JC 2025 29

15 July 2025

Digital Operational Resilience Act (DORA): Oversight of critical third-party providers

Guide on oversight activities

Public document

This guide does not produce any legal effect and cannot, in any way, replace the legal requirements laid down in the relevant applicable EU law.

Moreover, this guide aims to provide a user-friendly overview of DORA oversight on critical ICT-third party service providers. In this context, certain provisions of DORA and delegated and implementing acts have been summarised and/or omitted. For the complete description of the DORA oversight and the full text of the relevant provisions included in DORA and in delegated and implementing acts, please consult the Official Journal of the EU ELI: http://data.europa.eu/eli/reg/2022/2554/oj

This guide may be revised and reissued over time as oversight experience continues to develop.

Abbreviations

BoS	Board of Supervisors
CA	Competent Authority
CDR	Commission Delegated Regulation
CSP	Cloud Service Provider
CTPP	Critical Third-Party Provider
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
ECB	European Central Bank
EFTA	European Free Trade Agreement
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ESA	European Supervisory Authority
ESMA	European Securities and Markets Authority
EU	European Union
FE	Financial Entity
ICT	Information and Communication Technology
JC	Joint Committee
JET	Joint Examination Team
JON	Joint Oversight Network
JOV	Joint Oversight Venture
LO	Lead Overseer
MoU	Memorandum of Understanding
NIS	Network and Information Service
OF	Oversight Forum
OVS	Oversight
RfI	Request for information
RTS	Regulatory Technical Standard
TPP	Third-Party Provider

Table of Contents

1 Introduction

1. Recognising the pivotal role technology plays in the viability and competitiveness of the financial sector, as well as the growing reliance of **financial entities (FEs)** on external ICT services, the Digital Operational Resilience Act (DORA) introduces a comprehensive oversight framework for **critical third-party service providers (CTPPs)** of Information and Communication Technologies (ICT). The three **European Supervisory Authorities (ESAs)**[1] are empowered to oversee CTPPs on a pan-European scale, enhancing the overall digital operational resilience across the various Union financial areas. This oversight framework helps to address potential systemic and concentration risks arising from the financial sector's reliance on a limited number of ICT providers. It complements, rather than replaces, financial entities' own responsibilities for managing ICT-related risks and the supervision already exercised over them by **competent authorities (CA)**.

2. The ESAs are first responsible for designating as CTPPs those ICT service providers serving financial entities in Europe that are critical to each of the financial sector under their remit. Subsequently, each ESA assumes the role of **Lead Overseer (LO)** for the CTPPs within their respective financial sector. In this capacity, they conduct oversight activities in collaboration with the relevant CAs, ensuring a coordinated approach to ICT risk management across the financial landscape. The ESAs have powers to request information, conduct general investigations and inspections, issue recommendations, monitor their implementation, and impose periodic penalty payments on CTPPs. These oversight tasks are carried out by **Joint Examination Teams (JETs)**, composed by staff from the ESAs, from the relevant CAs supervising FEs in the EU and the NIS authorities supervising the CTPPs.

3. The governance of the framework is defined with the aim to promote convergence and a sound decision making process. It includes notably the **Joint Oversight Network (JON)** and the **Oversight Forum (OF)**, bodies created with the key responsibility to ensure the upholding of a coordinated, outcome-focused and proportionate framework[2], with a focus on harbouring trust, as well as oversight accountability and transparency.

4. The purpose of this guide is to explain the CTPP oversight framework, including its objectives, underlying principles, structure, activities, implementing processes, and expected outcomes. The guide provides an overview of: (i) the governance structure, (ii) the oversight processes, (iii) the founding principles, (iv) the tools available to the overseers; (v) the adoption process.

5. This guide is mainly addressed to the CTPPs, FEs, CAs, and the general public interested in understanding the DORA oversight framework and activities.

6. It is intentionally written to facilitate understanding of the regulatory framework and its practical application. It does not substitute the legal acts, which should be consulted in the Official Journal of the EU for the full text of the relevant provisions. It may be revised and reissued over time as oversight experience continues to develop.

[1] European Banking Authority (EBA) established by Regulation (EU) No 1093/2010, European Insurance and Occupational Pensions Authority (EIOPA) established by Regulation (EU) No 1094/2010 and European Securities & Markets Authority (ESMA) established by Regulation (EU) No 1095/2010.

[2] The proportionality of this framework is very much aligned with the EU's simplification and burden reduction approach, also with the objective to guarantee the EU's resilience.

2 Key concepts

7. The guide is built on the definitions set out by DORA. However, due to its operational nature, it also uses terminology and concepts related to the ESAs operating model. To facilitate an explicit and common understanding of these key concepts, the table below summarises the meaning of the main terms included in this guide:

Table 1: Key concepts

Lead Overseer, Joint Examination Teams and overseers	The Lead Overseer (LO) is one of the European Supervisory Authorities (ESAs) responsible to conduct the oversight activities for the CTPP(s) relevant for its financial sector. The LO is supported by Joint Examination Teams (JETs) including staff from the ESAs and relevant CAs. From an operational perspective, the ESAs are organised through a single joint-Directorate performing the oversight of CTPPs as "one team". This guide uses the concept of "overseers" to refer to the LOs.
DORA oversight activities	
▪ **Designation**	The annual process carried out by the ESAs to designate CTPPs. It is based on data included in the Register of Information of ICT third-party arrangements that FEs report to their CAs and other available data from all sources of information.
▪ **Risk assessment**	The annual process carried out by the overseers to define the intensity of CTPP oversight activities and set oversight priorities. It is the basis for the oversight planning.
▪ **Planning**	The process for deciding oversight examinations to come for the oversight of CTPPs. There are (i) individual annual oversight plans per CTPP and (ii) an overarching internal multi-annual oversight plan.
- **Individual plans**	The document prepared annually by the overseers and shared with the CTPP, outlining the oversight objectives and main actions to be carried out for the oversight of a CTPP.
- **Multi-annual plan**	It is the three-year plan providing the ESAs and CAs with oversight priorities over the coming three-years, enabling a high-level estimation and an efficient allocation of resources.
▪ **Examinations**	Tasks performed for the evaluation of the CTPP's situation in terms of risks.
- **Ongoing regular monitoring**	The continuous interaction between the overseers and the CTPPs outside of specific general investigation or inspection. The tasks performed during the ongoing regular monitoring include periodic information gathering and ongoing interactions with CTPPs on the state-of-play and any emerging issues (e.g. operational incident or new threat).
- **General investigations**	General investigations are horizontal or targeted reviews into particular risk areas. They are organised according to the oversight plan and are aimed to address newly identified areas of concerns or the review of remediation plans following previous examinations. They enable overseers to carry out more in-depth checks than is possible under on-going monitoring, by allocating more time and resources to the points of verification, and by interacting directly with the people concerned and requesting the necessary documents or data.
- **Inspections**	Inspections cover same kind of examinations as general investigations but entail a higher level of intrusiveness in order to establish a targeted, in-depth picture of the risks that CTPPs pose to FEs. They entail the right to request records, data and all other relevant documents.
- **Requests for Information**	The tool used by the overseers to request information from CTPPs without opening general investigations or inspections. For instance, requests for information may help clarify a particular situation on which overseers need visibility and explanations from the CTPP. The overseers have the power to submit requests to CTPPs either by simple request or by decision.
▪ **Recommendations**	Recommendations address any identified deficiencies at the CTPP within specific areas of assessment. The follow up of recommendations is performed as part of the ongoing regular monitoring and through reports specifying the actions taken or remedies implemented based on the recommendation.

3 Overview of the DORA oversight framework

3.1 Scope of the DORA oversight framework

6. The DORA oversight framework applies exclusively to ICT third-party service providers designated as critical by the ESAs. The designation is based on an annual assessment using several criteria that include systemic impact, interconnectedness, critical nature of services, limited substitutability, and the number and type of financial entities served. Once designated as critical, the ICT third-party service provider becomes subject to oversight by the ESAs.

7. The DORA oversight framework does not cover services provided by CTPPs to FEs which are not considered ICT services according to DORA or issues related to ICT services provided by the CTPPs to customers that are not regulated FEs under DORA[3].

3.2 Objectives of the DORA oversight framework

8. The DORA oversight framework equips the overseers with tools to monitor the activities and the risks that CTPPs pose to the financial sector. To do so, the overseers are required to assess whether CTPPs have in place comprehensive, sound, and effective rules, procedures, mechanisms and arrangements to manage those risks.

9. More holistically, the conduct of oversight activities contributes to (i) promoting convergence and efficiency in relation to supervisory approaches when addressing ICT third-party risk in the financial sector, and (ii) strengthening the digital operational resilience of FEs relying on CTPPs for the provision of ICT services that support the supply of financial services. Therefore, oversight activities are a direct contributor to the preservation of the Union's financial system stability and the integrity of the internal market for financial services.

10. Considering the objectives above, the expected outcome of the DORA oversight framework is to strengthen the collective understanding of the ESAs and the Competent Authorities of the risks posed by the CTPPs to the financial sector, and to mitigate those risks. Operationally speaking, tangible outcomes of the oversight activities would include[4]: (i) the designation of the critical ICT third-party service providers to the EU financial sector; (ii) the development of knowledge and understanding of the ICT services provided by the CTPPs and their related risks; (iii) the identification of areas where risk mitigation actions are needed; (iv) formalisation of the latter via specific recommendations addressed to CTPPs; (v) the possibility for CAs to benefit, in accordance with DORA, from relevant information gathered in the course of the oversight, including information stemming from recommendations for the supervision of FE's ICT and third-party risks.

