Frankfurt am Main,
5 March 2021

Preliminary BVI[1] position on a Proposal for a Regulation on the digital operational resilience of the financial sector (DORA) accompanied by a Directive

An important initiative that we fully support: the entire financial market will be significantly influenced by the increased availability of data, algorithms, the digitalisation of assets, new processes in custody and settlement, and reporting. The proposal for a Regulation on the digital operational resilience of the financial sector (DORA) accompanied by a Directive is an essential core element to deal with ICT related risks across sectors on EU level. The German supervisory authority BaFin has already provided guidance on this topic, in particular, in the area of cyber security in the internal governance processes. We therefore very welcome the aim of mitigation risks of digital transformation by strict and common rules on digital operational resilience to ensure a safe financial system across sectors in the EU.

Expansion of the scope of application: according to the Commission's objective, all financial entities should be covered by the scope of application. A minimum standard for all financial market participants is indispensable to make financial markets resistant to possible ICT security breaches. Nevertheless, certain market players are lacking and we propose the following improvements:

- **Providers of indices**: In Article 2(1) of the drafted DORA providers of indices should be added. Moreover, we propose to include amendments of the Regulation (EU) 2016/1011 (BMR) in such a way that these entities should be required to establish, implement and maintain organisational processes on ICT risks, including ICT business continuity and disaster recovery plans established in accordance with DORA.

- **Trading venues**: According to Article 2(1)(h) of the drafted DORA, trading venues should be included in the scope of DORA. However, we miss amendments on organisational requirements on ICT risks in the Directive 2014/65/EU (MiFID) or Regulation (EU) No 600/2014 (MiFIR) that regulated markets, systematic internalisers, multilateral trading facilities (MTF), and organised trading facilities (OTF) should be required to establish, implement and maintain organisational processes in ICT risks, including ICT business continuity and disaster recovery plans established in accordance with DORA.

- **Amendments to the CRD (Article 5(2), (3), (4), (5), (6) of the drafted Directive):** it seems that there is an editorial mistake that the references to Article 16, 17, 19 et seq. CRD should be amendments to MiFID and not of the CRD. In any case, investment firms are now excluded from the scope of the CRD. They have their own set of rules and regulations under the new Directive (EU) 2019/2034 on the prudential supervision of investment firms (IFD), which is why the IFD should be supplemented accordingly with organisational requirements on ICT risks and references to DORA. Therefore, the proposed amendments to Directive 2013/36/EU (CRD) in Article 5 of the new drafted Directive regarding investment firms should be reviewed.

[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 more than 3.6 trillion euros 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 du Trône 14–16
1000 Bruxelles

BVI Frankfurt
Bockenheimer Anlage 15
60322 Frankfurt am Main

Executive Board
Thomas Richter CEO
Rudolf Siebel MD

- **Regulators**: Also, national competent authorities, central banks and EU supervisory authorities should be subject to comparable minimum standards on ICT risk management and cyber risks as they extensively exchange data of supervised entities. For instance, the latest hacking of the ECB and certain national authorities revealed the potential vulnerabilities of securities regulators themselves – which might ultimately also harm market participants, and the whole financial system.

- **Article 2(1) of the draft DORA**: For reasons of better regulation, we propose to amend Article 2(1) of the draft DORA by references to certain EU legislation. For example: Article 2(1)(k) should not only mean 'management companies". A better approach would be 'management companies and self-managed UCITS investment companies within the meaning of Directive 2009/65/EC and managers of alternative investment funds as defined in Article 4(1)(b) of Directive 2011/61/EU.

