JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2023 83

10 January 2024

Final report

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

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

1. 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 (ECB) and European Union Agency for Cybersecurity (ENISA), 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.

The ESAs ran a public consultation between 19 June and 11 September 2023. The ESAs received 105 responses to the Consultation paper. The ESAs assessed the concerns raised to decide what, if any, changes should be made to the draft RTS. In the light of the comments received, the ESAs agreed with some of the proposals and their underlying arguments and have introduced changes to the draft RTS. These changes related to the classification approach, the specification of some classification criteria and their materiality thresholds, and to the approach for recurring incidents.

On the classification approach, ESAs have amended the draft RTS so that FEs classify incidents as major if the criterion 'Critical services affected' is met and (i) any malicious unauthorised access to network and information systems as part of the 'Data loss' criterion is identified or (ii) the materiality thresholds of any other two criteria are met.

With regard to the classification criteria and their thresholds, in turn, while maintaining a harmonised approach for the classification of incidents for all FEs within the scope of DORA, the ESAs clarified the various aspects of the classification in the criteria and introduced changes to the thresholds of the criteria 'Clients, financial counterparts, and transactions affected' and 'Data losses' to introduce further proportionality, address sector-specific issues raised and capture relevant cyber incidents.

Finally, to address concerns on the reporting burden for the FEs, the ESAs have amended the approach for classifying recurring incidents, which now focuses on incidents that have occurred at least twice, which have the same apparent root cause, and which would have met cumulatively the incident classification criteria. The assessment of recurrence is to be carried out on monthly basis.

Next steps

The final draft RTS will be submitted to the Commission for adoption. Following the adoption, the RTS will be subject to scrutiny by the European Parliament and the Council and then will be published in the Official Journal of the European Union.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

2. List of abbreviations

ACP – Advisory Committee on Proportionality

CA – Competent authority

CP – Consultation paper

CSIRT – Computer Security Incident Response Team

CTPP – Critical third-party provider

DORA – Regulation EU 2022/2554

ECB – European Central Bank

ENISA – The European Union Agency for Cybersecurity

ESAs – European Supervisory Authorities

EU – European Union

FE – Financial entity

ICT – Information and communication technology

IORP – institution for occupational retirement provision

NIS2 – Directive (EU) 2022/2555

PSD2 – Directive (EU) 2015/2366

RTS – Regulatory Technical Standards

TPP – third party provider

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. A Consultation paper (CP) on the draft RTS was published on 19 June for a three-month consultation period, which closed on 11 September 2023. The ESAs received 105 responses from a variety of market participants across the financial sector.

5. The ESAs have assessed the responses from the public consultation and have made changes to the draft RTS where relevant. The main issues raised by the stakeholders are presented in Section 5 of this report 'Accompanying documents' in the sub-section on feedback from the

public consultation. The Rationale section provides an overview of the most prominent aspects raised during the consultation and/or that resulted in more substantive changes to the draft RTS.

3.2. Rationale

6. The respondents to the public consultation commented on all aspects of the proposed draft RTS. The key points raised that led to changes to the draft RTS are reflected in this section, which focuses on:
    - The approach for classifying major incidents
    - The classification criteria and their materiality thresholds
    - Recurring incidents
    - Proportionality

7. The articles related to the classification of significant cyber threats, the criteria for assessment of relevance of major incidents in other Member States, and the details of major incident reports to be shared with other CAs remain largely unchanged.

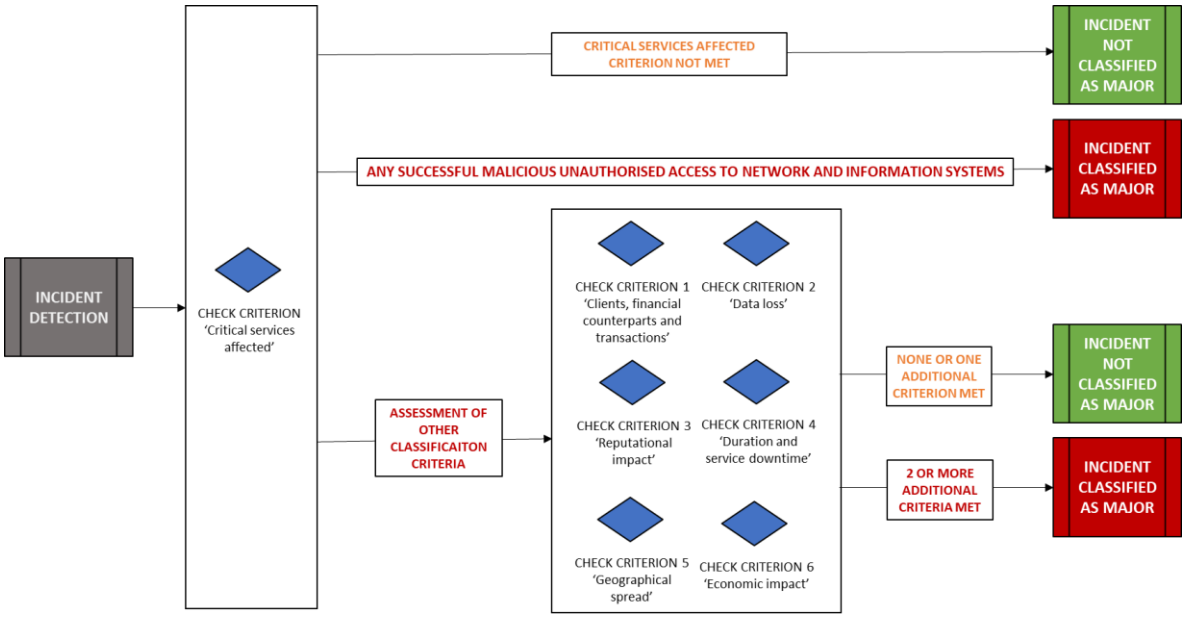
The approach for classifying major incidents

8. Many respondents to the public consultation viewed the classification approach as too complex, challenging to follow while FEs are handling the incidents, and posing the risk of overreporting. Some of these respondents also proposed changes in the weighting of different criteria that may fit better their respective sector (e.g. moving the criterion 'clients, financial counterparts and transactions affected' as a secondary criterion, upgrading the criterion 'duration and service downtime' to a primary criterion, etc). Several respondents also proposed the classification approach in the RTS focuses on the impact of the incident more directly.

9. The ESAs took into account the feedback received from the respondents to the public consultation on this topic and also holistically across all different questions from the public consultation and have amended the approach for classification of major incidents under DORA so that it is clearer, simpler and straight forward to perform at a time when FEs will be handling an incident. In particular, the ESAs have decided to treat the classification criterion 'critical services affected' as a mandatory condition for classifying an incident as major and to classify major incidents where either one of the following conditions is met:
    - any malicious unauthorised access to network and information systems as part of the 'Data loss' criterion is identified; or
    - the materiality thresholds of any other two criteria should be the additional triggers for major incident classification.

10. Accordingly, all criteria (except 'critical services affected') will be treated equally, without distinguish between primary and secondary criteria. The chart below illustrates the classification approach and the table below provides an overview of the classification criteria and their thresholds.

Figure 1: Approach for classifying major incidents under DORA



11. This amendment is also aligned with other general feedback on the classification approach received seeking closer alignment with the definition of major ICT-related (or security or operational payment-related) incident, which specifies that the incident should have a high adverse impact on the network and information systems that support critical or important functions of the financial entity.

Table 1: Overview of the classification criteria and their thresholds for major incidents under DORA as introduced in the final draft RTS

	Major ICT-related Incident or security or operational payment-related incident if critical services are affected and (i) any malicious unauthorised access to network and information systems identified, which may result to data losses or (ii) the thresholds of two additional criteria from the below are met						
	Mandatory condition	Additional classification criteria					
	Critical services affected	**Clients, financial counterparts and transactions**	**Data losses**	**Reputational Impact**	**Duration and Service Downtime**	**Geographical Spread**	**Economic Impact**
Materiality threshold	**The incident has had any impact on critical services**	Any of: a) >**10% of all clients** using the affected service; b) **>100 000 clients** using the **affected** service; c) **>30% of all financial counterparts** used by the FE; d) **>10%** of the daily average number of **transactions**; e) **>10%** of the daily average amount of **transactions;** f) any **identified impact on clients or financial counterpart** identified by the FE as relevant.	**Any impact on the availability, authenticity, integrity or confidentiality of data**, which has or will have an **adverse impact** on the implementation of the **business objectives** of the FE or on **meeting regulatory requirements**	Any **reputational impact set out in Article 2 a) to d) (overview below)**	a) **incident duration** is **longer than 24 hours**; or b) **service downtime** is **longer than 2 hours for** ICT services that support critical or important functions	**Any impact** of the incident identified in the territories of at **least two Member States**	Costs and losses incurred by the FE **exceed** or are likely to exceed **€100 000** (can be based on estimates where actuals cannot be determined)
Criteria Detail	Assess if the incident : a) affects ICT services or Network and information systems that support **critical or important functions of the FE; or** b) affects financial services that require authorisation, registration or are otherwise supervised by competent authorities; or c) represents a successful, malicious and unauthorised access to the network and information systems of the financial entity.	**1. all affected clients unable to make use of the service** provided by the FE during the incident or that were **adversely impacted by the incident.** These include also third parties explicitly covered by the contractual agreement between the FE and the client as beneficiaries of the affected service. **2.** all affected **financial counterparts with contractual arrangements with the FE.** **3. relevant clients and financial counterparts** whose impact will affect the business objectives of the FE or market efficiency. **4.** all **affected transactions** with monetary amount, with one leg in the EU. (FEs can use **estimates** from comparable reference periods where actuals not available)	1. **availability** of data – data on demand rendered temporarily or permanently inaccessible or unusable; 2. **authenticity** of data – compromised trustworthiness of the source of data; 3. **integrity** of data – data inaccurate or incomplete due to non-authorised modification 4. **confidentiality** of data – data being accessed by or disclosed to unauthorised party or system.	**Reputational impact evidenced by any of the below**: a**) incident reflected in the media**; or b) received **repetitive complaints**; or c) inability **to meet regulatory requirements**; or d) **likely loss of clients or financial counterparts** with a material impact on FE's business. **Level of visibility** of the incident to be taken into account.	**1. Duration** measured from the moment an incident occurs or is detected, until it is resolved. (estimate if not yet known) **2. Service downtime** measured from the moment service fully/ partially unavailable/ delayed to clients, financial counterparts or other internal or external users, until activities are restored to the same level before the incident.	**Assess significant** impact of the incident in **other EU Member States** on: a) **clients or financial counterparts;** b) **branches** of the FE or **other group financial entities;** (c) **Financial market infrastructures or third party providers** that may affect other FEs.	**Types of direct and indirect incurred costs** a) expropriated funds or financial assets liability, including theft; b) replacement or relocation costs; c) staff costs; d) contract non-compliance fees; e) customer redress and compensation costs; f) forgone revenues; g) communication costs; h) advisory costs. (based on available data at time of reporting)
Triggered Yes/No							

The classification criteria and their materiality thresholds

12. The classification criteria set out in the RTS cover 'Clients, financial counterparts and transactions affected', 'Reputational impact', 'Duration and service downtime', 'Geographical spread', 'Data losses', 'Critical services affected', and 'Economic impact'. The main changes introduced to the criteria in draft RTS following the public consultation relate to:

- 'Clients, financial counterparts and transactions affected'
- 'Duration and service downtime'
- 'Data losses'
- 'Critical services affected'

Criterion 'Clients, financial counterparts and transactions affected'

A) Clients affected

13. With regard to the clients-related part of the criterion, many respondents were of the view that the term 'clients' needed to be clarified, with regard, in particular, to address the following aspects:

- Uncertainty whether this criterion refers to the clients registered in the specific channel or service affected by the incident (web application, mobile application), or the clients that usually use this channel/service;
- Uncertainty on the scope of the term 'clients' and whether it includes effective clients, former clients whose data are still stored in the FE's ICT systems, or others;
- Possibility that clients may be interpreted differently by investment fund managers, whose clients are investment funds or vehicles, and private banks with individual clients' deposits;
- Clarity needed on whether competent authorities and central banks are clients for trade repositories; and
- Potential overlap of number of clients and the number of transactions affected.

14. Some of these respondents also put forward proposals on how to amend the specification of the clients-related part of the criterion, in particular to:

- Interpret clients as 'members' for the specific case of pensions funds, since they are considered as the ultimate beneficiaries;
- Focus this part of the criterion on clients suffering a material degradation in the service provided to them; and
- Focus the client-related part of the criterion on own clients only.

15. With regard to the materiality threshold of the clients affected, some respondents shared their concerns that:

    - some services are used by a few clients only and thus the threshold can be met very easily;
    - the 10% threshold is too low for a primary criterion, with different proposals made to raise it to 15, 20 or 25%;
    - The threshold may lead to overreporting;
    - The absolute threshold will lead to overreporting since it is too low, and it does not reflect proportionality and the risk entailed; and
    - The absolute threshold of 50 000 affected clients would not be indicative for a major incident.

16. The ESAs understand the concerns raised by market participants and have clarified the meaning of the term 'clients affected' to allow proper classification and subsequent calculation of the threshold. Accordingly, the ESAs have amended Article 1(1) of the draft RTS to clarify that clients cover also third parties explicitly covered by the contractual agreement between the financial entity and the client as beneficiaries of the affected service.

17. In addition, the ESAs have clarified in Article 1(1) that the impacted clients are those that are or were unable to make use of the service (partially or fully) provided by the financial entity during the incident or that were otherwise adversely impacted by the incident.

18. In relation to the materiality threshold for affected clients, the ESAs are of the view that the relative threshold of 10% is appropriate to cover incidents which affect a significant share of FE's clients and also taking into account that a combination of criteria is needed to classify an incident as major. The relative threshold is proportionate and is not impacted by the absolute number of clients. In relation to the absolute materiality threshold, the ESAs would like to highlight that it is envisaged to capture only large FE when an incident affects a large number of clients in cases where the relative threshold is not met. To address the concern raised by some respondents and to ensure that overreporting is avoided and proportionality fully embedded, the ESAs have arrived at the view that the absolute threshold should be raised from 50 000 to 100 000 clients.

B) Financial counterparts affected

19. Some respondents shared their concerns that the 10% threshold is too low for smaller entities and IORPs and may lead to overreporting, with a few proposing considering an absolute threshold or increasing the threshold to 15, 20 or 25%.

20. The ESAs agree with the concerns that the threshold may be too low, lead to overreporting and be particularly burdensome for smaller entities and IORPs. This is particularly evident by the fact that where a FE uses around 10 financial counterparts, an impact on one of them will

trigger the criterion. The ESAs have, therefore, decided to increase the relative threshold to 30%.

C) Transactions affected

21. With regard to the materiality threshold of the transactions-related part of the criterion, some respondents shared their concerns that:

- the reference to comparable reference periods is not clear;
- it is unclear how to calculate the impact when several currencies are affected;
- the relative threshold of 10% is too low and a few respondents proposed increasing it to 25%;
- the proposed absolute thresholds are (i) not suitable for some type of FE, (ii) too low for large entities, financial market infrastructures and other entities in the investment/market sector where the threshold of 15 000 000 EUR will be easily met, (iii) not proportionate, (iv) will lead to overreporting and (v) will be difficult to assess. Some proposals on the amendment of the threshold from the respondents focused on deleting the threshold, increasing it to 30 000 000 EUR, introducing tiered structure, or changing it to a relative threshold; and
- the threshold of the criterion being too high for small FEs.

