JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 93
29 November 2024

Mandate of the Oversight Forum as a Joint Committee Sub-Committee of the European Supervisory Authorities

1. Framework

1. In accordance with 32(4) of Regulation 2022/2554 (DORA)[1] the Oversight Forum (OF) is established for the purposes of supporting the work of the Joint Committee (JC) and of the Lead Overseer (LO) referred to in Article 31(1), point (b), in the area of ICT third-party risk across financial sectors. The OF shall prepare the draft joint positions and the draft common acts of the JC in that area. The OF shall regularly discuss relevant developments on ICT risk and vulnerabilities and promote a consistent approach in the monitoring of ICT third-party risk at Union level.

2. Tasks

2. The OF shall prepare the draft joint positions and the draft common acts of the JC in the area of digital operational resilience and more specifically the ICT third-party risk across financial sectors. This includes, but is not limited to:

   a) regularly discuss relevant developments on ICT risk and vulnerabilities and promote a consistent approach in the monitoring of ICT third-party risk at Union level, including in relation to ICT third-party service providers that are not designated as critical and subject to oversight by the ESAs;

   b) promote coordination 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;

   c) discuss the draft strategic multi-annual plan prepared by the LO in agreement with the Joint Oversight Network (JON);

   d) when consulted by the LO, provide information or advice in the context of the exercise of the LO's powers (information requests, general investigations and inspections, reports specifying the actions taken or remedies implemented by the critical ICT third-party service providers (CTPP), recommendations) or in relation to opinions to competent authorities (CAs) where a CTPP refuses to endorse recommendations; and

   e) additional tasks in relation to DORA where necessary.

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

3. Type of deliverables

3. On the basis of the preparatory work carried out by the ESA staff and, where applicable, the joint examination teams, the OF shall prepare the following draft deliverables linked to the oversight cycle. This includes, but is not limited to:

   a) undertake an annual collective assessment of the results and findings of the oversight activities conducted for all CTPPs;

   b) propose a recommendation to the JC on the ICT third-party service providers that should be identified as critical for financial entities, following an assessment that takes into account the criteria defined in Article 31(2) of DORA;

   c) propose a recommendation to the JC on the appointment of the LO for each CTPP, in accordance with the criteria defined in Article 31(1)(b) of DORA;

   d) submit comprehensive benchmarks for CTPPs to be adopted by the JC as joint positions of the ESAs; and

   e) conduct the preparatory work for the development by the ESAs of the yearly report on the application of Section II of DORA (Oversight Framework); and

   f) additional deliverables in relation to DORA, where necessary.

4. The Chairperson of the OF and the secretariat, in coordination with the JON, shall prepare a draft annual work plan which provides an overview of the deliverables of the OF for the upcoming year. The draft annual work plan shall be discussed and approved by the OF. The OF shall organise its work and its deliverables with regard to the JC's meeting schedule.

5. The authorities involved in the OF shall take all appropriate and necessary measures to ensure the OF is at all times staffed adequately to carry out its tasks and deliverables.

4. Internal organisation

4.1 Membership

6. In accordance with Article 32(4) of DORA, the OF shall be composed of:

   a) Members with voting rights, which shall be:

      i. the Chairpersons of the European Supervisory Authorities (ESAs); and

      ii. one high-level representative from the current staff of the relevant competent authority referred to in Article 46 of DORA (relevant CA) from each Member State.

   b) Observers without voting rights, which shall be:

      i. the Executive Directors of each ESA and one representative from each of the following bodies: European Commission, European Systemic Risk Board (ESRB), European Central Bank (ECB) and European Union Agency for Cybersecurity (ENISA);

      ii. where appropriate, one additional representative of a CA referred to in Article 46 of DORA from each Member State;

iii. where applicable, one representative of the CAs designated or established in accordance with Directive (EU) 2022/2555 responsible for the supervision of an essential or important entity subject to that Directive, which has been designated as critical information and communication technology (ICT) third-party service provider (CTPP).

