Frankfurt am Main,
11 September 2023

BVI[1] position on the ESAs' Consultation Paper 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

We take the opportunity to present our views on the consultation paper of the ESAs related to 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.

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.

☐ Yes
☒ No

In our view, the Draft RTS does not yet sufficiently consider the **proportionality principle, in particular for asset managers and investment firms providing services such as portfolio management or investment advice**. We understand that the rules of the Draft RTS have been mainly taken from the existing PSD2 reporting applying to banks whose business models are not comparable to those of asset managers and that provide critical IT infrastructure and are also subject to the NIS2 Directive. There are currently no requirements or guidelines on ICT incident reporting for asset managers or investment firms at European level. **We therefore request reviewing the Draft RTS whether the proposed rules are really suitable for asset managers and investment firms in particular or whether further exceptions are necessary here.**

In particular, we miss an explicit reference in Article 8 of the Draft RTS to the definition of major ICT-related incident (cf. Art. 3(10) DORA Regulation), which only refers to an incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity. It is our understanding that the current classification proposed in the Draft RTS captures all incidents, including those that impact systems that do not support critical and important functions. In our view, therefore, it is not enough to simply exceed the thresholds or determine whether certain conditions are met; the incidents must also still actually affect systems that support critical and important functions. **The Draft RTS, in particular Articles 6 and 8, should therefore be adapted accordingly.**

Moreover, from a practical perspective, the option of deciding between percentage and absolute thresholds appears particularly problematic in the case of thresholds. The question here is whether the ESAs base their classification on the threat to (parts of) the financial system or on the threat to the function of individual market participants. In the case of the former, absolute thresholds would be appropriate, which would then also have to be set correspondingly high. Smaller institutions would then be less likely to report a serious incident. For the latter, percentage thresholds would be appropriate.

[1] BVI represents the interests of the German fund industry at national and international level. The association promotes sensible regulation of the fund business as well as fair competition vis-à-vis policy makers and regulators. Asset managers act as trustees in the sole interest of the investor and are subject to strict regulation. Funds match funding investors and the capital demands of companies and governments, thus fulfilling an important macro-economic function. BVI's 116 members manage assets of some EUR 4 trillion for retail investors, insurance companies, pension and retirement schemes, banks, churches and foundations. With a share of 28%, Germany represents the largest fund market in the EU. BVI's ID number in the EU Transparency Register is 96816064173-47. For more information, please visit www.bvi.de/en.

BVI
Bundesverband Investment und Asset Management e.V.

Contact
Phone +49 69 15 40 90 0
www.bvi.de

BVI Berlin
Unter den Linden 42
10117 Berlin

BVI Brussels
Rue Belliard 15–17
1040 Bruxelles

BVI Frankfurt
Bockenheimer Anlage 15
60322 Frankfurt am Main

Executive Board
Thomas Richter CEO
Rudolf Siebel MD

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.

☐ Yes
☒ No

As mentioned in our answer to Q1, **we miss a reference to the adverse negative impact on network and information systems which support critical and important functions**. Therefore, the number of 'clients, financial counterparts and transactions' must only be related to those services where disruptions to systems affect critical and important functions.

Additionally, we strongly disagree with the proposal to assess the potential impact of the incident on market efficiency (cf. Article 1(3) of the Draft RTS). This should be deleted because such an impact is not required as a criterion for classification in Article 18 of the DORA Regulation either part of the definition of a major ICT related incident in Article 3(10) of the DORA Regulation. In particular, the definition of a major ICT related incident only refers to the impact on the network and information systems of the financial entity and not to the impact on market efficiency. Moreover, at the current stage, we do not have any information on the effort that such impact entail in practical implementation. In any case, such a proposal is not practicable with regard to the procurement of (external) data and the associated costs.

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.