22. In relation to these points raised by the respondents, the ESAs would like to point out that:

- on comparable reference periods, the ESAs agree with the respondents and have amended the requirement in Article 9(1)(d) and (e) of the draft RTS so that it refers to 'daily average' number/amount of transactions, instead of 'regular level of transactions carried out';
- on the use of different currencies, FEs can use the ECB's daily reference exchange rate;
- the relevant threshold of number of transactions affected of 10% is deemed appropriate, especially taking into account that a combination of criteria will be needed to classify an incident as major. The ESAs also did not receive convincing arguments on why 10% is not appropriate; and
- On the absolute threshold, the ESAs agree with the reasoning behind the concerns raised by the respondents and have amended the criterion to a relative one with a threshold of 10%.

23. Finally, it should be noted that the reference to 'transactions containing a monetary amount' for the classification purpose should not be understood in a narrow way, since it intends capturing all forms of exchange of financial instruments, crypto-assets, commodities, or any other assets, including in form of margin, collateral or other pledge, both against cash and against any other asset. For classification purposes, these should only cover transactions that involve assets whose value can be expressed in a monetary amount.

Criterion 'Duration and service downtime'

24. Many respondents to the public consultation sought clarification on the specification of the duration of the incident, in particular on how to understand the reference to 'fully or partially available' and 'activities/operations restored'.

25. In addition, several respondents objected to having a requirement to review system logs or other data sources to determine the moment the incident was detected and the moment it has been recorded. In their view, such checks will be expensive and require time to carry out.

26. With regard to the clarification on the interpretation of 'fully or partially available' and 'activities/operations restored', the ESAs understand that the underlying concern to be on how a 'service' should be interpreted. The ESAs would, therefore, like to clarify that the specification of 'service downtime' captures both ICT services and financial services, or in other words client facing and non-client facing systems. The ESAs have amended Article 3(2) of the draft RTS by including a reference to unavailability of the service to internal and external users.

27. In relation to the point on system logs, the ESAs agree that reviewing records in network or system logs may take time and be costly. To address this concern, the ESAs have amended Article 3 of the draft RTS by clarifying that the duration should be measured from the occurrence of the incident and where the occurrence is not known – from the detection of the incident. The ESAs have also specified that where the incident has occurred prior to the detection of the incident, FEs shall measure the duration from the records in network or system logs, but that in case they are unable to do so, FEs can apply estimates. It should be noted that these estimates should be calculated conservatively.

Criterion 'Data losses'

28. A few other respondents to the public consultation suggested clarifying that the 'data loss' criterion is only met in case of 'a real malicious use of the data' and that it is necessary to differentiate whether the data has been exploited or not, to avoid significant overreporting.

29. The ESAs would like to highlight that the criterion of data loss should be triggered as soon as there is a successful malicious and unauthorised access, irrespective of whether the data has been exploited or not. Any successful malicious unauthorised access could harm the FE (e.g. advance persistent threat (APT) attacks) and have a severe impact on its security systems, which can also be considered as critical or important functions of the FEs. Accordingly, the ESAs have introduced in Article 13 of the draft RTS a second trigger for the criterion 'data losses' covering cases of successful malicious unauthorised access to network and information systems. This will ensure capturing important major incidents such as those related to data breaches and data leakages and is consistent with the definition of 'security of network and information systems' under NIS2, which relates to 'the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the

availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems'.

30. A few of the respondents also highlighted that the loss of 'authenticity' should be better defined to differentiate it from loss of 'integrity'. One respondent suggested for authenticity to be deleted since it is covered by integrity.

31. The ESAs would like to stress that 'authenticity' and 'integrity' are two distinct properties introduced in Article 18 of DORA and thus 'authenticity' cannot be disregarded when assessing the classification criterion data losses. However, the ESAs agree with the respondents and have amended Article 5(2) of the draft RTS related to 'authenticity' by not referring to reliability of data and focusing on the need to determine whether the incident has compromised the trustworthiness of the source of data.

Criterion 'Critical services affected'

32. Many of the respondents to the public consultation were not supportive of the inclusion of the escalation to the senior management and the management body as part of the materiality threshold of the criterion 'critical services affected' since:

- the escalation to the management is a consequence of the classification of an incident;
- it will decrease internal reporting of incidents;
- will disadvantage FEs that have a robust incident response strategy and plans; and
- It will be disproportionate for smaller FEs.

33. The ESAs agree with the rationale provided and have removed the reference to the escalation to senior management and management body from the materiality threshold. In addition, as set out in paragraph 9 of this Final report, the ESAs have decided to treat the classification criterion 'critical services affected' as a mandatory condition for classifying an incident as major.

34. Another point raised by the respondents to the public consultation related to the clarification of the term 'critical services' and how it delineates from other similar terms, such as 'critical or important' function, 'network and information system'. Some respondents also questioned the reference to 'authorisation' in the assessment of the criticality of the service, with a few respondents seeking clarity on whether authorisation refers to authorised activities or internal approvals. Relatedly, a few respondents proposed to include a reference to 'registered' activities too.

35. To address these concerns, the ESAs introduced the following changes to Article 6 of the draft RTS in relation to the criterion 'critical services affected':

- Introduced a reference to 'network and information systems' to align better with the incident and major incident-related definitions of DORA;

- Clarified that the authorised services are 'financial services that require authorisation'; and
- Added a reference to registered or supervised services, and
- Clarify that a successful, malicious and unauthorised access to the network and information systems triggers the criterion of "critical services affected

Recurring incidents

36. A number of respondents expressed concerns about the operational burden that analysing incidents for similarities would entail, including the substantial use of internal resources and the difficulty in assessing the data. Some of them also mentioned proportionality concerns, as this requirement would disproportionately affect smaller entities.

37. Some respondents also commented on the assessment of recurring incidents by expressing concerns and seeking clarity on the reference to common 'root causes', 'same nature of the incident' and 'same impact of the incident'.

38. The ESAs have also received comments in relation to the reference time period for assessing recurring incidents, which ranged from 3 to 12 months, with a few respondents proposing to assess the recurrence periodically, and not on rolling basis.

39. Having assessed the feedback from the public consultation, the ESAs have arrived at the view that some changes will need to be introduced to the provisions related to recurring incidents, namely:

    - To ensure proportionality, the ESAs have exempted smaller FEs, namely those subject to the simplified ICT risk management framework and microenterprises, from the obligations to report recurring incidents;
    - Changing the approach for assessing recurring incidents from rolling to monthly basis. This time period was chosen in order to allow supervisors to obtain timely information about the incidents but at the same time not posing burden to the reporting entities; and
    - Focusing the common aspects of the recurring incident to the 'root cause' only and deleting references to 'similar nature and impact'.

40. With regard to the root cause analysis, it should be noted that the different types of root causes of the incidents are to be set out in the RTS and ITS on the content, timelines and process for reporting major incidents under DORA (Article 20a and 20b of DORA). Therefore, ESAs have amended the legal text to refer to said taxonomy.

41. With regard to the reference to the 'similar nature and impact', the ESAs have arrived at the view that consistent taxonomy will be challenging to set-up since the incidents vary in their

nature and impact and are specific to each FE. Accordingly, the ESAs have amended Article 15 of the draft RTS (previous Article 16) by removing the reference to similar nature and impact.

42. Finally, having assessed the feedback from the public consultation on the time-period for assessing recurring incidents, the ESAs have arrived at the view that monthly assessment for the previous 6 months should be adequate to capture recurrence. This approach balances well the needs of supervisors to receive incident information timely and of FEs of not being burdened with the assessment.

Proportionality

43. In the light of the feedback received from the public consultation and the Joint ESA ACP ad hoc advice on DORA from 5 May 2023, the ESAs have assessed the proportionality of the requirements proposed in the CP and introduced some changes to the draft RTS.

44. The ESAs would like to highlight that proportionality has been embedded holistically in the draft RTS. First, the combination of criteria used for classifying major incidents aims at ensuring that only incidents with significant impact on the FE (or the financial system) are being reported. The classification approach is also simple enough to be assessed and applied easily by small entities and microenterprises.

45. In addition, the levels of the classification thresholds have been set in such a way that they are not easily breached. The RTS uses relative thresholds for almost all criteria, so that it ensure proportionality. The only absolute thresholds used (absolute number of clients affected and economic impact) had been set out in such a way so that it is difficult to be met by smaller entities. Following the feedback from the public consultation, the ESAs have also increased the absolute number of clients affected from 50 000 to 100 000, thus ensuring further proportionality.

46. Relatedly, the ESAs have also increased the relative threshold of the criterion related to financial counterparts affected from 10% to 30% to decrease the cases where the criterion will be met, in order to address particular concerns raised on proportionality by the insurance and pensions sector. For proportionality considerations, the ESAs have also removed the absolute thresholds on the amounts of transactions and converted it to a relative threshold of 10%. The ESAs have also set the materiality threshold for the economic impact criterion 100 000 EUR. This absolute figure should be simple to calculate and high enough so that it is not easily met for each incident, especially for those affecting smaller FEs.

47. With regard to the ‘critical services affected’ criterion, to address proportionality concerns raised during the public consultation that, for smaller FEs, senior management may always or very often be involved in the handling of the incidents, the ESAs removed from the materiality threshold the reference to escalation to the senior management.

48. When it comes to recurring incidents, having assessed the feedback from the public consultation, the ESAs have amended the draft RTS to embed further proportionality, namely by:

- exempting smaller financial entities (i.e. those subject to the simplified ICT risk management framework under Article 16 of DORA and microenterprises) from the obligations to report recurring incidents; and
- changing the approach from assessing recurring incidents from rolling to monthly basis.

49. The Joint ESA Advisory Committee on Proportionality (ACP) ad hoc advice suggested the following aspects to be taken into account when developing the draft RTS

a) *When defining the criteria, 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, it should be taken into account that microenterprises and small and medium sized enterprises shall mobilize sufficient resources and capabilities to ensure that ICT-related incidents are managed swiftly and therefore the reporting burden should be minor for them.*

b) *In this context, the Proportionality Committees consider that it makes sense to distinguish the reporting requirement for financial entities that are small and medium sized, which could be quite different from what triggers a major incident report in a bigger/systemic institution. Bearing this in mind, striking the right balance will be essential as far as harmonisation of requirements and allowing for proportionality flexibility goes.*

c) *A possible proportionate approach could be that for bigger companies not all the criteria need to be met in order to classify an incident as a major incident whereas for smaller and medium-sized enterprises a different option would be adequate, for example requiring most or all of the criteria to be met in order to classify an incident as a major incident. According to this classification all major incidents need to be reported.*

d) *When introducing a threshold, the DORA regulation refers to absolute and relative thresholds. In principle, both absolute and relative thresholds already provide for proportionality. The Advice assumes that article 18 (1) (f) of DORA Regulation requires both absolute and relative thresholds to be applied to all entities. As such the Proportionality Committees believe that in defining relative thresholds, careful consideration needs to be applied on how they translate for small and medium-sized enterprises and ensure that they are at a level that would result in the right amount of reporting (i.e. capture the really impactful incidents for those entities).*

e) *While this would allow to reduce the reporting burden for small and medium-sized enterprises, managing the risk caused by an incident would still remain an obligation and in fact a priority for those entities.'*

50. With regard to a) above, the ESAs are of the view that the simple classification approach introduced in the draft RTS will facilitate all types of FEs, smaller firms in particular, in the classification of major incidents.

51. In relation to b) above, the ESAs have arrived at the view that the proposal deviates from the objective to introduce harmonised incident reporting requirements under DORA. In addition, it will pose additional challenges and burden for firms to navigate through different criteria and thresholds that may apply to them. Moreover, following directly this part of the advice would have posed a risk of introducing unlevel-playing field between FEs that may have similar level of complexity and nature of their operations.

52. With regard to c) above, the ESAs have introduced in the RTS a balanced approach where a combination of criteria needs to be met for classifying major incidents. This approach embeds proportionality and takes into account dependency between classification criteria.

53. When it comes to d) above, the ESAs have fully followed the advice since the large majority of the proposed classification thresholds are either binary (yes/no) or relative. Those materiality thresholds that use absolute amounts, such as ‘clients affected’ and ‘economic impact’ have a threshold set at a level that will unlikely be met for incidents affecting smaller FEs.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

4. Draft regulatory technical standards

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 or operational or security payment-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[1], and in particular Article 18(4) subparagaph three thereof,
Whereas:

(1) Given that Regulation (EU) 2022/2554 aims to harmonise and streamline incident reporting requirements covering 20 different types of financial entities, and considering 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 should be 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 may be affected by an incident without exceeding the relative thresholds, these cases should be captured through an absolute threshold mainly targeted at 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

[1] Insert OJ reference

major incident reporting under Directive (EU) 2366/2015[2], the Guidelines on periodic information and notification of material 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) In relation to the criterion of the amount and number of transactions affected, to determine the impact of an incident, the notion of transactions is broad and covers different activities and services across the sectorial acts applicable to financial entities. For the purposes of this Delegated Regulation, payment transactions and all forms of exchange of financial instruments, crypto-assets, commodities, or any other assets, also in form of margin, collateral or other pledge, both against cash and against any other asset, should be covered. Those transactions that involve assets whose value can be expressed in a monetary amount should be considered for classification purposes.

(5) The classification criteria should ensure that all relevant types of major incidents are captured. Cyber attacks related to intrusion into network or information systems may not be necessarily captured by many classification criteria. They, however, are important since any intrusion in the network and informaiton systems may harm the financial entity. Accordingly, the classification criteria of 'critical services affected' and 'data losses' should be specified in such a way to capture these types of major incidents, in particular malicious unauthorised access, which, even if the impacts are not immediately known, may lead to serious consequences, in particular data breaches and data leakages.

(6) 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.

(7) 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 entity within a single jurisdiction will be captured by the other criteria.

(8) Given that the classification criteria are interdependent and linked to each other, the approach for identifying major incidents in accordance with Article 19(1) of Regulation (EU) 2022/2554 should be based on combination of criteria where some criteria that are closely related to the definitions of ICT-related incident and major ICT-related incident set out in Article 3(8) and (10) of Regulation (EU) 2022/2554 should have more prominence in the classification of major incidents than others.

(9) 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

[2] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC ; (OJ L 337, 23.12.2015, p. 35).

enable capturing major incidents, by focusing, inter alia, on the impact on critical data, the specific absolute and relative thresholds of clients, financial counterparts or transactions that indicate a material impact on the financial entity, and significance of the impact in other Member States.

(10) Incidents that affect ICT services or network and information systems that support critical or important functions, or financial services requiring authorisation or malicious unauthorised access to network and information systems that support critical or important functions, should be considered as incidents affecting critical services of the financial entities. Malicious, unauthorised access to network and information systems that support critical or important functions of financial entities are considered to pose serious risks to the financial entity and as they may affect other financial entities, they should always be considered as major incidents which should be reported.

(11) Recurring incidents that are linked through a similar apparent root cause, which are individually not major incidents, can indicate significant deficiencies and weaknesses in the financial entity's incident and risk management procedures, Therefore recurring incidents should be considered as major collectively where they occur repeatedly over a defined period of time.

(12) Considering that cyber threats can have a negative impact on the financial entity and sector, the significant cyber threats which financial entities may submit should indicante the probability of materialisation and the criticality of the potential impact. Accordingly, the classification of a cyber threat as significant should be dependent on the likelihood that classification criteria and their thresholds would be met if the threat had materialised, and depending on the type of cyber threat and the information available of the financial entity. This approach should ensure clear and consistent assessment of the significance of cyber threats.

(13) Considering that competent authorities in other Member States should be made aware of incidents that impact financial entities and customers in their jurisdiction, the assessment of the impact in another jurisdiction in accordance with 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.

(14) The reporting and notification processes referred to in Articles 19(6) and 19(7) of Regulation (EU) 2022/2554 should allow the respective recipients to assess the impact of the incidents. Therefore, the transmitted information should cover all details contained in the incident reports submitted by financial entitiy to the competent authority.

