure platform according to a defined risk-based schedule and escalate suspicious findings to the security function.

Step 4: Implement incident investigation procedures

IIPs and RRMs may establish formal procedures for investigating security incidents and suspected policy violations affecting systems or data. Incident investigations may include evidence preservation, structured analysis, the documentation of findings and the implementation of corrective actions. Investigations may ensure that evidence integrity is maintained and that outcomes are documented and reported to management and, where required, competent regulatory authorities. For example, if unauthorised access to regulated data is detected, evidence may be preserved, access may be revoked, the incident may be analysed and the findings may be reported to management and regulators where applicable.

Operational guidance for reliability

Step 1: Establish system monitoring

IIPs and RRMs may identify critical systems and define monitoring requirements to assess availability, performance and operational health. Monitoring mechanisms may collect relevant metrics, including system availability, response times, error rates, resource utilisation and security-related events based on system criticality and risk profile. Alerting thresholds may be defined using a risk-based approach to enable timely detection of service degradation or abnormal behaviour. Monitoring data may be retained in line with operational, analytical and investigative requirements. For example, an IIP may monitor the availability, response time and error rates of its information system, with alerts triggered when availability drops below a defined threshold.

Step 2: Implement vulnerability management

IIPs and RRMs may implement a vulnerability management process to identify, assess, prioritise and remediate vulnerabilities affecting systems and applications. Vulnerability assessments may be performed at intervals defined through risk assessment, based on system criticality, threat exposure and change frequency. Identified vulnerabilities may be assessed for severity and impact, prioritised and addressed through appropriate remediation actions such as patching, configuration changes or compensating controls where immediate remediation is not possible. Remediation actions may be verified, and relevant activities may be documented. For example, an RRM may perform vulnerability assessments on its reporting systems at risk-defined intervals and document remediation and verification activities.

Step 3: Implement configuration management

IIPs and RRMs may implement configuration management to help ensure systems remain securely and consistently configured throughout their life cycle. Secure baseline configurations may be defined and maintained for critical systems. Systems may be monitored for configuration drift, and deviations may be assessed and remediated based on risk. Configuration changes may be managed through the formal change management process and tested prior to deployment where appropriate. For example, an IIP may define baseline configurations for database systems and remediate configuration drift when deviations are detected.

Step 4: Conduct periodic reliability reviews

IIPs and RRMs may conduct periodic reliability reviews to assess system performance, availability, incident trends and operational risks. The scope and frequency of reviews may be defined through a risk-based approach considering system criticality, operational complexity, incident history and change frequency. Reviews may identify recurring issues, performance degradation and improvement opportunities. Findings may be documented, and corrective actions may be implemented where necessary. Lessons learned may be captured to support continuous improvement. For example, systems with recurring incidents may undergo more frequent reliability reviews, while stable systems may be reviewed less frequently based on risk assessment.

Annex IV – Disruption report cardinality table

ID	Field	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
1	Is the IIP not able to disclose or report information? (Only for IIPs)	Mandatory when creating the disruption report	n/a			
2	Issue seems to exist at which level	Mandatory when creating the disruption report				
3	Specify the data quality dimensions affected	n/a		Mandatory when creating the disruption report	n/a	
4	Specify which security requirement is not (has not been) met	n/a			Mandatory when creating the disruption report	n/a
5	Specify severity of the security incident	n/a			Mandatory when creating the disruption report	n/a
6	Specify which platform requirement is not (has not been) met	n/a			Mandatory when updating the disruption report	Mandatory when creating the disruption report
7	Request for timeline extension for Article 24(2) and 29(2)	Optional				
8	Description of the disruption encountered	Mandatory when creating the disruption report				
9	Description of causes of disruption	Mandatory when updating the disruption report				
10	Description of contingency measures taken	Mandatory when updating the disruption report				
11	Description of actions taken to prevent reoccurrence	Mandatory when updating the disruption report				
12	Report ID of a related disruption report (if applicable)	Optional				
13	Data type(s) affected by the disruption	Mandatory when creating the disruption report				
14	Start date of the disruption period	Mandatory when creating the disruption report				
15	Planned end date of the critical disruption	Mandatory when creating the disruption report				
16	Date of the last data submission	Mandatory when creating the disruption report				
17	Last load ID (UMM thread ID) reported to ACER prior to the critical disruption	Mandatory when creating the disruption report				
18	Planned date of data (re)submission	Mandatory when updating the disruption report				

19	**Type of entities for which reporting is (has been) hindered/not possible**	Mandatory when creating the disruption report
20	**Number of entities for which the reporting is (has been) hindered/not possible**	Mandatory when creating the disruption report
21	**ACER/MIC/LEI/BIC/EIC/GS1 code of entities for which the reporting is (has been) hindered /not possible**	Mandatory when updating the disruption report
22	**If more than five entities, please upload a file with the respective ACER/MIC/LEI/BIC/EIC/GS1 codes**	Optional
23	**Were clients informed about unplanned downtime or disruption?**	Mandatory when creating the disruption report
24	**Were clients given instructions on alternative means of disclosure? (Only for IIPs)**	Mandatory when creating the disruption report
25	**Back-up contact person to the sender of this disruption report**	Mandatory when creating the disruption report
26	**Attachments**	Optional

Annex V – REMIT validation rules document

The REMIT validation rules document can be downloaded from ACER's website in an Excel format.