7. Each Member State shall designate the relevant CA whose staff member shall be the high-level representative referred in point 6, letter a), number ii. The designated CA shall inform the ESAs of its designation and, where applicable, indicate the national legislation through which that designation has been performed. Member States that have more than one authority competent for the financial sector shall designate only one relevant CA.

8. The relevant CA referred to in the previous paragraph shall designate from its staff members a high-level representative and an alternate who may replace the high-level representative in case this person is prevented from attending a meeting. The relevant CA shall designate only one high-level representative and only one alternate and inform the LO about these designations. Each Member State shall be assigned one vote.

9. In case there are multiple authorities responsible for the financial sector in one Member State and all of them want to be involved in the OF, each authority without high-level representative shall designate one observer to participate in the OF, where appropriate. Taking into account the objective to achieve a good sectoral balance, observers shall be invited to a meeting if the topic(s) to be discussed are of relevance for the competent authority, including where the competent authority is supervising one or more financial entities making use of CTPPs.

4.2 Members' profile and responsibilities

10. Members and Observers shall:

a) have sufficient seniority to speak on behalf of the authority they represent, commit their authority on the topics within the scope of the OF and have sufficient expertise in the areas relevant to the tasks and deliverables of the OF;

b) actively and constructively participate in, and contribute to, the OF's meetings and written procedures;

c) ensure timely delivery of the tasks to be assigned within the scope of the work plan of the OF;

d) be committed to the work and tasks of the OF and be in a position to attribute a high priority to such work and tasks.

4.3 Chairperson

11. The OF shall be chaired by the Chairperson of the ESAs who is chairing the Joint Committee.

12. The Chairperson shall strive to reach consensus amongst the Members of the OF and ensure the timely development of the deliverables presented in its annual work plan. In the event that consensus cannot be reached, any issue of controversial nature being discussed in the OF shall be remitted and presented by the Chairperson of the OF to the JC, which shall consider the issue and take a decision.

13. When carrying out their tasks, the Chairperson shall act objectively in the interest of the European Union.

4.4 Ongoing work and meetings

14. The OF meetings shall be directed by the Chairperson.
15. Selected ESA staff shall support the work of the OF and can attend its meetings. The Chairperson and Executive Directors of the ESAs shall appoint an ESA staff member with a sufficient level of seniority which shall advise and assist the Chairperson in the performance of his/her tasks and function as secretariat.
16. The OF shall have physical meetings at the premises of one of the ESAs or hold virtual meetings by means of videoconferencing.
17. The Chairperson shall plan the dates of meetings sufficiently in advance. Additional meetings can be scheduled if necessary and/or in case of urgency. Meetings should be arranged to follow the schedule of the JC and timelines for external and internal deliverables.

4.5 Substructures

18. Subject to the approval of the JC, the OF can set up substructure(s) to carry out specific technical tasks set out in the OF's work plan. Such substructure(s) do not have a separate work plan, but prepare work to be discussed and agreed by the OF, and shall be disbanded if the tasks assigned to them are completed.
19. Substructure(s) are composed by staff members of the authorities represented in the OF. The staff members shall have expertise and experience in the relevant area of work for the relative substructure.
20. Substructure(s) are chaired by a Member of the OF, ESA staff or, where appropriate, by a technical expert from an authority which is Member or Observer of the OF, who shall be appointed and confirmed by the OF.
21. Members of the OF and members of the substructure(s) of the OF representing the same authority should ensure that their positions are coordinated.
22. The provisions of points 4.2, 4.6 and 4.7 shall apply *mutatis mutandis* to such substructure(s).

4.6 Conflicts of interest

23. Any participant of the OF shall avoid any conflict of interest, which can be prejudicial to their independence in relation to any items on the agenda of the OF, and abstain from participating in and contributing to the respective discussion in case of having such interest.
24. The Chairperson of the OF shall ensure that any instance of a conflict of interests within the OF is handled properly.

4.7 Professional secrecy and confidentiality

29. Any participant of the OF shall comply with (1) their confidentiality duty, (2) the ESA's standards on professional secrecy as defined in Article 70 of the ESA Regulation and in Article 55 of DORA, as appropriate; and (3) the respective ESA's internal rules of procedure implementing these requirements.