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

(16) 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 ESAs

Stakeholder Groups 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[3],

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 are or were unable to make use of the service provided by the financial entity during the incident or that were adversely impacted by the incident. That number shall also include third parties explicitly covered by the contractual agreement between the financial entity and the client as beneficiaries of the affected service.
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 financial counterparts, the financial entity shall take into account the extent to which the impact on a client 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 Union.
5. Where the actual number of clients, financial counterparts or number or amount of transactions impacted cannot be determined, the financial entity shall estimate those numbers based on available data from comparable reference periods.

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

Article 2

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

1. For the purposes of determining the reputational impact of the incident, financial entities shall consider that a reputational impact has occurred where at least one of the following is met:
   a) the incident has been reflected in the media;
   b) the financial entity has received repetitive complaints from different clients or financial counterparts on client-facing services or critical business relationships;
   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 a material impact on its business as a result of the incident.
2. When assessing the reputational impact of the incident based on paragraph 1, financial entities shall take into account the level of visibility that the incident has gained or is very likely to gain in relation to each criterion listed in paragraph 1.

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 moment it was detected. In the cases where financial entities are aware that the incident has occurred prior to its detection, they shall measure the duration from the moment the incident 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 or are unable to verify records in logs or other data sources, 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, financial counterparts and/or other internal or external users to the moment when regular activities or 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 or operations have been restored, the downtime shall be measured from the start of the incident to the moment when that delayed service is fully provided. Where financial entities are unable to determine the moment when the service downtime has started, they shall measure the service downtime from the moment it was detected.

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 whether the incident has or had an impact in the territories of other Member States, in particular the significance of the impact in relation to:

a) the clients and financial counterparts affected;
b) branches of the financial entity or other financial entities within the group carrying out activities; or
c) financial market infrastructures or third-party providers, which potentially may affect financial entities to which they provide services, to the extent this information is available to the financial entity.

Article 5

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

1. To determine the data losses 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 temporarily or permanently 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 of the source of data.
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 an unauthorised party or system.

Article 6

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

For the purpose of determining whether the incident affects critical services, including the financial entity's transactions and operations, financial entities shall assess whether the incident:

a) affects or has affected ICT services or network and information systems that support critical or important functions of the financial entity;
b) affects or has affected financial services that require authorisation, registration or that are supervised by competent authorities; or
c) represents a successful, malicious and unauthorised access to the network and information systems 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 costs and losses, which they have incurred as a result of the incident, without accounting for financial recoveries:
   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. Costs and losses in accordance with paragraph 1 shall not include costs that are necessary to run the business as usual, in particular:
   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. Financial entities shall calculate the costs and losses based on data available at the time of classification. Where the amounts of costs and losses cannot be determined, financial entities shall estimate those amounts.

Section II

Major incidents and their materiality thresholds

Article 8

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

An incident shall be considered a major incident for the purposes of Article 19 of Regulation (EU) 2022/2554 where it has had any impact on critical services as referred to in Article 6 and where one of the following is met:

a) the materiality threshold of Article 13(b) has been met; or
b) two or more materiality thresholds specified in this Section have been met.

Article 9

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

1. The materiality threshold for the criterion 'clients, financial counterparts and transactions' 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; or
   b) the number of affected clients is higher than 100 000 clients using the affected service; or
   c) the number of affected financial counterparts is higher than 30% of all financial counterparts carrying out activities related to the provision of the affected service; or
   d) the number of affected transactions is higher than 10% of the daily average number of transactions carried out by the financial entity related to the affected service; or
   e) the amount of affected transactions is higher than 10% of the daily average value of transactions carried out by the financial entity related to the affected service; or
   f) any identified impact on clients or financial counterpart which have been identified as relevant as an outcome of the assessment made by financial entity under 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 impact set out in Article 2 a) to d) shall be considered as meeting the threshold of the reputational impact criterion.

Article 11

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

The materiality threshold for the duration and service downtime criterion shall be 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 that support critical or important functions.

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 geographical spread criterion.

Article 13

Materiality thresholds for the classification criterion 'Data losses'

The materiality threshold for the data losses criterion shall be met where:

a) any impact as referred to in Article 5 on the availability, authenticity, integrity or confidentiality of data has or will have an adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements; or
b) any successful, malicious and unauthorised access occurs to network and information systems not covered by item a), which may result to data losses.

Article 14

Materiality threshold for the classification criterion 'Economic impact'

1. The materiality threshold of the economic impact criterion in accordance with Article 7 shall be met where the costs and losses incurred by the financial entity 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 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 15

Recurring incidents

1. Recurring incidents that individually do not constitute a major incident shall be considered as one major incident where the incidents meet all of the following conditions:
   a) the incidents have occurred at least twice within 6 months;
   b) the incidents have the same apparent root cause as set out in the Annex III to Commission Implementing Regulation [insert number with publication in OJ of ITS on incident reporting][4];
   c) the incidents collectively categorise as a major incident in accordance with Article 8.
2. Financial entities shall assess the existence of recurring incidents on a monthly basis.
3. This Article shall not apply to microenterprises and financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554.

Section III

Significant cyber threats

Article 16

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 all of the following conditions are met:
   a) the cyber threat, if materialised, could affect or could have affected critical or important functions of the financial entity, or could affect other financial entities, third party providers, clients or financial counterparts, based on information available to the financial entity;

[4] [insert full title and OJ reference }

b) the cyber threat has a high probability of materialisation at the financial entity or other financial entities as set out in paragraph 2; and
c) the cyber threat could meet any of the criteria set out in Article 6 or any of the materiality thresholds set out in Articles 9 and 12, if the threat materialised. Where, depending on the type of cyber threat and available information, the financial entity concludes that the materiality thresholds set out in Articles 10, 11, 13 and 14 could be met, those thresholds may also be considered.

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 referred to in paragraph 1(a), including potential vulnerabilities of the systems of the financial entity that can be exploited;
b) the capabilities and intent of threat actors to the extent known by the financial entity; 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 IV

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

Article 17

Relevance of major incidents to competent authorities in other Member States

The assessment of whether the major incident is relevant for competent authorities in other Member States as referred to in 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 or has had a significant impact in another Member State in relation to 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 a third-party provider which potentially may affect financial entities to which they provide services, to the extent this information is available to the financial entity.

Article 18

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

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

Article 19
Entry into force

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]

5. Accompanying documents

4.1. Draft cost-benefit analysis / impact assessment

As per Article 10(1) of Regulation (EU) No 1093/2010 (EBA Regulation), 1094/2010 (EIOPA Regulation) and 1095/2010 (ESMA regulation), any draft RTS 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 FEs 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[5] entered into force 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 services (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.[6] 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 2025, 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 cyber threats 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

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

[6] 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

chosen 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-related 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 overreporting, 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 overreporting (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-related incidents and will prevent overreporting. 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 weighted 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.

- Option D: One primary criterion and single list of equally weighted secondary criteria or any successful malicious unauthorised access to network and information systems.

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 one 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.

Following the public consultation, a fourth option - Option D – was proposed, which is a combination of Option A and C. In this approach, to classify an incident as major the ‘Critical services affected’ criterion needs to be met as a pre-condition. In addition, any successful malicious unauthorised access to network and information systems needs to have been identified or at least two other classification criteria to be met. All these other criteria are of equally weighting. This approach has the advantage that on the one hand it focuses on one single criterion that is universal to all types of financial entities and that ensures that only incidents affecting critical services are classified as major. One of the thresholds of 'Data losses‘ is included as a separate trigger in order to capture malicious actions that would not be captured by other criteria, such as data leakages and data breaches. At the same time, the classification based on two other criteria, relies on a combination of interlinked criteria that will be triggered depending on the specific business model and sector of the FE, thus embedding proportionality and reflecting sector specificities.

Therefore, Option D has been chosen.

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 3 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 an absolute threshold 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 or 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 these RTS 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 D: 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 an 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 D: Both relative and absolute threshold (non- cumulative)

Similarly to financial counterparts, given the nature of transactions, that can be of various sizes and that FEs may rely on divergent number of transactions, 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 transactions that would be an appropriate threshold for all types of FEs. Therefore, applying the same rationale as for number of financial counterparts, Option B, which entails the application of relative thresholds only 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 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.[7] 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.

[7] 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.

The three scenarios are described in more detail 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 are 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 1. 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.

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[8], 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 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. Nevertheless, this scenario was assessed as a good compromise that allows to capture prominent major incidents across the financial sector.

Finally, scenario 4 proposes the use of a mandatory criterion, as an incident would need to be reported if 'Critical services affected', i.e. that the incident had any impact on critical services, is met. In addition, the materiality threshold of 'data losses' criterion related to any successful malicious unauthorised access to network and information systems needs to be met or, alternatively, at least two other classification criteria. These other criteria are all equally weighted. Using the available sample, the results of this scenario are similar to scenario 3. However, in addition to scenario 3, it ensures to capture the specific incidents that related to data breaches and data leakages associated with critical services, irrespective of other criteria not being met, thus capturing important cyber incidents. This proposed scenario seems most balanced and has, therefore, been proposed in the draft RTS.

Table 1. Share of payment incidents captured by each scenario

	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Share of payment incidents captured in the sample, of which:	93%	67%	87%	87%
Share of prominent major payment incidents captured	100%	100%	100%	100%
Share of less prominent major incidents captured	80%	0%	60%	60%

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 2 below.

Table 2: Cost and benefits of the draft RTS

Stakeholder groups affected	Costs	Benefits

[8] 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.

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.

4.2. Views of the ESAs Stakeholders Groups

General observations

The stakeholder groups ("SGs") recognise the importance of ensuring a high degree of ICT systems security and resilience. While all sectors of the financial services industry are potentially exposed to ICT security risks, the profile of such risks may vary considerably between different sub-sectors within the industry. In 2022, 119 incidents were reported by the Banking sector to ENISA under the NISD framework (Art. 15 & 16 NIS 1), an increase of 37% over the previous year. The Banking sector accounted for ca. 13% of all incidents reported to ENISA's CIRAS reporting platform for that period. Operators of financial market infrastructures (FMIs) reported another 8 incidents in the same period (+60%). In Banking, system failures were the most prevalent cause (66% of all incidents), followed by malicious activity (24%), and human error (9%). Of the much smaller sample of FMI incidents, however, as much as 63% were attributed to malicious activity, with only 37% caused by system failures.

It is important that the ESAs take the provisions in the NISD into account when criteria for incident reporting according to DORA are developed. DORA takes into consideration that double reporting stemming from potential overlaps between the reporting requirements according to NISD and reporting requirements according to DORA should be avoided. It is important that financial supervisory authorities make sure that this objective is maintained in the practical application of these regulatory frameworks at national level in each EU member state.

Detailed comments

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.

The SGs agree with the proposed overall approach for major incident classification and note, in particular, that the distinction between primary and secondary criteria, which is not specifically made in the Level 1 text, is a useful and pragmatic approach, which makes allowance for the diversity of, and sectoral specifics within the financial sector, and allows for the principle of proportionality to be applied the implementation of DORA in a structured and consistent manner.

The SGs also support the ESAs' choice to rely, as much as possible, on binary criteria. Given the risk and potential cost of under/overreporting, and the need to streamline processes and shorten response times, criteria should be straightforward to apply and unambiguous.

The SGs note that certain definitions in Level 1 legislation that are relevant for determining the scope of reporting requirements could possibly be referenced explicitly in the RTS for clarity. It should be reiterated, in particular, that the definitions of *"ICT-related incidents"* and *"cyber threats"* in Art. 3(8) and Art. 3(12) DORA, respectively, do not reference any element of causation so that reporting obligations under Art. 18(1) and voluntary reports under Art. (18(2) DORA are not limited

to incidents or threats that are attributable to malicious activity. Although malicious activity may attract more attention in the public and media stakeholders are mindful that the timely and specific reporting of accidental ICT incidents is equally critical.

ESAs' response

The ESAs welcome the support for the overall approach for classification of major incidents under DORA, the high-level approach for embedding proportionality and the choice of materiality thresholds.

With regard to the type of major incidents within the scope of the DORA and the RTS, the ESAs understand that incidents that go beyond malicious activity fall within the scope of the reporting framework. This includes operational incidents, too. This is evidenced by the link between the definitions in DORA of 'ICT-related incident' (Art. 3.8), 'operational or security payment-related incident' (Art. 3.9), 'major ICT-related incident' (Art. 3.10), 'network and information system' (Art. 3.2) and the NIS2 definition of 'security of network and information systems', which covers '*the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems*.'

With regard to criteria and thresholds of cyber threats as set out in Article 16 of the draft RTS, the ESAs are of the view that these are aligned with the definition of cyber threats in Article 2, point (8), of Regulation (EU) 2019/881, which specifies that cyber threats cover *'any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons'.*

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.

The SGs acknowledge the difficulty to specify absolute and/or relative thresholds given the diversity of, and sectoral specifics within the financial sector.

In the interest of legal certainty, the SGs suggest that the ESAs should consider reiterating in the RTS that any entity within the scope of DORA should also be considered, a priori, as a financial counterpart for the purposes of calculating the threshold values of *"financial counterparts affected"*.

The SGs observe that the proposed definition of *"relevance"* in Art. 1(3) of the RTS introduces a degree of ambiguity and discretionary latitude that is, arguably, not covered by the Level 1 text. It is not obvious that the term *"number and/or relevance"* in item a. of Art. 18(1) DORA specifies two

different criteria that would need to be defined separately in the RTS. The *"relevance"* aspect could instead be considered adequately captured by the relative materiality threshold (10%), while the *"number"* aspect of the criterion is captured by the absolute materiality threshold (50,000). In the interest of making primary criteria as unambiguous as possible, and given that the secondary criteria provide for some discretionary latitude already, it would appear advisable to concentrate on empirical, numerical thresholds for the primary criteria. If financial entities were to apply largely discretionary weightings to quantify the *"relevance"* of clients or counterparts quantitative materiality thresholds, both absolute and relative, could be rendered effectively meaningless. An incident that affects 10% or more of the client base or financial counterparts should be considered relevant in any event, regardless of the specifics of the individual parties affected. Moreover, a degree of discretion for financial institutions, which would accommodate sectoral differences and proportionality requirements, is already provided by the absence of an absolute threshold for *"financial counterparts affected"*. On this basis, Art. 1(3) of the RTS should be considered redundant.

The draft does not specify either if the concept “clients affected” refers to the clients registered in the specific channel/service affected by the incident (web application, mobile application,…) or to the clients that use the channel/service at the moment the incident occurs. Furthermore, it is necessary to stress that the threshold applies at entity level (rather than group level) which is consistent with the rest of DORA.

Article 9 of the RTS establishes that the materiality threshold of this criterion is met if the incident has “any identified impact on relevant clients or financial counterparts”. We consider that the article should refer to a significant impact in relevant clients (not to any impact). The proposed text is the following: “Any significant impact on relevant clients or financial counterparts”.

Regarding the *"amount or number of transactions affected"*, it does not appear immediately obvious from the wording of Art. 18(1) DORA that the co-legislators intended to restrict the scope of reportable incidents to *"transactions that have a monetary value"*. In its current form, the proposed Art. 1(4) of the RTS would exclude transactions that do not contain a monetary amount but which may, nevertheless, involve the exposure or loss of other valuable data, such as confidential customer information. In Art. 18(1) DORA, the co-legislators provide a choice of indicators between the *"amount or number of transactions affected"* (arg. *"or"*), which is preceded by the qualifier *"as applicable"*. While the indicator *"amount of transactions"* implies that transactions must contain a monetary amount the same does not apply for *"number of transactions"*. Some stakeholders are of the view, therefore, that the qualifier *"containing a monetary amount"* should be applied in the calculation of the criterion only, whereas the criterion *"number of transactions"* should be calculated without that restriction and include transactions that do not contain a monetary amount. These stakeholders note that ICT incidents that affect a material number of transactions tend to be indicative of potential operational risks and should therefore be within scope unless there is clear evidence to the contrary.