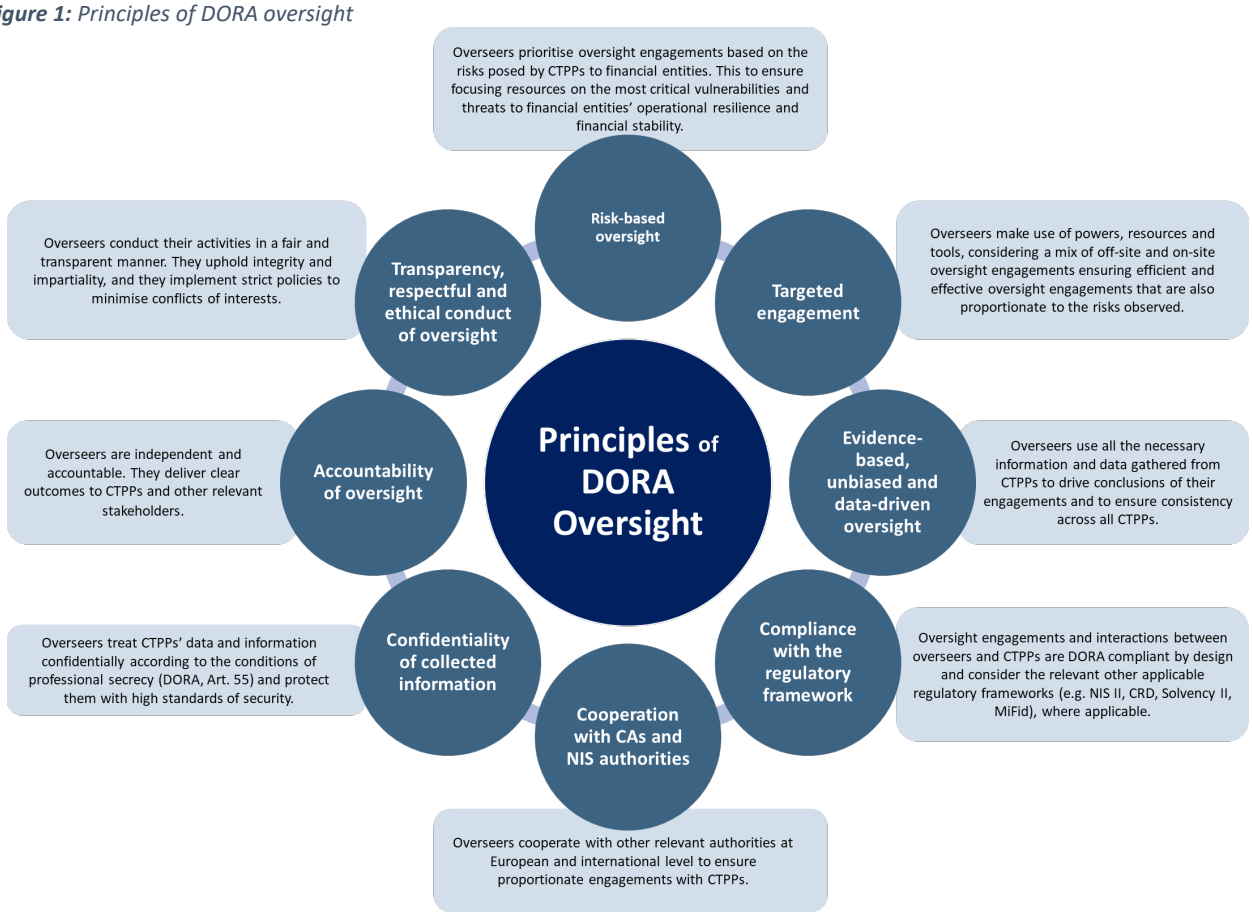
[3] ICT Services are defined in Article 3(25) of DORA and additional guidance can be found in Q&A DORA030. The following entities are not subject to the DORA oversight framework: a) ICT TPPs already subject to oversight mechanism frameworks supporting the fulfilment of tasks of the European System of Central Banks, as referred to in Article 127(2) TFEU. (e.g. SWIFT, Euroclear, TARGET2, and other systemic important payment systems), b) FEs providing ICT services to other FEs, c) ICT intra-group service providers, and d) ICT TPPs active in one Member State only providing services to financial entities active in that Member State. In case of b) FEs providing ICT services to other FEs and c) ICT intra-group service providers, CAs should consider in the context of their supervisory activities the ICT risks posed to financial entities by those financial entities providing ICT services, per DORA Recital 78.

[4] In the process this will also include the collective assessment for all CTPPs and promotion/coordination of measures to increase the digital operational resilience of financial entities, foster best practices on addressing ICT concentration risk and explore mitigants for cross-sector risk transfers (Article 32(2)), as well as the creation of comprehensive benchmarks for CTPPs to be adopted by the JC as joint positions of the ESAs (Art. 32(3)).

3.3 Principles of the DORA oversight framework

11. To achieve the objectives of the DORA oversight framework in a way that is consistent, trustworthy and results in a transparent outcome, the ESAs recognise a set of foundational principles to be applied transversally across the oversight activities. These principles are at the core of each oversight activity. The overseers consider the principles when they define the frequency, the scope, and the intensity of the oversight engagements. The following infographic depicts the foundational principles governing oversight activities:

Figure 1: *Principles of DORA oversight*



3.4 The role of CAs: relationship between oversight of CTPPs and supervision of FEs

12. The oversight framework complements the supervision of FEs' ICT risk carried out by the CAs. For this reason, a strong cooperation between the ESAs and the CAs is embedded into it. The CAs are participating in the conduct of oversight activities by involving expert staff to the JETs and they steer the outcomes of these activities through their membership within the governance bodies. Furthermore, CAs inform the overseers of material issues with a CTPP, which were identified in the supervision of FEs relying on that CTPP. In return, the overseers share relevant insights with CAs about the oversight activities, enabling the CAs to consider them for their own ongoing supervision of FEs.

13. As the information exchange between the ESAs and CAs is a key prerequisite for the success of the oversight framework, the ESAs have prepared ad-hoc Guidelines[5] detailing the procedures and conditions for the allocation and execution of tasks as well as the exchanges of information between CAs and the ESAs.

[5] https://www.esma.europa.eu/sites/default/files/2024-11/JC-GL-2024-36_Guidelines_on_DORA_oversight_cooperation.pdf

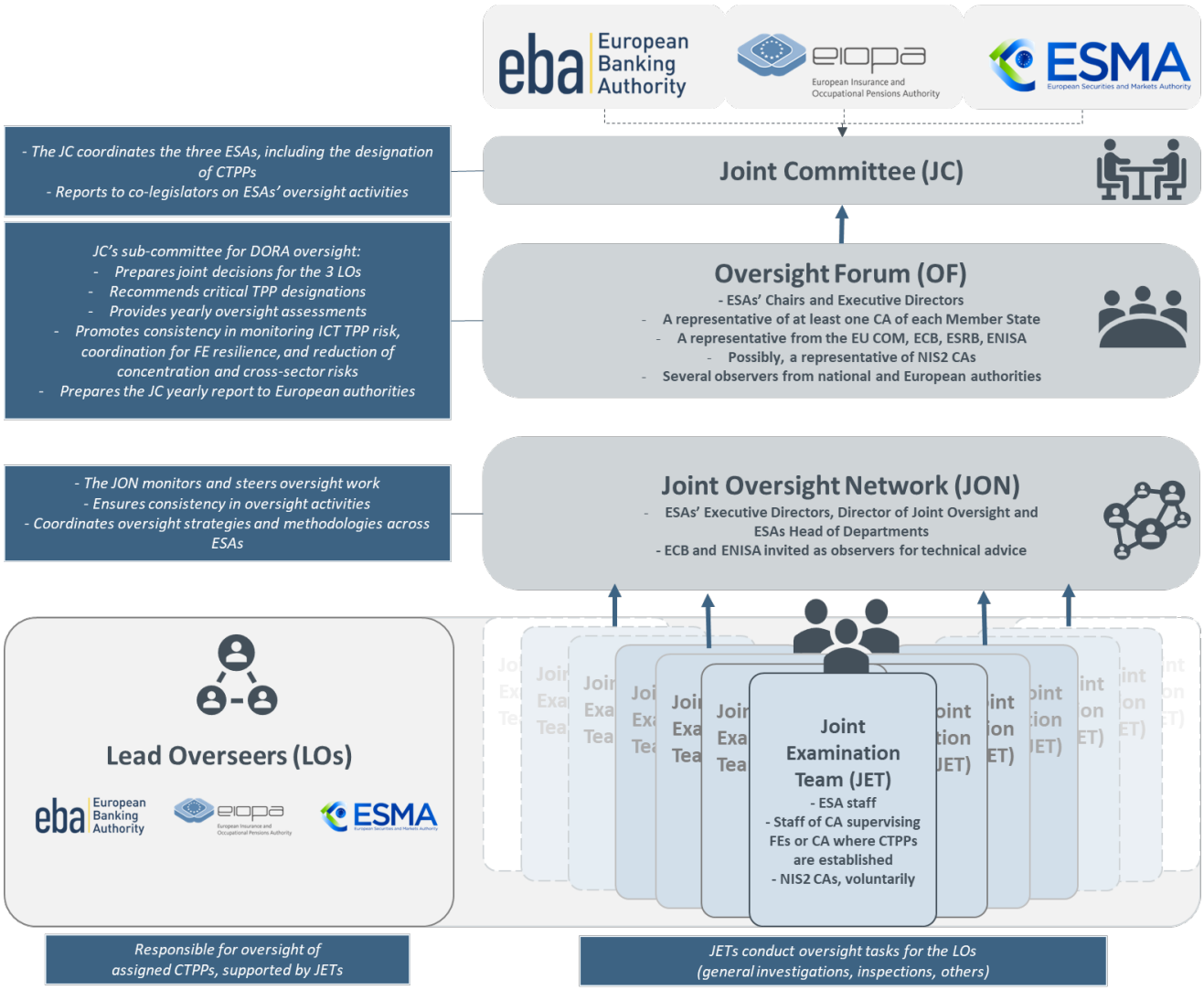
4 Governance and organisation of DORA oversight framework

14. The DORA oversight framework, like any other ESA activity, is integrated into the general governance of the ESAs, under the overall authority of the Board of Supervisors and the Joint Committee (Subsections 4.1.1 and 4.1.2). To take account of the genuinely collaborative nature of the framework, DORA also provides for specific bodies, the Oversight Forum and the Joint Oversight Network (Subsection 4.1.3), contributing to the preparation of decisions by the ESAs governing bodies.

15. Operationally, the oversight activity is carried out by ESAs acting as LOs, with dedicated teams called JETs, in which CAs participate[6]. For reasons of operational efficiency, the ESAs have decided to group their teams together to conduct their operations jointly, as a Joint Oversight Venture (JOV) (Subsection 4.1.4).

16. The infographic below and subsequent sub-sections provide a high-level overview of the roles and functions of each set of key actors.

Figure 2: *DORA oversight roles and functions*



[6] On a mandatory or voluntary basis, depending on the categories defined in Article 40(2) of DORA.

4.1.1 Governing bodies of the ESAs

17. The governance of the ESAs is ensured by their senior management under the authority of the Board of Supervisors (BoS)[7] and Management Board[8].

18. The decision-making processes of the ESAs apply according to the overall governance architecture of the ESAs as stipulated by the ESAs founding regulations.

19. In the context of the DORA oversight activities, for instance, the BoSs are involved in approving the designation of the CTPPs and the related appointment of the LO.

4.1.2 Joint Committee of the three ESAs

20. The Joint Committee (JC) is the most senior cross-sectoral committee across the three ESAs. In relation to CTPPs oversight, it adopts the relevant decisions upon recommendation of the Oversight Forum. In particular, the ESAs take decision for the designation of CTPPs through the JC and upon recommendation of the OF.

21. The Rules of Procedure of the JC are published on the three ESAs websites: JC Rules of Procedure.[9]

4.1.3 Oversight bodies and functions

4.1.3.1 Oversight Forum (OF)

22. The Oversight Forum (OF) is the standing committee of the ESAs dedicated to DORA oversight, set up as a Joint Committee sub-committee[10]. It carries out preparatory work both for certain individual acts addressed to CTPPs, and for the issuing of collective recommendations by the JC, ensuring a consistent approach to oversight activities. It is composed of the chairpersons of the ESAs, senior representatives from CAs and several observers from national and European authorities[11].

23. The OF regularly discusses relevant developments on ICT risk and vulnerabilities and promotes a consistent approach in the monitoring of ICT third-party risk at Union level. It is empowered to undertake yearly collective assessments of the results and findings of oversight activities for all CTPPs, to promote coordination measures that increase the digital operational resilience of FEs and to foster best practices on addressing ICT concentration risk. Where appropriate, the OF may seek the advice of independent experts. The OF is also involved in the designation of CTPPs and in the assessment of ICT third party dependencies of FEs.

24. The OF is required to submit (to the Joint Committee) comprehensive benchmarks for CTPPs[12] to be adopted by the Joint Committee as joint positions of the ESAs.

