JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Consultation paper

Draft Regulatory Technical Standards

on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554

Contents

1. Responding to this consultation

The ESAs invite comments on all proposals put forward in this paper and in particular on the specific questions summarised in 6.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 11.09.2023. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publicly disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with the ESAs' rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESAs' Boards of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of EBA, EIOPA and ESMA websites respectively.

2. Executive Summary

One of the objectives of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) is to harmonise and streamline the ICT-related incident reporting regime for financial entities (FEs) in the European Union (EU).

Article 18(3) of DORA mandates the European Supervisory Authorities (ESAs) to develop through the Joint Committee and in consultation with the European Central Bank and European Union Agency for Cybersecurity, common draft regulatory technical standards further specifying:

- The classification criteria for ICT-related incidents or, as applicable, operational or security payment-related incidents;
- Materiality thresholds for determining major incidents;
- The criteria and materiality thresholds for determining significant cyber threats; and
- Criteria for competent authorities (CAs) for assessing the relevance of incidents to CAs in other Member States and the details of the incidents to be shared with other CAs.

Article 18(4) of DORA further requires the ESAs to ensure that the requirements of the RTS are proportionate and that they follow standards, guidance and specifications published by ENISA.

In fulfilment of the mandate, the draft RTS presented in this consultation paper (CP) proposes the incident classification criteria and sets out their materiality thresholds. In addition, the CP proposes that the criteria 'Clients, financial counterparts and transactions affected', 'Data losses' and 'Critical services affected', 'Reputational impact', 'Duration and service downtime', 'Geographical spread', and 'Economic impact' should have different weights in the classification of major incidents, with the first three being primary criteria and the latter four being secondary criteria.

The CP further proposes to embed proportionality in the way the criteria are specified and materiality thresholds are set out, with some of the thresholds being targeted and more appropriate for larger institutions.

Furthermore, the ESAs propose in the CP that FEs classify incidents as major if the materiality thresholds are met for at least (i) two primary criteria or (ii) one primary criterion and two secondary criteria. The ESAs also propose that recurring incidents with the same apparent root cause, nature and impact that individually are not major but cumulatively meet the classification criteria are to be classified as major.

In relation to the classification of significant cyber threats, the CP proposes an approach based on the probability of materialisation of the threat, whether the threat could affect critical or important functions of the FE, and whether it could fulfil the conditions for major incident should it eventually materialise. Finally, the ESA propose that the assessment of the relevance to CAs in other Member States is to be based on the significance of the impact in the respective jurisdiction and that all details of the incidents shall be shared with other relevant CAs.

Next steps

The consultation period will run from 16 June 2023 to 15 September 2023. The final draft RTS will be published after consultation by 16 January 2024.

3. Background and rationale

3.1 Background

1. One of the objectives of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) is to harmonise and streamline the ICT-related incident reporting regime for financial entities (FEs) in the EU. To that end, DORA introduces consistent requirements for FEs on management, classification and reporting of ICT-related incidents.

2. In that regard, Article 18(3) of DORA mandates the European Supervisory Authorities (ESAs) to develop through the Joint Committee and in consultation with the ECB and ENISA, common draft regulatory technical standards further specifying the following:

    a) the classification criteria set out in Article 18(1) of DORA, including materiality thresholds for determining major ICT-related incidents or, as applicable, major operational or security payment-related incidents, that are subject to the reporting obligation laid down in Article 19(1) of DORA;

    b) the criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, to relevant competent authorities in other Member States', and the details of reports of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, to be shared with other competent authorities pursuant to Article 19(6) and (7) of DORA;

    c) the criteria to classify cyber threats as significant, including high materiality thresholds for determining significant cyber threats.

3. Article 18(4) of DORA requires the ESAs when developing the draft RTS to 'take into account the proportionality criteria set out in Article 4(2) of DORA, as well as international standards, guidance and specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors. For the purposes of applying the proportionality criteria set out in Article 4(2), the ESAs shall duly consider the need for microenterprises and small and medium-sized enterprises to mobilise sufficient resources and capabilities to ensure that ICT-related incidents are managed swiftly.'

4. The following chapter sets out how the ESAs are proposing to fulfill this mandate and the underlying reasoning and considerations. In addition, the Impact assessment section at the end of the CP provides additional choices and options that have been considered by the ESAs.

3.2 Rationale

5. Given that DORA aims to harmonise and streamline incident reporting for all FEs in its scope and that these FEs equally understand and apply at the time when they will be handling incidents, the ESAs have arrived at the view that the RTS requirements for classification of ICT-related incidents

or, as applicable, major operational or security payment-related incidents (both referred to as 'incidents'), and significant cyber threats will have to be simple, clear and proportionate, taking into account the specificities of the services, activities and operations of all FEs within the scope of DORA. To ensure continuity of reporting under existing incident reporting frameworks and cross-sectorial harmonisation, the ESAs have arrived at the view that the RTS requirements will have - to the greatest extent possible - be consistent with Directive (EU) 2022/2555 (NIS2), the various related Guidelines issued by ENISA under NIS1 (and, if possible, under NIS2), and other existing sectorial legal instruments, such as the revised EBA Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2), Guidelines on periodic information and notification of material changes to be submitted to ESMA by Trade Repositories, and others.

6. The draft RTS should allow for the capturing of all relevant major incidents that have a high adverse impact on the FE or at national or EU level. At the same time, the reporting of major incidents to the competent authorities (CAs) should not pose significant burden to FEs when they need to focus their resources in handling the respective incidents.

7. In addition, the ESAs are of the view that the draft RTS should facilitate (i) informing or triggering supervisory actions, including measures to the specific FE, (ii) preventing spill-over effect to other FEs that may be impacted and (iii) identifying current ICT risks that impact or may impact FE and third party providers (TPP), including risk from critical TPPs that may fall within the scope of ESAs' oversight.

8. In line with the mandate under Article 18(3) of DORA, the proposed draft RTS has the following distinct parts:
   - criteria for classifying incidents;
   - classification thresholds and criteria for determining major incidents and significant cyber threats; and
   - criteria to be applied for assessing whether the major incidents are relevant in other Member States and information to be shared with other relevant CAs.

3.2.1. Classification criteria and thresholds of major incidents

9. Article 18(1) of DORA prescribes the classification criteria, which are split in the draft RTS in seven distinct criteria, namely:
   - 'Clients, financial counterparts and transactions affected'
   - 'Reputational impact'
   - 'Duration and service downtime'
   - 'Geographical spread'
   - 'Data losses'
   - 'Critical services affected'
   - 'Economic impact'

10. To achieve the objective of DORA to introduce harmonised and streamlined rules for incident reporting, the ESAs have proposed to set out uniform and harmonised classification criteria for all FEs within the scope of DORA instead of the potential alternative of introducing entity-specific or sector-specific criteria or thresholds. Accordingly, the ESAs have strived to strike a suitable balance between providing sufficient clarification on each criterion while also avoiding an excessively granular approach where some FEs might be unintentionally excluded from the scope of the incident reporting framework.

11. The ESAs also acknowledge that there are differences between sectors, business models and regulatory requirements. At the same time, the ESAs are mindful that the harmonised requirements should not result in unintentional relaxation of or contradiction to the obligations set out in EU law (e.g. recovery times requirements set out in Article 12 of DORA), in particular in relation to financial market infrastructures (FMIs). Consequently, CAs and ESAs will be carrying out additional testing based on data from real incident reports and will further assess if the proposed classification approach and materiality thresholds cover the respective sector-specific requirements. This assessment may lead to additional calibration of the thresholds, in particular for FMIs, which may at times have more stringent requirements (e.g. higher availability requirements). In that regard, the ESAs will carefully consider the testing results and the related feedback from the respondents to the public consultation especially in relation to the materiality thresholds of the criteria 'Clients, financial counterparts and transactions affected', 'Duration and service downtime', 'Data losses' and 'Critical services affected'.

12. In what follows in the remainder of this chapter, the CP provides the general rationale for the classification of major incidents, followed by subchapters with the specification of the classification criteria and how the materiality thresholds have been set-up.