Also, the duration of the impact must be taken into account (not just an additional factor but as an overarching one) for the relevance of the impact on clients. That is, events which affect many clients but have a very short duration (seconds, minutes), should not be reported regardless of the number of clients potentially affected, even when the incident could impact many clients, its short duration makes the real effect on them quite limited.

ESAs' response

On the specification of 'financial counterparts' this is a term introduced in level-1, which is not specified there. Accordingly, the ESAs do not have a mandate to define the term in the draft RTS since it may amend the scope of DORA. The ESAs have specified in Article 1(2) of the draft RTS aspects related to the 'financial counterparts' to be taken into account in the classification of the incident.

Nevertheless, the ESAs understand that in the light of Article 17(3)(d) of DORA, 'financial counterparts' are other types of financial entities that acts as counterparts in the provision of services. The term 'financial counterpart' is different than the term 'central counterparties', which is a specific type of financial entities under DORA.

The ESAs agree that the relevance of the incident on clients/financial counterparts will be captured by the relative and absolute materiality thresholds set out in the RTS. However, there may be cases where smaller number of affected clients or financial counterparts may have impact on the business of the FE. The ESAs have therefore proposed it as a separate trigger of the criterion 'clients, financial counterparts and transactions affected', which is complementary to the number of clients or financial counterparts affected.

However, since the FEs differ in size and nature of their activities, and taking into account that FEs are best placed to assess whether clients and financial counterparts should be seen as relevant for their operations, the ESAs have arrived at the view that it is desirable to provide discretion to FEs on when this part of the criterion will be met, even if this results in the criterion not being triggered often.

The ESAs agree with the point raised and its rationale and have introduced changes to the draft RTS clarifying that the clients affected refers to all clients affected by the incident that were unable to make use of the service provided by the financial entity during the incident or that were adversely impacted by the incident. The ESAs have also clarified that the affected also third parties explicitly covered by the contractual agreement between the FE and the client as beneficiaries of the affected service.

With regard to the clarification on whether the thresholds apply at entity level or at group level, the ESAs do not see merit in reflecting this aspect in the draft RTS since DORA clearly provides that the incident classification and reporting obligations refer to individual entities. Accordingly, all requirements of the draft RTS shall be understood and applied in the same way.

The ESAs are of the view that where a client or a financial counterpart is deemed relevant for the business objectives of the FE, it by default indicates that impact on them will be significant for the FE. Accordingly, taking also into account that FEs will have discretion to decide whether or not clients or financial counterparts are relevant for meeting their business objectives, the ESAs have not introduced any changes to the draft RTS.

The ESAs are of the view that broad interpretation of the term 'transactions' will overlap with other classification criteria (e.g. critical services affected) and thus lead to overreporting. In addition, the proposed broad interpretation does not seem fully in line with Article 18(1)(a) of DORA. Finally, it should be noted that the approach for classifying major incidents taken in the draft RTS is holistic and relies on a combination of criteria to classify an incident. Therefore, the specific case provided where a number of transactions are affected indicating a potential operational risk, is likely to be captured with a combination of other criteria.

The ESAs view the classification of incidents as major as a holistic approach that is reflected in the classification approach in Article 8 of the draft RTS where more than one criterion needs to be met to classify an incident as major. In particular, the ESAs have identified strong correlation between the criteria 'clients, financial counterparts and transactions affected' and 'duration and service downtime', which was taken into account when deciding on the exact number of criteria that need to be met to classify an incident as major. Moreover, the materiality thresholds have been calibrated to ensure balanced classification approach. Accordingly, the ESAs have not introduced further changes to the draft RTS.

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.

The SGs agree with the classification of "reputational impact" as a secondary criterion and the proposed definition in Art. 2 of the RTS. In respect of the wording of item a. of Art. 2, the SGs observe that the notion that an incident has *"attracted media attention"* may be too vague and more precise wording may be preferable. Specifically, in order the cause reputational damage the incident would have been reported in the media or, at least, have prompted enquiries from the media. The SGs agree that no distinction should be made between different types of media. Social media, in particular, have proven very effective at propagating information and even triggering potential systemic events.

The wording in item b. of Art. 2 of the RTS (*"different clients or financial counterparts")* is exceedingly vague and does not provide sufficient guidance for determining the materiality threshold in accordance with Art. 10. The SGs assumes that the threshold should be set at such a level that complaints from only a few clients would not trigger the criterion. For reputational

damage to become a concern such complaints would have to be received, arguably, from a sizable number of clients and/or several financial counterparts.

In item d. of Art. 2 of the RTS the potential loss of clients or financial counterparts as a result of the incident is qualified with the clause *"with an impact on its business"*. The purpose of this qualifier seems unclear without further explanation since any loss of clients or counterparties should, a priori, have an impact on business. In the absence of further detail this wording could also be omitted.

Article 3(1) of the RTS requires a FE to measure the duration of an incident "*from the moment the incident occurs"*. This may in practice be difficult to specify depending on the circumstances. It may, therefore, be advised to replace the wording with *"from the moment the incident was detected".*

According to Art. 3(2) of the RTS, incident-related service downtime is deemed to end when *"regular activities/operations have been restored to the level of service that was provided prior to the incident."* In the absence of a precise reference point it could be difficult to determine to what level service would have to be restored. Moreover, it is unclear for the purposes of item b. of Art. 11 of the RTS whether it would be sufficient for the cause of the incident to be remediated temporarily, or whether it would have to be resolved permanently. Further clarification of this point may be useful.

Art. 11 of the RTS establishes that the materiality threshold is met if *"the service downtime is longer than 2 hours for ICT services supporting critical functions"*. However, some critical business processes or services are critical from a business continuity perspective only during specific time frames. For these services the impact of a service downtime will be more severe if the incident occurs during business hours than if it occurs during the night or the weekend. Some members of the SGs are of the view, therefore, that the 2-hour materiality threshold of this criterion should apply for such services only if they occur during business hours. Furthermore, they believe that the timespan of 2 hours, from a business continuity perspective, seems short, even if the downtime occurs during business hours.

Article 15 (1) of the RTS set the materiality threshold of the economic impact at 100,000 EUR or above. This threshold appears low in light of regular expenditures for resolving major incidents, especially for large and complex FEs. For the same reason, the ESAs believe that the proposed threshold will likely less affect smaller Fes. This , however, may potentially lead to a higher number of reported incidents for the purposes of the RTS at the level of larger FEs.

In addition, it should be taken into account that it will be really difficult for financial entities to have the details of the economic impact when the incident is detected (which is the moment when the incident has to be notified to the competent authorities). Therefore, it will be difficult to determine whether the materiality threshold of this criterion is met. Determining the economic impact of the incident will be complex even during the incident management process.

ESAs response

The ESAs agree with the rationale behind the proposal related to media attention, in particular that media attention should not only be attracted but that the actual incident needs to be reflected in the media (e.g. reported, posted, etc., depending on the type of media). The ESAs have amended Article 2(a) of the draft RTS accordingly.

However, the ESAs did not find merit in providing more details since the reference to the 'incident being reflected in the media' is proportionate and should encompass cases applicable to smaller FEs too (e.g. report in a local media).

The ESAs confirm that the part of the criterion related to complaints intends capturing large number of complaints related to the incident and not just a few isolated complaints. Accordingly, the ESAs have slightly amended Article 2(b) to address this concern by specifying that the FE shall have received repetitive complaints from different clients or financial counterparts on client-facing services or critical business relationships.

The ESAs would like to clarify that the intention behind Article 2(d) of the draft RTS is to indicate whether the loss of clients or financial counterparts may have significant material impact on the business of the FE, thus leading to potential reputational impact. The ESAs agree with the advice provided and have further clarified in Article 2(d) that the impact on the business of the FE should be material.

The ESAs are of the view that incidents may occur prior to their detection, therefore it is crucial to have the moment the incident has occurred as a starting point. However, the ESAs agree that there may be cases where the occurrence of the incident may not be known to the FE, in that case, the time of detection of the incident will be more appropriate, or an estimate on the occurrence.

The ESAs would like to clarify that the level of service that was provided prior to the incident refers to a period where the service is provided in normal business as usual circumstances.

When it comes to the point on temporary or permanent resolution of the problem, the ESAs have not introduced changes to the draft text since they deem it sufficiently clear that the reference to 'restored to the level of service that was provided prior to the incident has occurred' is sufficiently clear indication on the policy intention.

The ESAs would like to reiterate that the ESAs have chosen a holistic approach for the classification of major incidents under DORA, which means that a single criterion cannot trigger a major incident report in isolation. Therefore, in the example provided if the incident is not material since it occurs outside business hours and does not have any impact evidenced by the other classification criteria, it should not need to be reported. Moreover, the ESAs have slightly amended Article 11(b) by clarifying the service downtime should be looked at client and/or financial counterparts facing services, which should address to some extend the concern expressed.

However, the ESAs would like to highlight that there are many time critical financial services where 2 hour service downtime outside business hours will be very impactful to FEs, their counterparts or clients. Accordingly, the ESAs have not introduced any changes to the draft RTS.

The ESAs would like to reiterate that the ESAs have chosen a holistic approach for the classification of major incidents under DORA, which means that a single criterion cannot trigger a major incident report in isolation. Moreover, the criterion is likely to be triggered by larger FEs, thus being proportionately set.

It should also be noted that the Guidelines on major incident reporting under PSD2 contain the same classification criterion with a relatively similar threshold. Based on the incidents reported under these Guidelines, the criterion has hardly ever been met.

Finally, it should be noted that the threshold of 100 000 EUR is aligned with the operational risk framework under the Capital Requirements Directive and Regulation. The ESAs are of the view that ensuring alignment and harmonization between legal frameworks covering similar provisions is important. Accordingly, the ESAs did not find strong justification to increase the level of the threshold under the draft RTS.

The ESAs acknowledge that assessing the economic impact accurately might not be feasible in the initial phase of an incident. Therefore, the RTS specifies that FEs can resort to estimates. Also, the economic impact does not need to be reported, but only measured against the threshold. Furthermore, the listed types of cost need to be taken into account for the overall assessment, which does not mean that for the purpose of the incident classification all types of costs need to be assessed and listed individually. The approach allowing FEs to resort to estimates should also not pose burden of assessing the economic impact. Accordingly, the ESAs have not introduced any changes to the draft RTS.

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.

The SGs agree with the proposed definition of "data losses" in Art. 5 and the materiality thresholds in Art. 13. It is particularly important, in the given context, to concentrate on the perspective of the financial entity and the potential impact of data losses its core business activities. Data that may be considered merely *"temporarily unavailable"* from the perspective of the ICT system operator may effectively become *"inaccessible or unusable"* for the financial entity, especially when it relies on such data for critical, time-sensitive transactions.

The concept "authenticity" should be clarified in Article 5 of the RTS, since international security standards usually refer only to confidentiality, integrity and availability.

The SGs observe, in addition, that the definition of data losses *"in relation to confidentiality"* according to Art. 5(4) of the RTS does not make specific reference to potential losses of customers' personal data. Personal data of individual customers enjoy particular protection under Regulation 2016/679 (GDPR) – ICT systems that handle such data should, therefore, meet the highest standards of security and operational resilience, and receive particular supervisory attention. Moreover, lost or compromised customer data have the potential to cause significant consequential damage, e.g. through fraud and as a vector for cyberattacks. The notion of confidentiality in Art. 5(4) should be expanded to include, as a sub-criterion, whether the incident has resulted in the unauthorised disclosure of individual customers' personal data that fall under the protection of the GDPR.

Overall, the interplay between the GDPR (Articles 33 and 34) and "data losses" as per DORA needs to be clarified.

Additionally, consideration 42 of the RTS "Background" Section establishes that "any loss of critical data" will determine that the materiality threshold of this criterion is met. Even though Article 13 of the RTS refers to data losses with "significant impact", this article of the "Background" section should be clarified, to ensure that not every data loss will determine that the threshold of this criterion is met.

ESAs' response

The ESAs welcome the support on the specification of the criterion data losses and agree with the additionally proposed change to capture temporarily unavailable data in the data losses criterion. Accordingly, the ESAs have revised Article 5(1) of the draft RTS and clarified that to determine a data loss in relation to availability of data, FEs 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 temporarily or permanently.

The ESAs have already specified the reference to data loss related to authenticity. The response provided by the SG does not indicate what specific clarification has been sought.

Nevertheless, taking into account of other responses from the public consultation, the ESAs have decided to clarify that FEs shall take into account whether the incident has compromised the trustworthiness of the source of data .

The ESAs would like to clarify that the reference to losses that the incident entails in relation to the confidentiality of data cover all types of data, including personal data. In that regard, the ESAs do not find merit in referring explicitly to certain types of data.

The clarification sought in relation to the interplay between GDPR and DORA in relation to data losses is related to the interpretation of level-1 texts and goes beyond the mandate conferred by DORA on the ESAs under Article 18(3) of DORA.

The ESAs would like to clarify that the reference to 'critical data' intended reflecting the significance of the incident on the FE. Accordingly, since the impact of critical data by default is deemed significant, the ESAs have deleted the reference to significant from Article 13 of the draft RTS. Moreover, since Article 13 of the draft RTS introduces directly the cases when the threshold is triggered, namely the adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements, the ESAs have deleted the reference to 'critical', too.

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.

For the purposes of determining criticality, the SGs note that the terminology in item e. of Art. 18(1) DORA departs slightly from the terms used elsewhere in DORA, especially the term *"critical or important function"*, which is defined in item 22 of Art. 3 DORA. The SGs agree with the proposed approach of reinstating this reference in Art. 6 of the RTS. While rec. 70 DORA states explicitly that any functions deemed to be critical according to item 35 of Art. 2(1) BRRD should be included as such under DORA, further clarification would be welcome, especially, on the definition of "important functions". The BRRD requires credit institutions to specify *"critical functions"* (item 35 of Art. 2(1) BRRD) and *"core business lines"* (item 36 of Art. 2(1) BRRD) for the purposes of recovery and resolution planning. This assessment is subsequently reviewed, and monitored continuously, by supervisory and resolution authorities. A similar approach is taken in other jurisdictions, e.g. in the UK for the identification and supervision of *"important business services"* (PRA Policy Statement PS6/21 of March 2021 on operational resilience). To operationalise the term, financial entities within the scope of DORA could be required to provide an assessment of their *"critical or important functions"*, e.g. when documenting their ICT risk management framework in accordance with Art. 6(5) DORA. Credit institutions would be able to draw on the relevant documentation prepared in compliance with the BRRD requirements and relevant EBA and SRB guidance.

Article 6 of the RTS also includes in this criterion "incidents that affect services or activities that require authorisation". The concept "services that require authorisation" should be clarified.

"Authorisation" should not constitute a criterion to define criticality. Business Impact Analysis would be considered more appropriate, rather.

ESAs' response

The ESAs welcome the support expressed in the approach for specifying the criterion 'critical services affected'. On the proposal to clarify further the term 'critical or important functions', the ESAs would like to clarify that this is a term defined in Article 3(22) of DORA. Accordingly, the ESAs cannot amend a legal term defined in level-1 through a level-2 legal instrument.

The ESAs are of the view that the reference to services requiring authorisation is sufficiently clear and covers regulated services. Nevertheless, since there are services and activities that may require a registration with or that are supervised by the CAs referred to in Article 46 of Regulation (EU) 2022/2554, the ESAs have amended Article 6 of the draft RTS to reflect that.

Moreover, the services that require authorisation/registration/supervision are deemed critical by the ESAs and already covered in the definition of critical or important functions, hence the ESAs have decided to retain the reference in the specification of the criterion in order to provide greater clarity. The classification of the other services that support critical or important functions fall within the scope of the business impact analysis carried out by the FE.

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).

Capturing recurring incidents having the same root cause and with similar nature and impact may in practice be difficult to identify. *"Similarity of nature"* is a broad concept and may lead to significant over or even underreporting of major incidents. Article 16(2) of the RTS may be amended to: *"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."*

"Recurring incident" does not feature in the DORA Level 1 text and it would therefore be helpful to get clarification as to what is meant by "recurring".