---

[7] https://www.esma.europa.eu/about-esma/governance-structure/board-of-supervisors
https://www.eiopa.europa.eu/about/governance-structure/board-supervisors_en
https://www.eba.europa.eu/about-us/organisation-and-governance/governance-structure-and-decision-making/board-supervisors

[8] https://www.esma.europa.eu/about-esma/governance-structure/management-board
https://www.eiopa.europa.eu/about/governance-structure/management-board_en
https://www.eba.europa.eu/about-us/organisation-and-governance/governance-structure-and-decision-making/management-board

[9] Further information on the Joint Committee can be found in its Mandate.

[10] The Joint Committee of the ESAs is established by Article 54 of Regulation (EU) 1093/2010, Regulation (EU) 1094/2010 and Regulation (EU) 1095/2010.

[11] As of DORA Article 32(4), the Executive Directors of each ESA and one representative from the Commission, from the ESRB, from ECB and from ENISA, as well as other competent authorities as observers.

[12] DORA Article 32(3).

25. The OF mandate (JC 2024 93) is published on the websites of the ESAs: mandate of the OF.

4.1.3.2 Lead Overseer (LO)

26. For each CTPP, DORA foresees the appointment of a Lead Overseer (LO), which is the ESA responsible for the FEs having together the largest share of total assets out of the value of total assets of all FEs using the services of the relevant CTPP[13]. This stake is determined by the sum of the individual balance sheets of those FEs. It is important to note that the ESAs follow a joint approach to oversight, as laid out in the section on the Joint Oversight Venture.

27. The task of the LO is to conduct the oversight of the assigned CTPP and to perform the oversight activities. Therefore, the LO is the entity primarily in contact with the CTPP on all matters related to the oversight. The LO's adopts all the relevant acts, including decisions and recommendations concerning the assigned CTPPs.

28. The LO is responsible for assessing whether a CTPP has in place comprehensive, sound, and effective rules, procedures, mechanisms, and arrangements to manage the ICT risk which it may pose to FEs. The details of how this assessment needs to be conducted and what it needs to focus on are described in Article 33 of DORA, and further in the dedicated sections of this guide, covering the specific oversight activities.

29. To effectively oversee CTPPs, the LO is empowered to request relevant information and documentation, to conduct general investigations and inspections, to issue recommendations and request a remediation plan and reports specifying the actions that have been taken or the remedies that have been implemented by the CTPP in relation to recommendations.

30. To fund the oversight activities, the LO is tasked to charge oversight fees to CTPPs, which fully cover the LO's expenditures relating to the conduct of oversight tasks. To charge the fees, the LO collects the necessary data on applicable turnovers of the CTPPs, estimates the annual overall oversight costs, calculates and collects the relevant oversight fees. Other competencies of the LO include the power to impose period penalty payments to CTPPs in the cases referred to in Article 35, the power to issue opinions and public disclosures of penalty payments, and the ability to sign Memorandums of Understanding (MoUs) with third-country authorities.

4.1.3.3 Joint Oversight Network (JON)

31. The JON is set up by the overseers according to Article 34 of DORA to coordinate the conduct of oversight activities over CTPPs. It monitors and steers the conduct of oversight activities with the objective to prepare decisions and acts before they are submitted to the OF. Its members are the Executive Directors of the ESAs, the ESAs joint Director of DORA Oversight and high-level representatives of the LOs' staff. ENISA and ECB can nominate observers to the JON.

4.1.3.4 Joint Examination Teams (JETs)

32. When conducting oversight activities, the overseers are assisted by JETs. A dedicated JET is established

[13] For certain cases involving the (European Free Trade Association) EFTA states, the LO may be the EFTA Supervisory Authority.

for each CTPP according to Article 40 and the related Commission Delegated Regulation (CDR) on JET[14]. The JET works under the coordination of a designated staff member of the overseers, the 'LO coordinator'.

33. The JET assists and support the overseers in performing the oversight activities described in this Guide. Its members have a relevant ICT expertise, including on operational risk. The tasks of the JET are listed in Article 1 of the related CDR and include, among other things, the preparation and drafting of the individual annual oversight plan, drafting recommendations, or contribution to any horizontal oversight activities.

34. After the designation of the CTPPs and considering the annual oversight plans for all CTPPs, the following authorities are asked to nominate their staff as members of the JETs:

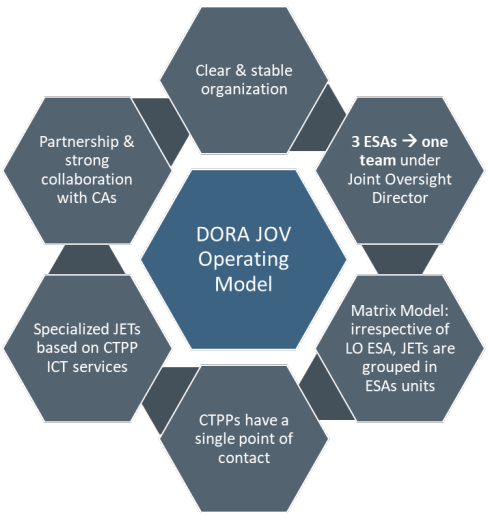
- the ESAs;
- the relevant CAs supervising FEs to which the CTPP provides ICT services;
- on a voluntary basis, the national CAs under NIS 2 supervising the CTPP;
- on a voluntary basis, one national CA from the EU Member State where the CTPP is established.

35. These authorities should ensure that the nominated staff meet the specific technical expertise required in the profiles needed in the JETs. The overseers apply a combination of criteria and principles[15] when identifying the number of staff members that should comprise each JET.

4.1.4 The DORA Joint Oversight Venture

36. To maximise synergies, ensure consistency in the oversight tasks and to achieve a more efficient use of resources, the three ESAs have set up a DORA joint oversight venture (JOV) led by a Joint Oversight Director. The establishment of this organisation, which has become operational since October 2024, ensures that the day-to-day oversight is performed with a cross-sectoral integrated approach. Operationally, all oversight activities are performed within the remit of the JOV. The graphic below summarizes the benefits of the joint structure for all involved stakeholders.

Figure 3: DORA JOV operating model



[14] Commission Delegated Regulation (EU) 2025/420 of 16 December 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards to specify the criteria for determining the composition of the joint examination team ensuring a balanced participation of staff members from the ESAs and from the relevant competent authorities, their designation, tasks and working arrangements

[15] See section 3.3 for further details.

5 DORA oversight activities

37. The DORA oversight entails the following activities performed by the overseers:

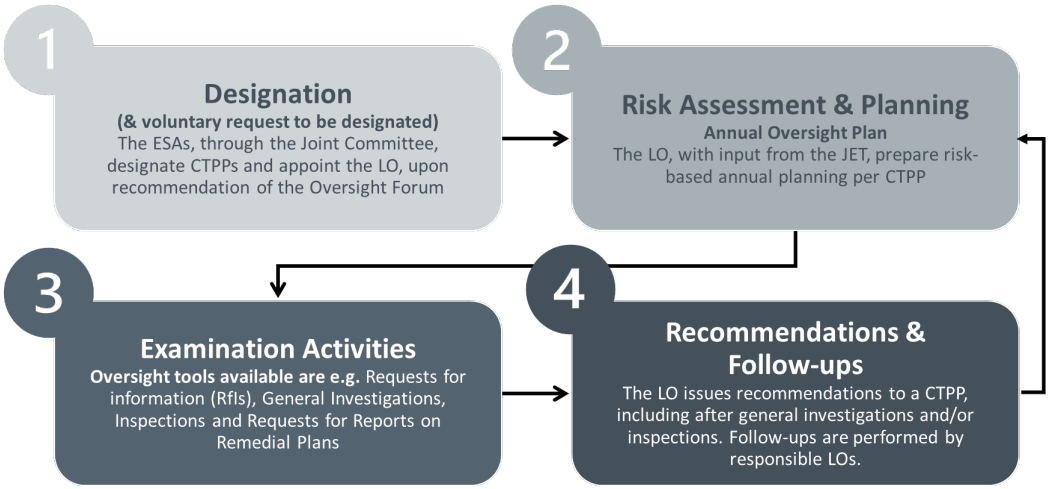
i. **Designation**: Every year, the ESAs publish the list of the CTPPs, which are designated based on the data included in the Registers of Information of the FEs' contractual arrangements with ICT TPPs and other available data. Following the designation, CTPPs will pay oversight fees to the overseers. TPPs not included in the list of CTPPs may apply to be re-assessed for designation as critical (opt-in process). That process entails the payment of a fixed fee and a six-month application assessment period by the ESAs.

ii. **Risk assessment & planning**: On an annual basis, the overseers conduct a risk assessment of the CTPP. The assessment aims to estimate the specific CTPP risk profile. Based on the results of this assessment, the overseers develop individual (i.e. specific to each CTPP) annual oversight plans and a multi-annual strategic plan covering the entire population of CTPPs. Individual oversight plans are communicated to each CTPP. The CTPPs can present a reasoned statement evidencing the expected impact on their customers that are not financial entities and, when appropriate, formulate solutions to mitigate risks.

iii. **Examinations**: In execution of the oversight plan, and on an ongoing basis, the overseers interact with CTPPs for the purpose of assessing the risks that they may pose to European FEs. The examinations are carried out including through the analysis of documentation received from CTPPs, general investigations, inspections and ongoing regular monitoring tasks.

iv. **Recommendations and follow-ups**: As result of the examinations, the overseers can issue non-binding recommendations on specific areas based, for example, on the findings of general investigations or inspections. As part of the ongoing monitoring tasks, the overseers, in collaboration with the CAs, follow up on the implementation of the recommendations by the CTPPs. The CTPPs may be requested to submit a remediation plan following the recommendations and reports outlining the actions/remedies taken or implemented by the CTPPs in relation to the recommendations. The overseers share the recommendations and information on the follow-up with the CAs supervising FEs using the services of the CTPP. Recommendations and follow-ups can thereafter feed into risk assessment & planning stage for the following year.

Figure 4: *DORA oversight activities*



5.1 Designation of CTPPs and expectations on CTPP interaction

38. This section describes how the ESAs assess the criticality of ICT third-party service providers to the financial sector, allowing to identify the CTPPs, and it introduces the procedural steps leading to the designation of CTPPs. Where applicable, the designation is performed at the level of the parent company of CTPPs[16].

5.1.1 Criticality assessment and designation of CTPPs

39. The criteria to be followed by the ESAs when designating CTPPs are defined in Article 31 of DORA and in the dedicated CDR[17]. Those criteria relate to the following four domains:

    a) the systemic impact on the stability, continuity or quality of the provision of financial services in the event that the relevant ICT TPP would face a large-scale operational failure to provide its services;

    b) the systemic character or importance of the FEs that rely on the relevant ICT TPP;

    c) the reliance of FEs on the services provided by the relevant ICT TPP in relation to critical or important functions of FEs that ultimately involve the same ICT TPP; and

    d) the degree of substitutability of the ICT TPP.

40. The criticality of TPPs is assessed against the four domains and evaluated with 11 criteria taken from the abovementioned CDR[18]. Six criteria are of a quantitative nature, while five are qualitative.

41. From a process perspective, the ESAs' evaluation follows a two-step assessment of the Registers of Information, which are reported from the FEs to their CAs, and in turn to the ESAs[19].

