Frankfurt am Main,
11 September 2023

BVI[1] position on ESA's Consultation Paper on draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554

We take the opportunity to present our views on the consultation paper of the ESAs related to Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554.

Q1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear? If not, please provide your reasoning and suggested changes.

☐ Yes
☒ No

- **Article 1 of the Draft RTS (complexity and risk considerations)**

We strongly disagree with the approach on complexity and risk considerations addressed in Article 1 of the Draft RTS. The proposed approach in Article 1 of the Draft RTS leads to the fact that all requirements specified in Articles 3 to 11 of the Draft RTS must be implemented in every financial entity without any gradation. This approach does not allow the application of the principle of proportionality, which according to Articles 4(1) and 28(10) of the DORA Regulation should be explicitly considered in the preparation of the draft RTS. Article 28(10) of the DORA Regulation requires the ESAs, when developing those draft regulatory technical standards, to take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations.

We recognise that the DORA Regulation establishes for the first time the requirement to also maintain a policy on the use of ICT services to support critical and important functions, however, neither the DORA Regulation itself nor the ESMA guidelines on cloud outsourcing currently require such detailed information. According to guideline 1, paragraph 12, of ESMA's guidelines, a firm (such as an asset manager) should only have a defined and up-to-date cloud outsourcing strategy that is consistent with the firm's relevant strategies and internal policies and processes, including in relation to information and communication technology, information security, and operational risk management. In particular, we do not currently understand why asset managers need to document much more information in their policies than ESMA requires in its cloud outsourcing guidelines. In particular, we cannot identify any ICT risk that has increased in the area of asset managers since the ESMA guidelines were issued and is now supposed to justify such extended requirements. At this point, we once again expressly oppose passing on the strict requirements developed by the EBA in the banking sector for banks and critical

[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

ICT infrastructure to all financial entities. This is disproportionate, is neither necessary nor does it result from the DORA regulation. Rather, we see this as an over-stepping of ESA's powers in establishing standards for the policy.

Not only in Germany, but also in the EU there is a very **heterogeneous structure of asset managers** which manage collective investment undertakings investing in securities or alternative assets such as real estate with significant differences in their size (with a workforce of less than 50 up to more than 1,000 employees), business models, and the type and number of arrangements with ICT third-party service providers supporting critical and importing functions. Managing real assets (e.g., real estate) is much less susceptible to ICT risks, since both the asset and the proof of ownership are not digital. Therefore, the characteristics of their ICT structure and ICT (concentration) risks depends mainly on their business models and interfaces to other business partners, brokers, ICT providers or other entities within the same group. This also applies to **investment firms** providing MiFID services such as portfolio management or investment advice, even if they do not qualify as small-sized investment firms in the sense of Article 16(1) of the DORA Regulation and therefore also required to implement such a policy. This must be considered in the requirements for the content of the policy on the use of ICT services supporting critical or important functions.

In addition, the proposed process in the Draft RTS is long and cumbersome, especially for smaller ICT arrangements supporting critical and important functions. In particular, the specified monitoring of ICT service providers and the associated documentation has the consequence that the involvement of ICT service providers would no longer mean any relief for the asset managers. The measures suggest that the financial entity cannot pass on any responsibility for a service provided to an ICT service provider. Due to the commissioning, the responsibility definitely always lies with the financial entity up to a certain point. However, an asset manager also delegates an activity to the ICT service provider for the reason that it does not have the (technical) expertise and/or human resources internally to perform the service itself. In our opinion, therefore, the measures should be weakened so that the financial entity continues to have the option of also handing over the associated responsibility for service provision to the ICT service provider.

Therefore, we suggest a graduated approach based on the proportionality principle and request that Article 1 of the Draft ITS be amended as follows:

'Article 1
~~Complexity and risk considerations~~ Proportionality principle

Financial entities shall comply with the requirements of the Articles 3 to 11 to the extent that this appears necessary under the principle of proportionality in order to comply with the statutory obligations under paragraph 2 of Article 28 of Regulation (EU) 2022/2554. The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers **shall be consistent with the financial entities' relevant strategies and internal policies and processes, and** shall take into account, for the purpose of Articles 3 to 11, elements of **the proportionality principle, including the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, the overall complexity of the use of ICT services, ~~increased complexity or risk,~~** including elements relating to the location of the ICT third-party service provider **~~or its parent company~~**, the nature of data shared with the ICT third-party service providers, the location of data processing and storage, whether the ICT third-party service providers are part of the same group of the financial entity and the potential impact of the related risks and disruptions on the continuity and availability of the financial entity's activities.'