The inclusion of this criterion in the RTS will determine that two non-significant incidents that affect critical services but do not affect a large number of clients and do not have a relevant economic impact as isolated incidents would have to be classified as major incidents when considered in an aggregated manner. This will result in a considerable increase in the number of incidents that have to be reported to the competent authorities by the financial entities. We consider that this criterion should not be included in the RTS unless reporting is required when the aggregated impact of individual events is significant.

ESAs' response

The ESAs acknowledge the concern raised about the potential overreporting due to the broad nature of the term 'similar nature' and have amended the requirement of Article 15 of the draft RTS (Article 16 from the consulted draft RTS) by referring to the same apparent root cause only, which will be further specified in the draft RTS on the content of the incident reports (Article 20a of DORA).

Article 3(8) and (9) of DORA define ICT-related incidents and operational or security payment-related incidents. Both definitions specify that these are 'single events or a series of linked events unplanned by the financial entity…' Accordingly, recurring incidents fall within the scope of these definitions since they are series of events that are unplanned by the FE. Article 15 of the draft RTS further specifies what recurring incidents are.

The ESAs agree with the SG that the aggregated impact of the individual events should be significant. This is the reason for the inclusion in the draft RTS of Article 15(1)(c), which specifies that the incidents shall collectively meet the materiality thresholds and categorise as a major incident in accordance with Article 8 of the draft RTS.

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.

The SGs agree with the general approach for classification of significant cyber threats. For the voluntary reporting framework under Art. 18(2) DORA to be successful, close cooperation among financial entities and between financial entities and third-party ICT service providers will be essential.

The SGs note, however, that it could be challenging for entities to assess the likelihood that a cyber threat could also affect another financial institution, third-party provider, client or financial counterpart. In addition, the detection of cyber threats could also expose vulnerabilities in the ICT systems of an entity. In the interest of encouraging all market participants to share information on cyber threats in a timely and pro-active manner, reporting should therefore focus on the specifics of the detected threat, its probability of materialisation, and potential for contagion. Sensitive information, especially related to the systems of the reporting entity, and the circumstances of the detection, should be kept to the necessary minimum.

ESAs' response

The ESAs agree that the information about significant cyber threats should focus on the specificity of the detected threat, its probability of materialisation and the potential contagion. The potential contagion is the reason why the information about the potential impact on another FE, third party provider, client or financial counterpart has been included in the specification of a significant cyber threat in Article 16 of the draft RTS. In addition, a threat assessment normally should take into account vulnerabilities at the financial entity's providers, clients and financial counterparts.

Nevertheless, the ESAs acknowledge that the information about the impact on other FEs and third party providers may not be available to the FE. Accordingly, the ESAs have amended Article 16(1)(a) of the draft RTS to reflect that.

With regard to the concern of sharing sensitive information referred to by the SG, it should be noted that the potential vulnerabilities of the systems of the FE that can be exploited are aimed for the FE to take into account in the classification of the significant cyber threat and are not required to be shared. The information to be reported on significant cyber threats falls within the scope of the RTS mandates under Article 20a of DORA.

4.3. Feedback on the public consultation

The ESAs publicly consulted on the draft proposal contained in this paper.

The consultation period lasted for three months and ended on 11 September 2023. 105 responses were received.

This section presents a summary of the key points and other comments arising from the consultation, the analysis and discussion triggered by these comments and the actions taken to address them if deemed necessary.

In many cases several industry bodies made similar comments or the same body repeated its comments in the response to different questions. In such cases, the comments, and ESAs' analysis are included in the section of this paper where ESAs consider them most appropriate.

Changes to the draft RTS have been incorporated as a result of the responses received during the public consultation.

Summary of responses to the consultation and the ESAs' analysis

Below is a summary of the responses to the consultation and the ESAs' analysis spread out by questions posed for the public consultation.

General comments

Topic	Summary of the comments received	ESAs' analysis
Consistency of terminology between DORA and the RTS	Several respondents highlighted that the RTS should use consistent terminology with DORA to avoid legal uncertainty. They proposed to use 'critical or important function' instead of the various terms currently proposed, such as 'the service', 'critical services affected', 'critical functions', 'non-critical services', and 'critical or important functions'.	The terms used throughout the RTS are in line with the text of DORA, such as the reference to criticality of services affected (Art. 18(1)(e) DORA) and critical or important functions (Art. 3(22) DORA). The use of various terms throughout the RTS relates to specific aspects of DORA. Nevertheless, the ESAs have tried limiting the number of different terms to the greatest extent possible.
Interplay between DORA and NIS2	Two respondents suggested providing clarity on the links between NIS2 and DORA where different terms have been used, namely 'significant incident' under NIS2 and 'major ICT-related incident' and 'significant cyber threat' under DORA.	The proposals goes beyond the scope of the mandate under Article 18(3) of DORA. Therefore, no change has been introduced. Nevertheless, it should be noted that Recital 16 of DORA clarifies that DORA increases the level of harmonisation of the various digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in comparison to those laid down in the current Union financial services law, and that this higher level constitutes an increased harmonisation also in comparison with the requirements laid down in NIS2 and that consequently, DORA constitutes lex specialis with regard to NIS2.
Reporting timelines	Several respondents commented on aspects related to the timelines of reporting of major incidents, the content of the reports for major incidents or the process of reporting major incidents.	The reporting timelines and the content of the reports for major incidents do not fall within the legal mandate set out in Article 18(3) of DORA. They fall within the mandate under Article 20a of DORA, which has been published for public consultation in December 2023. The process of reporting major incidents is set out in Article 19 of DORA.
Scope of the incidents under the RTS	A few respondents queried on the scope of the incidents to be classified in accordance with the RTS, in particular whether these cover also operational incidents. Two respondents also queried whether the incident classification and reporting should be done at individual FE level or, where applicable, at group level. Two respondents sought clarification on whether the RTS will apply to subsidiaries outside the EU.	The ESAs would like to highlight that, taking into account the definition of ICT-related incident (Article 3(8) of DORA), major ICT-related incident (Article 3(10) of DORA) and network and information system (Article 3(2) of DORA, as well as security of network and information systems (Article 6, point 2, of Directive (EU) 2022/2555), operational incidents fall within the scope of ICT-related incidents under DORA. In addition, it should be noted that Articles 18 and 19 of DORA also cover the reporting of operational or security payment-related incidents. The ESAs clarify that DORA introduces requirements for classification and reporting of ICT-related incidents to the individual FE. Therefore, the RTS shall be applied for each entity

Topic	Summary of the comments received	ESAs' analysis
		separately. Since this is stemming already from DORA itself, no changes have been introduced in the draft RTS. DORA and the RTS introduce legal requirements with EEA relevance, which means that any reference to the EU should be understood as EEA, depending on the respective EFTA adaptation of the text.

Approach for classification of major incidents under DORA

Topic	Summary of the comments received	ESAs' analysis
Approach for classification of major incidents	Many respondents highlighted concerns that the consulted classification approach may be challenging and too rigid, especially when the FE needs to assess the incident impact across different jurisdictions. Some respondents indicate that specifying the classification criteria and introducing materiality thresholds will introduce complexity for FEs at the time when FEs are handling the incident. A few were of the view that FEs are asked to assess more data. Several respondents were of the view that the RTS should focus on the impact of the incident more directly. Small groups of or individual respondents proposed ways on how to simplify the incident classification, namely by: • reporting all incidents with duration over 5 minutes or relying on FEs' internal subjective assessment; • relying on any three criteria for major incident classification; • take into account only four criteria - operational losses, regulatory impact, legal impact and	The ESAs took into account the feedback received from the respondents to the public consultation on this topic and also holistically across all different questions from the public consultation and have amended the approach for classification of major incidents under DORA so that it is clearer, simpler and straight forward to perform at a time when FEs will be handling an incident. In particular, the ESAs have decided to treat the classification criterion 'critical services affected' as a mandatory condition for classifying an incident as major and to classify major incidents where either one of the following conditions is met (i) any malicious unauthorised access to network and information systems as part of the 'Data losses' criterion is identified or (ii) the materiality thresholds of any other two criteria should be the additional triggers for major incident classification. Accordingly, all other criteria (except 'critical services affected') are treated equally, without distinguish between primary and secondary criteria. This amendment is also aligned with other general feedback on the classification approach received that proposed for the classification approach to be more closely aligned with the definition of major ICT-related (or operational or security payment-related) incident, which specifies that the incident should have a high adverse impact on the network and information systems that support critical or important functions of the financial entity. In addition, the proposed approach leveraged on various proposals to (i) treat the criterion 'clients, financial counterparts and transactions affected' as a secondary criterion and other proposals for some of the other criteria, in particular 'duration and service downtime' to be considered primary criteria. Finally, the simplification of the classification approach, taking into account some of the specific changes introduced in the classification criteria and thresholds, should not change the expected scope of incidents that are to be classified as major. With regard to some of the specific remarks made by the respondents, the ESAs discarded them because:

Topic	Summary of the comments received	ESAs' analysis
	image/reputation impact, and to classify the incidents in four categories: minor/low, significant/moderate, major/high and critical/very high; • using the classification approach set out in the ECB methodology for reporting significant cyber incidents; • taking a risk-based approach, similar to some other sections and parts of DORA; • focus the classification requirements on qualitative thresholds; or • following the PSD2 incident reporting approach where one primary criterion should be met or three secondary for payment-related incidents.	• The impact of the incidents is captured holistically through the use of various criteria; • Limiting the duration of the incident to 5 minutes as a trigger for reporting major incidents will lead to overreporting; • Fully subjective assessment by FEs for the classification of major incidents goes contrary to the objective of DORA and the RTS of harmonisation of the incident classification and reporting for all FEs; • DORA (Article 18) sets out the classification criteria to be taken into account in the classification of major incidents, which are further specified in these RTS. The RTS cannot change these criteria or disregard any of them, or rely on other methodologies for reporting major incidents that are different to those in DORA. • The classification of an incident is set out in DORA which distinguishes between incidents and major incidents. Introducing different and broader categories of incidents to those set out in DORA is not legally feasible and is not in line with the mandate. • Quantitative thresholds have been used for the criteria where this is directly requested from DORA (e.g. number of clients, number of transactions, duration of the incident, costs and losses from the incident). Therefore, quantitative thresholds need to be used for these criteria in order to be compliant with the legal mandate conferred by DORA. • On following the PSD2 approach, it should be noted that the RTS is very much aligned with the classification of major incidents under PSD2. Nevertheless, they cannot be fully identical since introducing a sector-specific classification approach will go against the objective of DORA of bringing about harmonisation on the incident classification and reporting.
Weighting classification criteria	Various stakeholders proposed changes in the weighting of different criteria arguing that it relates to the criticality of the respective criterion for their sector. For instance a few stakeholders suggested to consider 'clients, financial counterparts and transactions affected' as a secondary criterion, while small groups of respondents suggested considering the 'service downtime', 'economic impact' or 'geographical spread' as primary criteria.	Based on the views of the respondents where different criteria are deemed crucial for particular sectors and taking into account other points raised, such as the need to be closely aligned with the definition of incidents (Art. 3(8) and (9) of DORA) and major incidents (Art. 3(10) and (11) of DORA), the ESAs have arrived at the view that all classification criteria shall be treated equally, with the only exception being the criterion 'Critical services affected', which is a precondition for classifying an incident as major and should always be mandatory.
Overreporting concerns	A few respondents were of the view that the consulted classification approach will lead to overreporting and covering incidents that are non-major, with a few explicitly referring to the use of two primary criteria and others referring to the low	The ESAs and CAs have carried out thorough testing during the development of the consultation paper and during the public consultation and arrived at the view that the number of major incidents expected should not lead to overreporting, taking into account the incident reports that have been tested by the ESAs. In addition, the ESAs clarify that the holistic approach under the draft RTS relies on a combination of criteria (which are often linked to each

Topic	Summary of the comments received	ESAs' analysis
	level of classification thresholds. One respondent highlighted that some classification criteria overlap.	other) to classify an incident as major. Therefore, a single threshold should not lead to overreporting by itself. Nevertheless, the ESAs have amended certain materiality thresholds, in particular those for 'clients, financial counterparts and transactions affected' and 'duration and service downtime', which should address further some of the concerns raised and include further proportionality. In addition, the ESAs have slightly amended the classification approach whereby major incidents are classified by three criteria, namely critical services affected and two additional criteria, or, in the specific case of some cyber-attacks, by critical services affected and the identification of malicious unauthorised access to network and information systems of the FE. This should address further the concerns expressed by stakeholders.
Proportionality and sector-specificity	Several comments were received on proportionality where respondents made proposals: • To introduce proportionality in the classification approach to ensure capturing only significant incidents. • To clarify how proportionality is taken into account in the different classification criteria. • To avoid thresholds with fixed absolute amounts/numbers. • To avoid having relative thresholds. A few respondents were of the view that the classification criteria may not fully follow one-size-fits-all approach. The respondents did not provide many specific proposals on how to reflect sector specificities better, with individual ones only proposing particular criteria to be updated to primary ones or that the criterion 'clients, financial counterparts and transactions affected' should be considered as a secondary criterion.	Proportionality has been embedded holistically in the classification approach taken in the RTS. The classification approach proposed for public consultation and the classification approach set out in this Final report have been designed in such a way to ensure proportionality. The combination of criteria aims at ensuring that only incidents with significant impact on the FE (or the financial system) are being reported. In addition, the levels of the classification thresholds are set in such a way that they are not easily breached. In addition, the RTS uses mainly relative thresholds for the purpose of ensuring proportionality. The only absolute thresholds used (absolute number of clients affected and economic impact) had been set out in such a way so that it is difficult to be met by smaller entities. Following the feedback from the public consultation, the ESAs have also increased the absolute number of clients affected threshold from 50 000 to 100 000, thus ensuring further proportionality. Moreover, the absolute threshold for the amounts of transactions affected has been removed since it was deemed inappropriate for most entities that would use it, in particular those in the investment sector. Said threshold has been substituted with a relative one of 10%. In addition, the ESAs have introduced the following additional specific changes to the RTS to ensure further proportionality: • Exempted smaller institutions (those subject to the simplified risk management framework and microenterprises) from the obligation of reporting recurring incidents; • Increased the relative threshold of financial counterparts affected from 10% to 30% to address particular concerns raised by the insurance and pensions sector; and • Amended the specification of affected users to provide greater clarity, in particular applicable for the investment, pension and insurance sectors. Finally, it should be noted that some criteria may not apply in certain cases, which means that these criteria can be disregarded by the FEs if it does not apply to them.