30. The Chairperson of the OF may request to hold a partial or fully restricted meeting without observers, when deemed necessary.

4.8 Review of the mandate

31. This mandate will, every two years, be subject to review and endorsement by the Joint Committee and subsequent approval by the ESAs' Board of Supervisors, and adapted to reflect any developments, as relevant and appropriate.

4.9 Effective date

33. This mandate shall apply from 17 January 2025.

Annex I: Legal mandate of the OF

- Recital 86: The OF should carry out preparatory work both for the individual decisions addressed to CTPPs, and for the issuing of collective recommendations in particular in relation to benchmarking the oversight programmes for CTPPs, and identifying best practices for addressing ICT concentration risk issues.

- Article 31: The OF should provide recommendations in relation to:

    - designating the ICT third-party service providers that are critical for financial entities, following an assessment that takes into account specific criteria;

    - appointing as LO for each CTPP the ESA that is responsible for the financial entities having together the largest share of total assets out of the value of total assets of all financial entities using the services of the relevant CTPP, as evidenced by the sum of the individual balance sheets of those financial entities.

- Article 31(10): The OF shall assess the ICT third-party dependencies of financial entities based on reports on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided.

- Article 32(1): The OF is established for the purposes of supporting the work of the JC and of the LO in the area of ICT third-party risk across financial sectors. The OF shall prepare the draft joint positions and the draft common acts of the JC in that area.

  The OF shall regularly discuss relevant developments on ICT risk and vulnerabilities and promote a consistent approach in the monitoring of ICT third-party risk at Union level.

- Article 32(2): The OF shall, on a yearly basis, undertake a collective assessment of the results and findings of the oversight activities conducted for all CTPPs and promote coordination 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(3): The OF shall submit comprehensive benchmarks for CTPPs to be adopted by the JC as joint positions of the ESAs.

- Article 32(4): The OF shall be composed of:

    - the Chairpersons of the ESAs;

    - one high-level representative from the current staff of the relevant CA referred to in Article 46 from each Member State;

    - the Executive Directors of each ESA and one representative from the Commission, from the ESRB, from ECB and from ENISA as observers;

- where appropriate, one additional representative of a CA from each Member State as observer;

- where applicable, one representative of the competent authorities designated or established in accordance with Directive (EU) 2022/2555 responsible for the supervision of an essential or important entity subject to that Directive, which has been designated as a critical ICT third-party service provider, as observer.

The OF may, where appropriate, seek the advice of independent experts appointed in accordance with paragraph 6.

- Article 32(5): Each Member State shall designate the relevant competent authority whose staff member shall be the high-level representative referred in paragraph 4, first subparagraph, point (b), and shall inform the LO thereof. The ESAs shall publish on their website the list of high-level representatives from the current staff of the relevant CA designated by Member States.

- Article 32(6): The independent experts referred to in paragraph 4, second subparagraph, shall be appointed by the OF from a pool of experts selected following a public and transparent application process.

  - The independent experts shall be appointed on the basis of their expertise in financial stability, digital operational resilience and ICT security matters. They shall act independently and objectively in the sole interest of the Union as a whole and shall neither seek nor take instructions from Union institutions or bodies, from any government of a Member State or from any other public or private body.

- Article 32(9): The ESAs, through the Joint Committee and based on preparatory work conducted by the Oversight Forum, shall, on yearly basis, submit a report on the application of this Section to the European Parliament, the Council and the Commission.

- Article 35(3): When consulted by the LO, OF to provide input concerning the exercise of powers according to Article 31(1) (information request, conduct general investigations and inspections, request of reports specifying the actions taken or remedies implemented by the CTPP, issue recommendations).

- Article 40(3): Within 3 months of the completion of an investigation or inspection, the LO, after consulting the OF, shall adopt recommendations to be addressed to the CTPP pursuant to the powers referred to in Article 35.

- Article 42(7): When consulted by the LO, OF to provide input concerning the issuing of non-binding and non-public opinions to CAs, in order to promote consistent and convergent supervisory follow-up measures, as appropriate.