- **Structure and content of the Draft RTS**

Irrespective of the implementation of the proportionality principle, the **structure of the proposed Draft RTS** is not readily apparent to the user at first glance. Rather, we consider the structure (in combination with the content) far too complex to implement the requirements adequately even in smaller companies. For example, Article 3 of the Draft RTS governs both the content of the policy and general governance requirements. In the other Articles 4 – 11 of the Draft RTS, it is also not always clear whether the requirements are intended to specify the content of the policy or rather to establish general governance rules. In addition, the relationship of the governance requirements in Article 3 of the draft RTS to Article 4 of the draft RTS with further rules on relations with ICT providers, also with sub-contractors, is also not clear.

Moreover, different terms such as 'the policy shall ensure', 'the policy shall require', 'the policy shall explicitly specify', 'the policy shall specify' should be avoided. For practical purposes, it would be considerably easier if the draft RTS first listed in a separate article all the relevant points that should be included in a policy for every financial entity. A gradation could then be made so that, if necessary, additional minimum content or requirements are defined for financial entities with, for example, a particularly large number of ICT contracts that support critical and important functions, and additionally increased concentration risk (measured by the financial entities' own internal outcome in accordance with Article 29 of the DORA Regulation). In this context, it should be clarified that the use of ICT third-party providers in third countries is not risky per se, but that a risk analysis is necessary for this - as for all other providers.

Moreover, we also consider the **contents** of the individual requirements in Articles 3 to 11 of the Draft RTS for the policy to be too far-reaching, especially to the extent that individual processes are specified here for which no further Level 2 measures are to be required under the DORA Regulation (e.g., due diligence, conflicts of interests, monitoring). There should be more flexibility here, also in line with the contractual agreements, the ESMA guidelines on cloud outsourcing and the Level 1 requirements. The content of the policy should rather be consistent with the financial entities' relevant strategies and internal policies and processes, based on the minimum requirements for contractual agreements in Article 30 DORA Regulation, as these requirements apply equally to all financial companies.

For these reasons, we therefore suggest a fundamental revision of the draft RTS.

- **Article 2 (group application)**

We request the ESAs that Article 2 of the Draft RTS on the application of the policy on use of ICT services supporting critical or important functions provided by ICT third-party service providers on a (sub-) consolidated basis be deleted. The further specification on the application of the policy at group level is not part of the mandate given to the ESAs for the establishment of Level 2 measures in Article 28(10) of the DORA Regulation. Rather, the mandate is limited only to the content of the policy. The fact that this policy is also to be applied on a consolidated basis already follows from Level 1 in Article 28(2) DORA Regulation.

Irrespective of this, the nature and manner of governance rules on a consolidated or sub-consolidated basis is already derived from prudential regulations (such as Article 109 CRD IV), which also incorporates the requirements of the DORA Regulation through the DORA Directive (EU) 2022/2556 (for example, Article 4(2) DORA Directive with amendments in Article 74(1) CRD IV, to which group consolidation in Article 109 CRD IV also refers). Thereafter, parent undertakings must ensure that the arrangements, procedures, and mechanisms (including the policy to be addressed herein) at the group level are consistent and well-integrated and that all data and information relevant to supervision can be provided.

However, we understand the current proposal of Article 2 of the Draft RTS to mean that a policy developed for the parent undertaking (e.g., a bank) based on its individual ICT risk situation may need to be implemented equally across the group for each subsidiary and entity. This is far too far-reaching and does not comply with the requirements of the DORA Regulation, in particular, in cases where the subsidiary as a financial entity is itself in scope of the DORA Regulation which explicitly allows the application of the proportionality principle for affected financial entities (e.g., asset managers as subsidiaries of a banking group). This therefore means that a subsidiary without a significant ICT structure or due to its business models does not have to implement the requirements of the parent policy on a 1:1 basis. The latter only has to ensure consistent implementation on group level.

Q2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?