42. The first step consists of the application of the quantitative criteria to the consolidated registers of information received from CAs. In the second step, the ESAs apply the five additional sub-criteria to the dataset resulting from the application of the first step.

43. The ESAs make use also of any other additional available information. The combination of these two steps delivers the list of CTPPs, as displayed in the graphic below.

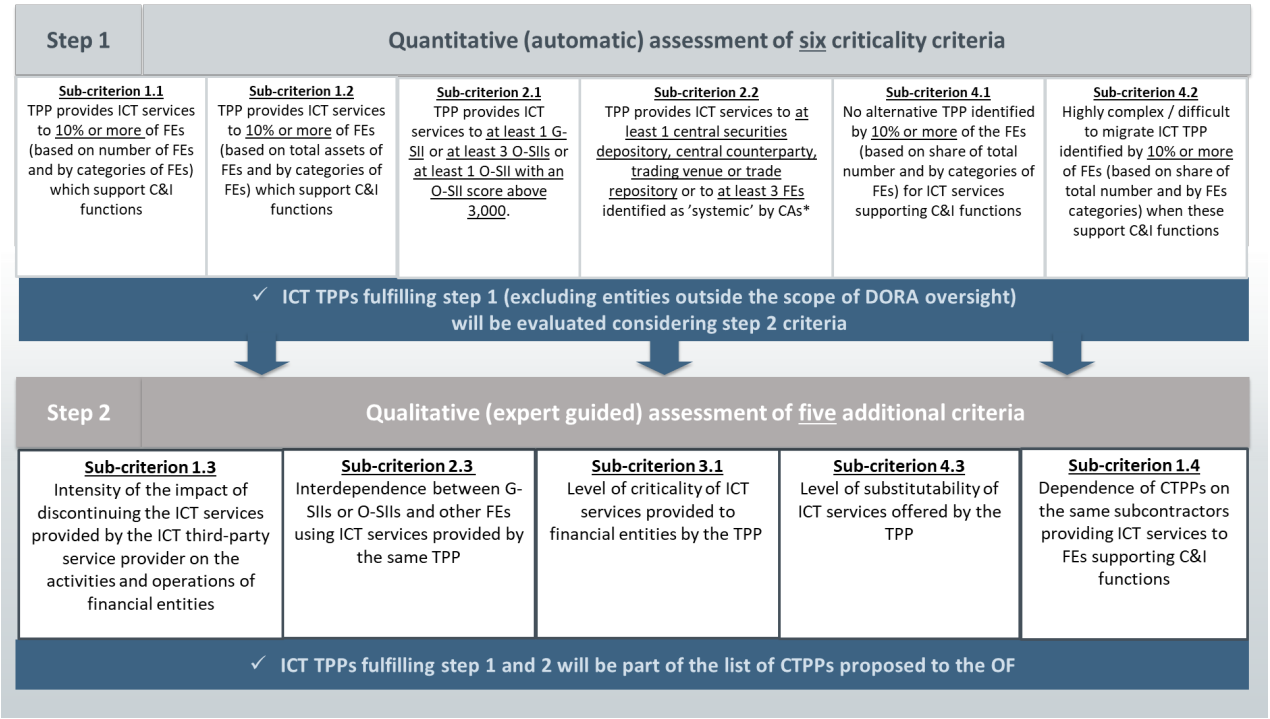
[16] The ESAs designate group structures as CTPP (i.e. focus on the parent company, with the ability to oversee all the subsidiaries providing the identified ICT services to the FEs).

[17] Digital Operational Resilience Regulation - European Commission (europa.eu).

[18] Commission Delegated Regulation (EU) 2024/1502 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities. The criteria are based on DORA Article 31(2).

[19]

Figure 5: Criticality assessment criteria



44. Following the assessment of the criteria, the LO notifies the ICT third-party service providers about the results of the criticality assessment. Following this notification, the providers have six weeks to submit a reasoned statement to the ESAs with any relevant information for the purposes of the criticality assessment.

45. The designation is followed by publication of the list of CTPPs. ICT TPPs that are not included in the list have the option to voluntarily request an assessment for CTPP designation. The information to be provided in the opt-in application and the way to assess applications are specified in Article 1 of the CDR on harmonisation of conditions enabling the conduct of oversight[20].

5.1.2 Key expectations for the coordination points of EU-CTPPs and subsidiaries of non-EU CTPPs

46. Once designated as critical, a CTPP is required to collaborate with the overseers in good faith and assist them in fulfilling their tasks as defined in Article 33 of DORA, specifically assessing whether the CTPP has comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risk it may pose to FEs.

47. To effectively perform their tasks, the overseers will establish a continuous dialogue with the CTPP, which must be properly organised to manage the multiple requests anticipated from the overseers.

48. Given the number of interactions expected for the conduct of oversight, it is important to clarify expectations on the corporate substance of the CTPP's coordination point or subsidiary liaising with the overseers.

[20] Commission Delegated Regulation (EU) 2025/295 of 24 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards on harmonisation of conditions enabling the conduct of the oversight activities

49. The Annex provides an overview of the key expectations for the coordination points of EU-CTPPs and subsidiaries of non-EU CTPPs.

5.2 Risk assessment and oversight planning

50. The overseers have implemented a dedicated Oversight Risk Assessment Process (ORAP), aimed at assessing the risks posed by CTPPs to FEs to choose a proportionate and risk-based approach for their examinations. This process is run on a yearly basis. It is informed by the data gathered through previous oversight activities and additional sources (e.g., the assessment of the threat landscape, incident notifications, outcomes of FEs' supervision performed by CAs, etc.).

51. The risk assessment identifies the risk profile of each CTPP, which is based on the identification and high-level assessment of the risks faced by the CTPP and the controls that have been put in place to mitigate these. The identification and assessment of CTPP-specific risks is performed against the various types of inherent and external risks, which have been identified as relevant for the CTPP, based on the ICT services it provides to FEs.

52. The risk assessment drives the identification of oversight priorities to address the identified risks concerning one or more ICT services, which are used as an input for the annual individual oversight plan, as well as the multi-annual oversight plan.

5.3 Examinations

53. The activities of a JET consist, on the one hand, in maintaining an **on-going monitoring** of the CTPP situation, and, on the other hand, in carrying out various examinations in the form of **general investigations** or **on-site inspections,** as foreseen in the annual oversight plan. Moreover, instances including the emergence of an unexpected situation, such as an incident or a new threat, may lead to the opening of a **Request for Information (RfI)**, enabling the overseer to assess the need for investigative action, such as an inspection.

54. This range of actions provides a gradual and proportional approach to deepening verifications, based on the significance of the identified risks. The following section provides high-level descriptions for each, contextualised within the DORA oversight framework.

55. The findings from examinations support the overseers' recommendations to the CTPP. These examination results are incorporated into the risk assessments and oversight plans for the following year, enabling continuous monitoring of residual risks and progress in compliance.

56. The following graphic depicts the interrelationships between examinations (general investigations and inspections), the ongoing regular monitoring and the annual risk assessment and individual annual oversight plan:

Figure 6: JET activities

5.3.1 Ongoing regular monitoring

57. Ongoing regular monitoring serves as the foundation for effective oversight, forming the background to the interactions between the overseers and the CTPPs as part of general investigations and inspections. This process primarily but not exclusively involves desktop-based tasks, including the systematic collection, analysis, and assessment of both firm-specific and sector-wide information obtained from CTPPs.

58. Ongoing regular monitoring activities generally, but not exclusively, entail:

    i. **Meetings with CTPPs**: At both managerial and staff level, such meetings aim to maintain an updated understanding and knowledge of the CTPP and to complement the information already gathered during the risk assessment, through direct interaction with the individuals in charge of specific risk matters.

    ii. **Collection and assessment of periodic data and information:** The overseers maintain a minimum level of information obtained for any type of CTPP, based on regular or ad-hoc information received through periodic information reporting and analysis. It informs on potential risks and provides the opportunity to monitor CTPPs across the board (data-based peer comparison). One essential type of information requested by overseers is the CTPPs' various periodic reports. It streamlines oversight activities by establishing a harmonised, efficient process for information collection, review, and fee calculation. This approach ensures consistency across all CTPPs, improves planning for both overseers and providers, and enhances the accuracy and completeness of critical information.

59. The periodic information collected is analysed regularly and feeds back (among information from other sources) into the annual risk assessments with respect to entity-specific issues, thereby creating a continuous cycle of information and regulatory interaction.

60. Examples of periodic information reporting include organisational charts, ICT budget documentation, information security testing reports, risk management work programme and reports, audited financial statements, etc.

61. Through these activities, the overseers develop a comprehensive and continuous understanding of CTPPs' organisation, business models, strategic developments, and associated risks, ensuring that oversight activities are documented over time. Furthermore, ongoing regular monitoring allows the identification of potential vulnerabilities, such as weaknesses in ICT risk management frameworks, governance structures, or strategic risk approaches. Additionally, it serves as a mechanism to track the implementation of previous recommendations and assess whether deficiencies have been effectively addressed.[21] The insights derived from ongoing regular monitoring feed into the annual risk assessment and the individual annual oversight plan, as well as into both general investigations and inspections.

5.3.2 Requests for information

62. Outside the context of general investigations and inspections, the overseers also have the power to request CTPPs to submit information either by '**Simple Request**' (Simple RfI) or by '**Decision'** (Decision RfI)[22]. This is particularly suited to the context of the emergence of a new situation, which could not have been covered by the oversight plan. It allows overseers to ask the CTPP for some preliminary information in order, for example, to decide if some examinations are needed.

Table 2: Types of RfI

Simple RfI	The Simple Request for Information (RfI) is a standard type of information request for CTPPs. While CTPPs are expected to respond to Simple RfIs, there are no financial penalties associated with missing the set deadline. However, it is crucial that the information provided is accurate and not misleading.
Decision RfI	A Decision RfI is a formal request governed by strict procedural guidelines. Non-compliance with the request, including failure to respond within the specified timeframe or providing incomplete information, will incur penalties for the CTPP.

63. RfIs clearly and precisely indicate the information needed, as well as its scope and the timeframe for responding.

5.3.3 General investigations

64. General investigations are formal reviews performed by overseers covering one or more risk areas of the CTPPs. The objective of a general investigation is to gather information[23] on how CTPPs manage the risks associated to the services provided to FEs.

65. General investigations are formal, structured interactions between overseers and CTPPs. These investigations are initiated by a decision and written authorisation from the overseers, which outline key elements such as the individuals conducting the investigation, the subject matter and purpose, an explanation of the specific areas under scrutiny, information about potential periodic penalty payments and available remedies or recourse. This decision serves as a framework for the investigation process, ensuring transparency and clarity for all parties involved. There are several potential types of reviews that may be employed, jointly or independently, within the context of general investigations,

[21] The report mentioned in Article 35 also allows to track the implementation of the recommendation.
[22] According to DORA Article 37(2) and (3).
[23] During the course of a general investigation, authorised individuals have several powers, including the ability to obtain and examine all records, data, procedures, and other materials relevant to scope of the general investigation. This is not to be confused with the RfI, a separate DORA oversight power to gather information used outside general investigations and inspections.

depending on the specific need of oversight. The table below provides examples of possible types of general investigations:

Table 3: Types of general investigations

"Regular" general investigation	General investigation to gain a high-level understanding of, inter alia, the risks, business operations, the most critical ICT services and trends.
Thematic (horizontal) investigation	Primary tool used to assess common risks and trends across the CTPPs, as well as any other emerging risks, to assess their scale and nature. Usually, these investigations start from macro or sectoral analyses conducted off-site, through data collections and questionnaires, and may be followed by dedicated on-site inspections.
Targeted investigation (deep dive)	Carried out following the identification of a specific risk at the level of a single CTPP. These activities will help gain an understanding of specific areas of concern for a single CTPP and will be characterised by a mix of off-site activities and simple meetings based on cooperation with the CTPP.
Follow-up investigation	These investigations follow up on previous oversight activities and go more into detail than simple on-going monitoring. For instance, with reference to the implementation of recommendations such investigations check in detail the progress made by CTPPs in implementing the recommendations issued during previous oversight activities, particularly in relation to a high-risk area.