- **ICT third-party service providers:** As certain financial entities such as stock exchanges, CRAs and index providers also offer ICT services, they should be also qualified as ICT third-party service providers. We therefore propose to clarify that the definition of ICT third-party service providers in Article 3(15) of the drafted DORA also includes financial entities in the meaning of Article 2(1) when they provide these services. Moreover, the financial industry is at risk of serious data losses in the event of contractual disputes. DORA needs to cover ICT providers in the narrow e.g. (hardware, software, cloud, IT infrastructure providers) as well in a wider sense (electronic automated data sources such as exchanges, index providers, rating agencies, research and analytic firms) and (market) data distributors (MDD) such as Bloomberg, Refinitiv, Factset. Without secure access to their data and services, operational resilience of financial services in general and in specific cases also financial stability is at risk. E.g. in 2017 S&P ordered a data cut-off in the Bloomberg TOMS system at two banks in Europe which interrupted their trading operations without proper warning. Only because of luck, a flash crash in the market was avoided at the time when the banks trades could not be completed. The importance of exchanges as ICT providers can be seen by looking at Deutsche Börse Group. In 2020 two exchange outages not only prevented equity and derivative trading for several hours at the Frankfurt venue. Also, the Vienna, Prague, Budapest, Zagbreb, Ljubljana, Sofia and Valleta exchanges went down, all of which also use the Deutsche Börse trading system. **Therefore, operational resilience needs to be defined widely, encompassing not only ICT risk, human errors, but also contractual disputes with ICT providers. Data cut before proper dispute resolution needs to be avoided at all cost. We interpret the current proposal in this direction, according to which all types of breaches of contract are to be covered, including all other types of intentional or non-intentional events. An explicit clarification in this sense would nevertheless be desirable.**

Contractual arrangements vs. outsourcing of ICT services: We see the need to improve the proposed requirements on contractual arrangements in the context of scope and the interrelationship between the sector-specific delegation rules and the new DORA proposals to cover activities provided by ITC third-party providers as follows:

- **Contractual arrangements on the use of ICT services (Article 26 and 27 of the legislative DORA proposal):** With respect to enforcement a direct application of the DORA rules applicable to ICT third-party providers is preferable to the indirect application (Article 26 and 27) through inclusion of specific DORA obligations in the contracts with EU financial entities. We do not necessarily argue for the full regulation of all activities of an ICT third-party provider like a financial entity but only for the direct application of the applicable DORA rules to ICT third-party providers. This is

similar to the situation of a listed company which while in general being subject only to corporate law, still needs to abide by specific financial services rules e.g. on listing or ad hoc reporting which are supervised and enforced by NCAs. The current DORA contract-based approach simply results in less enforcement as contract-based DORA obligations can be enforced only by civil law courts adjudicating on a contract dispute between an EU financial entity and an ICT third-party provider in or outside the EU. As many ICT providers are based in third countries, e.g. the US, the DORA related provisions in the ICT contract may never be enforced at all, as legal action is too expensive vs the value of the contract. For example, a rating data feed from a US rating agency could be priced at USD 20,000 p.a. These kind of CRA contract would usually also provide for application of US law. The legal costs in the US are simply too high to sue for such a small contract value.

- **Contractual arrangements vs. outsourcing:** As we understand the legislative DORA proposal the scope is limited to require the content of key contractual provisions between financial entities and ICT third-party providers without any statement if and to what extent such an agreement qualifies as outsourcing. We therefore suggest deleting the wording '*outsourcing'* or '*sub-outsourcing*' in the legislative DORA proposal (such as the headline of Article 26, Article 31(1)(d)(iii) of the legislative DORA proposal).

- **Relationship between the ESAs guidelines on outsourcing and DORA (recital 28):** The legislative DORA proposal addresses the topic of outsourcing and refers in ***Recital 28*** to the existing EBA guidelines on outsourcing, which are to (continue to) be authoritative in the relationship between supervised financial entities and ICT service providers. We do not consider this approach to be compatible with the aim to establish uniform rules in the EU on ICT governance. This applies even more as EIOPA and ESMA also established guidelines on cloud outsourcing which are based on the EBA guidelines but differ in certain points (such as the content of contractual agreements between financial entities and cloud service providers) and do not allow a common understanding across sectors. In maintaining a guideline-based approach, we see the danger that the previous guidelines of the ESAs are not (any longer) consistent with the new requirements of the new EU Regulation, in particular with the new key contractual provisions of Article 27 of the legislative DORA proposal.