Classification of major incidents

13. This CP proposes an approach for the classification of major incidents under DORA that requires a combination of criteria with their respective thresholds to be met. This approach:

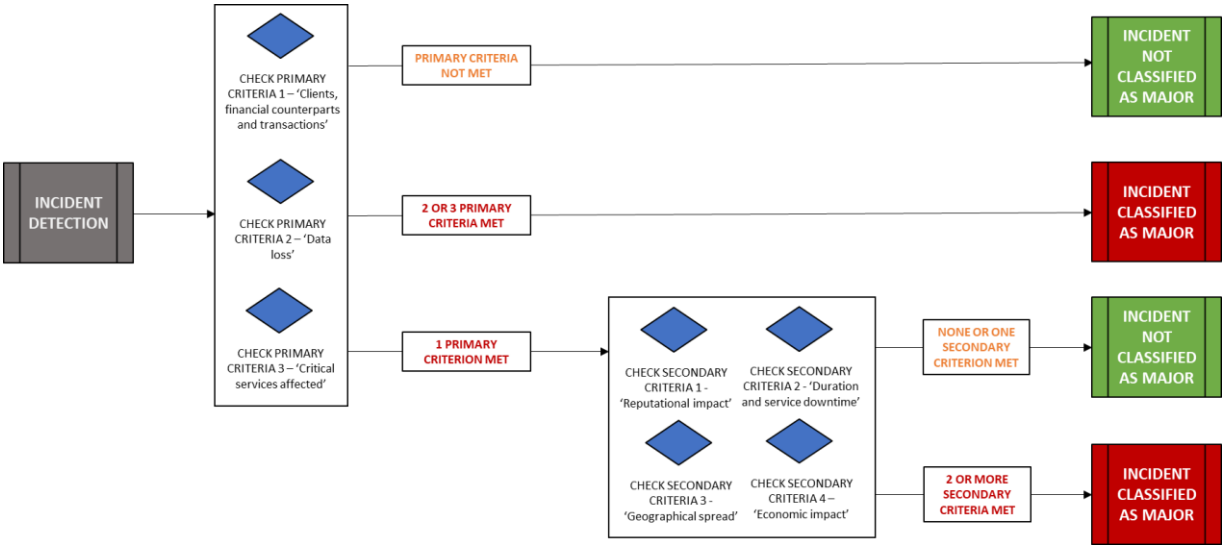
- reflects existing interdependencies between the different criteria, so to perform a holistic assessment of the impact of all relevant dimensions of major incidents;
- indicates the leading (primary) criteria for the purpose of classification of major incidents;
- ensures proportionality in the classification of major incidents;
- avoids unnecessary regulatory and reporting burden for the FEs within the scope of DORA;
- captures in scope all major incidents that are relevant for supervisors by avoiding over or under reporting;
- defines harmonised and simple criteria for the classification of major incidents.

14. The CP, therefore, proposes to classify incidents as major if any of the following conditions are fulfilled (also visually represented in Figure 1 below):

- the classification thresholds of two primary criteria have been met; or

- the classification thresholds of three or more criteria (primary and secondary) specified have been met, including at least one primary criterion.

Figure 1 – Incident classification chart



15. The ESAs propose that the primary criteria are: 'Clients, financial counterparts and transactions', 'Data losses' and 'Critical services affected'. These were chosen because the other criteria appear ancillary or complementary, or are interlinked with, or dependent on, the primary criteria. Accordingly, the secondary criteria would be 'Reputational impact', 'Duration and service downtime', 'Geographical spread' and 'Economic impact'.

16. With regard to the option to combine two primary criteria for classifying a major incident as such, the ESAs have arrived at the view that this will be useful to capture major incidents where critical services are affected, and data losses incurred. However, in line with paragraph 11 above, 'one-size-fits-all' approach for all materiality thresholds may pose challenges for classification of major incidents for certain types of financial entities (e.g. FMIs) and will be subject to additional testing and ponderation. To this end, feedback from the industry will be welcomed to ensure that this approach would not lead to over-reporting or under-reporting (e.g. for FMIs).

Q1. Do you agree with the overall approach for classification of major incidents under DORA? If not, please provide your reasoning and alternative approach(es) you would suggest.

'Clients, financial counterparts and transactions affected' (Articles 1 and 9 of the draft RTS)

17. To ensure that the criterion captures relevant incidents for all FEs within the scope of DORA, the ESAs have arrived at the view to treat separately, and as alternative triggers for incident reporting, the different aspects of this criterion, namely 'number of clients', 'number of financial counterparts', 'relevance of clients or financial counterparts' and 'amount or number of transactions' affected. The ESAs have also considered that this criterion, including its distinct parts, is of high relevance for the purpose of classification of major incidents and have, therefore, proposed that it is a primary criterion.

18. In relation to the 'number of clients affected' part of the criterion, the ESA have specified in the draft RTS propose in this CP that the term captures all clients, which may be natural or legal persons, that have been affected by the incident. The ESAs are of the view that FEs are best positioned to identify their clients, and hence no further elaboration of this term is proposed in the CP, other than specifying that the clients shall make use of the service provided by the respective FE. The clients will have to be considered the ultimate beneficiaries of the service also in some specific cases where certain intermediaries are involved in the provision of the financial service (e.g. in the insurance sector or in the case of asset management services).

19. When it comes to the specific materiality threshold to be used for the 'number of clients affected' part of the criterion, the ESAs have arrived at the view to use both a relative and an absolute threshold. The ESAs propose for the relative threshold to be calculated based on the clients affected by the incident divided by the number of all clients of the FE using that service. The relative threshold will have to ensure that the criterion is applied consistently by all FEs. The ESAs have considered various relative thresholds from 5% to 25% depending on the specific sector, FE type and the overall approach for classification of major incidents (whether a single criterion can indicate a major incident or a combination of criteria). The ESAs have, therefore, arrived at the view that, to ensure a balanced approach and taking into account that the 'number of clients affected' component of the criterion will not by itself trigger the reporting of a major incident, a threshold of 10% is most appropriate. The relative threshold will have to be calculated based on the number of clients affected by the incident (or an estimation in case data is not available) divided by all clients using the affected service of the financial entity.

20. The absolute threshold for the "number of clients affected" criterion has been set proportionately with the aim to apply to large FEs only where a significant number of clients are affected but the relative threshold is not being met. In the latter case, the ESAs propose to use a high absolute number of 50 000 clients, leveraging on the EBA Guidelines on major incident reporting under PSD2.

21. In relation to the 'number of financial counterparts affected' part of the criterion, the ESAs have specified in the draft RTS that the term captures all financial counterparts that have concluded a contractual arrangement with the FE and that have been affected by the incident. Similarly to 'clients affected', the ESAs have arrived at the view that no further clarification of the term 'financial counterpart' needs to be specified, because FEs are best placed to know which are the financial counterparts with which they interact, and to avoid that some financial counterparts are inadvertently excluded from the scope of this criterion, especially given the breadth of financial entity types within the scope of DORA.

22. When it comes to the materiality thresholds to be used for the 'number of financial counterparts affected' part of the criterion, the ESAs propose to use a relative threshold only and to set its value at 10%, based on the same rationale as the 'clients' part of the criterion. The CP does not propose an absolute threshold, given the challenge to identify a value that would be meaningful, appropriate and applied consistently for all FEs within the scope of DORA.

23. In relation to the 'relevance of clients or financial counterparts' part of the criterion, the ESAs propose in the draft RTS that FEs shall assess the extent to which the impact on a client and/or a financial counterpart will affect the implementation of the business objectives of the financial

entity. The FEs will have discretion to decide which are the clients or counterparts that may have impact on their business objectives due to the specificities of the activities of the different FEs and their respective business models. The materiality threshold proposed is qualitative and binary (i.e. a yes/no answer) allowing the FE to decide whether important clients or financial counterparts have been affected as a result of the incident subsequently impacting the implementation of the business objectives of the financial entity, as well as the potential impact of the incident on market efficiency.

24. In relation to the 'amount or number of transactions affected' part of the criterion, the ESAs understand that, based on the provision of Article 18(1)(a) of DORA, the term 'transactions' may not apply to all services, activities or operations of all FEs within the scope of DORA and that transactions have to have a monetary value based on the wording of DORA. The CP therefore proposes that the transactions will have to have a monetary amount and that at least one part of the transaction is to be carried out within the EU. This approach also aims at narrowing down potentially divergent interpretations of the term, by excluding from its scope economic transactions in the broad sense or IT-generated transactions at IT system level. The ESAs also avoided introducing specific examples of 'transactions' to ensure that the requirements are business model neutral and future proof, as well as to avoid limiting the scope of DORA.

25. When it comes to the materiality thresholds for the 'amount or number of transactions affected' part of the criterion, the CP proposes to use both relative and absolute threshold with values of 10% of the volume of transactions and 15 000 000 EUR value of transactions. The rationale behind the approach and the values chosen follows the same principle as the one for the 'clients' part of the criterion mentioned in paragraphs 19 and 20 above.

26. Since it may be challenging at times for FEs to identify the number of clients affected, or the financial counterparts or number or amount of transactions impacted, the draft RTS envisages that FEs can resort to estimates.

Q2. Do you agree with the specification and materiality thresholds of the criterion 'Clients, financial counterparts and transactions affected', as proposed in Articles 1 and 9 of the draft RTS? If not, please provide your reasoning and suggested changes.

'Reputational impact' (Articles 2 and 10 of the draft RTS)

27. Reputational impact is referred to in Article 18(1)(a) of DORA, together with the criteria affected clients, financial counterparts and transactions. However, the ESAs have arrived at the view to propose to use this criterion separately to the others, and to do so for two reasons. First, if reputational impact is used cumulatively with each of the other parts of the criterion for the purpose of classification of major incidents, many major incidents of interest to CAs would not be captured. Second, if reputational impact is used as a separate criterion with equal weighting to 'clients', 'financial counterparts' or 'transactions', it will likely lead to a high number of reported incidents that are not significant and impose a disproportionate compliance burden for FEs.

28. When it comes to the specification of the criterion, the ESAs have arrived at the view that a balance should be struck between incidents that have received some exposure to the general public on the

one hand and those that have received significant exposure and thus may have a detrimental impact on the FE or market efficiency on the other. Accordingly, the CP proposes that, when assessing the criterion, FEs will have to take into account the level of visibility the incident itself and/or its impact have gained as an indicator of potential reputational impact. The draft RTS specifies how reputational impact can materialize as a result of the incident, such as the attraction of media attention, the complaints received from various clients or financial counterparts, incompliance with regulatory requirements as a result of the incident or whether the FE has lost or is likely to lose clients or financial counterparts.

29. The threshold proposed is qualitative and binary (yes/no answer) with the FE indicating whether the incident has caused any reputational impact or not based on the indicators mentioned in the preceding paragraph.