66. General investigations consolidate any resulting findings into an investigation report. This may inform the issuance of any recommendations to correct potential areas of non-compliance identified during the general investigation, as well as the subsequent request, after the completion of the oversight activities, of reports specifying the actions that have been taken or the remedies that have been implemented by the CTPPs in relation to the recommendations made.

5.3.4 Inspections

67. Inspections are used as a method to oversee CTPPs with an increased level of intrusiveness, versus what is afforded by general investigations and, to an even lesser extent, by ongoing regular monitoring. Inspections may be conducted at any business premises of the CTPPs, at the head offices or any operational building, secondary premises of the CTPP and may also be conducted off-site if this is suitable for the overseers. Inspections aim to achieve a deeper understanding of CTPPs' business operations, risk management and internal controls, among other aspects, through the gathering of information[24]. Compared to general investigations, inspections typically also entail a more direct and immediate communication with the CTPP. During inspections, JETs perform on-site as well as off-site inspection tasks.

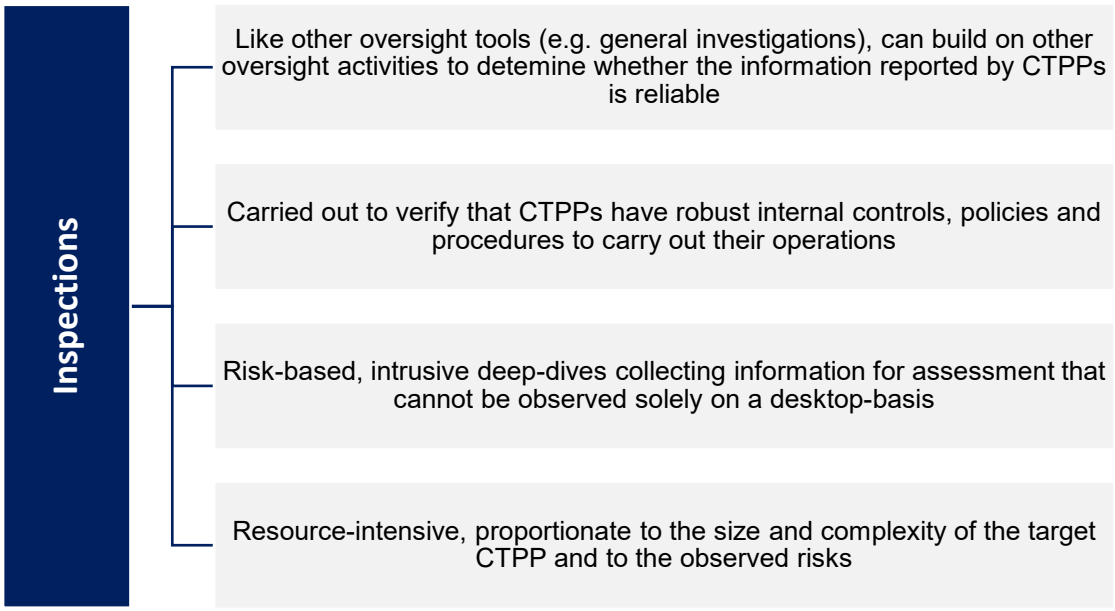
68. Based on the risk assessment performed, the overseers determine the frequency of inspections for each CTPP. The main inspections for a given year are based on the annual risk assessment and included in the individual annual oversight plan, which will determine how such inspections will help achieve the

[24] During the course of an inspection, authorised individuals have several powers, including accessing business premises and covering all ICT systems, networks, devices, information and data for the provision of the relevant ICT services and relating to scope of the inspection. This is not to be confused with the RfI, a separate DORA oversight power to gather information used outside general investigations and inspections.

annual oversight objectives. However, the overseers may also engage in further inspection depending on information collected during the oversight year and on new risks emerging in the market.

69. Similarly to general investigations, inspections are governed by a decision and written authorisation from the overseers, which outline several key elements such as the individuals who will conduct the inspection, the subject matter and purpose, and the start date of the inspection. The decision also provides an explanation of the specific areas or topics to be examined. Additionally, it includes information about the possibility of periodic penalty payments and on available remedies. The decision ensures that all aspects of the inspection are clearly defined and communicated to the parties involved. The following graphic summarises some of the key aspects that define inspections. Noteworthy to highlight is that inspections are intended to be risk-based, forward-looking and action-oriented. Their primary goal should be to gain a better visualisation and understanding of practices, processes, layout, and equipment of CTPPs.

Figure 7: Inspections



70. On-site inspections are tailored to thoroughly examine specific risk areas. Despite this customization, all on-site inspections share common stages. These stages are reflected in the annual oversight plan and encompass several key phases:

    i. The process begins with inspection planning and initial information gathering, followed by scoping and pre-inspection tasks. It then progresses to on-site information gathering and analysis.

    ii. The inspection is carried out by the mandated JET members at the premises of the CTPP which are relevant for the examinations. It aims at checking and assessing a CTPP's situation and the risks it can pose to FEs.

    iii. The inspection concludes with the preparation of an inspection report that presents the facts and preliminary findings of the inspection. It is shared with the CTPP for verification.

    iv. The inspection report undergoes a quality assessment and post-inspection tasks are performed.

v. On the basis of the findings and following a quality assessment, the JET prepares preliminary recommendations.[25]

vi. Material findings, preliminary recommendations and any possible remediation timings are discussed with the CTPP, notably at a closing meeting. Recommendations are adopted through the oversight governance process.

71. While each inspection is uniquely designed to address particular risk areas, this framework provides a consistent structure for the inspection process, ensuring thoroughness and uniformity across different inspections.

Figure 8: Common stages of inspections

5.3.5 Communication Language

72. English serves as the operational working language for the ESAs and CAs involved in the DORA oversight framework.

73. English is also the preferred language for communications between the overseers and the CTPPs. However, the overseers comply with the language requirements referred to in Regulation 1 of 1958[26].

[25] The detailed step by step procedure on recommendations can be found in Section 6.
[26] Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385).

5.4 Recommendations and follow up

74. As a result of examinations, overseers are empowered to issue recommendations to CTPPs and to follow up on these recommendations. Each recommendation is directly linked to a specific finding from the examination. The overseers communicate these recommendations transparently to the CTPP, clearly connecting each finding to its corresponding recommendation. This process ensures that CTPPs understand the basis for each recommendation and the specific areas that require attention or improvement.

5.4.1 Recommendations

75. Overseers can issue recommendations to the CTPP for areas of assessment identified in DORA Article 33(1)[27] and all elements listed in Article 33(3) of DORA relating to the rules, procedures, mechanisms and arrangements that CTPPs have in place to manage the ICT risks they may pose to FEs, including:

- the use of specific ICT security and quality requirements or processes, in particular in relation to the roll–out of patches, updates, encryption and other security measures.
- the use of conditions and terms under which the CTPPs provide ICT services to FEs.
- any planned subcontracting, where the LO deems that further subcontracting may trigger risks for the provision of services by the FE, or to financial stability.
- refraining from entering a further subcontracting arrangement.

76. The recommendations are provided with an indication of their sensitivity and the priority expected for remediation.

77. The overseers decide how detailed recommendations should be with respect to the actions requested to the CTPPs depending on the nature of the findings. Overseers articulate their recommendations with clarity about the envisaged:

- ultimate outcome, regardless of the specific internal actions that will be taken for that purpose, provided that these actions will not generate further risks in other areas;
- timeline to complete the remedial actions. Some actions might be identified as short-term ones (e.g., 3-6 months), while more complex remediations will be afforded longer periods (e.g., up to 1-2 years).

78. As part of the process of issuing recommendations, CTPPs are granted 30 days to provide information evidencing the expected impact of the recommendation on customers that are not FEs and formulating solutions to mitigate risks.

79. Finally, when a recommendation is issued, the CTPPs have the duty to formally notify the overseers their intention to follow the recommendation.

[27] DORA Article 35(1) for areas of assessment identified in DORA Article 33(1). These recommendations are non-public, they are submitted to the CTPP, but CAs are informed about it, while FEs are made aware of the associated risks.

5.4.2 Follow up on recommendations

80. When a CTPP notifies the overseers its intention to follow a recommendation, the overseers request the CTPP to share a remediation plan explaining how they plan to address the findings associated with the recommendation. Such remediation plans outline the actions and the measures that the CTPP plans to take or implement to comply with the issued recommendation. The remediation plan, together with the reports on the progress on the implementation, is the tool used by the overseers during the ongoing regular monitoring to follow up on the recommendations.

81. In addition to the overseers' role *vis-a-vis* the CTPPs, the oversight framework foresees a specific role for CAs in relation to the follow up of recommendations. More specifically, as the CAs exercise supervisory responsibility over FEs, CAs ensure appropriate follow-up on the risks identified in the recommendations concerning FEs making use of the services of the CTPPs. As part of the follow up actions, the overseers can ask CAs to report their assessment on the impact that these measures have on FEs.

82. If a CTPP decides not to follow a recommendation, it must provide a reasoned explanation. Should the overseers find this explanation insufficient, DORA mandates that they publicly disclose the CTPP's identity. This disclosure will include information about the type and nature of the non-compliance[28]. This measure ensures transparency and accountability in the oversight process, encouraging CTPPs to take recommendations seriously and implement necessary changes to maintain compliance with DORA regulations.

83. In those cases, CAs may, among other things, decide to issue warnings to FEs depending on the risks associated with the recommendation. Finally, in such cases, after consulting the OF, the overseers can issue non-binding and non-public opinions to CAs to promote consistent and convergent follow-up measures. As a measure of last resort, CAs may require a FE to suspend, or even terminate, the use or deployment of a service provided by a CTPP.

[28] In accordance with Article 42(2) of DORA.

6 DORA oversight processes

84. This section provides an overview of the administrative processes followed by the overseers when executing the oversight activities.

85. The processes vary for each oversight activity. However, the initial steps are standardised across all activities and can be summarised in a general process as specified in Subsection 6.1.