☐ Yes
☒ No

- **Reputational impact (Articles 2 and 10 of the Draft RTS)**

We understand that the criterion on whether the ICT-related incident has caused reputational impact is already required in Article 18(1)(a) of the DORA regulation and must therefore considered. However, in our view, the reputational risk should be treated differently from the other criteria because of the time aspect in the event of an incident. As a rule, companies start the risk assessment of an incident immediately after knowing about the incident. Thus, in the event that the incident does not immediately meet the description of reputational impact proposed by the ESAs, one would conclude that reputation has not suffered as a result of the incident. However, to the extent that the case would become public, for example, four weeks after a risk assessment was completed, and the company would suffer significant reputational damage in the aftermath, the question arises as to whether a risk assessment would need to be conducted again, combined with a re-examination of all other criteria. This would cause considerable additional effort on behalf of the financial entity and may be accompanied by additional reporting obligations to the supervisory authority. **Therefore, we suggest treating the reputational risk as a separate independent criterion, apart from the question of whether it is a primary or secondary criterion. Article 8 of the Draft RTS should therefore be adapted accordingly.**

In this context, the proposed criteria in **Article 2 of the Draft RTS** also have different time components. On the one hand, a media event should already have attracted attention (letter (a) of Article 2 of the

Draft RTS). On the other hand, it should suffice as a criterion that the company first anticipates whether there is a probability of losing clients in the event of an incident (letter (d) of Article 2 of the Draft RTS). The latter point in particular is difficult to implement and evaluate in practice.

Moreover, we disagree with the suggestions made for defining the reputational impact in **Article 2 of the Draft RTS**. Reputational risk is defined neither in the AIFMD, UCITS Directive nor in the IFD, although it is to be considered as part of the operational risks in the risk management process. However, asset managers and investment firms have their own discretion to define and monitor this accordingly on the basis of their risk and business strategy. Therefore, the criteria for the reputational impact should also not be set too narrowly in the Draft RTS. This applies all the more as this is combined with the proposed requirement in Article 10 of the Draft RTS that any reputational impact defined in Article 2 of the Draft RTS should lead to a major incident.

In particular, we understand the criterion 'reputational impact' in the way that a certain circumstance must have a direct impact on the financial entity. Media attention or complaints from clients alone is not sufficient here. Rather, this must then also be linked to the impact on the company. For example, certain successful cyberattacks in the banking sector may be reported in the media, but this would then possibly have no consequence for the specific company. We therefore suggest linking the 'impact' (e.g., the concrete effect on the company's business) to the individual criteria.

We therefore suggest at least amending **Article 2 of the Draft RTS** as follows:

Article 2

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

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

a) The incident has attracted **national** media attention~~; or~~ **with an adverse significant impact on the financial entities' business as a result of the incident; or**

b) The financial entity has received complaints from different clients or financial counterparts~~; or~~ **with an adverse significant impact on the financial entities' business as a result of the incident.**

~~c) The financial entity will not be able to or is likely not to be able to meet regulatory requirements; or~~

~~d) The financial entity is likely to lose clients or financial counterparts with an impact on its business as a result of the incident.~~

- **Duration and service downtime (Articles 3 and 11 of the Draft RTS)**

In general, we agree with the assumption to refer to the service downtime and to the duration of the incident. **However, we strongly disagree with the proposed thresholds in Article 11 of the Draft RTS for the duration of the incident (no longer than 24 hours) and the service downtime (no longer than 2 hours) because these thresholds are based on business models of banks with time-critical services.**

Asset managers and investment firms do not provide time-critical services. They regularly base their processes on a tolerable downtime of 24 to 48 hours, as the business model of asset managers does not involve direct, mass transactions in a few seconds, as is the case with payment services, for example. Therefore, the proposed two-hour limit as downtime for services supporting critical functions and the 24-hour limit as duration of the incident is not appropriate because these limits will always lead to a

report by asset managers and investment firms, even though there is no major ICT incident at all. **Here, too, an increase in the limits (e.g., 72 hours for the duration of the incident and 24 to 48 hours for the service downtime) or a gradation (for example, based on the outcome of the business impact analyses of Article 11(5) of the DORA Regulation and depending on the extent of the ICT risk), is needed in line with the principle of proportionality.**