'Duration and service downtime' (Articles 3 and 11 of the draft RTS)

30. Article 18(1)(b) of DORA refers to service downtime as part of the duration of the incident. However, the ESAs are of the view that both indicators are important for measuring the impact of an incident, with service downtime more relevant for time-critical services. The duration of the incident is a measurement that is necessary to capture those incidents that don't cause service downtime. The ESAs have therefore arrived at the view that both 'duration of an incident' and 'service downtime' will have to be used for the assessing this criterion and that either 'service downtime' or 'duration of an incident' should be able to trigger this classification criterion.

31. The CP proposes that the duration of an incident needs to be measured from the moment the incident occurs until the moment when the incident has been resolved. In relation to 'service downtime', the CP proposes that it is measured from the moment the service is fully or partially unavailable to clients and/or financial counterparts, or from the moment a critical function is not available to the financial entity itself, until the moment when regular activities/operations have been restored to the level of service that was provided prior to the incident. In cases where there is a delay in the provision of service (e.g. belated settlement of transactions due to missed settlement cycle), this needs also to be included in the measurement, even if regular activities/operations have already been restored.

32. The ESAs acknowledge that there may be cases where the FE does not know when the incident has occurred or the service downtime has started. The CP therefore proposes that in such cases, the occurrence of the incident or the start of the service downtime should be calculated from the moment the incident/service downtime is detected or when there is a detectable record at a network/system level. The detectable record should not be understood as recording in an incident management system but a traceable log in a network or a system.

33. When it comes to the specific materiality thresholds, the ESAs have arrived at the view that the threshold for service downtime should be consistent with existing incident reporting frameworks (e.g. Guidelines on major incident reporting under PSD2, Guidelines on reporting of periodic information and material changes by Trade Repositories (TRs) supervised under EMIR and SFTR, and the ECB/SSM Cyber Incident Reporting Framework). This is to ensure continuity of reporting under existing incident reporting frameworks and consistency with other related legal

requirements (in particular in the case of TR). The CP therefore proposes a threshold of service downtime of critical functions longer than 2 calendar hours, unless more stringent requirements exist in level one for certain types of financial entities, in particular for central counterparties, central securities depositories, trading venues and data reporting service providers. However, since this threshold will apply to FEs that have not yet been subject to incident reporting requirements prior to DORA (e.g. institutions for occupational retirement provisions, insurance intermediaries), feedback from market participants will be welcomed on whether the 2-hour service downtime threshold is appropriate for their business. In relation to the 'duration of the incident', the ESA consider appropriate a threshold of 24 calendar hours since it would be proportionate and capture incidents where no service downtime occurs or those with service downtime of non-critical functions. However, there are more stringent availability requirements for certain FEs, namely central counterparties and data reporting service providers, such as those set out in Article 12(3) of DORA, which may require shorter thresholds for service downtime for these particular entities. This criterion will thus be further assessed and potentially calibrated in the context of the additional testing that NCAs will conduct, as indicated in Paragraph 11.

34. Finally, since it may be challenging for FEs to identify the actual moment when the incident will be resolved, the draft RTS envisages that FEs can resort to estimates.

'Geographical spread' (Articles 4 and 12 of the draft RTS)

35. When specifying the criterion 'Geographical spread' the ESAs considered whether it should be assessed in a cross-border context only or also at national level and have arrived at the view that due to the different size of Member States and due to the potential complexity for FEs having to carry out the required assessment and that it may add a disproportionate reporting burden, the criterion does not include an assessment of the geographical spread within a single Member State. When it comes to the impact of the major incidents to other Member States, the ESAs have arrived at the view that an impact in two Member States will suffice to trigger the materiality threshold for major incidents, provided that there is material impact in both jurisdictions.

36. When considering the impact in different jurisdictions, to avoid unnecessary complexity and disproportionate reporting burden, the ESAs discarded the possibility of assessing the impact of these against other classification criteria, such as affected clients, financial counterparts or transactions. The ESAs have, therefore, arrived at the view to base the criterion on the FE's own assessment of the material impact in two or more jurisdiction(s) based on the affected clients and financial counterparts, branches or subsidiaries within a group, and financial market infrastructures or third party providers that may be shared with other FEs. Any significant impact based on these indicators should be a trigger for the classification criterion. When it comes to the materiality threshold, the CP proposes a qualitative binary threshold (yes/no answer), with the FE indicating whether the incident has had a material impact in two or more Member States.

'Economic impact' (Articles 7 and 15 of the draft RTS)

37. Based on the experience under the Guidelines on major incident reporting under PSD2, where the identical criterion has almost never been used by reporting entities and was generally perceived by the industry as too complex, the ESAs have arrived at the view that there is a need for the DORA

RTS to prescribe in detail the types of direct and indirect gross costs and losses incurred as a result of the incident. In so doing, the CP proposes also to exclude specific costs (via a non-exhaustive list), such as costs that are necessary to run the business as usual. When preparing this list, the ESAs assessed a large list of potential costs and losses to be assessed by the FE in the process of classification of the incident and then arrived at the view to apply the principle of proportionality and limit the costs and losses to those that are most essential, clear and in line with the existing operational risk framework.

38. With regard to the materiality threshold for the criterion, the ESAs propose to use a simple approach by relying only on a single absolute number of EUR 100 000 or above for the gross direct and indirect costs and losses incurred by the incident. This approach is proportionate since it is likely that it will apply mainly to large FEs and would allow evidencing a significant impact to the FE, while smaller FEs would not frequently incur the burden of having to report.

39. The ESAs have discarded the option of a relative threshold, since it may be difficult to identify the appropriate metrics for the assessment of the amount of costs and losses and would have required an approach that would have to diverge between different types of FEs within each sector. For instance, while for the banking sector a relative threshold based on the Tier-1 capital could have been used, its application would not have been possible for certain types of FEs that do not report this figure. Instead, it would have been necessary to develop different indicators for those other sectors. These could have been, for example, revenues, profits or assets, but due to the different nature of the FEs within the scope of DORA, and the different size and complexity of their business models, these latter indicators have been discarded as they are not comparable or do not offer a meaningful measurement of the economic impact. Finally, the ESAs have arrived at the view that the combination of the absolute and relative threshold would have been too complex and that the absolute threshold alone is better suited to gauge the economic impact, that it is comparable across sectors, and that it respects the proportionality principle.

40. Finally, since it may be challenging for FE to know the exact costs and losses at the time of the incident, the draft RTS envisages that FEs can resort to estimates.

Q3. Do you agree with the specification and thresholds of the criteria 'Reputational impact', 'Duration and service downtime', 'Geographical spread' and 'Economic impact', as proposed in Articles 2, 3, 4, 7, 10, 11, 12 and 15 of the draft RTS? If not, please provide your reasoning and suggested changes.

'Data losses' (Articles 5 and 13 of the draft RTS)

41. Pursuant to Article 18(1)(d) of DORA, FEs shall assess the impact on data losses that the ICT-related incident entails in relation to availability, authenticity, integrity or confidentiality of data. The ESAs have further specified in the draft RTS what constitutes data losses related to availability, authenticity, integrity and confidentiality. To that end, the CP proposes a description related to all of these properties, based on terms used by ENISA and available international standards.

42. Moreover, with regard to the materiality threshold, the CP proposes a qualitative binary threshold (yes/no answer), with the FE indicating whether the incident has entailed any loss of critical data related to availability, authenticity, integrity or confidentiality. The CP also specifies that impact on such critical data needs to have an adverse impact on the implementation of the business objectives of the financial entity or the meeting of regulatory obligations in order to meet the materiality threshold.

43. During the development of the specification of the criterion and its threshold, the ESAs took into account that the criterion is of high relevance for the purpose of classification of major incidents and, therefore, propose that it is a primary criterion. In the specific cases of data breaches, which can lead to losses of confidentiality of data and at times to losses of integrity of data, the ESAs arrived at the view that these incidents are particularly relevant for supervisors and that they may not necessarily trigger other criteria, with the exception of 'critical services affected'. The ESAs, therefore, propose to introduce an option to classify major incidents based on two primary criteria in order to capture these types of incidents. However, as indicated in paragraph 16 of this CP, the consequences of this approach will need to be carefully assessed for certain types of financial entities. This will inform whether the proposed approach for all FEs needs to be revised or whether a FE-specific threshold or an approach needs to be considered.

Q4. Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13? If not, please provide your reasoning and suggested changes.

'Critical services affected' (Articles 6 and 14 of the draft RTS)

44. The ESAs have considered that the criterion 'critical services affected' should allow for the capture of specific cases where the incident has impacted (i) the provision of financial services that require authorization/registration in the EU or (ii) ICT services that support critical or important functions of the FE.

45. However, based on the experience gathered of incidents reported under PSD2, a large proportion of the incidents are likely to have an impact on the services, activities or operations of all FEs within the scope of DORA. To avoid significant overreporting and also to ensure that only incidents with high adverse impact are categorized as major, the ESAs have therefore arrived at the view that the threshold will have to also be dependent on whether the incident has been escalated to the senior management or the management body of the FE according to internal policies, and that such escalation is different to and is to be distinguished from regular reporting.

