German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

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

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Berit Schimm
Telephone: +49 30 2021- 2111
E-mail: b.schimm@bvr.de

Berlin, 2023-09-08

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

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

	Question	Yes/ No	Comments GBIC
Q1	Do you agree with the overall approach for classification of major incidents under DORA?	No	We see various challenges to classify a security incident in a reasonable time according to the scheme presented (see our answers to Q2 - Q8). In DORA article 3 (10) a major ICT-related incident is defined as an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity. Therefore please restore the linkage to critical or important functions or critical services throughout the whole classification process/ criteria (also beyond article 6).
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? (primär)	No	Art. 1: The number of affected customers (1) are difficult to estimate in practice. Thus, these values are significantly less accurate than the number of affected transactions (4). Moreover, the number of affected transactions often correlates with the number of affected customers, so these two criteria are not independent. We therefore advocate including only the number of affected transactions as a primary criterion in Art. 1 and using the number of affected customers and contractual partners as a supplementary reference or as a secondary criterion to substantiate the number of transactions. The thresholds for "number of transactions" and – if not deleted for "affected customer" - should remain at the level of PSD2 (25 % primary and 10 % secondary criterion.) If thresholds are too low, there is a risk that non-material events will also have to be reported, which leads to confusion regarding truly significant events and a significantly higher administrative burden. The term "financial counterparts" is not legally defined and should therefore be clarified in the RTS. The relative materiality threshold for contracting parties should be higher than that for customers, as there are usually significantly fewer contracting parties than customers. With 10 contracting parties, already one affected contracting party would meet the primary criterion, which would be inappropriate. We advocate applying the value of 25% for contracting parties. Fixed amount limits does not fit the heterogeneous institutions. Depending on the size of an institution, the criterion should be varied. Example: A regional bank has different dimensions than a B2B settlement bank. We propose to use only percentage. Art 9.1 (f): 'Any impact' can be interpreted to include non-critical operations and would lead to over reporting, especially if firms are expected to estimate because of the lack of access to appropriate information at their clients or counterparts. As stated above, firms do not have access that would allow for the assessment of impact on clients or financial counterparts or the subsequent impact that would have on objectives and market efficiency. Therefore, financial entities would be forced to guess and will likely error on the

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

			side of caution which will result in a significant increase in the amount of reporting. We suggest to delete 9.1 (f).
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? (sekundär)	No	**Art. 2 and 10:** Generally: The majority of listed points feels to be of subjective nature. Therefore, we propose to add in the part "financial entities shall take into account the level of visibility" "as a result of the incident, as determined by the financial entity". In our experience, short and short-lived media reports as well as ad hoc customer complaints do not lead to any significant permanent damage to reputation. We consider the classification criteria c) and d) to be sufficient to implement the requirements of DORA Art. 18.1 a) (reputational damage) and request the deletion of the classification criteria a) and b). Detaills: • Criterion a): Almost any incident, even an uncritical one, can appear immediately in news tickers or social media - sometimes exaggerated. If a) will not be deleted we suggest that the term media be more narrowly defined as follows: ''The incident has attracted the attention of nationwide media, which are recognized as exercising objective reporting." • Criterion b): Few complaints cannot and must not be a reason to establish a primary criterion. Otherwise, the adequacy and comparability with the other criteria would not be given. Some customer complaints are common in relation to incidents, it is when these are not resolved to the customer's satisfaction that there can be reputational risks or there is a large quantity that cannot be processed. If b) will not be deleted we suggest the following wording: "The financial institution has received significantly clustered complaints from different customers or financial partners on the same issue." • Criterion c) non-compliance with regulatory requirements - not every short-term non-compliance has a reputational impact. **Art. 3 and 11:** We consider the downtime of 2 hours for critical functions to be too short because an interruption of 2 hours is only a non-critical business interruption for most critical functions. Even not every critical or important function is time-critical. Therefore it should be possible for companies to set the time limit for classification under Article 11 themselves along their availability criteria for the service. If the proposal will be not accepted we recommend at least a downtime of 4-8 hours as materiality threshold. Further, the "Duration" criterion should be more clearly defined. With the current definition "…until the moment when the incident is resolved", it is unclear whether this means only restoration of normal operations, e.g. after a virus attack, or if it includes also all entailing investigations about attackers, initiation of legal measures etc. (which regularly takes much longer than 24 hours). Our amendment: "Art. 11.

