Annex: Table summarising information exchanges

The following table summarises the information exchanges between the LO/ESAs (marked grey) and CAs (marked green) as indicated by these Guidelines. The table is not intended to introduce any new guidance, but to reflect the guidance included in the Guidelines. If there are any differences between the Guidelines and this table, the information included in the Guidelines prevails.

Information exchange	Timeline	Related Article in the Level 1 text	GL
Section 1: General considerations			
LO, in consultation with relevant CAs, reduce or extend the timelines	-	-	2.1
LO, in consultation with the JON, to present to the OF difference of opinions regarding the oversight cooperation and information exchanges	-	-	3.1
Where possible, CAs and LO to make available to each other, relevant information from their dialogue with NIS2 authorities	-		4.1
Section 2: Designation of CTPPs			
CAs to make available the full register of information to the ESAs	Without undue delay following the receipt of the register of information	28(3)[13] 31(1)(a)[14], (2), (6)[15] and (10)[16] Article 35(2) of the ESAs' founding regulation[17]	5.1
CAs to make available to the ESAs any relevant quantitative or qualitative information at their	-		5.2

[13] Article 28(3): As part of their ICT risk management framework, financial entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers…

[14] Article 31(1)(a): The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 32(1), shall designate the ICT third-party service providers that are critical for financial entities, following an assessment that takes into account the criteria specified in paragraph 2.

[15] Article 31(6): The Commission is empowered to adopt a delegated act in accordance with Article 57 to supplement this Regulation by specifying further the criteria referred to in paragraph 2 of this Article, by 17 July 2024.

[16] Article 31(10): For the purposes of paragraph 1, point (a), competent authorities shall, on a yearly and aggregated basis, transmit the reports referred to in Article 28(3), third subparagraph, to the Oversight Forum established pursuant to Article 32....

[17] Article 35(2) of the ESAs' founding regulation: The Authority may also request information to be provided at recurring intervals and in specified formats. Such requests shall, where possible, be made using common reporting formats.

Information exchange	Timeline	Related Article in the Level 1 text	GL
disposal to facilitate the criticality assessment			
Upon request, CAs to make available additional available information acquired in their supervisory activities	-		5.3
ESAs to make available to CAs information about the TPP that submitted a request to be designated as critical	Within 10 working days following the receipt from the TPP	31(5)[18], (11)[19] and (13)[20]	6.1
LO to share with CAs notification of the CTPP about any changes to the structure of the management of the subsidiary established in the Union	Within 10 working days following the receipt from the CTPP		6.2 (a)
LO to share with CAs information about the TPP that has been designated as critical and the starting date of designation	Within 10 working days after the submission of the notification		6.2 (b)
Section 3: Core oversight activities			
LO to make available to CAs the draft annual oversight plan	Prior to the finalisation of the annual oversight plan	33(4)[21] Recital 3 of draft Regulatory Technical Standards on the conduct of oversight activities in relation to the joint examination	7.1
CAs may provide comments on the draft annual oversight plan	Within 30 working days following the receipt		7.3
LO to make available to CAs, the annual oversight	Within 10 working		7.4

[18] Article 31(5): … After designating an ICT third-party service provider as critical, the ESAs, through the Joint Committee, shall notify the ICT third-party service provider of such designation and the starting date as from which they will effectively be subject to oversight activities.

[19] Article 31(11): The ICT third-party service providers that are not included in the list referred to in paragraph 9 may request to be designated as critical in accordance with paragraph 1, point (a).

[20] Article 31(13): The critical ICT third-party service provider referred to in paragraph 12 shall notify the Lead Overseer of any changes to the structure of the management of the subsidiary established in the Union.

[21] Article 33(4): Based on the assessment referred to in paragraph 2, and in coordination with the Joint Oversight Network referred to in Article 34(1), the Lead Overseer shall adopt a clear, detailed and reasoned individual oversight plan describing the annual oversight objectives and the main oversight actions planned for each critical ICT third-party service provider. That plan shall be communicated yearly to the critical ICT third-party service provider.

Information exchange	Timeline	Related Article in the Level 1 text	GL
plan and the multi-annual oversight plan.	days following the adoption	teams under DORA	
LO to make available to CAs any material updates to the annual oversight plan and the multi-annual oversight plan	Without undue delay following the adoption of the updates		7.5
CAs may provide comments on the material updates to the annual oversight plan	Within 30 working days following the receipt		7.5
LO to confirm to the CAs of the identity of the authorised persons for the investigation or inspection	At least 3 weeks before the start of the investigation or inspection Or With the shortest possible delay in case of an urgent investigation or inspection	36(1), 38(5)[22] and 39(3)[23]	8.1
LO to inform CAs where the authorised persons find that a CTPP opposes an inspection, including imposing any unjustified conditions to the inspection	-	39(7)[24]	8.3

[22] Article 38(5): In good time before the start of the investigation, the Lead Overseer shall inform competent authorities of the financial entities using the ICT services of that critical ICT third-party service provider of the envisaged investigation and of the identity of the authorised persons.