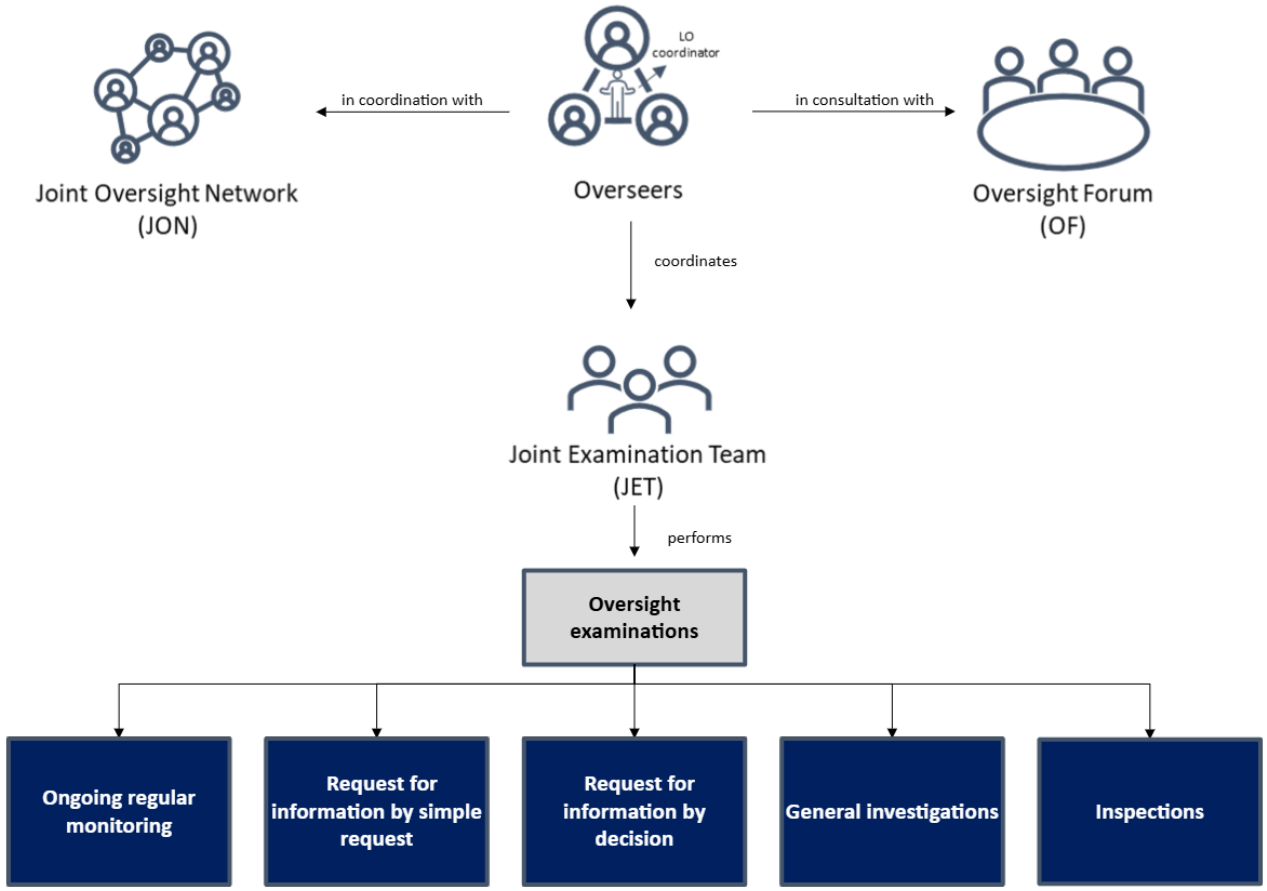
86. The other subsections illustrate the processes regarding the:

    i. Request for Information by simple request (Subsection 6.2);
    ii. Request for Information by decision (Subsection 6.3);
    iii. General investigations (Subsection 6.4);
    iv. Inspections (Subsection 6.5);
    v. Issuance and follow up of recommendations (Subsection 6.6); and
    vi. Oversight activities outside the Union (Subsection 6.7)

87. The diagrams provided illustrate the processes in a simplified manner. For complete and detailed processes, refer to the respective legal references and legal texts.

6.1 General process for requests for information, general investigations, inspections

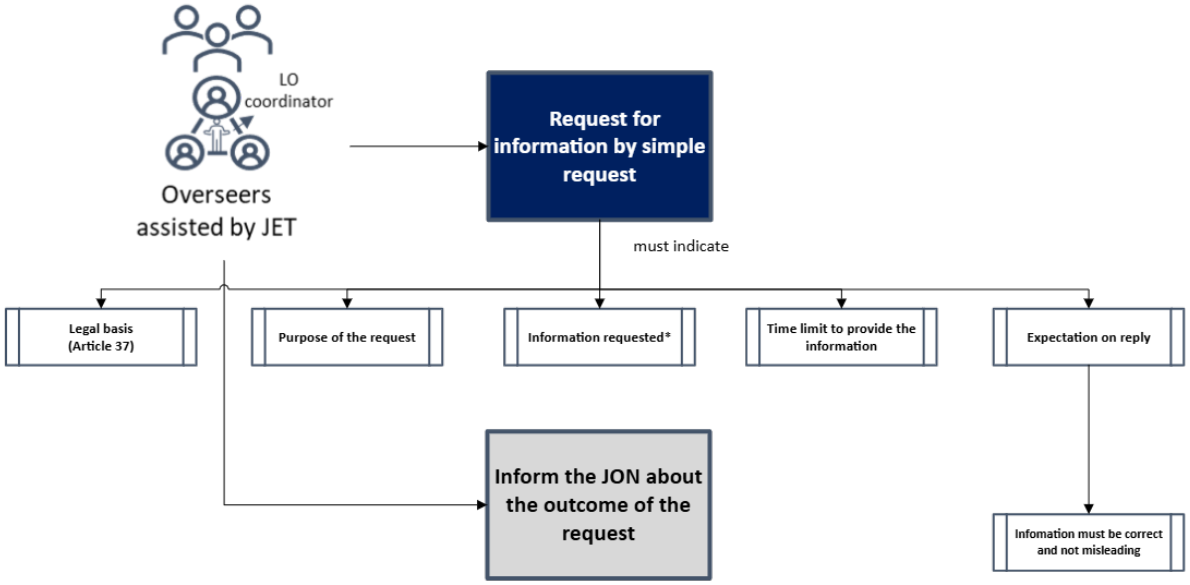
Figure 9: General process for oversight activities



Description of Figure 9	Figure 9 shows the general process for examinations. Such examinations are performed by the overseers in coordination with the JON and in consultation with the OF and, where applicable, should be approved by decision. The day-to-day work to perform the examinations is done by the JET under the coordination of an appointed staff member of the overseers (the 'Lead Overseer coordinator').
Legal references	• *Articles 35-42, DORA*

6.2 Request for information by simple request

Figure 10: Request for information by simple request

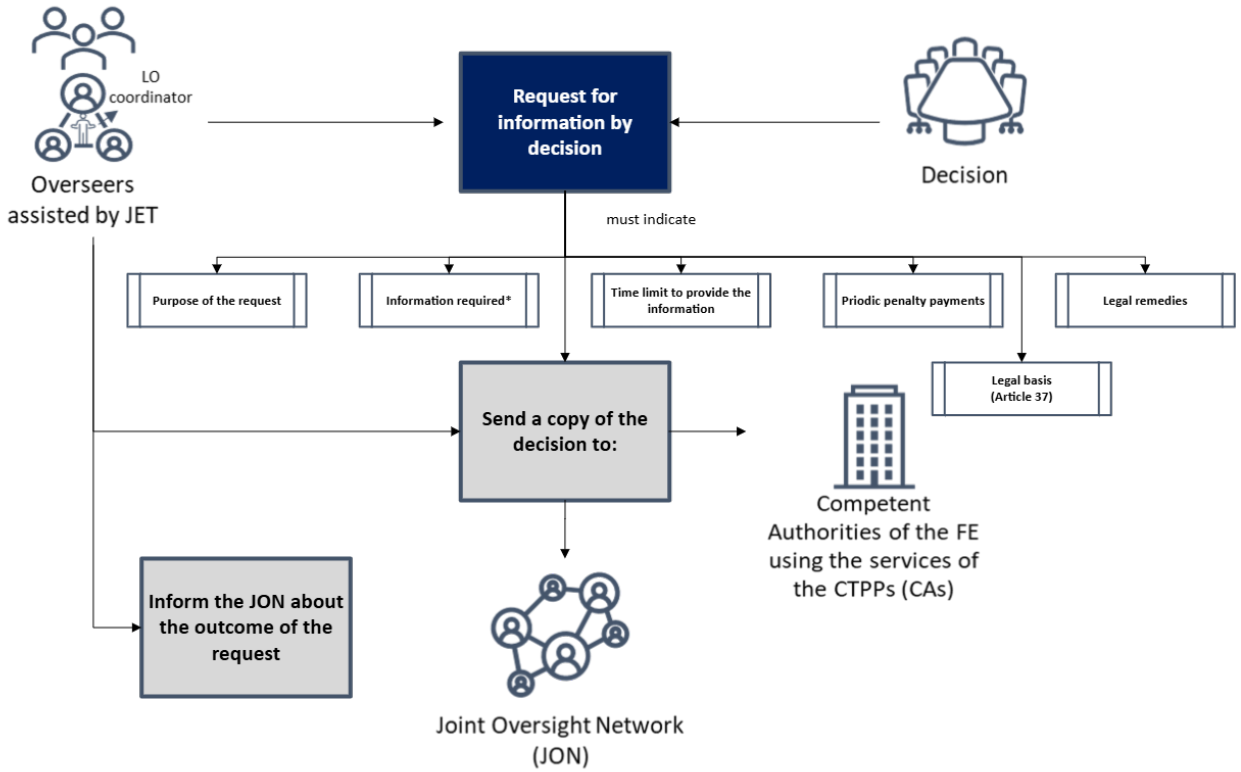


* Information that can be requested includes the information indicated in Article 2 of the RTS on harmonisation of conditions enabling the conduct of the oversight activities.

Description of Figure 10	Figure 10 shows the process to request information by simple request. When making a simple information request, the overseers must cite the legal basis, state the purpose of the request, specify the required information, set a deadline for the CTPP to provide the information, and inform the CTPP that responding is voluntary, but the reply must not be incorrect or misleading. The overseers should request information ensuring the regular coordination within the JON and in consultation with the OF, as specified in Section 6.1. Finally, the overseers should inform the JON about the outcome of the request for information.
Legal references	• *Article 35(1)(a), 36(1)(a), and 37(1), (2) and (4) of DORA* • *Article 2 of the CDR on harmonisation of conditions enabling the conduct of the oversight activities.*