46. The ESAs have also discarded alternative approaches, such as (i) leaving it to the discretion of the FEs to assess the critical services based on their own business impact analysis or (ii) defining critical services per type of FE. Leaving the assessment to the discretion of FEs was discarded since it will lead to divergent approaches and lack of harmonisation of the incident reporting under DORA. Defining critical services per type of FE, in turn, was discarded because it would overcomplicate the classification of incidents, thus bringing about additional reporting burden to FEs and potentially resulting in certain types of incidents being unintentionally excluded from the incident reporting under DORA.

47. With regard to the threshold, the CP proposes a qualitative binary threshold (yes/no answer), with the FE indicating whether any critical service has been affected and whether the incident has escalated to the senior management or management body of the FE.

Q5. Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14? If not, please provide your reasoning and suggested changes.

Recurring incidents (Article 16 of the draft RTS)

48. The definitions of 'ICT-related incident' and 'operational or security payment-related incident' as set out in Article 3(8) and (9) of DORA[1] indicate that the legislators envisaged for the respective incidents also to comprise series of linked events unplanned by the FE. The ESAs have, therefore, arrived at the view that some recurring incidents that are connected in terms of root cause, nature, impact, and service concerned, and that individually do not meet the classification thresholds for major incident reporting, indicate significant issues and deficiencies in the ICT risk and incident management procedures of the FE. Accordingly, the CP proposes that these recurring incidents will have to be classified as major where in aggregate they meet the classification criteria and materiality thresholds in the preceding 3 months.

49. The ESAs have assessed potential concerns about the additional operational burden that such a requirement may pose, i.e. to set-up systems (or make available personnel) to track such recurring incidents and also considered the risk of over-reporting of incidents to CAs. However, the ESAs are of the view that the advantages listed in paragraph 48 above outweigh these particular concerns.

50. In addition, the ESAs found that capturing recurring incidents will add little burden on FEs, on top the organizational changes that they will have anyway to implement to comply with Article 17(3) of DORA, which prescribes that as part of the incident management process, FEs shall establish procedures 'to identify, track, log, categorise and classify ICT-related incidents…'

51. Finally, the ESAs have considered that capturing recurring incidents may be crucial for collecting supervisory data for some FEs, such as central securities depositories, central counterparties, trading venues, trade repositories, data reporting service providers, credit rating agencies, administrators of critical benchmarks and securitization repositories. The ESAs found that those entities tend to be affected by fewer and less recurring incidents than other market participants. This may require capturing recurring incidents for a period longer than 3 months, that is currently proposed in Article 16, and up to 12 months, for these and potentially other types of FEs, considering information we have from existing incident reporting regimes in some of these sectors. At the same time, the specific timeline may be adjusted after additional thorough testing during the public consultation, complementary to the feedback from market participants, in line with paragraph 11 above.

[1] Article 3(8) of DORA defines ICT-related incident as *'single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity'.*

Q6. Do you agree with capturing recurring incidents with same apparent root cause, similar nature and impact, that in aggregate meet the classification criteria and thresholds as major incidents under DORA, as proposed in Article 16? If not, please provide your reasoning and suggested changes.
Please also indicate how often you face recurring incidents, which in aggregate meet the materiality thresholds only over a period of 6 to 12 months based on data from the previous two years (you may also indicate the number of these recurring incidents).

3.2.2. Classification criteria and thresholds for significant cyber threats (Article 17 of the draft RTS)

52. Article 18(2) of DORA prescribes that FEs 'shall classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk'. The mandate under Article 18(3) of DORA requires the ESAs to specify in the draft RTS the criteria set out in Article 18(2) of DORA, including high materiality thresholds for determining significant cyber threats.

53. To this end, the ESAs assessed the definitions of cyber 'threat' and 'significant cyber threat' in Article 3(12) and (13) of DORA, with the latter specifying that the threat could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident, and the approach taken by ENISA under the NIS Directive. As a result of the assessment, and taking into account the fact that significant cyber threats shall be reported on a voluntary basis as set out in Article 19(2) of DORA, the ESAs propose to take a simple and pragmatic approach in the specification of the criteria and thresholds to encourage FEs to report these threats to CAs. Accordingly, the CP proposes that the specification of the criteria for assessing the criticality of the services at risk to be dependent on whether the cyber threat:

- could affect critical or important functions of the FE, other FEs, third party providers, clients or financial counterparts;
- has a high probability of materialisation at the FE or other FEs; and
- could fulfil the conditions of major ICT-related incidents if it materialises.

54. The ESAs have arrived at the view that the potential impact of significant cyber threats of interest to CAs relates on impact not only to the FE itself but to other FEs as well, since the reporting FE may have prevented a threat that could pose a risk to other FEs. It also puts CAs into a position to become aware of resultant risks.

55. The ESAs discarded the possibility of introducing specific thresholds for cyber threats, to avoid introducing too much complexity and reporting burden on FEs. The ESAs have, therefore, arrived at the view that the thresholds to be assessed need to be the same as those for ICT-related incidents.

56. With regard to assessing of the probability of materialisation of the cyber threat, the CP proposes that the assessment takes into account (i) applicable risks, including potential vulnerabilities of the

systems of the financial entity that can be exploited, (ii) the capabilities and intent of threat actors, and (c) the persistence of the threat and any accrued knowledge about ICT-related incidents that have impacted the financial entity.

Q7. Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17? If not, please provide your reasoning and suggested changes.

3.2.3. Relevance of the major incident in other Member States and details to be shared with other authorities (Article 18 and 19 of the draft RTS)

57. When specifying the relevance of the major incident in other Member States as mandated under Article 18(3)(b) of DORA, the ESAs have arrived at the view to leverage on the criterion 'Geographical spread' and the rationale behind the approach taken, which is elaborated in detail in paragraphs 35 and 36 of this CP. The ESAs have found it of paramount importance to focus on the impact of the incident in the host Member State and its root cause, so that potential vulnerabilities and spill-over effects to other FEs and clients are identified and the risk of contagion mitigated.

58. When it comes to the details of the incident reports to be reported to other competent authorities at national or cross-border level, the ESAs have arrived at the view that all details will be of relevance.

59. The ESAs have discarded the approach where different types of information are forwarded to the different authorities (e.g. law-enforcement authorities, resolution authorities and NIS2 authorities at national level, as well as DORA CAs in host Member States) due to the potential complexity of the assessment and likely delays in the process at a time when timely actions need to be taken by the supervisors.

60. In addition, to allow for easier identification of potential spill-over effects and contagion risks, the ESAs have arrived at the view that the information submitted to the respective authorities is not to be anonymised. This should not pose a threat to the security of the information since it will be bound by professional secrecy requirements and, in the case of exchange of information in accordance with Article 19(7) of DORA, carried out in a secure and confidential way.

Q8. Do you agree with the approach for assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities, as proposed in Articles 18 and 19? If not, please provide your reasoning and suggested changes.

4. Draft regulatory technical standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats

COMMISSION DELEGATED REGULATION (EU) …/…

of XXX

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,
Having regard to 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, and in particular Article 18(4) subparagaph 3 thereof,
Whereas:

(1) Given that Regulation (EU) 2022/2554 aims to harmonise and streamline incident reporting requirements and the scope of the Regulation covers 20 different types of financial entities and that at the time of classification of incidents financial entities will be handling the incident, the classification criteria and the materiality thresholds should be specified in a simple way that takes into account the specificities of the services and activities of all these financial entities and should apply consistently to them without introducing criteria and thresholds targeted at a specific type of financial entity.

(2) In accordance with the proportionality requirement set out in Article 18(4) of Regulation (EU) 2022/2554, the classification criteria and the materiality thresholds should reflect the size and overall risk profile, and the nature, scale and complexity of the services of all financial entities. Therefore, the criteria and materiality thresholds have been designed in such a way that they apply equally to all financial entities, irrespective of their size and risk profile, and do not pose reporting burden to smaller financial entities. However, in some cases a significant number of clients and transactions may be affected by an incident without exceeding the relative thresholds, these incidents should be captured through absolute thresholds and are mainly targeted at and more appropriate for larger financial entities.

(3) In relation to incident reporting frameworks, which have existed prior to the entry into force of Regulation (EU) 2022/2554, continuity for financial entities should be ensured. Therefore, the classification criteria and thresholds should be aligned with and leverage on the provisions which had been established in the EBA Guidelines on major incident reporting under PSD2, the Guidelines on periodic information and notification of mate-

rial changes to be submitted to ESMA by Trade Repositories, the ECB/SSM Cyber Incident Reporting Framework and others. The classification criteria and thresholds should also be suitable for the financial entities that have not been subject to incident reporting requirements prior to Regulation (EU) 2022/2554.

(4) Since the classification of incidents under Article 18 of Regulation (EU) 2022/2554 applies to credit institutions together with the operational risk framework under the Directive (EU) 2018/959, the approach for assessing the economic impact based on the calculation of costs and losses should, to the greatest possible extent, be consistent across both frameworks to avoid introducing incompatible or contradicting requirements.

(5) The criterion in relation to the geographical spread of an incident should focus on the cross-border impact of the incident, since the impact of an incident to the activities of a financial entitiy within a single jurisdiction will be captured by the other criteria.

(6) Given that the classification criteria are interdependent and linked to each other, the approach for identifying major incidents under Article 19(1) of Regulation (EU) 2022/2554 should be based on combination of criteria where some criteria should have more prominence in the classification of major incidents than others.