Criterion 'Clients, financial counterparts and transactions affected'

Topic	Summary of the comments received	ESAs' analysis
Clients affected	Some respondents are of the view that the number of affected clients is difficult to estimate as some clients have access to services they do not use. Some also argue that there might be cases where the incident does not imply direct data losses thus being difficult to estimate the number of affected clients. They proposed disregarding the criterion. Many respondents have also highlighted concerns on the specification of clients, namely on the: • Uncertainty whether this criterion refers to the clients registered in the specific channel or service affected by the incident (web application, mobile application), or the clients that usually use this channel/service; • Uncertainty on the scope of the term 'clients' and whether it includes effective clients, former clients whose data are still stored in the FE's ICT systems, or others; • Possibility that clients may be interpreted differently by investment fund managers, whose clients are investment funds or vehicles, and private banks with individual clients' deposits; • Clarity needed on whether competent authorities and central banks are clients for trade repositories; and • Potential overlap of number of clients and the number of transactions affected. Some of these respondents also put forward proposals on how to amend the specification of the clients-related part of the criterion, in particular to: • Interpret clients as 'members' for the specific case of pensions funds, since they are considered as the ultimate beneficiaries; • Focus this part of the criterion to clients suffering a material degradation in the service provided to them; and • Focus the client-related part of the criterion to own clients only.	The impact on clients as part of the classification criterion has been set out in Article 18 of DORA. The RTS cannot change or disregard a level-1 provision. With regard to the plausibility of assessment, the ESAs did not find convincing arguments why it is not possible, especially since FE can rely on estimations based on available historic data. The ESAs understand the concerns raised by market participants and have clarified the specification of 'clients affected' to allow proper classification and subsequent calculation of the threshold. Accordingly, the ESAs have amended Article 1(1) of the draft RTS to clarify that clients cover also third parties explicitly covered by the contractual agreement between the FE and the client as beneficiaries of the affected service. In addition, the ESAs have clarified in Article 1(1) that the impacted clients are those that are or were unable to make use of the service (partially or fully) provided by the financial entity during the incident or that were otherwise adversely impacted by the incident. The ESAs would also like to highlight that the clients affected relate to the specific service affected by the incident and that the own clients of the FE should cover all clients (currently registered) that can make use of the service. The ESAs would also like to stress that all classification criteria are interlinked and impact evidenced by one criteria is often evidenced by the impact in another criteria (e.g. clients and transactions affected, loss of availability and service downtime, etc). This is the reason why the ESAs have chosen a classification approach based on a number of criteria that need to be met. For the cases where clarity was sought by respondents to the public consultation on what constitutes clients for trade repositories, the ESAs would like to confirm that CAs and central banks can be considered as clients for trade repositories. The same applies to all other FEs where the government or other national agencies/institutions are using their service. With regard to the relative materiality threshold, the ESAs are of the view that a threshold of 10% is appropriate to cover incidents which affect a significant share of FE's clients and also taking into account that a combination of criteria is needed to classify an incident as major. The relative threshold is proportionate and is not impacted by the absolute number of clients. In relation to the absolute materiality threshold, the ESAs would like to highlight that it is envisaged to capture only large FEs when an incident affects a large number of clients in cases where the relative threshold is not met. To address the concern raised by some respondents and to ensure that overreporting is avoided and proportionality fully embedded, the ESAs have arrived at the view that the absolute threshold should be raised from 50 000 to 100 000 clients.

Topic	Summary of the comments received	ESAs' analysis
	With regard to the materiality threshold, some respondents shared their concerns that: • some services are used by a few clients only and thus the threshold can be met very easily. • the 10% threshold is too low for a primary criterion, with different proposals made to raise it to 15, 20 or 25 %. • The threshold may lead to overreporting. • The absolute threshold will lead to overreporting since it is too low, does not reflect proportionality and the risk entailed. • The absolute threshold of 50 000 would not be indicative for a major incident.	
Financial counterparts affected	Some respondents sought clarity on the specification of financial counterparts since it is a term not legally defined in DORA. Clarification was also sought on the distinction between 'counterparties' and 'counterparts' and it was suggested that the ESAs define the term 'financial counterparts'. A few respondents also suggested focusing the criterion on financial counterparts that have suffered a material degradation to the service provided. A few indicated that the number of financial counterparts affected is difficult to estimate and correlates with the number of affected transactions. Clarity was also sought on whether intragroup financial counterparts should be taken into account in the calculation of the threshold. With regard to the materiality threshold, some respondents shared their concerns that the 10% threshold is too low for smaller entities and IORPS and may lead to overreporting, with a few proposing considering an absolute threshold or increasing the threshold to 15, 20 or 25%.	On the specification of 'financial counterparts' this is a term introduced in level-1, which is not specified there. Accordingly, the ESAs do not have a mandate to define the term in the draft RTS since it may amend the scope of DORA. The ESAs have specified in Article 1(2) of the draft RTS aspects related to the 'financial counterparts' to be taken into account in the classification of the incident. With regard to the proposal for FEs to focus the criterion on the degradation of the service provided to financial counterparts, the ESAs are of the view that this will pose burden to FEs to assess, if they have the information in the first place. Moreover, this will go against the quantitative nature of the criterion envisaged in DORA. The ESAs have, therefore, not amended the specification of this part of the criterion. On the point related to correlation with transactions affected, see the response provided in the issue above on clients. With regard to the type of counterparts to be taken into account, the ESAs would like to clarify that the criterion covers all financial counterparts, including intragroup ones. With regard to the materiality threshold, the ESAs agree with the concerns that the threshold may be too low, lead to overreporting and be particularly burdensome for smaller entities and IORPs. This is particularly evident by the fact that where a FE uses around 10 financial counterparts, an impact on one of them will trigger the criterion. The ESAs have, therefore, decided to increase the relative threshold to 30%.

Topic	Summary of the comments received	ESAs' analysis
Relevance of clients and financial counterparts	Several respondents sought clarity on the term 'business objectives of the financial entity'. Several respondents viewed the part of the criterion subjective. A few stakeholders were of the view that collecting data on the relevance to a counterpart will be burdensome and costly. Several respondents expressed concerns on the materiality threshold focused on 'any impact' on relevant clients. They viewed it as too generic, leading to overreporting and difficult to assess. They proposed to either delete it or clarify that the impact should be significant.	The business objectives of each FE vary and depend on their business model and nature of activities. In that regard, FEs are best placed to assess whether and how an incident affects their own business objectives. The ESAs would like to clarify that the focus is on the relevance of the counterpart for the FE and not the other way around. On the materiality threshold, the ESAs are of the view that only incidents with significant impact should be reported, this is evidenced by the fact that the impact should be on relevant clients/financial counterparts that may have an impact on the business objectives or market efficiencies. The ESAs have slightly redrafted Article 9(1)(f) of the draft RTS to clarify this. Moreover, FEs have discretion on this assessment, which should not bring reporting burden to them.
Transactions affected	Some respondents argued that DORA does not narrow down the transactions affected to those that have a monetary amount and queried whether non-economic transactions should be included. A few respondents viewed the transactions' part of the criterion not suitable for all FEs within the financial sector, in particular pension funds. A few respondents queried whether the criterion covers delayed or non-executed transactions. With regard to the materiality threshold, some respondents shared their concerns that: • the reference to comparable reference periods is not clear; • it is unclear how to calculate the impact when several currencies are affected; • the relative threshold of 10% is too low and a few respondents proposed increasing it to 25%; • Absolute thresholds are (i) not suitable for some type of FE, (ii) too low for large entities, financial market infrastructures and other entities in the investment/market sector where the threshold of 15 000 000 EUR will be easily met, (iii) not proportionate, (iv) will lead to overreporting and (v) will be difficult to assess. Some proposals on	The ESAs have specified the part of the criterion related to 'transactions affected' in such a way that unambiguously specifies that the scope focuses on transactions with monetary amount. The ESAs view this fully aligned with the requirement of Article 18(1)(a) of DORA, which also refers to 'amount' of transactions. However, it should be noted that the reference to 'transactions containing a monetary amount' for the classification purpose should not be understood in a narrow way, since it intends capturing all forms of exchange of financial instruments, crypto-assets, commodities, or any other assets, including in form of margin, collateral or other pledge, both against cash and against any other asset. For classification purposes, these should only cover transactions that involve assets whose value can be expressed in a monetary amount. The ESAs understand that the transactions' part of the criterion may not apply to all types of FEs within the scope of DORA since their operations may not have a monetary amount. These FEs will just not use the criterion for classification of major incidents. On the type of transactions affected, the ESAs would like to clarify that the criterion covers all types of transactions impacted by the incident (including both delayed and non-executed transactions). With regard to the specific comments made by the respondents on the materiality thresholds, the ESAs would like to clarify that: • on comparable reference periods, the ESAs agree with the respondents and have amended the requirement in Article 9(1)(d) and (e) of the draft RTS so that it refers to 'daily average' number/amount of transactions, instead of 'regular level of transactions carried out'; • on the use of different currencies, FEs can use the ECB's daily reference exchange rate; • the relevant threshold of number of transactions affected of 10% is deemed appropriate, especially taking into account

Topic	Summary of the comments received	ESAs' analysis
	the amendment of the threshold from the respondents focused on deleting the threshold, increasing it to 30 000 000 EUR, introducing tiered structure, or changing it to a relative threshold; and • the threshold of the criterion being too high for small FEs.	that a combination of criteria will be needed to classify an incident as major. The ESAs also did not receive convincing arguments on why 10% is not appropriate; and • On the absolute threshold, the ESAs agree with the reasoning behind the concerns raised by the respondents and have amended the criterion to a relative one with a threshold of 10%.

Criterion 'Duration and service downtime'

Topic	Summary of the comments received	ESAs' analysis
Clarification of the criterion	Several respondents sought clarification on what is to be considered a resolved incident. Several respondents objected to having a requirement to review system logs or other data sources to determine the moment the incident was detected and the moment it has been recorded. They argued these reviews would be expensive and require time to carry out. Many respondents sought clarification on the specification of the duration of the incident, in particular on how to understand the reference to 'fully or partially available' and 'activities/operations restored'.	In relation to the reference to resolution of the incident, the ESAs would like to clarify that an incident is to be considered resolved when activities, operations and/or services have been restored to the level prior to the incident. This is to ensure that availability and performance of the service is to the level prior to the incident. With regard to the system logs, the ESAs agree that reviewing records in network or system logs may take time and be costly. To address this concern, the ESAs amended Article 3 of the draft RTS by clarifying that the duration should be measured from the occurrence of the incident, if the occurrence is not known – from the detection of the incident. The ESAs have also specified that where the incident has occurred prior to the detection of the incident, FEs shall measure the duration from the records in network or system logs, but that in case they are unable to do so, FEs can apply estimates. It should be noted that these estimates should be calculated conservatively. With regard to the clarification on the interpretation of 'fully or partially available' and 'activities/operations restored', the ESAs understand that the underlying concern is on how a 'service' should be interpreted. The ESAs would, therefore, like to clarify that the specification of 'service downtime' captures both ICT services and financial services, or in other words client facing and non-client facing systems. Accordingly, the ESAs have amended Article 3(2) of the draft RTS by including a reference to unavailability of the service to internal and external users.
Materiality threshold of the 'service downtime'	Many respondents expressed concerns with the threshold of the service downtime. Some of them indicated that: • an incident can be longer than 24 hours, but that services could be recovered;	The ESAs would like to reiterate that the reference to services covers both ICT services and financial services. Therefore, the services impacted may not necessarily be the client facing services. In addition, as indicated in the analysis to the previous issues, the restoration of the level of the service prior to the incident intends covering both availability and performance.

Topic	Summary of the comments received	ESAs' analysis
	• It is possible that ICT services are down, but the critical functions continue to operate and clients are not affected;. • a distinction can be made between ICT service downtime and availability of services for clients.	In that regard, the ESAs view the threshold related to service downtime' appropriate and have not introduced any changes to it.

Criterion 'Economic impact'

Topic	Summary of the comments received	ESAs' analysis
Difficulty of timely assessment	Some respondents were of the view that the identification of the potential economic impact during the classification of incidents may be very hard to assess, especially at the early stages of the incident. They indicated that the various costs listed in Art. 7 of the RTS may not be known at the time of incident classification, may be challenging to estimate due to a lack of data, influence by external factors or may be subject to imprecise estimations. Moreover, some costs may only emerge long after reporting, such as customer complaints and prolonged lawsuits for damages. The respondents provided various example of costs that cannot be assessed immediately. Accordingly, individual respondents proposed to: • define a timeframe as of when subsequent costs and losses should not be accounted as a direct impact of an incident. • allow for very rough estimation to ensure firms are not delaying their reports. • delete this criterion. • use this criterion as post-incident review information rather than a trigger for the classification of an incident as major.	The ESAs acknowledge that assessing the economic impact accurately might not be feasible in the initial phase of an incident. Therefore, the RTS specifies that FEs can resort to estimates. Also, the economic impact does not need to be reported at the initial stage, but merely measured against the threshold, which does not require very precise calculations. Furthermore, the listed types of costs need to be taken into account for the overall assessment, that does not mean that for the purpose of the incident classification all types of costs need to be assessed and listed individually. This best effort approach that relies on estimations should not pose burden of assessing the economic impact. With regard to the proposal for including a timeframe for the calculation of the economic loss, the ESAs are of the view that this will be burdensome to FEs and may limit the assessment of the actual economic impact. Finally, the classification criteria, including economic impact, to be taken into account in the assessment on whether an ICT-related incident is major are set out in Article 18(1) of DORA. The ESAs cannot change DORA through the draft RTS. The ESAs have, therefore, not reflected this proposal in the draft RTS.
Threshold of the	Some respondents were of the view that the absolute threshold does not	The ESAs view the absolute threshold approach more appropriate from a cross-sectoral perspective, as there are not

Topic	Summary of the comments received	ESAs' analysis
economic impact criterion	ensure proportionality. They proposed to raise the threshold or that each FE defines the relevant applicable threshold in relation to the economic impact or that a tiered approach is adopted. Possible relative measurements proposed were to use: • % of the company's yearly gross turnover. • % of the operating costs of the financial entity during the financial year • as defined in PSD2 (i.e. > Max (0.1% Tier 1 capital (10), EUR 200,000) Or > EUR 5 million) • defined by the entity itself. One respondent was of the view that the threshold of 100 000 EUR for the criterion 'Economic impact' is too high for smaller entities and suggested decreasing to 50 000 EUR.	good relative measurements that could uniformly be applied across the banking, investment, insurance and pensions sectors. The absolute threshold is less complex to calculate compared to the different options proposed by these respondents. Moreover, the materiality threshold for the criterion 'Economic impact' of 100 000 EUR may be too high for some smaller entities. However, the threshold has been set at this level deliberately in order to ensure proportionality and that it does not easily apply to smaller FEs. Having assessed the contrasting views, the ESAs have arrived at the view that the EUR 100,000 threshold is adequate as for most financial entities, especially smaller ones, an incident would rarely meet that threshold, which is also evidenced by the experience from the PSD2 incident reporting where a similar criterion and threshold exist.
Clarifications on the types of costs and losses	Individual stakeholders requested clarifications on various points related to the types of costs and losses in Article 7 of the draft RTS. In particular: • Whether or not advisory costs should be included • Not considering all type of staff costs but only extraordinary staff costs • Delete losses due to forgone revenues, since it is challenging to be attributed to an incident and the wide range of factors impacting forgone revenues • Whether any technology costs related to fixing an incident to return it to its original state fall under business-as-usual costs • To exclude indirect costs from the calculation since they are challenging and costly to estimate and may be widely interpreted by some FEs • To clarify what is meant by internal and external communication • A suggestion to have an open list of costs and losses	The ESAs would like to clarify the following aspects in relation to the individual points raised: • On advisory costs, these are included in the types of costs and losses in Article 7 of the draft RTS. They are only to be taken into account to the extent that they are incurred by the incident and exceed the business-as-usual costs. • On staff costs, all staff costs need to be included, if difficult to determine, FEs can estimate. • On the losses due to forgone revenues, these are consistent with the operational risk framework under the Capital Requirements Directive and Regulation and, therefore, the ESAs would like to retain them. • On the remark related to business-as-usual costs, the ESAs would like to highlight that fixing an incident to return to the original state is not running the business as usual and would thus need to be included in the costs and losses to measure the economic impact. • On indirect costs, they are referred to in DORA, therefore cannot be excluded. It should be noted that indirect costs are assessed from FE's perspective only, which was clarified in the draft RTS to address the concern raised. • On communication, 'internal communication' refers to a communication within the FE or its financial group, while 'external communication' covers communication to external parties (outside the FE), including clients, financial counterparts, and others. • On the open list, FEs do not need to identify each type of cost individually for the classification of incidents but should reflect on them in the overall assessment.