6.3 Request for information by decision

Figure 11: Request for information by BoS decision

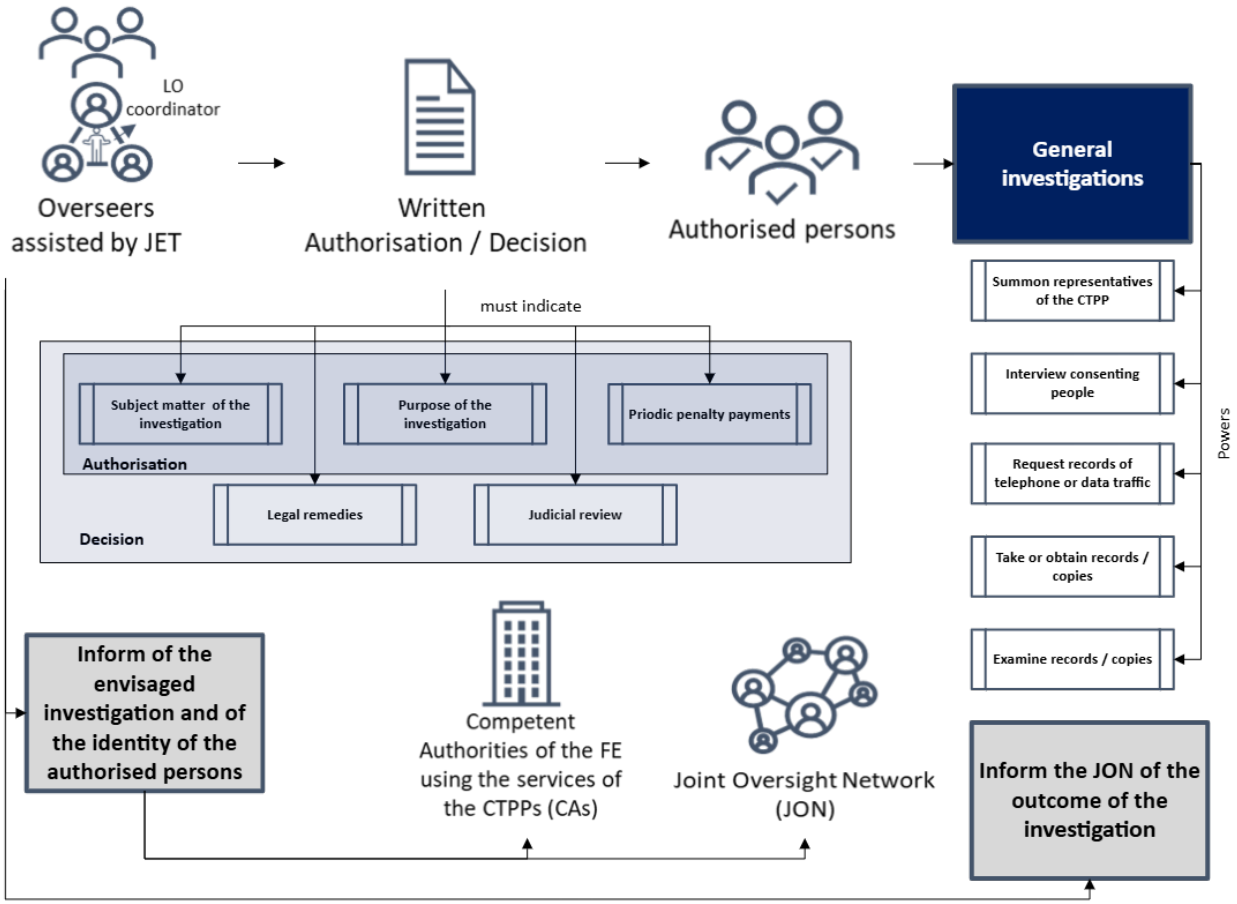


* Information that can be requested includes the information indicated in Article 2 of the RTS on harmonisation of conditions enabling the conduct of the oversight activities.

Description of Figure 11	Figure 11 shows the approval process to request information by decision. The overseers should issue such decision with regular coordination within the JON and in consultation with the OF, as specified in Section 6.1. The decision must cite the legal basis of such power, state the purpose of the request, specify the required information, set a deadline for the CTPP to provide the information, and mention potential periodic penalties. The overseers must also provide indications on the right to appeal the decision. The CTPP must supply the requested information and is responsible if the information is incomplete, incorrect or misleading. The overseers must promptly share the decision with relevant Competent authorities and the JON. Finally, the overseers should inform the JON about the outcome of the request for information.
Legal references and Guidelines	• *Article 35(1)(a), 36(1)(a), and 37(1) (3-5), DORA* • *Article 2 of the CDR on harmonisation of conditions enabling the conduct of the oversight activities* • *Guideline 9 of the Guidelines on ESAs-competent authorities oversight cooperation*

6.4 General investigations

Figure 12: General investigations

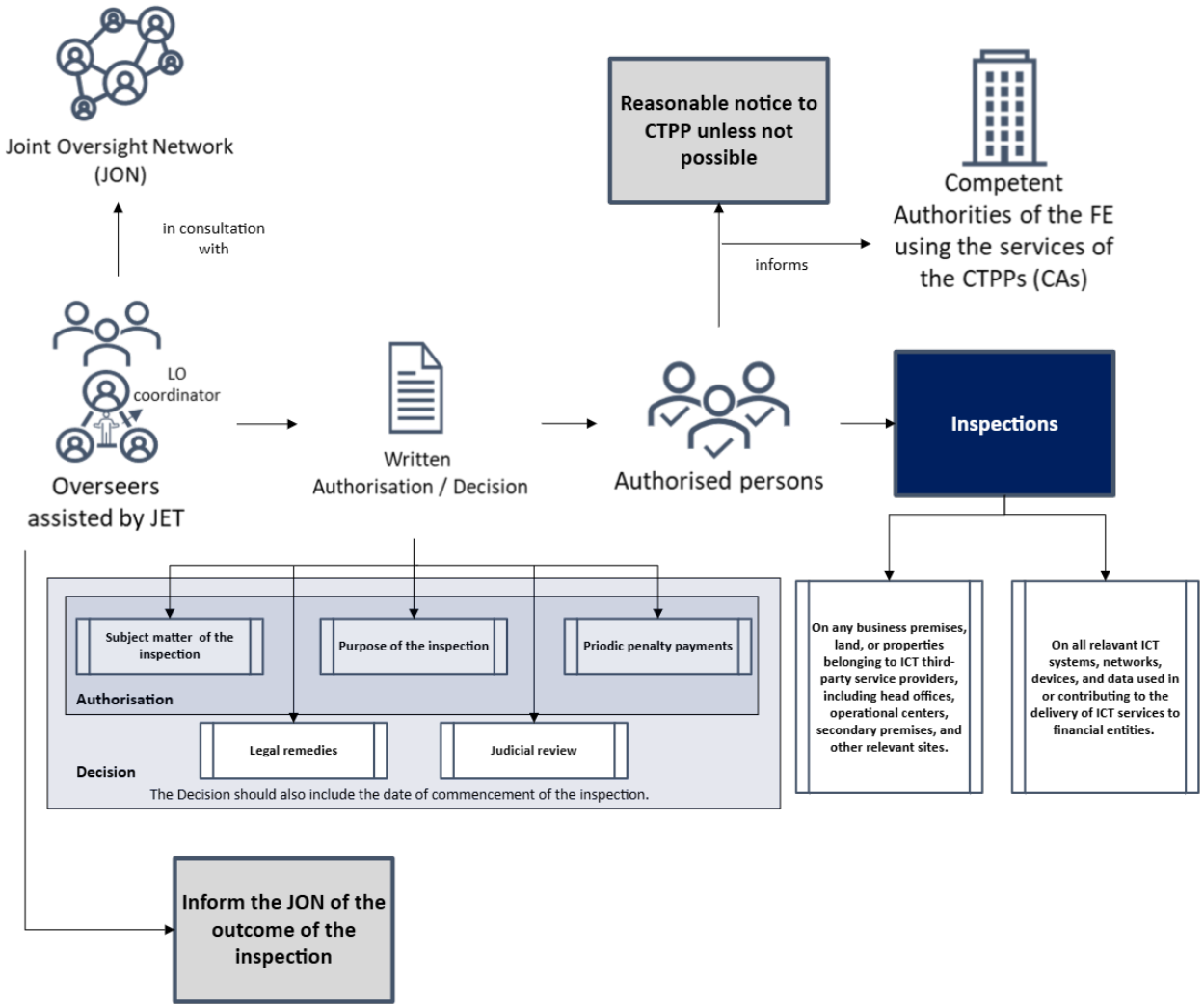


Description of Figure 12	Figure 12 shows the approval process to initiate and conduct general investigations. This activity is performed with regular coordination within the JON and in consultation with the OF, as specified in Section 6.1. Before proceeding, the overseers prepare the written authorisation specifying: (i) the investigation's subject matter and purpose; (ii) the periodic penalty payments applicable in case of non-compliance under Article 35(6); (iii) the authorised individuals that will perform the investigations. The overseers prepare also the decision that should include: (i) the investigation's subject matter and purpose; (ii) the periodic penalty payments applicable in case of non-compliance under Article 35(6); (iii) the legal remedies available under the funding Regulations of the ESAs; and (iv) the right to request a review of decisions by the Court of Justice of the EU. Before the start of the investigation, the overseers inform the CAs of the FEs using the service of the CTPP about the planned investigation. This notification includes information on the envisaged investigation and the identity of the authorised individuals. Additionally, the overseers communicate all relevant information about the investigation to the JON to ensure transparency and coordination. During the investigation, the authorised individuals have several powers. They may request for and examine all records, data, procedures, and other materials relevant to their tasks, irrespective of the storage medium; take or obtain certified copies or extracts of these

	documents for further analysis; summon representatives of CTPP to provide oral or written explanations about facts or documents related to the investigation, and their answers must be recorded; interview other consenting individuals to collect additional information; and request telephone and data traffic records as necessary. Article 2 of the CDR on harmonisation of conditions enabling the conduct of the oversight activities includes a non-exhaustive indication of the information that can be requested by the overseers. The representatives of the CTPP are required to provide all requested materials and information and they shall not be incomplete. Non-compliance or incomplete responses may result in the imposition of periodic penalty payments as referred to in Article 35(6). Within three months of completing an investigation, the overseers issue recommendations to the CTPP after consulting the OF (See section 5.4).
Legal references and Guidelines	• *Article 35(1)(b), Article 36(1)(b), Article 38 and Article 40(1)(3), DORA* • *Article 2 of the CDR on harmonisation of conditions enabling the conduct of the oversight activities* • *Guideline 7 of the Guidelines on ESAs-competent authorities oversight cooperation*

