Frankfurt,
11 March 2024

BVI[1] position paper on ESA's recommendations on the first set of rules under DORA for ICT and third-party risk management and incident classification

The three European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) published in January 2024 the first set of final draft technical standards under the DORA aimed at enhancing the digital operational resilience of the EU financial sector by strengthening financial entities' Information and Communication Technology (ICT) and third-party risk management and incident reporting frameworks. There have been significant changes compared to the consultation process. Nevertheless, we still have concerns about the final recommendations and the following suggestions for improvement:

I. Principle of proportionality

In the final recommendations, the ESAs use different terms and criteria for the application of the proportionality principle. This can lead to the principle of proportionality being interpreted and applied differently in the respective regulatory measures. However, this is not in line with the requirements of Article 4 of the DORA Regulation. Although the proposals contain elements for assessing proportionality, they do not uniformly explain which legal consequences result from this. We therefore suggest, at least, to implement the following clear statement in the first Articles of each RTS based on the wording in Article 4 of the DORA Regulation such as:

"Considering the wide variety of financial entities covered by Regulation (EU) 2022/2554 regarding their size, overall risk profile, the nature, scale and complexity of their services, activities and operations, as specifically provided for in this Regulation, financial entities should apply the requirements defined in this Regulation in a proportionate manner, taking into account the increased or reduced elements of complexity or the overall risk profile."

Proportionality can also be implemented, for example, through the granularity of requirements, the frequency of updates, a risk-based approach (i.e., the smaller the company, the more focus on higher risks), the granularity of process descriptions or the frequency of training or reviews of policies. For example, one principle-based approach could be that financial entities with a small number of employees or without a large ICT infrastructure could be obliged to set up such detailed processes only for ICT services supporting critical and important functions. It is also conceivable to use the annual value budgeted by the company for IT expenses (e.g., on a five-year basis) as a benchmark. Moreover, the proportionality principle should not only be based on size, but also on the potential eco-nomic damage that can occur due to ICT incidents.

[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 114 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 27%, 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

II. Concerns about the development of further guidelines by the ESAs

According to the final recommendations, the ESAs should be able to consider developing further guidance in the areas that have been removed from the consultation proposals due to the lack of an explicit mandate at Level 1 in the DORA Regulation. This applies to, for example, the final RTS on ICT risk management framework on Governance. We are very concerned about this approach because it explicitly undermines the mandates developed in the DORA Regulation for the ESAs to act. This can also lead to the already high level of detail in the rules being increased even further.

III. Specific proposed amendments in the respective RTS drafts

We have the following specific proposals for amendments to the individual RTS proposals:

1) RTS on ICT risk management framework and on simplified ICT risk management framework

Segregated and independent internal audit function (Article 28(4) and (5) of the draft RTS): Article 28(4) of the Draft RTS which requires an appropriate segregation and independence of control functions and internal audit functions for financial entities applying the simplified ICT risk management framework should be deleted. According to Article 24 of the Delegated Regulation (EU) 2017/565 with reference to Article 16(5) of Directive 2014/65/EU) and in view of the proportionality principle, investment firms are not obliged to implement a segregated and independent internal audit function. Financial entities subject to the simplified risk management framework should therefore only be required to perform specific internal audits where applicable, only to the extent that they actually have an internal audit function. (cf. Article 28(5) of the draft RTS).

This applies all the more as the simplified ICT risk management framework of Article 16 of the DORA Regulation does not contain an obligation comparable to Article 6(6) of the DORA Regulation applying to all other financial entities to review the ICT risk management by the internal audit. The ESAs' reference in their feedback statement to the application of Article 6(6) of the DORA Regulation independently of the MiFID also to the simplified ICT risk management framework therefore is contrary to applicable law. Such an obligation should not be introduced under DORA Level 2 either. Otherwise, small investment firms would only be obliged to introduce an internal audit function for the purposes of ICT risk management and to organise audits for this purpose. This does not appear proportional.