☐ Yes
☒ No

In general, we request the ESAs to explicitly review **Article 3 of the draft RTS** again to check if the requirements stated there are indeed in line with the mandate in Article 28(10) DORA Regulation. This is because according to the requirements of the DORA Regulation, only the contents of the policy and not further governance rules for the financial undertakings are to be defined. The governance rules are already derived from the DORA Regulation alone or from the sector-specific requirements of the financial undertakings, without there being mandates to the ESAs to create further detailed rules. The DORA Regulation as such is already very challenging and should therefore not be further overloaded with non-required and possibly duplicated requirements. In particular, this applies to the following proposed requirements:

- The proposal in **Article 3(1) of the draft RTS to consider a multi-vendor strategy** in any case also in the policy goes beyond the requirements in Article 6(9) of the DORA Regulation. According to this, there is precisely no obligation to do so. Rather, financial entities may, in the context of their digital operational resilience strategy, define a holistic ICT multi-vendor strategy, at group or entity level.

- An **annual review obligation** proposed by the ESAs in **Article 3(2) of the Draft RTS** goes too far, in particular for smaller financial entities or entities with a lower ICT structure and is no longer covered by the mandate for a draft RTS. Here, the wording should remain at level 1 in Article 28(2) of the DORA Regulation ('regularly'), which offers more flexibility, especially for smaller financial entities without large ICT structure.

- The proposal in **Article 3(5) of the draft RTS** cannot in fact be fulfilled in practice or will present many financial entities with an almost impossible requirement. Thereafter, the policy shall foresee that the financial entity assesses **that the ICT third party service provider has sufficient resources to ensure that the financial entity complies with all its legal and regulatory requirements**. It is not clear here what sufficient resources at the ICT provider should have to do with the financial company being able to fulfil its own legal requirements. In practise, the financial company can only be obliged to carefully select the ICT provider and to monitor the tasks performed within the framework of the contract. At most, it can be required here to assess that the ICT provider has sufficient resources to fulfil the contractually assured tasks. Furthermore, the interaction of the explanations in paragraph 10 of the consultation paper (page 5), Article 4 of the Draft RTS (which also includes subcontractors) and the further due diligence requirements in Article 7 RTS is confusing and not comprehensible for practical application. Duplication should be avoided.

- With the wording **'*the policy shall ensure*'** (e.g., Article 3(7) of the Draft RTS) it is also unclear what this should mean for practice. The financial company itself can only set up measures and procedures to ensure that certain requirements are met. A policy as such cannot do that. If the proposed regulation means that the policy should set out requirements for this, then this should also be explicitly stated as such.

- **Article 3(8) of the Draft RTS** with further requirements for internal auditing should be critically reviewed again to see whether the requirements stated there are consistent with those in Article 28(6) of the DORA Regulation.

- **Article 3(9) of the Draft RTS** with further requirements for relevant contractual arrangements should be critically reviewed again to see whether the requirements stated there are consistent with those in Article 28 of the DORA Regulation.

Q3: Is article 4 appropriate and sufficiently clear?

☐ Yes
☒ No

We suggest that **Article 4 of the Draft RTS** be critically reviewed and, if necessary, adapted in terms of what information financial entities must keep in the register of information and 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 in accordance with the internal processes defined and contractual arrangements agreed. At this point, we are particularly opposed to having to provide detailed information on the respective subcontractor and refer in this respect to our comments on the ITS draft on an information register.

Q4: Is article 5 appropriate and sufficiently clear?

☐ Yes
☒ No

Here too, we consider the requirements in **Article 5 of the Draft RTS on the main phases of the life cycle for the use of ICT services supporting critical or important functions provided by ICT third-party service provider** to be far too detailed and no longer compatible with the principle of proportionality. Here, it should be sufficient to simply state this point, where relevant, as an additional rule only applicable to financial entities such as banks with a critical ICT structure as it is required by the EBA in its outsourcing guidelines, but to leave that topic on the own discretion (including the concrete implementation) of other financial entities. This would also be in line with the ESMA guidelines on cloud outsourcing that do not require such rules for asset managers or investment firms.

Q5: Are articles 6 and 7 appropriate and sufficiently clear?

☐ Yes
☒ No

Here too, we consider the requirements, in particular, in **Article 7 of the Draft RTS on due diligence** to be far too detailed and no longer compatible with the principle of proportionality. Here, it should be sufficient to simply state this point as relevant to the content of the policy, but to leave the concrete implementation to the companies themselves. This would also be in line with the ESMA guidelines on cloud outsourcing and the sector-specific rules under the AIFMD and UCITS Directive as well as MiFID II. For asset managers and investment firms in particular, the requirements should be reduced to the minimum set out by ESMA in its cloud outsourcing guidelines (cf. Guideline 2). At this point, we once again expressly oppose passing on the strict requirements developed by the EBA in the banking sector for banks and critical ICT infrastructure to all financial entities. This is dis-proportionate, is neither necessary nor does it result from the DORA regulation. Rather, we see this as an over-stepping of ESA's powers in establishing standards for the policy.