6.5 Inspections

Figure 13: Inspections

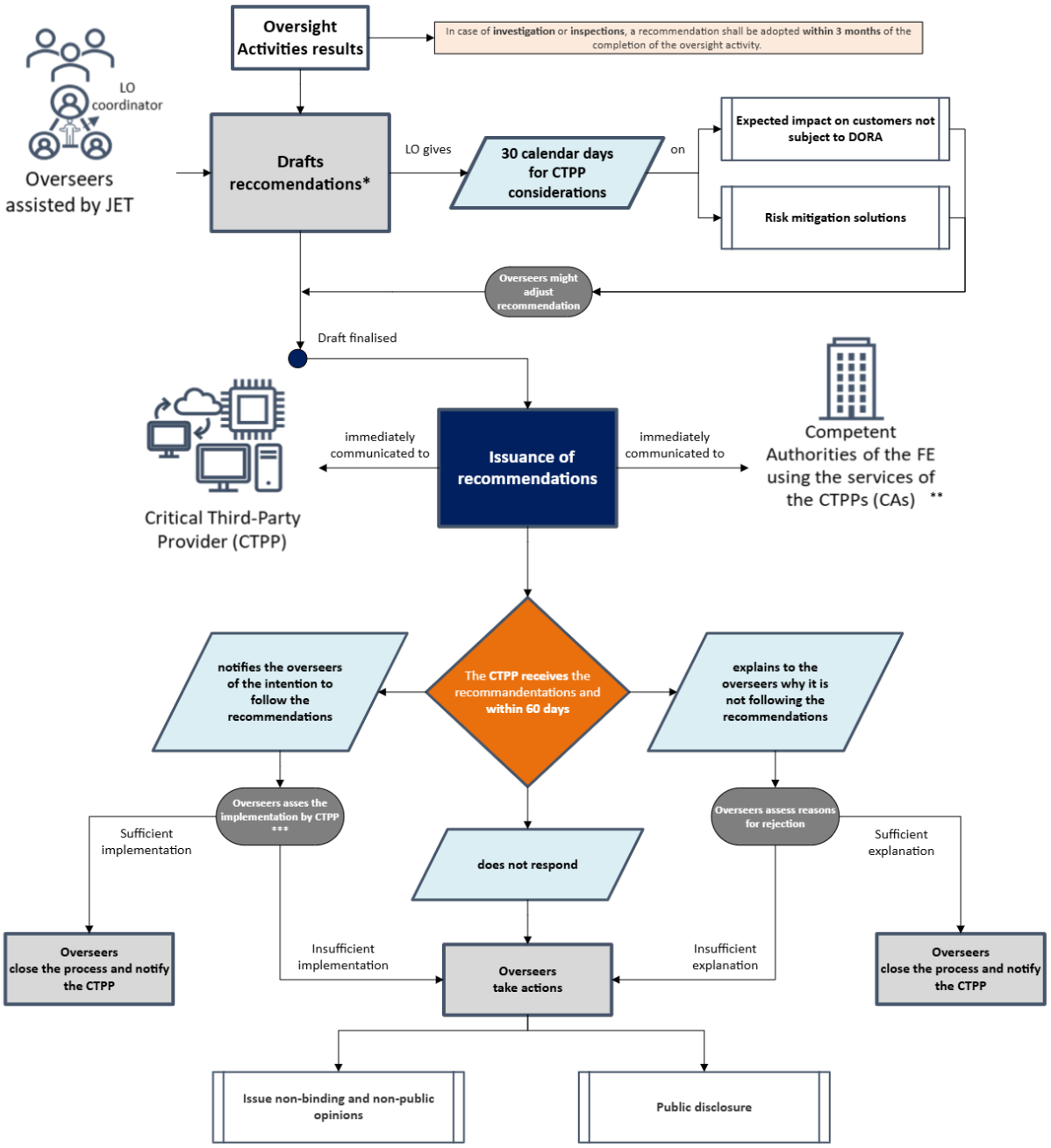


Description of Figure 13	Figure 13 shows the approval process to conduct inspections. These may involve examinations of business premises, land, or properties belonging to ICT third-party service providers, including head offices, operational centres, secondary premises, and other relevant sites. Additionally, inspections may encompass all relevant ICT systems, networks, devices, and data used in or contributing to the delivery of ICT services to FEs. The essence of inspecting is going onsite, but the regulation also caters for offsite examinations. The overseers should perform inspections with regular coordination within the JON and in consultation with the OF, as specified in Section 6.1. Before proceeding, the overseers prepare the written authorisation specifying: (i) the inspection's subject matter and purpose; (ii) the periodic penalty payments applicable in case of non-compliance under Article 35(6); (iii) the authorised individuals that will perform the inspection. The overseers prepare also the decision that should include: (i) the inspection's subject matter and purpose and the date of commencement of the inspection; (ii) the periodic penalty payments applicable in case of non-compliance under Article 35(6); (iii) the legal remedies; and (iv) the right to request a review of decisions by the Court of Justice.

	The overseers inform the CAs of FEs using the services of the CTPP about the planned inspection. The overseers provide reasonable notice to the CTPP before an onsite inspection, unless the notice is not possible in cases of emergencies, crisis situations, or circumstances where advance notice could compromise the effectiveness of the inspection. Authorised persons conducting onsite inspections request for documents and gather information and are also empowered to enter the premises and seal business locations, books, or records for the duration and extent necessary for the inspection and gather information on the ICT systems, networks, devices, information and data either used for, or contributing to, the provision of ICT services to financial entities relevant for the scope and purpose of the inspection. The representatives of the CTPP are required to comply with inspections. Opposition to an inspection may result in consequences, including informing CAs of FEs utilising the services of the CTPP. This could lead to requirements for FEs to terminate their contractual relationships with the non-compliant CTPP. Within 3 months of completing an inspection, the overseers will consult the Oversight Forum and issue recommendations to the CTPP (See section 5.6).
Legal references and Guidelines	• *Article 35(1)(b), Article 36(1)(b), Article 39 and Article 40(1)(3), DORA* • *Guideline 7 of the Guidelines on ESAs-competent authorities oversight cooperation*

6.6 Issuance and follow up of recommendations

Figure 14: Recommendations



* Recommendations can be issued on the areas indicated in Article 33(3) of DORA with a particular attention to the areas identified in Article 35(1)(d) of DORA.
** CAs assess CTPPs' measures based on LO's recommendations (Article 6(2) RTS), take actions per Article 42 DORA, and inform the LO of their assessment and decisions regarding FEs.
*** The LO can request reports on actions taken or remedies implemented by the CTPP regarding the recommendations. These reports should be sent to the JON and the CAs of FEs using the CTPP's ICT services.

Description of Figure 14Error! Reference source not found.	Figure 14 shows the approval process to issue a recommendation. The overseers should perform this activity with regular coordination within the JON and in consultation with the OF as specified in Section 6.1. The overseers can draft recommendations addressing the areas described in Section 5.4.1 of this Guide. In case of general investigations or inspections, recommendations shall be adopted within three months of the completion of the oversight activity.

	The overseers submit the draft recommendation to the CTPP. The latter is given 30 calendar days to submit its considerations regarding evidence of potential impacts on customers not subject to DORA and any proposed solutions to mitigate identified risks. Once this period concludes, the overseers might adjust the recommendation as necessary, ensuring that they reflect both the oversight findings, and the input received from the CTPP. The adopted recommendation should be communicated without delay to the CTPP and to the CAs of the FEs using its ICT services. Upon receiving the recommendation, the CTPP has 60 calendar days to notify the overseers of its intention to follow the recommendation or to provide a reasoned explanation for not doing so. If the CTPP notifies the overseers of its intention to follow the recommendation, the overseers can request reports on actions taken or remedies implemented by the CTPP regarding the recommendations. On this basis, the CTPP shall provide a report containing a description of actions taken and remedies mitigating the risks identified in the recommendations. To enable the monitoring of the implementation of the actions that have been taken or the remedies that have been implemented by the CTPP in relation to the recommendations received, the CTPP shall share with the overseers, upon request, interim progress reports (and related supporting documents) and/or final reports (and related supporting documents). These reports should be sent to the JON and the CAs of FEs serviced by the CTPP. The overseers will then assess the implementation of the proposed measures. • If the overseers consider the implementation sufficient, it closes the process and notifies the CTPP. • In case the CTPP provides explanation for non-compliance, which is considered sufficient by the overseer, the latter closes the process and notifies the CTPP. • If the CTPP does not respond to the recommendation after 60 days or refuses to endorse the recommendation and its explanation for non-compliance is deemed insufficient or if the CTPP, the overseers take further steps. These steps include public disclosure of the non-compliance or issuing non-binding and non-public opinions to CAs to promote consistent supervisory follow-up measures. As part of their supervision of FEs, the CAs supervising FEs relying on the CTPPs shall assess the impact of the measures taken by the CTPPs based on the recommendations of the overseers, taking into account the elements described in Article 6(2) of the RTS on harmonisation of conditions enabling the conduct of the oversight activities, then may follow-up based on Article 42 of DORA. CAs should inform the overseers of the assessment performed and the potential decisions taken towards the FEs.
Legal references ang Guidelines	• *Article 35(1)(c)(d) (3) and (4), Article 36(3), Article 40(3-4), Article 42 DORA* • *Articles 3 and 6 of the CDR on harmonisation of conditions enabling the conduct of the oversight activities* • *Section 4 of the Guidelines ESAs-competent authorities oversight cooperation*

6.7 Oversight Activities outside the Union

88. In cases where the overseers are unable to achieve oversight objectives through interaction with EU subsidiaries or by conducting oversight activities only on premises within the Union, the overseers may exercise their powers on premises located in a third country. These premises must be owned or used by a CTPP to provide services to Union FEs. The overseers can request information, conduct investigations, and perform inspections[29].

89. The overseers may only exercise these powers in a third country if certain conditions are met:

    i. the inspection must be deemed necessary to perform its duties fully and effectively;

    ii. the inspection must be directly related to the provision of ICT services to Union FEs;

    iii. the CTPP must consent to the inspection; and

    iv. the relevant third-country authority must have been notified by the overseers and raise no objections to the inspection.

90. If the overseers wish to conduct oversight activities in a third country, the ESAs shall conclude administrative cooperation arrangements with the third-country authority to ensure smooth coordination of oversight activities, including general investigations and inspections. The cooperation arrangements should also establish mechanisms for transmitting relevant information, notifying authorities of violations by third-country ICT service providers, sharing updates on regulatory developments, and allowing participation of the third-country authority in inspections, if necessary.

91. In cases where the overseers cannot conduct the oversight activities outside the Union, they shall exercise their powers based on the available facts and documents. The overseers must document and explain the consequences of the inability to carry out the oversight activities. These consequences must be considered in the overseers' recommendations under Article 35(1)(d).

Legal references	• *Article 36, DORA*

[29] Not all the powers available in cases of general investigations and inspections are available in case in which such tools are used in third countries (see Article 36(1) of DORA).

Annex

Key expectations for the coordination points of EU-CTPPs and subsidiaries of non-EU CTPPs

1. The ESAs have defined the following expectations taking into account:
    a) the requirements for EU and non-EU CTPPs, respectively, to designate one legal person as a coordination point (Article 31(4) of DORA) and to establish a subsidiary in the Union (Article 31 (12) of DORA);
    b) need to ensure a level playing field for all CTPPs;
    c) types of interactions between the overseers and the CTPP; and
    d) principle of proportionality (Article 4 of DORA).
2. The ESAs expect that EU and non-EU CTPPs which are part of a group:
    a) designate one legal person, established in the EU, which is part of the group, as a coordination point to ensure adequate representation and communication with the overseers; and
    b) notify the overseers of any changes to the structure of the management within their group.
3. The ESAs expect the coordination points of EU-CTPPs and subsidiaries of non-EU CTPPs to have a corporate structure and seniority of staff proportionate to the nature, scale, complexity of the CTPP's business. In this context, the ESAs expect that they have:
    a) the capacity to provide the overseers with sufficient information about the services provided by the CTPP to FEs in the EU;
    b) the authority, technical capacity, equipment, business premises and financial resources to pull the type of information defined in Article 2 of Commission Delegated Regulation (EU) 2025/295[30], and ensure that relevant staff of the CTPP is available to address the requests of the overseers;
    c) the ability to provide the overseers with all the relevant accounting and financial information relating to the CTPP[31] to calculate the annual oversight fees;
    d) access to the financial resources to cover the yearly payment of oversight fees or, by liaising with the relevant group entities, the periodic penalty payment the overseers may charge the CTPP according to Article 35(6-11) of DORA;
    e) a sufficient number of staff with appropriate knowledge and competence which are able to engage with the overseers – at different levels of seniority – during the oversight activities and follow-up of recommendations;
    f) management with sufficient authority and knowledge to commit the CTPP on the oversight activities and to which escalation can be made; and
    g) business offices space sufficient to allow the conduct of on-site inspections by the JETs.

[30] Delegated regulation - EU - 2025/295 - EN - EUR-Lex
[31] In particular, see Article 2(2) of Delegated Regulation (EU) 2024/1505