(7) With a view to ensure that the major incidents received by competent authorities under Article 19(1) of Regulation (EU) 2022/2554 serve both for supervisory purposes and in preventing contagion across the financial sector, the materiality thresholds should enable capturing major incidents, by focusing, inter alia, on the impact on critical data impacted, the specific customer facing and entitiy specific critical services and whether the impact has been escalated, the specific absolute and relative thresholds of clients, financial counterparts or transactions that indicate a material impact on the financial entity, significance of the impact in other Member States.

(8) Given that recurring incidents with similar root cause and nature, which individually are not major incidents, can indicate significant deficiencies and weaknesses in the financial entity's incident and risk management procedures, such recurring incidents should be considered as major in aggregate form, if they occur in a similar manner over a defined period of time.

(9) Considering the need for supervisors to be aware of cyber threats that can have a negative impact on the financial entity and sector, competent authorities should be aware of those threats that may affect critical or important functions, have high probability of materialisation and would constitute a major incident if they materialise.

(10) Considering that competent authorities in host Member States should be made aware of incidents that impact financial entities and customers in their jurisdiction, the assessment of the impact in host jurisdiction under Article 19(7) of Regulation (EU) 2022/2554 should be based on the root cause of the incident, potential contagion through third party providers and financial market infrastructures, as well as the impact on significant groups of clients or financial counterparts.

(11) The reporting referred to in Articles 19(6) and 19(7) of Regulation (EU) 2022/2554 should allow the respecitive recipients to assess the impact of the incidents.Therefore, the reports should cover all details from the incident reports submitted by financial entitiy to the competent authority.

(12) This Regulation is based on the draft regulatory technical standards submitted to the Commission by The European Supervisory Authorities.

(13) The European Supervisory Authorities have conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the […] Stakeholder Group established in accordance with Article 37 of Regulations (EU) No 1093/2010, 1094/2010 and 1095/2010 of the European Parliament and of the Council[2],

HAS ADOPTED THIS REGULATION:

Section I

Classification criteria

Article 1

Classification criterion 'Clients, financial counterparts and transactions' in accordance with Article 18(1) point (a) of Regulation (EU) 2022/2554

1. The number of clients affected by the incident as referred to in Article 18(1), point (a) of Regulation (EU) 2022/2554, shall reflect the number of all affected clients, which may be natural or legal persons, that make use of the service provided by the financial entity.
2. The number of financial counterparts affected by the incident, shall reflect the number of all affected financial counterparts that have concluded a contractual arrangement with the financial entity.
3. In relation to the relevance of clients and/or financial counterparts, the financial entity shall take into account the extent to which the impact on a client and/or a financial counterpart will affect the implementation of the business objectives of the financial entity, as well as the potential impact of the incident on market efficiency.
4. In relation to the amount and number of transactions affected by the incident, the financial entity shall take into account all affected transactions containing a monetary amount that have at least one part of the transaction carried out in the EU.
5. Where the actual number of clients, financial counterparts or number or amount of transactions impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods.

Article 2

Classification criterion 'Reputational impact' in accordance with Article 18(1)(a) of Regulation (EU) 2022/2554

[2] Regulation (EU) No 109x/2010 of the European Parliament and of the Council …[+*full title*] (OJ L [number], [date dd.mm.yyyy], [p.].).

For the purposes of determining the reputational impact of the incident, financial entities shall take into account the level of visibility that the incident has gained in the market. In particular, financial entities shall take into account whether one of the following are met:

a) The incident has attracted media attention; or
b) The financial entity has received complaints from different clients or financial counterparts; or
c) The financial entity will not be able to or is likely not to be able to meet regulatory requirements; or
d) The financial entity is likely to lose clients or financial counterparts with an impact on its business as a result of the incident.

Article 3

Classification criterion 'Duration and service downtime' in accordance with Article 18(1)(b) of Regulation (EU) 2022/2554

1. Financial entities shall measure the duration of an incident from the moment the incident occurs until the moment when the incident is resolved. Where financial entities are unable to determine the moment when the incident has occurred, they shall measure the duration of the incident from the earlier between the moment it was detected and the moment when it has been recorded in network or system logs or other data sources. Where financial entities do not yet know the moment when the incident will be resolved, they shall apply estimates.
2. Financial entities shall measure the service downtime of an incident from the moment the service is fully or partially unavailable to clients and/or financial counterparts to the moment when regular activities/operations have been restored to the level of service that was provided prior to the incident. Where the service downtime causes a delay in the provision of service after regular activities/operations have been restored, the downtime shall be measured from the start of the incident to the moment when that delayed service is provided. Where financial entities are unable to determine the moment when the service downtime has started, they shall measure the service downtime from the earlier between the moment it was detected and the moment when it has been recorded.

Article 4

Classification criterion 'Geographical spread' in accordance with Article 18(1)(c) of Regulation (EU) 2022/2554

For the purpose of determining the geographical spread with regard to the areas affected by the incident, financial entities shall assess the impact of the incident in the territories of at least two Member States. Financial entities shall assess the significance of the impact of the incident in the concerned Member State's territory, including on:

a) The clients and financial counterparts affected; or

b) Branches of the financial entity or other financial entities within the group carrying out activities in the respective Member State; or
c) Financial market infrastructures or third-party providers that may be common with other financial entities.

Article 5

Classification criterion 'Data losses' in accordance with Article 18(d) of Regulation (EU) 2022/2554

1. To determine the data loss that the incident entails in relation to the availability of data, financial entities shall take into account whether the incident has rendered the data on demand by the financial entity, its clients or its counterparts inaccessible or unusable.
2. To determine data losses that the incident entails in relation to the authenticity of data, financial entities shall take into account whether the incident has compromised the trustworthiness and reliability of data or their source.
3. To determine data losses that the incident entails in relation to the integrity of data, financial entities shall take into account whether the incident has resulted in non-authorised modification of data that has rendered it inaccurate or incomplete.
4. To determine losses that the incident entails in relation to the confidentiality of data from an incident, financial entities shall take into account whether the incident has resulted in data having been accessed by or disclosed to unauthorised parties or systems.

Article 6

Classification criterion 'Critical services affected' in accordance with Article 18(1)(e) of Regulation (EU) 2022/2554

For the purpose of determining the criticality of the services affected, including the financial entity's transactions and operations, financial entities shall assess whether the incident has affected services or activities that require authorisation, or ICT services that support critical or important functions of the financial entity.

Article 7

Classification criterion 'Economic impact' in accordance with Article 18(1)(f) of Regulation (EU) 2022/2554

1. For the purpose of determining the economic impact of the incident, financial entities shall take into account the following types of direct and indirect gross costs and losses, which have been incurred as a result of the incident:
   a) expropriated funds or financial assets for which the financial entity is liable, including assets lost to theft;
   b) replacement or relocation costs of software, hardware or infrastructure;

c) staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff;
d) fees due to non-compliance with contractual obligations;
e) customer redress and compensation costs;
f) losses due to forgone revenues;
g) costs associated with internal and external communication;
h) advisory costs, including costs associated with legal counselling, forensic and remediation services.

2. When assessing the direct and indirect costs and losses under paragraph 1, financial entities shall not take into account costs that are necessary to run the business as usual, including at least:
   a) costs of general maintenance of infrastructure, equipment, hardware, software, infrastructure and skills of staff;
   b) internal or external expenditures to enhance the business after the ICT related incident, including upgrades, improvements, risk assessment initiatives and enhancements; and
   c) insurance premiums.
3. Where the amounts of direct and indirect costs and losses cannot be determined, financial entities shall estimate those amounts based on available data.

Section II

Major incidents and their materiality thresholds and significant cyber threats

Article 8

Major incidents in accordance with Article 19(1) of Regulation (EU) 2022/2554

1. An incident shall be considered a major incident for the purposes of Article 19 of Regulation (EU) 2022/2554 where the incident fulfils one of the following conditions:
   a) The thresholds as specified in this section of two primary criteria referred to in paragraph 2 have been met; or
   b) The thresholds as specified in this section of three or more criteria referred to in paragraphs 2 and 3 have been met, including at least one primary criterion.
2. The following criteria shall be primary criteria:
   a) ‘Clients, financial counterparts and transactions’ as set out in Article 1;
   b) ‘Data losses’ as set out in Article 5; and
   c) ‘Critical services affected’ as set out in Article 6.
3. The following criteria shall be secondary criteria:
   a) ‘Reputational impact’ as set out in Article 2;
   b) ‘Duration and service downtime’ as set out in Article 3;
   c) ‘Geographical spread’ as set out in Article 4; and
   d) ‘Economic impact’ as set out in Article 7.

Article 9

Materiality thresholds for the classification criterion 'Clients, financial counterparts and transactions'

1. The materiality threshold for criterion 'Clients, financial counterparts and transactions' referred to in Article 8(2)(a) shall be met, where any of the following conditions is met:
   a) the number of affected clients is higher than 10% of all clients using the affected service of the financial entity; or
   b) the number of affected financial counterparts is higher than 10% of all financial counterparts used by the financial entity related to the affected service; or
   c) the number of affected clients is higher than 50 000 clients; or
   d) the number of affected transactions is higher than 10% of the regular level of transactions carried out by the financial entity related to the affected service; or
   e) the amount of affected transactions is higher than EUR 15 000 000; or
   f) any identified impact on relevant clients or financial counterpart in accordance with Article 1(3).
2. Where the actual number of clients, financial counterparts or number or amount of transactions impacted cannot be determined, the financial entity shall estimate these based on available data from comparable reference periods.