Criterion 'Geographical spread'

Topic	Summary of the comments received	ESAs' analysis
Application of the criterion	Many respondents indicated that the criteria are likely to be triggered frequently and that it will put a disadvantage to FEs that provide services across borders. Several respondents highlighted that it will be difficult to assess the impact in another Member State. Two respondents asked whether the criterion differentiates between right of establishment or freedom to provide services. Some respondents proposed: • Removing the criterion; • CTPPs to report on the incident impact on the FEs' customers; • Focus the criterion on a Member State potentially at risk.	The ESAs would like to highlight that the classification criterion has been set out in DORA. The RTS cannot change the criterion, remove it or disregard it. The criterion itself aims at capturing the impact in a Member State, the significance of which is based on an assessment of the FE. With regard to the frequency of the criterion being met, it should be noted that an identical criterion under the PSD2 Guidelines on major incident reporting has been met in 1/3 of the incidents categorised as major in the recent years. Therefore, the ESAs do not expect overreporting on that basis. When it comes to the point on FEs being put in a disadvantageous position when they provide services across borders, it should be noted that the draft RTS envisages a holistic approach for classification of incidents as major relying on a combination of criteria to classify an incident as major. Therefore, a single criterion being met should not lead to disproportionate classification of incidents. The classification approach embeds proportionality and the criterion further includes it since it leaves at discretion to FEs to assess whether or not the impact in another Member State has been material. In addition, FEs need to develop an understanding of how an ICT incident affects their clients and counterparts, also in other Member States. The ESAs are of the view that the 'geographical spread' criterion should not be solely assessed from the perspective of where the FE is impacted, but also from where its clients, counterparts, transactions are significantly impacted. With regard to the impact on financial market infrastructures or third party providers, the ESAs would like to clarify that this is subject to such information being available to the FE. With regard to the proposal for CTPPs to report the number of affected clients, it should be noted that DORA introduced the obligation to report major incidents to FEs. FEs can outsource the reporting of major incidents to third parties under Article 19(5) of DORA.
Materiality threshold	Many respondents found the materiality threshold of impact in 'at least two Member States' too low and that it will be met in almost all cases. Several respondents highlighted that the materiality threshold focuses on the size of the service rather than on its materiality, thus argued it is disproportionate. Some of these also argued that the threshold may be unintentionally broadened and provided an example of a client travelling to another Member State, which can potentially fulfil the criterion. Relatedly one respondent sought clarity on the impact on clients.	On the frequency of the criterion being met, the alleged disproportionate application and the impact on third party providers and financial market infrastructures, please refer to the analysis of the issue above. With regard to the impact of the incident, it should be noted that this criterion focuses on the impact in other Member States, while the exact impact of the incident is fully assessed through other criteria. This is the reason for the holistic approach taken for the classification of major incidents (see also the analysis of the issue above). The ESAs acknowledge that the impact of the incident should be assessed against all Member States and, if there is any impact in at least two Member States, FEs to consider the criterion being met. The ESAs have amended Article 4 of the draft RTS accordingly.

Topic	Summary of the comments received	ESAs' analysis
	Some respondents proposed: • Raising the threshold to impact in at least 3 Member States or even more; • Introducing a tiered approach to the threshold for entities to adapt based on their own structure, type, operations, size and risk profile; • Introducing a percentage of the business volume impacted; • Focus the impact on the FEs and not on third party providers or financial market infrastructures.	DORA and the RTS establish a harmonised, cross-sectoral approach for classification and reporting of major incidents. Differentiating the classification threshold between sectors would result in a more complex framework, while it is not clear what benefits this would bring here. The ESAs also view the approach taken with the threshold of the criterion in line with the general feedback received from the respondents that the classification approach and assessment should be simple and not posing burden for their assessment. Introducing tiered thresholds or a threshold relative to business volumes will overcomplicate the assessment. Finally, the ESAs are of the view that it is of paramount importance for the criterion to focus on impact at two or more Member States, since DORA will be lex specialis to NIS2, which would mean that CAs in host Member States may only be informed from the CA of the FE in the home Member State of incidents impacting branches in their jurisdiction or FEs providing services based on the freedom to provide services.

Criterion 'Reputational impact'

Topic	Summary of the comments received	ESAs' analysis
Scope of the criterion	The majority of the respondents were of the view that the classification criterion is too vague, broad, and subjective. Some of them shared a concern that the criterion may lead to overreporting since the conditions can easily be met. In addition, several respondents indicated that elements of the criterion may be difficult to measure at the early stages of the incident. Some respondents were of the view that proportionality has not been reflected in the criterion. Some of the proposals put forward related to: • Take into account the relevance of the media – local, national or international; • Take into account the type of media coverage and number of media reflecting the incident; • Clarify what counts as a complaint; • Introduce a specific number or relevance of complaints;	The ESAs are of the view that FEs are best placed to identify the level of visibility of the incident. Therefore, the criterion has not been amended significantly. However, to address some of the concerns raised by the respondents, the ESAs would like to highlight that the media attention should not only be attracted but that the actual incident needs to be reflected in the media (e.g. reported, posted, etc., depending on the type of media), thus evidencing the impact. The ESAs have amended Article 2(a) accordingly. With regard to the specific proposals on distinguishing by types and number of media, the ESAs have not found the proposal convincing since national and local media may still provide significant publicity depending on the size of the entity. Moreover, a specific number may not evidence greater publicity than one large media. With regard to the complaints-related part of the criterion, the ESAs clarified that the complaints should be repetitive in nature, thus evidencing a recurring issue where a number of complaints have been received, not just a few isolated complaints. The ESAs have also clarified that the complaints shall relate to 'client-facing services or critical business relationships'. On what is to be considered a complaint, the ESAs are of the view that this is a widely used term introduced in large number of level-1 acts that does not require further clarification.

Topic	Summary of the comments received	ESAs' analysis
	• Clarify the breach of regulatory requirements and introduce an element indicating significance or likelihood of imposition of sanctions or supervisory measures; • excluding pension funds from the application of Art. 2(d); • to consider two elements of Art. 2 to be met;	When it comes to the breach of regulatory requirements, the ESAs find the requirements sufficiently clear and easy to apply by FEs. The proposal by the respondents to focus on sanctions or supervisory measures has been viewed as more challenging to implement since it would depend on the assessment of the CA, which is outside the control of the FE. In relation to the loss of clients, the ESAs would like to clarify that the intention behind Article 2(d) of the draft RTS is to indicate whether the loss of clients or financial counterparts may have significant material impact on the business of the FE, thus leading to potential reputational impact. The ESAs have amended the Article to reflect that. The ESAs also acknowledge that parts of the criterion may not be known at the early stages of the incident but, equally, for some incidents they may be available. For that reason, the ESAs have not removed any of the items from Article 2. Finally, the ESAs view the requirements as proportionate since they apply equally to all types of FEs, will not pose reporting burden, and provide FEs with the flexibility to assess whether the classification criterion is met based on the nature, size and complexity of their business.

Criterion 'Data losses'

Topic	Summary of the comments received	ESAs' analysis
Clarification of key terms of the RTS	Many respondents suggested clarifying the terms 'significant impact', 'critical data' and 'an adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements' should be defined in the draft RTS and that they are too broad. A few respondents proposed drafting amendments for significant impact and one proposed that FEs should have discretion for determining what level of 'data loss' is significant. On critical data, a few respondents highlighted that it is not clear whether critical data is related to the data processed by critical or important function or not. A few respondents suggested clarifying that FEs should have discretion to decide which data	With regard to the term 'significant impact', the ESAs are of the view that the reference to 'significant' is not needed since the significance (or the material event that disrupts the execution of a critical or important function) should be assessed based on whether the availability, authenticity, integrity or confidentiality of data is affected that has or will have an adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements. The ESAs are of the view that FEs should have discretion to carry out this assessment. In relation to the comments on 'critical data', many respondents did not provide any suggestions on how to define critical data or how to improve overall the proposed text. The ESAs are of the view that FEs are best placed to identify which data is critical for their operations, which, in turn, should evidence that the loss of these data will have a significant impact on the FE. The ESAs would also like to clarify that the reference to critical data did not limit to data that is 'processed by critical or important function' if there is a high adverse impact on network or information systems that support critical or important functions. The ESAs agree with the proposed change and have amended Article 13 of the draft RTS to clarify that the impact on critical data should

Topic	Summary of the comments received	ESAs' analysis
	is critical. A few respondents proposed limiting the threshold to incidents that have caused actual harm or are clear to eventually cause actual harm. On the 'an adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements', a few respondents indicated it is difficult to measure. One respondent was of the view it is not tied to more objective measurable criteria such as percentage of data losses and proposed to introduce a 10% threshold for this data loss. Another respondent suggested taking a sector-specific approach.	'have or will have an adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements'. In addition, since Article 13 of the draft RTS introduces directly the cases when the threshold is triggered, namely the adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements, the ESAs have deleted the reference to 'critical'. With regard to the sentence 'an adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements', the ESAs would like to highlight that the intention is to capture incidents where loss of data will have a significant impact on business objectives (such as impact on operations, profit, market share, security, competitive position and others) as well as on meeting regulatory requirements (e.g. known non-compliance with legal requirements). Moreover, FEs know their business objectives and are aware when they are incompliant with legal requirements, therefore, they are best placed to identify such impact. In addition, specific thresholds have been discarded by the ESAs as an option since it will be challenging to define % of data loss that will be meaningful and appropriate and equally applicable to all FEs within the scope of DORA. Accordingly, the ESAs have not amended the draft RTS. With regard to the proposal for a sector-specific approach, the ESAs view this going against the harmonisation of incident reporting and that it will introduce more complexity with little added value since FEs are best placed to assess the impact on the business objectives and the compliance with legal requirements.
Interplay with GDPR	Several respondents sought clarity on the interplay with GDPR and suggested aligning between the two. A few respondents proposed assessing the compliance with GDPR and focusing on data breaches. One respondent proposed clarifying the level of confidentiality or sensitivity of data to understand whether it is harmful to the FE.	The clarification sought in relation to the interplay between GDPR and DORA in relation to data losses is related to the interpretation of level-1 texts and goes beyond the mandate conferred by DORA on the ESAs under Article 18(3) of DORA. In addition, the ESAs would like to clarify that DORA introduces requirements for digital operational resilience, which is different in scope and objectives to GDPR. GDPR focuses on personal data while DORA has a larger scope. When it comes to the assessment of confidentiality, in accordance with Article 5 and 13 of the draft RTS, it is for the FE to evaluate the level of confidentiality of the data.
Clarity on data loss and its threshold	A few respondents shared the concern that the term 'data loss' is not defined and that it can be interpreted differently especially if looking at intellectual property, privacy and business. A few other respondents suggested clarifying that data loss entails 'a real malicious use of the data' and that it is necessary to differentiate whether the data has been exploited or not, to avoid significant overreporting.	The ESAs would like to clarify that Article 5 specifies the term data losses with regards to the properties of availability, authenticity, integrity and confidentiality of data. In addition, the aim of DORA regulation is the digital operational resilience and, therefore, it differs from other standards and regulation that are different in their objective and scope. The ESAs are of the view that the criterion of data loss should be triggered as soon as there is a successful unauthorised malicious access, irrespective of whether the data has been exploited or not. Any successful malicious unauthorised access could harm the FE (e.g. APT attacks) and have a severe impact on its security systems, which can also be considered as critical or important functions of the FEs. Accordingly, the ESAs have introduced in Article 13 of the

Topic	Summary of the comments received	ESAs' analysis
	One respondent suggested focusing the data loss criterion on deletion of data.	draft RTS a second trigger for the criterion 'data losses' covering cases of successful malicious unauthorised access to network and information systems. This will ensure capturing important major incidents such as those related to data breaches and data leakages and is consistent with the definition of 'security of network and information systems' under NIS2, which relates to '*the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems*'. With regard to the proposal to focus the criterion on deletion of data, the ESAs have arrived at the view that such an approach will be too restrictive and lead to under-reporting.
Authenticity specification	A few respondents highlighted that authenticity should be better defined to differentiate it from integrity. One respondent suggested for authenticity to be deleted since it is covered by integrity.	Authenticity and integrity are two distinct properties introduced in Article 18 of DORA and thus authenticity cannot be disregarded when assessing the classification criterion data loss. The ESAs agree with the respondent and have amended Article 5(2) of the draft RTS related to 'authenticity' by not referring to reliability of data and focusing on the need to determine whether the incident has compromised the trustworthiness of the source of data.
Unavailability of data	Several respondents proposed clarifying that data losses that the incident entails in relation to the availability of data should only focus on permanently unavailable data. A few of them were of the view that temporary unavailability is already covered by the criteria 'Clients, financial counterparts and transactions' or 'Service downtime' and that it should not be duplicated with the criterion 'Data loss'. One respondent indicated that a brief unavailability of data will not necessarily be considered as a data loss and suggested that the criterion either focuses on the permanently nature of the data loss or that the data is required to perform critical functions of the FE. Two respondents were of the view that the current formulation is too rigid and lacks proportionality.	The ESAs are of the view that the formulation of the data losses criterion is not too stringent since the materiality threshold in Article 13 narrows down the data loss cases to those that have or will have an adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements. Therefore, FEs have discretion to decide which data losses are significant and qualify as such. The ESAs are also of the view that many temporary data losses will not have the described significant impact and accordingly will not meet the classification threshold. With regard to the proposals to focus the criterion on permanently inaccessible, the ESA are of the view that it may be too restrictive and open for interpretation. Finally, with regard to the proposal to limit the scope to the performance of critical functions, it should be noted that the ESAs have reflected this in a different way – by making the criterion 'critical services affected' conditional for the classification of an incident as major.

Criterion 'Critical services affected'

Topic	Summary of the comments received	ESAs' analysis
Escalation to the senior management	Many respondents commented on the inclusion of the escalation procedure to the senior management and the management body in the materiality threshold. Some of these respondents proposed to remove the escalation to the management from the materiality threshold since: • It may lead to overreporting, especially if the criterion is a primary one; • is usually a consequence of the nature of the incident; • may decrease the internal reporting; • will disadvantage FEs that have a robust incident response strategy and plans. • It will be disproportionate for smaller FEs. In addition, a few respondents suggested clarifying (i) the escalation process and its purpose, including by distinguishing from normal reporting for information already envisaged in DORA, (ii) the terms senior management and management body and that (iii) the impact of the incident is significant. A few respondents also proposed to change the 'escalation to the senior management' to the activation of a crisis unit'.	The ESAs agree with the views expressed by many of the respondents on this issue and acknowledge that the proposed link to escalation to senior management a criterion that is now a condition for the reporting of major incidents (previously a primary criterion) is not desirable and may bring challenges for financial entities to apply it as outlined by the respondents. Accordingly, the ESAs have removed it from the threshold of critical services affected.
Proportionality	Some respondents highlighted that the criterion is too broad and may lead to overreporting. A few respondents emphasised on this impact on the insurance sector. It was also proposed to follow a tiered approach since the interruption will diverge based on the size of the FE and their activities. With regard to the escalation of incidents to the senior management, smaller FEs may be disproportionately affected since almost all incidents may need to be escalated.	The ESAs would like to clarify that proportionality has been embedded holistically in the classification approach taken in the draft RTS where a combination of criteria and their thresholds need to be met to qualify an incident as major. A single criterion will not trigger a reporting obligation. The thresholds can only be regarded as risk-adequate and proportionate in their entirety. The ESAs are of the view that the current approach is balanced and suitable for all financial entities, while ensuring that supervisors get information about all relevant incidents and avoiding overreporting (based on the tests carried out). With regard to proportionality concerns on small FEs, the ESAs agree that such an escalation may be disproportionate and in line with the concerns covered in the previous issue and have agreed to remove the reference to escalation to the senior management from the materiality threshold.

