Frankfurt,
4 March 2024

BVI[1] Position on the ESAs' Consultation paper on Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents

We take the opportunity to present our views on the consultation paper of the ESAs related on Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents.

***Question 1**: Do you agree with paragraph 7 and 9 of the Guidelines on the assessment of gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.*

No. We do not agree with paragraph 7 and 9 of the drafted Guidelines on the assessment of gross and net costs and losses. In principle, we agree that the guidelines should not be considered in isolation from the other DORA requirements for the classification of major ICT-related incidents, considering the economic impact of the incident (Article 18(1)(f) DORA Regulation), and the final report submitted to the relevant competent authority (Article 19(4)(c) DORA Regulation). However, in contrast to Article 11(10) and (11) DORA Regulation, Article 18(1)(f) DORA Regulation explicitly addresses direct and indirect costs on an absolute and relative basis at Level 1. The proposed approach with a breakdown by gross costs and losses, the financial recoveries and the net costs and losses of each major ICT-related incidents based on the (validated) financial statements such as the profit and loss account of the relevant accounting year goes far beyond the requirements of Level 1 in Article 11(10) of the DORA Regulation and the mandate of the ESAs in Article 11(11) of the DORA Regulation which requires a mere estimation of aggregated annual costs and losses caused by major ICT-related incidents. Rather, we have the impression that this breakdown is intended to provide concrete evidence for the supervisory authority as to which costs have actually been incurred. However, the actual impact figures, which are to replace the estimates, are only to be submitted in the final report within the meaning of Art. 19(4)(c) of the DORA Regulation.

In general, we see the annual cost estimate as an instrument of ICT risk management, which is also systematically integrated in Chapter II, Section II of the DORA Regulation under the processes for ICT risk management. Such costs and losses are considered in existing asset management practices and due to sector-specific supervisory requirements, in the assessment of material operational risks on the basis of a plausibility check. The new detailed proposal would therefore lead to two procedures being required in future: one based on plausibilisation (on an annual/quarterly basis) and one based on the detailed breakdown (with different calculation periods if the financial year is not the calendar year). This leads to an additional expense for asset managers and investment firms which, in our view, is contrary to the purpose of the provision, namely, to submit the statement only on request to the supervisory

[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

authority. Against this background, **it should be sufficient to state the cost estimate on a purely net basis (possibly also per incident)**.

This is not the only reason why we do not share the ESAs' impact assessment that the breakdown into gross/net costs and financial recoveries would not result in any additional material burden (since the raw data will already exist in a disaggregated form in the final report and these gross and net costs and financial recoveries could be used here). The ESAs themselves make it clear elsewhere in the consultation paper (cf. paragraph 22, page 9) that the values proposed for the purpose of annual estimates may well deviate from the reported data in the final report within the meaning of Art. 19(4)(c) of the DORA Regulation. This means that financial entities cannot therefore use data that is already available. Irrespective of this, the final report for a major ICT-related incident may also be submitted at a later date, meaning that the data for the annual estimate should certainly be available earlier. We therefore ask the ESAs to minimise the effort involved in this annual cost estimate.

***Question 2**: Do you agree with paragraphs 5, 6 and 8 of the Guidelines on the specification of the one-year period, the incidents to include in the aggregation and the base of information for the estimation of the aggregated annual gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.*

No. We do not agree with paragraphs 5, 6 and 8 of the drafted Guidelines on the specification of the one-year period according to which the reference period should be the completed accounting year. In practice, the company's financial year may differ from the calendar year. As mentioned above in our answer to question 1, asset managers already carry out quarterly and annual cost estimates on a calendar year basis for the purposes of the risk management process. In practice, this would therefore result in additional work for companies with a different accounting year, as they would then have to calculate and estimate costs once on a calendar year basis and then again on an accounting year basis. **We therefore propose to base the estimates on the calendar year. Irrespective of this, we have no further objections to the proposals as to which cases should be included in the cost estimate.**

***Question 3**: Do you agree with paragraph 10 and 11 and the annex of the Guidelines on the reporting of annual costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.*

No. We refer to our answers to questions 1 and 2, with which we reject the proposed detailed statement of costs and losses. A template is generally helpful in practice. However, this should be reduced to a mere net cost statement (possibly also per incident).

****