Article 10

Materiality thresholds for the classification criterion 'Reputational impact'

Any reputational impact in accordance with Article 2 shall be considered as meeting the threshold of the criterion for major incidents under Article 8(3)(a).

Article 11

Materiality thresholds for the classification criterion 'Duration and service downtime'

The materiality threshold for the criterion for major incidents under Article 8(3)(b) is met where:

a) the duration of the incident is longer than 24 hours; or
b) the service downtime is longer than 2 hours for ICT services supporting critical functions, without prejudice to stricter availability and recovery requirements set out in Regulation (EU) 2022/2554 and other EU legislation.

Article 12

Materiality thresholds for the classification criterion 'Geographical spread'

Any impact of the incident in the territories of at least two Member States in accordance with Article 4 shall be considered as meeting the threshold of the criterion for major ICT-incidents under Article 8(3)(c).

Article 13

Materiality thresholds for the classification criterion 'Data losses'

Any significant impact in accordance with Article 5 on availability, authenticity, integrity or confidentiality of critical data, which would have an adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements shall be considered as meeting the thresholds of the criterion for major incidents under Article 8(2)(b).

Article 14

Materiality thresholds for the classification criterion 'Critical services affected'

Any impact on critical services in accordance with Article 6, which has been escalated by the financial entity to its senior management or management body, shall be considered as meeting the threshold of the criterion for major incidents under Article 8(2)(c).

Article 15

Materiality threshold for the classification criterion 'Economic impact'

1. The materiality threshold of the economic impact in accordance with Article 7 is met where the gross direct and indirect costs and losses incurred by the financial entitiy from the major incident have exceeded or are likely to exceed EUR 100 000.
2. When assessing the economic impact, financial entities shall sum up the gross costs and losses set out in Article 7(1).
3. Where the actual costs and losses cannot be determined, the financial entity shall estimate those based on available data.

Article 16

Recurring incidents

1. Recurring incidents that individually do not constitute a major incident shall be considered as one major incident where the incidents, in aggregate and over a period of the preceding 3 months from the last occurrence, meet the materiality thresholds in accordance with Article 9 to 15.
2. For the purposes of paragraph 1, recurring incidents shall occur at least twice, have the same apparent root cause and shall be with similar nature and impact.

Article 17

Criteria and high materiality thresholds for determining significant cyber threats

1. For the purposes Article 18(2) of Regulation (EU) 2022/2554, a cyber threat shall be significant, where it fulfils all of the following conditions:
   a) the cyber threat could affect critical or important functions of the financial entity, other financial entities, third party providers, clients or financial counterparts;
   b) the cyber threat has a high probability of materialisation at the financial entity or other financial entities; and
   c) the cyber threat could fulfil the conditions set out in Article 8 if it materialises.
2. When assessing the probability of materialisation for the purposes of paragraph 1(b), financial entities shall take into account at least the following elements:
   a) applicable risks related to the cyber threat, including potential vulnerabilities of the systems of the financial entity that can be exploited,
   b) the capabilities and intent of threat actors, and
   c) the persistence of the threat and any accrued knowledge about incidents that have impacted the financial entity or its third-party provider, clients or financial counterparts.

Section III

Relevance of major incidents in other Member States and details to be reported to other competent authorities

Article 18

Relevance of major incidents to competent authorities in other Member States

The assessment of the relevance of major incidents to competent authorities in other Member States under Article 19(7) of Regulation (EU) 2022/2554 shall be based on whether the incident has a root cause originating from another Member State or whether the incident has had a significant impact in another Member State on one of the following:
   a) clients or financial counterparts; or
   b) a branch of the financial entity or another financial entity within the group; or
   c) a financial market infrastructure; or
   d) a third-party provider providing services to financial entities in the other Member State, which is likely to have an impact on those financial entities, to the extent this information is available.

Article 19

Details of major incidents to be reported in accordance with Article 19(6) and (7)

The details of the reports to be submitted in accordance with Article 19(6) and (7) of Regulation (EU) 2022/2554 shall comprise the same level of detail, without any anonymisation, as the reports of major incidents received from financial entities in accordance with Article 19(4) of that Regulation.

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,
[*Please choose one of the options below.*]

For the Commission
The President

[For the Commission
On behalf of the President

[Position]

Accompanying documents

5. Draft cost-benefit analysis / impact assessment

As per Article 16(2) of Regulation (EU) No 1093/2010 (EBA Regulation), 1094/2010 (EIOPA Regulation) and 1095/2010 (ESMA regulation), any guidelines and recommendations developed by the ESAs shall be accompanied by an Impact Assessment (IA) which analyses 'the potential related costs and benefits'.

This analysis presents the IA of the main policy options included in this Consultation Paper (CP) on regulatory technical standards (RTS) on the criteria for the classification of ICT-related incidents, materiality thresholds for major incidents and significant cyber threats.

A. Problem identification

According to Article 17 - 19 of the Regulation 2022/2554 (DORA), financial entities shall detect and classify ICT-related incidents and report major ICT-related incidents or, as applicable, operational and security payment-related incidents to the DORA national competent authorities (NCAs). At the moment of entry into force of the Regulation 2022/2554, the ICT-related reporting thresholds and taxonomies varied significantly at national level. Due to these divergences, there are multiple requirements that financial entities must comply with, especially when operating across several MSs and when part of a financial group.

This divergence becomes a more significant problem in the context of the requirement in the Regulation 2022/2554 for financial entities to report the major ICT-related incidents to their NCAs, to enable NCAs to fulfil their supervisory roles and to prevent contagion in the market. Divergence in definitions and classifications could lead to unharmonised data reporting and interpretations, as well as subsequent divergent treatment of similar ICT-related incidents by the supervisory authorities, despite these incidents being of the same nature and/or significance. This in turn may lead to regulatory arbitrage, as well as increased risk to the cyber security of financial entities.

B. Policy objectives

To enable CAs to fulfil their supervisory roles and to prevent contagion in the market, these RTS aim to set out classification criteria of ICT-related incidents to be used by financial entities. The classification and subsequent assessment against materiality thresholds will be the basis for the reporting framework of the major ICT-related incidents, by allowing to identify which incidents are major and therefore need to be reported to the CAs, and which ones are not. Financial entities shall carry out similar but simplified assessment to identify significant cyber threats.

The general objectives of this RTS include ensuring cyber security, operational efficiency, and cross-border comparability of incidents. The specific objectives include ensuring to the extent possible simplicity and clarity of criteria, harmonisation across sectors and entities, while considering sector specificities if and where necessary and the need to ensure proportionality.

C. Baseline scenario

The baseline scenario is the situation when the current definitions and taxonomy is kept, without further changes or further harmonisation. This includes:

- ENISA taxonomy, NIS 2
- PSD2 payment-related major incidents

The Directive (EU) 2022/2555 or Network and Information Security (NIS 2) Directive[3] was adopted on 17 January 2023, at the same time as DORA. It is an expansion of NIS Directive, which was the first piece of EU-wide legislation on cybersecurity aiming to achieve a high common level of cyber security across the EU. NIS1, and subsequently NIS2, are considered as the horizontal framework for cybersecurity in the EU and serves as a baseline standard for a minimum harmonisation of all sectoral legislation in this field.

One of the requirements of NIS2 is that "essential and important entities" notify, without undue delay its relevant authority of any incident that has a significant impact on the provision of their (significant incident). An incident is considered significant if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

In addition, the baseline includes also the Guidelines on major incident reporting under PSD2 (EBA/GL/2021/03) published by the EBA in 2017 and revised in June 2021.[4] The guidelines require payment service providers (PSPs) to establish a framework to maintain effective incident reporting procedures, including for the detection and classification of major operational or security incidents.

Finally, the baseline also includes the text of the Regulation 2022/2554 that applies from 17 January 2023, but without the additional RTS specifying the criteria for classification of major ICT-related incidents and cyber threats.

D. Options considered

In the process of developing the RTS a holistic approach was necessary to provide a classification of the ICT-related incidents and cyberthreats that would consider the various aspects of cyber security as well as the differences across sectors. Therefore, the policy options that were in the end chosen

[3] https://eur-lex.europa.eu/eli/dir/2022/2555

[4] https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20major%20incident%20reporting%20under%20PSD2%20EBA-GL-2021-03/1014562/Final%20revised%20Guidelines%20on%20major%20incident%20reporting%20under%20PSD2.pdf

should be assessed in the context of all the other options as well, as it is in combination that they reach the desired general and specific objectives.

5.1. General issues

Policy issue 1: Combination of criteria used to define major ICT-related incidents

Options considered:

- Option A: Triggering the reporting by all criteria
- Option B: Triggering the reporting by combination of criteria
- Option C: Triggering the reporting by one single criterion

Option A suggest using all the criteria and their thresholds for classification of ICT-incidents as major. This approach will exclude significant number of incidents from the DORA incident reporting framework and thus lead to significant underreporting. This option was therefore discarded.

Option C suggest that one single criterion could trigger the reporting. Requiring one criterion to be fulfilled would lead to one of the two scenarios:

- Having a single criterion triggering a major ICT incident reporting will lead to significant over-reporting, thus putting burden on financial entities and CAs, and that supervisors may be prevented from focusing all their attention to the incidents that are really major and/or those that may have a systemic impact. In addition, some criteria (e.g. geographical spread) cannot be stand-alone.
- Alternatively, if the criteria are made stricter to avoid over-reporting (e.g. by increasing the threshold or reducing the number of conditions to be fulfilled), it could lead to losing relevant information about the incidents, especially when applied to certain sectors.