- **Geographical spread (Articles 4 and 12 of the Draft RTS)**

According to Article 18(1)(c) of the DORA Regulation, the geographical spread should be considered with regard to the areas affected by the ICT-related incident, particularly if it affects **more than two Member States. We therefore disagree to reduce this Level 1 requirement to at least two Member states in Article 4 of the Draft RTS.**

We also see disadvantages here for companies that operate across borders due to their group structure. This is because they will regularly meet this criterion, regardless of whether the incident actually has an impact outside the group in several countries.

- **Economic impact (Articles 7 and 15 of the Draft RTS)**

We understand the problems of the ESAs to set a relative threshold for the economic impact on each financial entity because of the differences of business models and own capital requirements. However, the amount of 100,000 EUR for determining the level of economic impact as an absolute threshold appears too low insofar as consulting costs (including costs related to legal advice, forensic services, and remediation measures) are to be included here. These costs in particular can regularly exceed 100,000 EUR, even for small and medium-sized companies. **We therefore propose to delete this cost item or to set a higher level of the absolute threshold (at least 1 million EUR).**

The BVI has been offering to its members an industry-wide data bank for operational risks ('BVI OpRisk loss data bank') since 2004. It helps asset managers to become aware of risks that they might not be able to identify on the basis of their own data alone. The database collects claims arising from asset manager loss risks that may result from inadequate internal processes and from human or system failure at the fund company or from external events. Included are legal, documentation and reputational risks as well as risks resulting from the trading, settlement and valuation processes operated for a fund. Currently, 39 companies with assets under management of 1.8 trillion euros in mutual and special funds are participating. This corresponds to a market share of 74 percent in terms of funds launched in Germany (as of December 31, 2022). According to our BVI OpRisk loss data bank, the **average figure per damage is around 75,000 euros in the period 2012 to 2022**. However, these damages do not include consulting costs (including costs related to legal advice, forensic services, and remediation measures).

Moreover, we kindly ask to review the proposed criteria for the economic impact on whether the proposed rules are really suitable for all financial entities in view of applying the proportionality principle or whether further exceptions are necessary here. In principle, such cost estimation can also be performed and documented by small financial entities or for financial entities with a limited ICT structure and a lower ICT risk profile. However, here too, weaker requirements should be defined for these financial entities, as they generally have less budget available for the calculation of such major ICT incidents compared to large companies in the financial sector which are being part of the critical IT infrastructure and are also subject to the NIS2 Directive.

Moreover, for us it is not clear how the requirements listed in Article 7 of the Draft RTS on the direct and indirect costs and losses of ICT incidents relate to the requirements under **Article 11(10) and (11) of the DORA Regulation** on the aggregate annual costs and losses to be estimated from major ICT-related incidents, which are still to be developed in the second batch of DORA policy products. According to Article 11(10) of the DORA Regulation, financial entities shall report to the competent authorities, upon their request, an estimation of aggregated annual costs and losses **caused by major ICT-related incidents.** As we understand it, a mere estimate is sufficient here, whereas under the new proposal, specific cost items are to be identified and aggregated for the mere assessment of the existence of a major ICT incident. There is therefore a contradiction of values here.

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.

☒ Yes
☐ No

In general, we agree with the proposed approach to capture data losses even if this will lead to own assessments and interpretations made by the financial entities. However, these rules (Article 13 of the Draft RTS) should only be applied if data losses of network and information systems are involved that support critical and important functions. Therefore, we refer to our answer to Q1.

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.