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

			a): the duration of the incident is longer than 24 hours until the moment normal operations are restored. b): the service downtime exceeds the time for ICT services supporting critical functions that the financial entity has defined in their availability requirements for the service." **Art. 4. and 12:** So far, it is not yet clear why the criterion of geographical spread leads to higher risk and can be a trigger for the materiality threshold of a major incident. For globally operating bank applications are used in 2 or more EU countries. That means nearly all major incidents will meet this threshold and fullfil this secondary criteria. This results in the majority of EU impacting incidents only need a single primary criteria to be DORA reportable. It should be also clarified, that criterion 4 is only relevant if the financial entity offers its services in more than one EU country (not only national). According to background paragraph 36 of the RTS the ESAs have, therefore, arrived at the view to base the criterion on the FE's own assessment of the material impact in two or more jurisdiction(s) based on the affected clients and financial counterparts, branches or subsidiaries within a group, and financial market infrastructures or third party providers that may be shared with other FEs.' However, 'materiality' is not reflected in article 12 and we recommend amending to include it. **Art. 7 and 15:** According to the ESAs, the criterion was hardly ever used for PSD2; this should also be the case here, as costs usually only become visible after some time, i.e. could only lead to a very late follow-up report; it is extremely unlikely that other criteria are not used in parallel - the effort of the estimates is too high for the limited gain in knowledge (in addition, ESA guidelines are planned anyway, where banks are to determine/ estimate the aggregated annual costs and losses). We propose to delete the criterion or otherwise set the reporting threshold to 5 million or 0.1% of hard core capital (see PSD2 / SSM).
Q4	Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13? (primär)	No	Data availability is closely related to downtime (see article 3); if a service fails, data is always inaccessible during this time. This criterion is therefore included twice and 5.1 should be deleted from the article 5 data losses.
Q5	Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14? (primär)	No	It would potentially lead to more reportable incidents because the RTS also includes all activities requiring an authorisation which have partially not been reportable up to now. Art. 14 should refer to "significant impact", otherwise there would be massive over reporting. The requirements should not lead to the exclusion of informal information to senior management, which may occur for

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

			other reasons, if escalation to the FE's senior management is part of the materiality threshold.
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?	No	We see enormous problems and efforts in the implementation. The text in the RTS would require the complex implementation of a tracking and could lead to overreporting (e.g. in the case of phishing waves) and is not useful for reporting. The rules on recurring incidents imply that all incidents, even those that are not serious, must be documented because they could potentially contribute to a serious incident when aggregated. In addition, the rolling procedure requires that for each incident an analysis must be made as to whether there have already been similar incidents in the last 3 months in terms of cause, type and impact. For these reasons, we do not consider the recurrent incident policy to be appropriate and proportionate. As the rules are not explicitly required by DORA, we request that the procedure be deleted. At least thresholds should be defined for incidents, above which documentation for recurring incidents begins in the first place, so that not every minor incident has to be documented. Our suggestion: 25% of the thresholds for serious incidents. Furthermore, in this context the number of recurring incidents - two - is much too low, we suggest at least four times. Amendment: "For the purposes of paragraph 1, recurring incidents shall occur at least four times." Additionally, not all criteria of Art. 1 to 7 are suitable for summation according to Art. 16. In our view, suitable criteria for summation are: • Transaction volume (Art. 1 No. 4), • geographical spread (Art. 4), • economic impact (Art. 7). • Examples of unsuitable criteria: - on Art. 9 No. 1 a) - number of customers affected: If the same 5% of customers are affected 3 times in succession, the statement that in total 15% of customers are affected is meaningless and inappropriate. - to Art. 11 b) - Downtime: If incidents have caused 3x repeated downtime of 1 hour each, the statement of a total downtime of 3 hours is meaningless and inappropriate.
Q7	Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17?	No	We believe that the level of complexity is not optimal and may be unmanageable for many financial entities who will need to maintain their own internal classification system for cyber threats in order to properly monitor risk. We do not believe it is possible for a financial entity to assess impacts or effects on other financial entities, third-party providers, clients or counterparts. We believe it is better to limit cyber threat analysis to the financial entity itself and not expect any analysis of other entities. While many firms will monitor threats and may become aware of threats to another financial entity, this is done on an ad-hoc basis, mostly based on threat intelligence. We therefore recommend the following amendments:

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

			Art. 17.1 (a): delete "other financial entities, third party providers, clients or financial counterparts" in the sentence "the cyber threat could affect critical or important functions of the financial entity…". Art. 17.1 (b) delete "or other financial entities" in the part "the cyber threat has a high probability of materialisation at the financial entity…" Predicting the materialization of a threat is difficult, as this usually depends on a variety of factors. It should therefore be described more specifically on which criteria this assessment can be made. There needs to be attribution to determine the capabilities and intent of threat actors. The ability to attribute a cyber attack to a particular cyber threat actor or group may require significant time and the assistance of external threat intelligence (e.g., government agencies). A financial entity on its own may not be able to attribute. We suggest that attribution should be an objective of information sharing and should, therefore, be removed from the classification criterion for a single entity. It should be made possible for third-party ICT service providers, rather than financial service providers, to assess the materiality of cyber threats on the basis of their operational responsibility and expertise and to report to the financial service provider on this.
Q8	Do you agree with the approach for assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities, as proposed in Articles 18 and 19?	No	The industry strongly objects to the proposed changes to the approach given in the level 1 DORA text. Sharing of unredacted, non-anonymised data on incidents without the explicit consent of the financial entity could create material risks to the financial entity's security. We believe this approach is likely to result in far more risk to EU financial services than it mitigates, by increasing the circulation of highly sensitive information. In addition, the inclusion of not only financial authorities, but also national law enforcement agencies in the scope of sharing creates significant risk as the political and security alignment of these organisations could itself questionable. We believe that the proposed approach, if pursued, could be challenged at the highest level by some home authorities.