Finally, using a combination of criteria to trigger the reporting (Option B) is more proportionate and will ensure capturing the most relevant major ICT incidents and will prevent over-reporting. It also allows for various ways of combining features that would flag an incident as major. Therefore, Option B was retained.

A more detailed analysis of the several scenarios of how the criteria can be combined are shown in the next section “Scenario analysis”.

Policy issue 2: The weights allocated to criteria for major incidents

Options considered:

- Option A: Single list of equally waited criteria for major incidents.
- Option B: Split between higher impact and lower impact thresholds for each criterion (similar to the approach in PSD2)
- Option C: Split between primary and secondary criteria for major incidents

A combination of criteria can be applied in multiple ways. One approach would be to have a single list of equally weighted criteria, where an incident would be classified as major when a certain number of criteria (say any 3 criteria from the list) would be fulfilled. This approach is simple, but is not optimal,

since the interplay between criteria is not captured, and may lead to the reporting of some incidents that are not relevant.

Another approach is the one used in PSD2, where the thresholds of the criteria are split into so-called "Higher impact" and "Lower impact". In this approach each criterion has two thresholds, one associated with a lower impact and one with a higher impact. An incident would be classified as major when at least one criterion is fulfilled at "higher impact" or at least three criteria at "lower impact". This approach is more proportional, as it allows to capture more incidents with high impact, and restrict the reporting of incidents with lower impact related only to one or two criteria, ensuring the reporting only of relevant incidents. The drawbacks of this approach are that the thresholds for these criteria are difficult to calibrate for all the different types of financial entities covered by the RTS and may lead to lack of harmonisation and sector-specific thresholds. Moreover, it is also more complex and burdensome to implement for the financial entities.

Another proposed approach is the split of criteria into primary and secondary. This approach is similar to the PSD2 approach, but less complex and burdensome, because it does not set two sets of thresholds for each criterion. Instead, it identifies indicators that are primary and secondary. This designation does not mean and indicator is less important than another, but simply that the indicators are complementary to each other and those that are primary have more dependencies with other criteria.

Policy issue: Level of harmonisation across sectors:

Options considered:

- Option A: Full harmonisation
- Option B: Harmonisation with specific sectoral specificities
- Option C: Approach with sector specificities

A harmonised approach to classify incidents as major is assessed as simple, easier to implement, and would ensure alignment with other institutions and regulations that already are in place. The benefits would be a harmonised reporting framework, focused on safety and efficiency, that will be the same for all sector and entities. While some criteria and thresholds may be less relevant for some sector (e.g. 'transactions' to the insurance sector) or financial entities (e.g. 'transactions' to credit rating agencies), there are others that are, which ensures that all sectors have criteria and thresholds that allow capturing holistically the major incidents in their sectors. The criteria and thresholds are consistent and embed proportionality.

A harmonised approach considering several sector specificities was also considered (Option B), in particular with regard to insurance undertakings (where for example service downtime over 24 h may not be major), and market infrastructures (where even a small duration of service downtime can be critical). While sectoral differences are acknowledged, these differences were captured using alternative criteria that would ensure the differentiation of the magnitude of these incidents (for example in terms of impact on financial system).

Finally, a purely sectoral approach was considered as well (Option C). While such an approach would have to be adapted to the specific features of the incidents in each sector, it would lead to a very fragmented framework for incident classification and reporting, significant burden to financial entities providing several financial services, and will be an important impediment to assess the cyber risk

posed by these incident at financial system level. This approach will also go contrary to the objectives of DORA to harmonise and streamline incident reporting requirements.

Therefore, Option A was preferred.

Policy issue: Proportionality in terms of size and complexity

Options considered:

- Option A: Different thresholds by size and complexity
- Option B: Proportionality is embedded in criteria (relative and absolute thresholds)

Two options were considered with respect to the application of proportionality in the classification criteria and thresholds. On the one hand, different thresholds could have been considered for financial entities of different sizes and complexity and for different financial entities within the scope of DORA (Option A). One challenge of such an approach would be to find an appropriate categorisation and metric of financial entities from all the sectors in the scope of the RTS, which would also reflect a comparable size and complexity. An insurance undertaking, a bank and an investment firm of a similar size in terms of total assets are not comparable and cannot use the same thresholds when identifying major ICT-related incidents. Moreover, such an approach will overcomplicate the legal framework and introduce significant burden for financial entities to classify incidents.

Another option was to embed proportionality in common criteria and thresholds (Option B), by ensuring the use of both absolute and relative thresholds in a non-cumulative manner (see policy issue below). While not relevant in every single case, such an approach ensures that the criteria are relative to the type and size of the financial entity, and also sets floors to ensure that stricter criteria are applied to larger companies and less strict to smaller ones. This approach was therefore chosen.

5.2. Classification criterion Clients, financial counterparts and transactions

Policy issue 3: Thresholds for the number of clients, financial counterparts and transactions

With respect to the criterion in Article 18 (1) (a) of the Regulation 2022/2554 related to “the number and/or relevance of clients or financial counterparts affected and, where applicable, the amount tor number of transactions affected”, several approaches to setting thresholds were considered. The thresholds were assessed separately for each indicator.

3.1. Number of clients

- Option A: Absolute threshold only
- Option B: Relative threshold only
- Option C: Both relative and absolute threshold (cumulative)
- Option D: Both relative and absolute threshold (non cumulative, using OR operator)

Applying only an absolute threshold (Option A) would be difficult to calibrate to be relevant for all financial entities in the scope of the RTS. Moreover, it will likely exclude any smaller financial entities where even a smaller number of clients may be significant for the FE. It may also require introducing specific thresholds for the different financial entities within the scope of DORA.

Applying only a relative threshold (Option B) would allow setting a percentage level for all entities, hence being proportionate to financial entities irrespective of their type and size. However, in cases

of large institutions, with large number of clients, the relative threshold would be quite high, and important incidents affecting a significant number of clients, albeit below the relative threshold, may be unreported.

Applying both an absolute and relative threshold in a non-cumulative manner (Option D) allows to reach a good balance, whereby incidents relative thresholds would allow major incident reporting to be triggered equally for all financial entities. Incidents impacting larger financial entities, where even a small share of clients may represent a large number, could trigger the absolute threshold, leading to a proportionate treatment.

The application of both relative and absolute thresholds in a cumulative manner (Option C) was also considered but discarded since it was deemed too restrictive and un-proportional as it would lead to the triggering of materiality thresholds rarely, thus leading to significant underreporting.

Option D is the preferred one.

3.2. Financial counterparts

- Option A: Absolute threshold only
- Option B: Relative threshold only
- Option C: Both relative and absolute threshold (cumulative)
- Option C: Both relative and absolute threshold (non- cumulative)

In the case of financial counterparts, the same options were considered as for clients. Given the nature of financial counterparts, that can be of various sizes and that financial entities may rely on divergent number of financial counterparts, applying the absolute thresholds to their number is not meaningful and would not be proportional. It would also be impossible to find a number of financial counterparts that would be an appropriate threshold for all the financial entities. Therefore, applying only absolute threshold, or a combination of relative and absolute thresholds was not seen as appropriate. Instead, a relative threshold only (Option B) was chosen as the most appropriate approach.

3.3. Transactions

- Option A: Absolute threshold only
- Option B: Relative threshold only
- Option C: Both relative and absolute threshold (cumulative)
- Option C: Both relative and absolute threshold (non- cumulative)

Applying the same rational as for number of clients, Option D, which entails the application of both relative and absolute thresholds in a non-cumulative manner, was chosen as preferred option.

Policy issue 4: Relevance of clients and financial counterparts

- Option A: Quantitative thresholds only;
- Option B: Qualitative thresholds only, where relevance for financial entity is based on own assessment;

With respect to the relevance of clients and financial counterparts, which is also included in the criterion in Article 18 (1)(a) of the Regulation 2022/2554, a number of quantitative criteria (Option A)

were considered, such as the number and volume of transactions with each client or financial counterpart, the type of clients (e.g. financial market infrastructures would be more relevant), measurement of impact and interconnection. All these measures however are business specific or entity specific. Therefore, it would be challenging to find common thresholds and rules that would work for all the financial entities in the scope of the RTS.

Another approach is to require a qualitative assessment of the relevance of the clients or financial counterparts by the financial entity itself, using their own risk assessment (Option B). As financial entities are most knowledgeable of their business, and the relevance of the clients and financial counterparts to their activities, this approach was deemed appropriate.

5.3. CLASSIFICATION CRITERION ECONOMIC IMPACT

Policy issue: Threshold for economic impact

- Option A: Absolute and relative thresholds
- Option B: Relative threshold only
- Option C: Absolute threshold only

When classifying the incidents, financial entities should consider their economic impact on the financial entity by estimating "direct and indirect costs and losses, of the ICT-related incident in both absolute and relative terms". In order to assess the magnitude of these costs and losses, and therefore the economic impact, several thresholds were considered.

In line with the level 1 text, Option A considered the application of both an absolute and a relative threshold. Such an approach would ensure that the relative threshold captures the economic impact relative to the business size or capital size while the absolute one sets a minimum impact amount above which the incidents would qualify under the criterion irrespective of the size of the financial entity. Such an approach however was difficult to implement due to lack of one common denominator metric of size or capital that would be meaningful for all financial entities under the scope of RTS and that can be used as a relative threshold. For example, while Tier 1 capital was considered as adequate for banks, such a metric is not available for most other entities. In a similar manner, using total assets would not be meaningful for investment firms and would require clarification on the types of assets for the investment sector. Finally, other metrics leveraging on revenues or profit were also not deemed appropriate due to the way how some business models of certain financial entities are structured. Therefore, the criterion may not apply equally and proportionately to all financial entities.