☐ Yes
☒ No

We strongly disagree with the approach proposed under Articles 6 and 14 of the Draft RTS. In particular, Article 6 of the Draft RTS should be replaced with a reference to the definition of major ICT-related incidents provided under the DORA Regulation and a more principle-based approach. The proposed approach is significantly at odds with the definition of significant ICT incidents in point 10 of Article 3 of the DORA Regulation, the principles-based approach of DORA in defining critical and important functions in point 22 of Article 3 of the DORA Regulation, and the solutions proposed to date by the ESAs for dealing with the assessment of critical and important functions in other Level 2 frameworks currently under consultation. We therefore expressly oppose the introduction of new definitions or criteria for when a critical or important function exists.

As mentioned in our answer to Q1, the definition of major ICT-related incident (cf. Art. 3(10) DORA Regulation) only refers to an incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity. It is therefore essential whether the functions are performed at all by means of network and information systems. This may well be relevant to all activities for banks that have been subject to PSD2 reporting to date. However, this does not apply equally to other financial companies that have different business models.

Financial entities should therefore assess the critical services affected by the incidents only for incidents with an impact on network and information systems that support critical and important functions of the financial entity. This assessment should be made on their own discretion and business impact considering the underlying ICT structure and ICT risks for the performance of the activities. We thus disagree with the ESAs' proposal to classify all authorised activities as critical. This is because, particularly

in the asset managers' business models, there are some activities that are not performed at all or only with the help of a small ICT infrastructure (e.g., activities related to the purchase and sale of alternative assets, which are typically not handled via IT systems but via contract negotiations and entries in registers with notarised contracts; or investment advice as a MiFID service). Therefore, to classify these as critical per se is too broad.

Therefore, Article 6 of the Draft RTS should be amended at least as follows:

> Article 6
> Classification criterion 'Critical services affected' in accordance with Article 18(1)(e) of Regulation (EU) 2022/2554
>
> For the purpose of determining the criticality of the services affected, including the financial entity's transactions and operations, financial entities shall assess whether the incident has ~~**affected services or activities that require authorisation, or ICT services**~~ **a high adverse impact on the network and information systems** that support critical or important functions of the financial entity. **Financial entities should assess the critical services affected by the incidents referred to in sentence 1 based on their own discretion and business impact considering their underlying ICT structure and ICT risks for the performance of the activities.**

However, we agree with the proposal in **Article 14 of the Draft RTS** that an assessment of a major ICT related incident should also depend on whether the incident has been escalated to the senior management or the management body of the financial entity according to internal policies, and that such escalation is different to and is to be distinguished from regular reporting.

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).

☐ Yes
☒ No

We object to the approach in Article 16 of the Draft RTS of including recurring incidents (which in aggregate meet the materiality thresholds only over a certain period of time) in the consideration of material incidents for the following reasons:

- There is already a lack of legal basis. Recurring incidents are not covered by Article 18(1) of the DORA Regulation as a criterion for the classification of ICT incidents. Similarly, recurring incidents are not covered by the mandate to the ESAs to further specify these criteria for the classification in Art. 18(3) DORA. Nor can such a recurring event be derived from the definition of ICT-related incident in point 8 of Article 3 of the DORA Regulation. Rather, only a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems and have an adverse impact on the availability, authenticity, integrity, or confidentiality of data, or on the services provided by the financial entity are covered there. This is not comparable with the proposed recurring incidents which should occur at least twice, have the same apparent root cause and shall be with similar nature and impact.

- For practical implementation, it is not entirely trivial to assess how the recurring events in their entirety reach the materiality thresholds after the last event. For this purpose, each (minor) incident would have to be comprehensively documented according to which criteria/thresholds are fulfilled/not fulfilled in order to then enable an overall view after a certain period of time on recurring events. Such a far-reaching documentation obligation for non-major incidents cannot be derived from Level 1. To do this, companies would have to set up a completely new process that would pool far-reaching resources. This is all the truer as the financial entities would then have to check at least every three months (or longer period of time) whether recurring cases occur in total.