[23] Article 39(3): In good time before the start of the inspection, the Lead Overseer shall inform the competent authorities of the financial entities using that ICT third-party service provider.

[24] Article 39(7): Where the officials and other persons authorised by the Lead Overseer find that a critical ICT third-party service provider opposes an inspection ordered pursuant to this Article, the Lead Overseer shall inform the critical ICT third-party service provider of the consequences of such opposition, including the possibility for competent authorities of the relevant financial entities to require financial entities to terminate the contractual arrangements concluded with that critical ICT third-party service provider.

Information exchange	Timeline	Related Article in the Level 1 text	GL
LO to make available to the JON and the CAs, relevant scope of the request for information submitted to the CTPP	Within 10 working days following the adoption of the request for information to the CTPP	36(1)[25],37(1)[26] and 37(5)[27]	9.1
LO to make available to CAs of: • major incidents with direct/indirect impact on FEs when reported by the CTPP (upon request by LO); • relevant changes in the strategy of the CTPP on ICT third-party risk; • events that could represent important risk to the provision of ICT services; • reasoned statement from the CTPP evidencing the expected impact of the draft oversight plan.	-	33(4)[28] Article 3(2), letter l of Draft regulatory technical standards on the harmonisation of conditions enabling the conduct of the oversight activities under Article 41(1) points (a), b) and (d) of Regulation (EU) 2022/2554	9.2
CAs to make available to the LO, communications of the CTPP with the CAs for the purposes of all	-	33(1)[29]	9.3

[25] Article 36(1): When oversight objectives cannot be attained by means of interacting with the subsidiary set up for the purpose of Article 31(12), or by exercising oversight activities on premises located in the Union, the Lead Overseer may exercise the powers, referred to in the following provisions, on any premises located in a third-country which is owned, or used in any way, for the purposes of providing services to Union financial entities, by a critical ICT third party service provider, in connection with its business operations, functions or services, including any administrative, business or operational offices, premises, lands, buildings or other properties…

[26] Article 37(1): The Lead Overseer may, by simple request or by decision, require critical ICT third-party service providers to provide all information that is necessary for the Lead Overseer to carry out its duties under this Regulation, including all relevant business or operational documents, contracts, policies, documentation, ICT security audit reports, ICT-related incident reports, as well as any information relating to parties to whom the critical ICT third-party service provider has outsourced operational functions or activities.

[27] The Lead Overseer shall, without delay, transmit a copy of the decision to supply information to the competent authorities of the financial entities using the services of the relevant critical ICT third-party service providers and to the JON.

[28] Article 33(4), third subparagraph: Upon receipt of the draft oversight plan, the critical ICT third-party service provider may submit a reasoned statement within 15 calendar days evidencing the expected impact on customers which are entities falling outside of the scope of this Regulation and where appropriate, formulating solutions to mitigate risks.

[29] Article 33(1): The Lead Overseer shall conduct the oversight of the assigned critical ICT third party service providers and shall be, for the purposes of all matters related to the oversight, the primary point of contact for those critical ICT third party service providers.

Information exchange	Timeline	Related Article in the Level 1 text	GL
matters related to the oversight			
Section 4: Follow-up of the recommendations			
LO to make available to CAs: • notification of CTPP to follow recommendations; • the CTPP's remediation plan; • the reasoned explanation of the CTPP for not following the recommendations; and • the report specifying the actions taken or remedies implemented by the CTPP	Within 10 working days following the receipt by the LO	35(1)(c)[30] and 42(1)[31]	11.1 a)
LO to make available to CAs, the fact that the CTPP failed to send the notification within 60 calendar days after the issuance of recommendations to the CTPP	Within 10 working days after the expiration of the 60 calendar days		11.1 b)
LO to make available to CAs: • assessment as to whether the CTPP's explanation for not following the LO's	Within 10 working days following the adoption by the LO	35(1)(c), 35(6)[32], 35(10)[33], 42(1), 42(8)(a-d)[34]	11.1 c)

[30] Article 35(1)(c): The Lead Overseer has the power to request, after the completion of the oversight activities, reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third party service provider in relation to the recommendations issued.

[31] Article 42(1): Within 60 calendar days of the receipt of the recommendations issued by the Lead Overseer, critical ICT third party service providers shall either notify the Lead Overseer of their intention to follow the recommendations or provide a reasoned explanation for not following such recommendations.