Option B considered the application of a relative threshold only. Since all the challenges and drawbacks of the relative threshold explained in Option A apply, this approach was not seen as feasible.

Finally, Option C considered using an absolute threshold only for the estimate of costs and losses. This approach therefore does not need to be used with a reference value other than the value of the cost or loss incurred as a result of the incident. It also easier to implement, will not introduce reporting burden and embeds proportionality, as smaller entities are less likely to cross this threshold.

Therefore, given the above arguments, Option C was chosen.

Scenario analysis

This section looks at the results from applying several approaches (scenarios) to combining the criteria and their materiality thresholds when identifying major incidents on a samples of major incidents that are available at the moment to the ESAs and to the national competent authorities.[5] In the course of the analysis a multitude of approaches where considered, but we are presenting here only three, to give an idea of the trade-offs that were encountered.

The three scenarios are described in more detail in Table 1 below. All these scenarios include all the criteria and their thresholds, but differ between them by a few elements:

- the rule on how the criteria a combined
- the thresholds for the service downtime
- the definitions of reputational impact
- the definition of critical services affected
- the application of the data losses criterion

The results from each scenario for the case of payment-related operational and security incidents based on a carefully selected sample of incidents are presented in table 3. These incidents cover major incidents that are of high prominence and that should be captured by DORA and a smaller subset of major incidents that may be considered of less relevance for supervisors and as overreporting. The same scenarios have been tested also by ESMA to their supervised entities and by the national authorities. The results for these tests will be presented in a descriptive manner, where relevant.

Scenario 1, where two criteria should be fulfilled, of which at least one should be primary, captures all the prominent major payment incidents, but leads to the overreporting of the less prominent major incidents in our sample (80%). There is a high probability that such a scenario will capture many incidents that have not been classified as major under PSD2. Similar potential overreporting has been revealed by the testing of few national authorities. With regard to the supervised entities by ESMA, the proposed criteria captured all their incidents. This scenario therefore was not seen as optimal due to the probability of high overreporting.

Scenario 2 uses a similar rule as scenario 1 for combining the criteria, but includes some modifications to how the criteria are defined. In particular, the duration and service downtime of the incident are paired with the data availability, while high level escalation of the incident has been moved from a feature of the "Reputational impact" criterion, to a feature of the criterion "Critical services affected". This scenario resulted in a 100% capture of all the prominent major payment incidents, and none of the less prominent ones, which indicated a good calibration of the thresholds for payment-related major incidents. On the other hand, based on ESMA's estimation, this scenario resulted in significant decrease of the incidents that will be captured from the investment sector, including some prominent major incidents. The same will likely apply to the other financial entities in the investment sector. While this scenario is optimal for the payment's sector, it will lead to significant underreporting of FEs supervised by ESMA and important supervisory data not being available to ESMA and CAs in the investment sector. The proposed scenario was not seen as optimal.

[5] Since the ESAs and the national authorities do not have information on the minor incidents, the analysis of the extent of capture of the non-major incidents is not possible.

Finally, scenario 3 proposes a reintegration into one criterion of authenticity, integrity, confidentiality, and availability of data, which in previous scenarios were split. Moreover, this scenario proposes a new rule of combining the criteria: Three criteria, of which at least one primary, or two primary criteria.

This scenario allows to capture all the relevant incidents in the investment sector, with potential small decrease of incidents reported to ESMA from their supervised entities, but all prominent major incidents being captured. Applying the same rule to payment-related incidents, however, would lead to the same share of reported incidents as in scenario 1. Unlike scenario 1 however, the number of incidents that qualify for each individual criterion is smaller than in scenario 1. Since the share of incidents captured is lower for the primary criterion Critical services affected (73% vs 93%), and similar for the other primary criteria[6], it is expected that the incidents captured outside of the population currently reported as major under PSD2 will be lower compared to Scenario 1. Although for payment incidents most currently reported major incidents will be captured, together with potential additional incidents not currently within the scope of reporting under PSD2, the result is still slightly on the overreporting side, this scenario was assessed as a good compromise that allows to capture prominent major incidents across the financial sector. This proposed scenario seems most balanced and has, therefore, been proposed in the draft RTS.

[6] For criterion data losses, due to it being split in scenario 1 into two criteria (one secondary, and one primary that can trigger the classification as major on its own), the result is ambiguous as it depends on the individual features of each incident hand their combination.

Table 2. Application of three scenarios on a sample of payment incidents

		Scenario 1		Share of incidents captured by each criterion	Scenario 2		Share of incidents captured by each criterion	Scenario 3		Share of incidents captured by each criterion
	Criterion	RULE: Two criteria, at least one primary			RULE: Two criteria, at least one primary			RULE: Three criteria, of which at least one primary or Two primary criteria*		
1	**Clients, financial counterparts and transactions**		Primary	87%		Primary	87%		Primary	87%
2	**Reputational Impact**	*Includes High level of internal escalation*	Secondary	80%	*No high level of internal escalation*	Secondary	40%	*No high level of internal escalation*	Secondary	40%
3	**Duration and service downtime including**	*2 hours duration, 24 hours service downtime*	Secondary	67%	*2 hours duration, 4 hours service downtime + data losses availability*	Secondary	47%	*2 hours duration, 24 hours service downtime*	Secondary	67%
4	**Geographical Spread**		Secondary	40%		Secondary	40%		Secondary	40%
5	**Data losses**	*authenticity, integrity or confidentiality*	Single criterion	13%	*authenticity, integrity or confidentiality*	Single criterion	13%	*authenticity, integrity, confidentiality or availability*	Primary	73%
		availability	Secondary	67%	*Erased and Paired with service downtime*	NA				
6	**Critical services affected**	*No high level of internal escalation*	Primary	93%	*Includes High level of internal escalation*	Primary	73%	*Includes High level of internal escalation*	Primary	73%
7	**Economic impact**		Secondary	27%		Secondary	27%		Secondary	27%

Table 3. Share of payment incidents captured by each scenarios

	Scenario 1	Scenario 2	Scenario 3
Share of payment incidents captured in the sample, of which:	93%	67%	87%
Share of prominent major payment incidents captured	100%	100%	100%
Share of less prominent major incidents captured	80%	0%	80%

Cost-Benefit Analysis

Overall, the RTS on the criteria for the classification of ICT-related incidents, materiality thresholds for major incidents and significant cyber threats will bring the financial entities, and CAs both costs in terms of implementation and benefits in terms of better awareness of and monitoring of major ICT-related incidents, and ultimately ensuring financial stability of the system.

The costs and benefits are listed in Table 1 below

Table 1: Cost and benefits of RTS

Stakeholder groups affected	Costs	Benefits
Financial entities	Costs related to the changes in processes and infrastructure to reflect the classification criteria and threshold related to the ICT-related incidents.	Awareness and monitoring of risks stemming from ICT-related incidents. Benefitting from harmonised criteria at EU level, which allows the EU level monitoring of ICT-related incidents, on top of the internal risk assessments. Better cyber security, operational efficiency, and cross-border comparability of incidents. Subsequent better protection of clients and entity from external malicious actors and less risk for the reputation of the financial entity. Early indication for and prevention from major ICT-related incidents that have affected one financial entity but that can have a spill-over effect.
Competent authorities	Costs related to the processing of additional flow of information related to major-ICT related data.	Harmonised terminology and information across MSs and across sectors, that will facilitate the analysis and discussions of the relevant risks. Better cyber security, operational efficiency, and cross-border comparability of incidents Increased financial stability of the financial system
Consumers	None	Better quality service provision and better protection from cyber risks and threats posed by malicious actors.

Overall, benefits of the RTS are assessed as being significantly higher and relevant for all the stakeholders involved, compared to the costs.

6. Overview of questions for consultation

Q1. Do you agree with the overall approach for classification of major incidents under DORA? If not, please provide your reasoning and alternative approach(es) you would suggest.

Q2. Do you agree with the specification and materiality thresholds of the criterion 'Clients, financial counterparts and transactions affected', as proposed in Articles 1 and 9 of the draft RTS? If not, please provide your reasoning and suggested changes.

Q3. Do you agree with the specification and thresholds of the criteria 'Reputational impact', 'Duration and service downtime', 'Geographical spread' and 'Economic impact', as proposed in Articles 2, 3, 4, 7, 10, 11, 12 and 15 of the draft RTS? If not, please provide your reasoning and suggested changes.

Q4. Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13? If not, please provide your reasoning and suggested changes.

Q5. Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14? If not, please provide your reasoning and suggested changes.

Q6. Do you agree with capturing recurring incidents with same apparent root cause, similar nature and impact, that in aggregate meet the classification criteria and thresholds as major incidents under DORA, as proposed in Article 16? If not, please provide your reasoning and suggested changes. Please also indicate how often you face recurring incidents, which in aggregate meet the materiality thresholds only over a period of 6 to 12 months based on data from the previous two years (you may also indicate the number of these recurring incidents).

Q7. Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17? If not, please provide your reasoning and suggested changes.

Q8. Do you agree with the approach for assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities, as proposed in Articles 18 and 19? If not, please provide your reasoning and suggested changes.