  This may also lead to the continued existence of different supervisory approaches to assessing the commissioning of an ICT service as outsourcing or third-party procurement of services in the areas of securities, banking or insurance supervision. This risk is increased by the fact that according to the legislative DORA proposal, the ICT service providers commissioned by the financial undertakings are to be obliged to lay down contractual rules on the commissioning of further third parties. If the ICT service provider is a critical provider, the responsible lead supervisor (i.e. EBA, EIOPA or ESMA) should then have certain rights, e.g. to issue uniform recommendations to review these agreements or '***sub-outsourcing'***. In our view, this will lead to further fragmentation of the existing supervisory rules in the area of ICT outsourcing. **Therefore, we suggest that clear criteria for the relationship between outsourcing and mere commissioning (external procurement) of ICT service providers should be defined in the DORA Regulation for all supervised entities to achieve a broad common understanding and practice in the European financial markets. However, the application of the delegation rules should then be part of the sector-specific rules such as the AIFMD or UCITS Directive.**

Exit strategies (Article 25(9) and 27(2)(k) of the legislative DORA proposal): in the asset management, ICT services are regularly provided by a limited group of data providers and vendors. Therefore, the proposed exit strategies required in Article 25 (9) of the DORA proposal are inappropriate as long as only one ICT service provider is able to provide the services needed. Identifying alternative solutions could be very difficult or would involve high costs and burden. Moreover, assets managers at the beginning of the ICT contractual relationship cannot address all the risks that may emerge at the level of ICT third-party service provider. Thus, an exit strategy capability must be clearly outlined within contract. However, exit plans or even exit strategy formalisations must be proposed only with a risk-based approach in Article 25(9) of the DORA proposal. It is necessary to amend Article 27(2)(k) of the legislative DORA proposal to provide for a minimum period (e.g. three years or until the date of the first-instance court/arbitration ruling) for the transitional period to be contractually agreed in the exit strategy. In any case, we suggest an appropriate transition period in order to adapt existing ICT contracts to the new minimum standards in the Regulation, or to find a replacement service provider if the previous contracting parties (e.g. third countries providers) do not accept such an adjustment. Workable solutions must also be found if no other provider is available.

Reporting: Notification of major security incidents and exchange of information: The new requirement to notify major security incidents can be very useful as long as there is an exchange of information between the supervised entities and supervisory authorities which are also collecting other cyber risk incident notifications other than from AM companies (e.g. under the NIS directive or the European Critical Infrastructure directive). It would be desirable for all financial market participants to have access to all cyber-relevant information and to exchange information on security incidents, regardless of their affiliation to a particular regulatory regime.

Specific supervisory rules for critical ICT service providers: The proposed process to identify critical ICT service providers by different EU authorities (such as EBA, ESMA or EIOPA depending on the proportion of activity provided by the ICT entity in the banking, insurance or securities sector) seems very complex and not appropriate in an interconnected financial market. This can lead to a situation that different lead supervisors are responsible for a specific critical ICT service provider (e.g. Bloomberg). Furthermore, the selection of only one ESA as lead supervisor carries the risk that sector-specific business models, which are not regularly supervised by this authority, may not be adequately considered. We suggest that a committee with representatives of all sectors - like ESA Joint Committee - should be responsible. We advise against a general ban of using critical ICT service providers established in a third country as it is stated in Article 28(9) of the DORA proposal. It should be possible to conclude a contract with those providers if they have an EU branch.

Proportionality principle: If the detailed DORA requirements on ICT governance and risk management are part of the sector-specific organisation requirements which already base on principle-based requirements (including applying the proportionality principle), we do not see the need to legally state additional rules on that principle. However, it could be helpful to amend ***Recital 20*** of the drafted DORA that a proportionate application of the requirements is not only limited to financial entities which are micro enterprises as defined in Commission Recommendation 2003/361/EC. The new rules applicable to all financial entities should be tailored to risks and needs of their specific characteristics in terms of their size and business profiles.

****