[32] Article 35(6): In the event of whole or partial non-compliance with the measures required to be taken pursuant to the exercise of the powers under paragraph 1, points (a), (b) and (c), and after the expiry of a period of at least 30 calendar days from the date on which the critical ICT third-party service provider received notification of the respective measures, the Lead Overseer shall adopt a decision imposing a periodic penalty payment to compel the critical ICT third-party service provider to comply with those measures.

[33] Article 35(10): The Lead Overseer shall disclose to the public every periodic penalty payment that has been imposed, unless such disclosure would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.

[34] Article 42(8): Upon receiving the reports referred to in Article 35(1), point (c), competent authorities, when taking a decision as referred to in paragraph 6 of this Article, shall take into account the type and magnitude of risk that is not addressed by the critical ICT third-party service provider, as well as the seriousness of the non-compliance, having regard to the following criteria:

(a) the gravity and the duration of the non-compliance;

(b) whether the non-compliance has revealed serious weaknesses in the critical ICT third-party service provider's procedures, management systems, risk management and internal controls;

(c) whether a financial crime was facilitated, occasioned or is otherwise attributable to the non-compliance;

(d) whether the non-compliance has been intentional or negligent.

Information exchange	Timeline	Related Article in the Level 1 text	GL
recommendations is deemed sufficient and, if so, the LO's decision concerning amendment of recommendations; • assessment of the reports specifying the actions taken or remedies implemented by the CTPP; • decision imposing a periodic penalty payment on the CTPP; • assessment as to whether the refusal of a CTPP to endorse recommendations could adversely impact a large number of financial entities, or a significant part of the financial sector			
CAs to make available to LO: • notification to the financial entity of the possibility of a decision being taken; • individual warnings issued by CAs and relevant information which allows the LO to assess whether such warnings have resulted in consistent approaches mitigating the potential risk to financial stability	Within 10 working days following the adoption by the CA	42(4)[35], (7)[36] and (10)[37]	11.2 a)
Where possible, CAs to make available to LO, outcome of the consultation with NIS2 authorities prior to taking a decision.	Within 10 working days following the consultation	42(5)[38]	11.2 b)

[35] Article 42(4): Where a competent authority deems that a financial entity fails to take into account or to sufficiently address within its management of ICT third-party risk the specific risks identified in the recommendations, it shall notify the financial entity of the possibility of a decision being taken, within 60 calendar days of the receipt of such notification, pursuant to paragraph 6, in the absence of appropriate contractual arrangements aiming to address such risks.

[36] Article 42(7): Where a critical ICT third-party service provider refuses to endorse recommendations, based on a divergent approach from the one advised by the Lead Overseer, and such a divergent approach may adversely impact a large number of financial entities, or a significant part of the financial sector, and individual warnings issued by competent authorities have not resulted in consistent approaches mitigating the potential risk to financial stability, the Lead Overseer may, after consulting the Oversight Forum, issue non-binding and non-public opinions to competent authorities, in order to promote consistent and convergent supervisory follow-up measures, as appropriate.

[37] Article 42(10): Competent authorities shall regularly inform the Lead Overseer on the approaches and measures taken in their supervisory tasks in relation to financial entities as well as on the contractual arrangements concluded by financial entities where critical ICT third party service providers have not endorsed in part or entirely recommendations addressed to them by the Lead Overseer.

[38] Article 42(5): Upon receiving the reports referred to in Article 35(1), point (c), and prior to taking a decision as referred to in paragraph 6 of this Article, competent authorities may, on a voluntary basis, consult 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.

Information exchange	Timeline	Related Article in the Level 1 text	GL
CAs to make available to LO: • the material changes to existing contractual arrangements of financial entities with CTPPs made to address the risks identified in the recommendations; • the start of executing exit strategies and transition plans of the financial entities	Within 10 working days following the receipt of the information from financial entities	28 and 42(10)[39]	11.2 c)
CAs to inform LO of: • intention to notify a financial entity of the possibility of a decision being taken if the financial entity does not adopt appropriate contractual arrangements to address the specific risks identified in the recommendations; • all relevant information regarding the decision; • whether they intend to carry out an urgent decision	-	42(4) and (10)	12.1
LO to make available to CAs, non-binding assessment of potential impact the decision might have for the CTPP whose service would be temporarily suspended or terminated	Within 10 working days from the receipt of the information referred to in GL 12.1 or With the shortest possible delay in case of an urgent decision		12.2

[39] Article 42(10): Competent authorities shall regularly inform the Lead Overseer on the approaches and measures taken in their supervisory tasks in relation to financial entities as well as on the contractual arrangements concluded by financial entities where critical ICT third-party service providers have not endorsed in part or entirely recommendations addressed to them by the Lead Overseer.