2) RTS on criteria for the classification of ICT-related incidents

a) **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 providing services such as portfolio management odr investment advice 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, 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.**

b) **We object to the approach in Article 15 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 major ICT-related incidents:** 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 ICT-related incidents cannot be derived from Level 1. To do this, financial entities 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 month whether it is a recurring incident (cf. the new approach under Article 15(2) of the draft RTS. **Should the Commission continue to adhere to taking recurrent incidents into account as well, there is an urgent need to replace the proposed monthly inspection obligation with an event-driven inspection obligation in Article 15(2) of the draft RTS.**

c) **Classification criterion 'Clients, financial counterparts and transactions' (Article 1 and 9 of the draft RTS):** We ask the EU Commission to clarify what is meant by the term 'clients' in the asset management sector. The term 'clients' is only used here in formal legal terms when asset managers carry out MiFID-relevant activities (outside the fund business). In their core competence of fund management, there are no clients, only investors. In practice, an ICT-related incident could also affect investors of an investment fund. However, the number of investors is generally not known to asset managers, particularly in the mutual fund sector (only the number of units held by investors). The 'number of clients' criterion is therefore difficult to assess in the asset management sector if investors are also taken into account here. We therefore propose the following clarification (e.g. via a recital):

   'In the case of investment funds, under the criterion 'clients, financial counterparts and transactions' the diversity of investment funds' structures must be taken into account as well as the difficulty to identify the ultimate beneficiaries. Insofar as the number of investors of the managed investment funds affected by an ICT-related incident is known or can be estimated by the asset manager as a financial entity, these are to be understood as clients within the meaning of this criterion. If the asset

manager has delegated functions such as portfolio or risk management to a third party, the third party is deemed to be one client without having to look through to the fund's underlying investors.'

3) RTS on ICT TPP policy

a) **Proportionality principle:** We request that the approach to applying the principle of proportionality contained in recital 4 be transferred directly to Article 1 of the draft RTS. In this respect, we refer to our comments under I. above.

b) **Subcontracting**: We suggest that **recital 6 and Article 4 of the draft RTS** be critically reviewed and adapted in terms of what rules the DORA Regulation provides for dealing with subcontractors. The requirements for subcontractors should not be too high. Instead, we suggest that this RTS should only stipulate that the policy should set requirements for dealing with subcontractors based on Article 30(2)(a) of the DORA Regulation and in accordance with the internal processes defined and contractual arrangements agreed. In concrete terms, this means that the policy only needs to state rules on whether the subcontracting of ICT services that support critical and important functions or essential parts thereof is permitted and - if this is the case - which conditions then should apply to this subcontracting.

4) ITS on the register of information

a) **Proportionality**: Even though the ESAs have significantly adapted the requirements for the scope and content of the information register, these are still very demanding overall and cannot be easily implemented without technical support. This leads to additional costs, particularly for smaller financial entities, which could have been significantly reduced through proposals with simpler structures for the register. In this respect, we refer to our comments under I. above.

b) **Subcontracting**: **We still consider the documentation requirements for subcontractors to be far too extensive. According to drafted template RT.05.02, the register should also list all subcontractors that effectively underpin the provision of these ICT services, i.e. all the subcontractors providing ICT services whose disruption would impair the security or the continuity of the service provision**. We recognise that the addition of the criterion of a disruption that would impair the security or the continuity of the service provision should in principle make things easier. In practice, however, this would lead to additional burden, because in addition to the question of whether the service of the subcontractor supports critical and important functions, all subcontractors would then also have to be analysed and delimited in terms of the criterion of impairment of security and continuity of service provision. However, as there is usually no direct contractual relationship with the subcontractor, such documentation and assessment by the financial entity is not possible. We therefore request that at least this addition be deleted.

Moreover, we suggest that the general necessity of documenting contracts with subcontractors on the basis of the Level 1 regulations be reviewed once again. Such an approach is not required in Article 28(3) of the DORA Regulations which limits the information of the register to all contractual arrangements on the use of ICT services provided by ICT third-party service providers on the first level without sub-contractors. If the EU legislator had wanted to include information about subcontractors, it would have explicitly mentioned them, as it has done elsewhere in the DORA regulation (such as Article 29(2) of the DORA Regulation).