Topic	Summary of the comments received	ESAs' analysis
		Since the respondents did not propose specific additional changes to address the concerns raised, the ESAs have not further amended the draft RTS.
Clarification of terms	Some respondents highlighted that the RTS should use consistent terminology with DORA to avoid legal uncertainty and overlaps. Several respondents suggested clarifying the term critical services and how it delineates from other similar terms, such as 'critical or important' function, 'network and information system'. A few respondents suggested not defining critical services affected and leaving it for the discretion of FEs to decide based on their business impact analysis. Some respondents questioned the use of 'authorisation' in the assessment of the criticality of the service. A few respondents sought clarity on whether authorisation refers to authorised activities or internal approvals. A few respondents proposed to include a reference to 'registered' activities too.	The terms used throughout the RTS are in line with the text of DORA, such as the reference to critical or important functions (Art. 3(22) DORA) or criticality of the services affected Art. 18(1)(e) DORA). The broader definition leaves room for FEs to have flexibility and discretion based on their business impact analysis, but at the same time provides some tangible services (authorised/registered/supervised) that should always be taken into account. To address some of the concerns raised the ESAs introduced the following changes to Article 6 of the draft RTS in relation to the criterion 'critical services affected': • Introduced a reference to 'network and information systems' to align better with the incident and major incident-related definitions of DORA; • Clarified that the authorised services are 'financial services that require authorisation'; • Added a reference to registered or supervised services.

Recurring incidents

Topic	Summary of the comments received	ESAs' analysis
Assessment of recurring incidents	Several respondents sought clarity on the common 'root causes' and the 'same nature of the incident' to be taken into consideration when assessing recurring incidents. They proposed that ESAs should develop a root cause taxonomy. One respondent proposed that such similarity should be understood as incidents impacting the same software or systems. A few respondents were of the view that not all of the classification criteria are suitable for aggregation. Two of	The ESAs agree that consistent taxonomy is key for the effective identification of recurring incidents. With regard to the root cause, it should be noted that the different types of root causes of the incidents are to be set out in the RTS and ITS on the content, timelines and process for reporting major incidents under DORA (Article 20a and 20b of DORA). Therefore, ESAs have amended the legal text to refer to said taxonomy. With regard to the reference to the 'similar nature and impact', the ESAs have arrived at the view that consistent taxonomy will be challenging to set-up since the incidents vary in their nature and impact and are specific to each FE. Accordingly, the ESAs have amended Article 15 of the draft RTS (previous Article 16) by removing the reference to similar nature and impact.

Topic	Summary of the comments received	ESAs' analysis
	them indicated that only transaction volume, geographical spread, and economic impact can actually be aggregated.	When it comes to the aggregation of the classification criteria for recurring incidents, the ESAs are of the view that all criteria can be aggregated. In addition, adding specific instructions on which criteria should be aggregated and how, would render the approach to classification of recurrent incidents excessively complex. Accordingly, the ESAs have not introduced changes to the RTS on this particular point.
Reporting burden	A number of respondents expressed concerns about the operational burden that analysing incidents for similarities would entail, including the substantial use of internal resources and the difficulty in assessing the data. Some of them also mentioned proportionality concerns, as this issue would disproportionately affect smaller entities. They proposed the following changes to address their concerns: • reducing the assessment period to 2 weeks, • raising the number of recurrences to three or more; • allowing entities to apply expert judgment and only analyse as recurrent certain incidents, and • having recurrent incidents reported on an annual or quarterly basis (instead of rolling).	The ESAs would like to highlight that FEs are required under Article 17(2) of DORA to 'monitoring, handling and follow-up of ICT-related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.' This obligation applies to all ICT-related incidents and the recurring incidents under the draft RTS are in line with them. Having assessed the feedback from the public consultation, the ESAs have arrived at the view that some changes will need to be introduced to the provisions related to recurring incidents, namely: • To ensure proportionality, the ESAs have exempted smaller financial entities (those subject to the simplified ICT risk management framework and microenterprises) from the obligations to report recurring incidents; • Changing the approach from assessing recurring incidents from rolling to monthly basis. This time period was chosen in order to allow supervisors to obtain timely information about the incidents but at the same time not posing burden to the reporting entities; and • Focusing the common aspects of the recurring incident to the 'root cause' only and deleting references to 'similar nature and impact'. With regard to the proposal for FEs to have discretion on the assessment of the recurring incidents, the ESAs do not agree with the respondents since this will go against the objective of DORA of harmonising incident reporting requirements for all FEs.
Legal basis	Some respondents shared concerns on the legal feasibility of capturing recurring incidents. They viewed that this would require collecting additional documentation not required under DORA.	The ESAs would like to clarify that the definitions of an 'ICT-related incident' and an 'operational or security payment-related incident' refer to 'single event or a series of linked events unplanned by the financial entities' (emphasis added). Accordingly, the ESAs are of the view that the capturing recurring incidents is in line with these definitions. With regard to the documentation, the ESAs are of the view that it is in line with the provisions of Article 17(2) and (3) of DORA, as highlighted already.
Concerns of overreporting	Many respondents shared concerns on potential overreporting due to current lack of clarity on the potential numbers of recurring incidents. These respondents also shared concerns that FEs may err on the safe side and report incidents that may meet the	Based on the information provided by the FEs that collect and assess recurring incidents, there is no evidence on potential overreporting. Moreover, the incidents that will be considered recurring will need to have the same root cause and collectively meet the classification thresholds, which shall address the risk of overreporting further.

Topic	Summary of the comments received	ESAs' analysis
	thresholds but that do not necessarily do so. A few respondents who have experience with recurring incidents indicated that they are to classify a few or no recurring major incidents.	Finally, to ensure proportionality and address the concerns raised by the respondents, the ESAs have amended the requirements so that smaller institutions (those subject to the simplified risk management framework and microenterprises) are exempted from the obligation of reporting recurring incidents.
Period for capturing recurring incidents	The ESAs have received divergent views with some respondents supporting capturing recurring incidents and others providing comments. Two respondents supported a 3-month period and two supported a 12-month period, with one of the latter having understood they need to carry out the assessment for recurring incidents once for that period.	Having assessed the feedback the ESAs have arrived at the view that monthly assessment for the previous 6 months should be adequate to capture recurrence. This approach balances well the needs of supervisors to receive incident information timely and of FEs of not being burdened with the assessment.

Approach for classification of significant cyber threats

Topic	Summary of the comments received	ESAs' analysis
Assessment of impact of cyber threats on other entities	A group of respondents suggested limiting cyber threat analysis to the FE itself since, in their view, it is challenging to assess the impact on third parties and other entities.	The ESAs are of the view that a threat assessment should also take into account vulnerabilities at the FE's providers, clients and financial counterparts. The ESAs acknowledge this is not always possible with the same level of detail as an internal vulnerability assessment, but are of the view that this should be encouraged to the extent possible. It should be noted that FEs are not required to make guesses on other entities' risk exposure and cybersecurity measures, but only to report the information if known to them.
Clarification of 'probability of materialisation'	Some respondents proposed changes to Article 17 in relation to the probability of materialisation. A few respondents highlighted that they do not find appropriate the use of the term 'applicable risk' when assessing a 'probability of materialisation'. A few others suggested that the implemented countermeasures should also be taken into consideration in estimating the potential 'probability of materialisation'. A few respondents were of the view that the term "high probability" should be clarified further so that FEs	The ESAs would like to clarify that the applicable risk refers to the extent a threat can affect the financial entity, its third party providers, clients and financial counterparts. This follows from the first paragraph of the Article. Therefore, there is a close link between the two and ESAs have clarified it by Amending Article 17(2)(a). The ESAs are of the view that taking countermeasures into account would transform the threat assessment from a gross risk (before mitigating measures are considered) to a net risk (after they are considered). FEs differ in their level of preparedness, and FEs that will be the first to detect a threat may tend to be better prepared and have a lower assessment of their own residual risk relative to a threat. Therefore, what makes a threat significant from the perspective of DORA is the level of inherent risk, more than the residual risk.

Topic	Summary of the comments received	ESAs' analysis
	can determine the volume of the possible threats to be reported. They viewed it, despite being dependent on the identified risks and vulnerabilities, as too vague.	The ESAs would like to highlight that risk analysis normally uses probability buckets such as "low", "high", or "very high" instead of numerical probabilities. The reference to 'high probability' is therefore aligned with terminology already in use in risk departments. Accordingly, the ESAs have not introduced any changes to the draft RTS.
Confidentiality rules	Several respondents indicated that definition of a significant cyber threat is too broad and conflicts with the confidentiality of threat intelligence according to MoUs and NDAs. A few other respondents were of the view that providing information to clients about significant cyber threat would go against the spirit of the cyber intelligence sharing community which seeks to prevent oversharing of information. They indicated this could damage trust with clients and potentially impact market stability. One respondent was of the view that cyber threat information should be treated as confidential by supervisors and in any communication between supervisors. Another one proposed that the ESAs should introduce (i) criteria for the sharing of this information (with the financial entity, competent authority(s) and among competent authorities) and (ii) specific safeguards to protect the data such as anonymisation and use of secure channels for transmission.	The ESAs view the requirements of the RTS consistent with Art. 19(3) of DORA, which specifies that 'in the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking'. Therefore, it should not be a problem if a contract restricts the FE's capacity to share threat intelligence to other parties. In the case of clients, this sharing of information is an 'appropriate protection measure'. It is not clear in which case trust could be damaged or market stability impacted if FEs inform their clients of a cyber threat that may affect them. Accordingly, the ESAs have not amended the draft RTS. The comments on confidential treatment and sharing of cyber threat information relate to provisions that are under DORA, namely Art. 19(3) and Art. 21. The proposed changes go beyond the ESAs' mandate set out in Article 18(3) of DORA.
Threat actors	A few respondents commented on the capabilities of threat actors. One respondent highlighted that FEs have limited knowledge on threat actors and suggested that subparagraphs (b) and (c) of Art. 17(2) can be complemented with "to the extent known by the financial entity" to give consideration to factors known by the entity. A few respondents were of the view that the capabilities and intent of threat actors is an excessive criterion when assessing the probability of materialisation and not aligned with the principle of proportionality or with a risk-based approach.	The ESAs view the comment from the first respondent in line with the intention behind the provision. However, to make it even clearer, the ESAs have clarified in the RTS that the information about the capabilities and intent of the threat actors should be considered onto the extent known by the FE. The capabilities and intent of threat actors may be known in advance, for instance when a threat actor has successfully performed complex cyberattacks, or when it is known for targeting the financial sector, therefore it is an important risk factor. Finally, it should be noted that the assessment will be based on the information that is available to the FE.

Topic	Summary of the comments received	ESAs' analysis
Specification of the criteria for significant cyber threats	A few respondents indicated that the proposed criteria and thresholds may capture most cyber threats, unless FEs consider only threats that are likely to have a severe impact (in 1.a) and will likely fulfil the conditions set out in Article 8 of the RTS (in 1.c). A few other respondents also viewed the specification of the criteria for 'cyber threats' too general and failing to take into account the variety of entities in scope. A few respondents highlighted the classification criteria for significant cyber threats do not specify if they cover external threats only or also internal threats.	The specification of the criteria for significant cyber threats in Art. 17(1) covers several criteria aiming at filtering non-significant threats (e.g. potentially affected functions, probability of materialisation, and possible impact in accordance with the incident classification). Article 17(b) of the draft RTS provides that the "cyber threat has a high probability of materialisation", which means that provisions in paragraphs 1(a) and 1(c) are to be considered fulfilled only if the threat is likely to affect critical or important functions, and to fulfil the conditions set out in Article 8 of the RTS. Therefore, the scope of captured cyber threats should be narrowed down sufficiently and focuses on potential significant impact. Moreover, the definition of a cyber threat in DORA refers to Art. 2(8) of NIS2, which does not make a difference between internal or external threats. Finally, to ensure that the criteria for significant cyber threats are proportionate, aligned with Article 18(2) of DORA and not posing burden to FEs, the ESAs slightly amended Article 16(1)(c) by focusing the potential impact, if the threat materialised, to critical services affected and any of the thresholds of the criteria geographical spread and clients/financial counterparts/ transaction affected. The remaining incident classification criteria are conditional, depending on the type of threat and information available, since their thresholds may not be easily assessed.

Assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities

Topic	Summary of the comments received	ESAs' analysis
Security of sharing incident information	Many respondents are concerned about the security risks of sharing incident-reports. Several highlighted the risk of centralisation of incident information and that all authorities receiving incident reports should ensure high ICT security standards for protection of the data. Several respondents were not clear on whom the incident report should be shared with. A few of them sought clarity on what is meant by 'competent authorities in other Member States' and expressed	The ESAs would like to highlight that the concerns expressed by the respondents relate to information sharing provisions that are set out in Art. 19 of DORA, which are outside the scope of the mandate. Nevertheless, it should be noted that any shared information among CAs should fall under general professional secrecy requirements and confidential handling. With regard to some of the concerns raised on the security in the transmission of information to and from the ESAs set out in Article 19(6) and (7) of DORA, this cannot be specified in the RTS since it is not within the scope of the mandate. However, the ESAs duly take note of these concerns and are fully aware of them and will take them into account for the implementation/set-up of a tool(s) for incident reporting between CAs and ESAs under DORA.

Topic	Summary of the comments received	ESAs' analysis
	concerns that incident information should not be shared broadly. Several respondents asked for FEs to be made aware when the ESA's forward the report to CAs in other Member States.	In relation to sharing of the information, the ESAs would like to clarify that the assessment of relevance under Article 17 of the draft RTS covers all Member States but that the sharing of information in other Member States applies only to the relevant impact DORA host CAs. With regard to sharing of incident reporting information, the ESAs would like to highlight that this is covered by DORA where Article 19(6) clearly indicates the authorities whom incident reports can be shared with at national level and Article 19(7) indicates the authorities the ESAs (and ECB) need to forward the incident to. In relation to the sought clarification on the reference to 'competent authorities in other Member State', the ESAs have separated the reference of Articles 19(6) and (7) of DORA so that it is clear that the ESAs will only share reports with the relevant competent authorities in the impacted host Member State, which are the DORA CAs. The request for ESAs to inform FEs on when they have shared the report with CAs in other Member States goes beyond the provisions of DORA and the mandate of the RTS. However, the RTS set out in Article 17 the criteria for assessing relevance in other Member States, therefore, whenever the threshold of two or more affected Member States is met, the ESAs will forward the incident to the relevant DORA CA in that Member State.
Anonymisation of reports	Many respondents proposed anonymisation of reports. One respondent indicated that it may be too burdensome for large-scale third-party providers to report anonymised.	The ESAs would like to clarify that the objective of sharing of incident information is for relevant CAs to be able to identify the FE that is affected so that they can subsequently identify any potential impact on other FEs. This contributes to the incident reporting objective of preventing systemic impact and spill-over effects. With regard to the outsourcing-related concern, it should be noted that FEs are fully responsible for the fulfilment of the incident reporting requirements as set out in Article 19(5) of DORA, therefore, the ESAs do not see the concern on anonymisation bringing burden as valid.
Assessment of thresholds	Several respondents indicated that the threshold of two affected Member States may be reached quickly, thus leading to the criterion being often met. It was suggested a risk-based approach for foreign branches. Stakeholders also highlighted that a FE may not always have access to the required information to assess whether the conditions in Article 18 of the RTS are met or not and that this may be outsourced to a third-party provider.	The ESAs clarify that the holistic approach under the draft RTS relies on a combination of criteria (which are often linked to each other) to classify an incident as major. Therefore, a single threshold should not lead to overreporting by itself. In addition, FEs have discretion in their assessment of the impact in other Member States, therefore a risk-based approach is implicitly taken. In relation to the point that FE may not have all information about the impact of the incident in other Member States, the ESAs would like to highlight that the requirement of Article 17 of the draft RTS already envisages that this should be done 'to the extent this information is available to the financial entity'. With regard to the outsourcing, DORA and the RTS do not prevent FEs from outsourcing the assessment of the impact to a third party provider.

Topic	Summary of the comments received	ESAs' analysis
		Finally, the ESAs would also like to clarify that where there is an impact in other Member States but that the FE is not impacted in the home Member Stat, the FE is expected to report the major incident.