- There is also the question of whether the results of such analyses actually lead to the financial entity having to file a report. We have no data on recurring incidents. In view of the consultation taking place over the summer break, it was not possible for our members to analyse a comprehensive analysis of past (non-major) incidents over the past two years using the new proposed primary and secondary criteria. However, according to an evaluation of our BVI-OpRisk claims database, technically induced business interruptions have not had much practical relevance in the past. In the last two years, our members have reported a total of two cases. Here, other events like internal criminal acts (e.g., falsification of documents) and errors in process management process (e.g., errors in recording & processing such as input, booking errors, faulty data quality and program errors) predominate.

- Based on the proposal in Article 16 of the Draft RTS, there are also still many open questions as to how the recurring incidents should be assessed and reviewed in practice. For example, should the regular review be carried out on a rolling basis or on each reporting date? What are incidents with 'the same apparent root cause' and 'with similar nature and impact'? Which values should be aggregated in concrete terms? We see problems here, especially with comparable incidents, if the same client group is repeatedly affected. In this case, offsetting makes no sense at all.

- Should the ESAs continue to adhere to taking recurrent incidents into account as well, there is an urgent need to apply the proportionality principle. Here it would be helpful, within the framework of the proportionality principle, to make it easier to assess recurring cases (or even to refrain from doing so altogether), depending on whether the financial entity itself uses a comprehensive ICT structure, the extent of its ICT risk, as well as the nature of the documented data.

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.

☐ Yes
☒ No

We understand the criteria in **Article 17 of the Draft RTS** to be relevant to the financial entity's assessment of whether or not a cyber threat is significant. In our view, this assessment specified in Article 18(2) of the DORA Regulation must be carried out in every case, regardless of whether the financial entity then voluntarily reports a significant cyber threat under Article 19(2) of the DORA Regulation or not. Against this background, we consider the requirements for the assessment to be too far-reaching and too burdensome because financial entities are regularly not equipped with experts who could foresee and assess novel cyber threats. Moreover, it is not clear whether the cyber threat should be assessed on the basis of an abstract or rather concrete danger to the individual financial entity. After all, this is precisely why they use certain software to ward off any threats. This applies in particular to the evaluation of the impact on other financial entities or other third-party providers and to the proposed

assessment whether the cyber threat could fulfil the conditions set out in Article 8 of the Draft RTS if it materialises (cf., Article 17(1)(c) of the Draft RTS). In particular, the latter requirement would mean that every threat would have to be examined for the primary and secondary criteria. We consider this to be too formalistic and far-reaching. A more pragmatic approach should be adopted here.

We therefore request that the ESAs adhere exclusively to the criteria set forth in Article 18(2) of the DORA Regulation. These include only the criticality of the services at risk (including the transactions and operations of the financial entity), the number and/or relevance of the financial clients or counterparties affected, and the geographic spread of the risk areas. The geographic spread should therefore also be treated uniformly in the Draft RTS.

When assessing significant cyber threats, our members have expressed a desire to be guided by the situation reports of ENISA, national offices (e.g., BSI) or the outcome of their firewalls rather than conducting their own extensive analyses. In particular, the requirements should not require financial entities to make special inquiries of their clients and business partners about the attackers or the impact of the threats. In this context, it is practically impossible to assess the capabilities and intentions of an attacker. This requirement should also be deleted (cf. Article 17(2)(b) of the Draft RTS).

We therefore suggest amending Article 17 of the Draft RTS at least as follows:

Article 17

Criteria and high materiality thresholds for determining significant cyber threats

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

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

☒ Yes
☐ No

Regarding the relevance of major incidents to competent authorities in other Member States (**Article 18 of the Draft RTS**), we refer to our answer to Q3.

The majority of our members are in favour of non-anonymised disclosure of reported ICT incidents within the authorities and thus support the proposals of the ESAs (cf. **Article 19 of the Draft RTS**).

However, in doing so, we assume that the authorities also meet high ICT security standards so as not to be exposed to targeted cyberattacks themselves and thus risk data loss.

****