Q6: Is article 8 appropriate and sufficiently clear?

☐ Yes
☒ No

We request the ESAs that Article 8 of the Draft RTS on conflict of interests be deleted. The conflict-of-interest management of asset managers and investment firms is already regulated independently of the DORA Regulation in the UCITS Directive, the AIFM Directive and the MiFID. Due to the changes made to these framework Directives by the DORA Directive (EU) 2022/2556 (cf., Articles 1, 3 and 5 DORA Directive), conflicts of interest resulting from the use of ICT services are also explicitly considered here. Companies must already develop their own policies for this in accordance with the sector-specific requirements. We therefore consider it an unnecessary duplication of regulations to document the handling of conflicts of interest arising from any ICT contracts again separately in an additional policy. This is especially true as the DORA Regulation does not address the issue of conflicts of interest at all. Instead, Article 1 of the draft RTS should stipulate that the policy on the use of ICT services is in line with the other policies and procedures of the financial entity. In this respect, we refer to our answer to question 1.

Moreover, Article 8(2) of the Draft RTS states that if ICT services are provided by intra-group ICT service providers, the policy must specify the conditions under which ICT services supporting critical or important functions must be offered at an independent price (on an **'arm's length' basis**). 'Arm's length,' in our view, refers to a business relationship in which the prices and terms are structured as if the parties involved were independent companies, to ensure that there are no unfair advantages or disadvantages due to group structures. In this context, it therefore means that the prices for intra-group ICT services must be in line with market prices as if the services were purchased from external third parties in order to ensure fair valuation and avoid potential conflicts of interest. In the not unusual case that the intra-group ICT service provider charges higher prices (which sometimes correspond to the cost price), this would nevertheless possibly contradict the idea of 'arm's length' and the requirements described in Article 8(2) of the Draft RTS. From our point of view, it should be taken into account at this point that if higher prices for intra-group services are based on a justifiable and traceable expense that has actually been incurred, and these higher prices are in line with standard industry practices and market conditions, this is not considered to contradict the idea of 'arm's length'. Accordingly, it should be possible to deviate from the 'arm's length" conditions, provided that this is shown by comprehensible cost calculations/calculations. Therefore, also this proposed restriction goes well beyond the issue of 'conflicts of interest' and partly concerns interference in business decisions, so that this Article would be contrary to a free market economy.

Q7: Is article 9 appropriate and sufficiently clear?

☐ Yes
☒ No

Here too, we consider the requirements in **Article 9 of the Draft RTS on contractual clauses for the use of ICT services supporting critical or important functions** to be far too detailed and no longer compatible with the principle of proportionality. Here, it should be sufficient to simply state this point as relevant to the content of the policy, but to leave the concrete implementation to the financial entities themselves. This is all the truer as the DORA Regulation now defines concrete requirements for the minimum content of contracts for the first time. Therefore, there is no need to transfer the requirements previously laid down in the EBA or ESMA guidelines in this regard to the RTS.

Therefore, **Article 9(2) of the Draft RTS** should be deleted because it creates double regulation and is superfluous, as the minimum requirements for contract content are already laid down in Article 30 of the DORA Regulation. It then follows from this which minimum contract content must be stated in the policy.

Moreover, **Article 9(3) of the Draft RTS** is also far too far-reaching and will lead to an enormous new implementation effort for asset managers and investment firms. We suggest deleting this paragraph because it is in no way derived from the DORA Regulation that financial entities should also check any certificates of ICT service providers or that ICT service providers should hold such certificates in a binding manner. For example, in practice there may be different agreements on who selects the certifier (the financial entity or the ICT service provider) and what specific requirements should be placed on a suitable third-party certifier who would carry out the verification of ICT services and controls. Rather, the way control measures are to be carried out should be at the discretion of financial entities and should be carried out depending on their own risk assessments. This is how we currently understand the requirements at Level 1 in the DORA Regulation. The requirements set out here go far beyond this and would no longer allow for flexible solutions in practice, especially for smaller ICT arrangements supporting critical and important functions without any or a lower concentration risk at financial entity level. At the very least, paragraph 3 should be open in the sense of the proportionality principle so that there is no obligation, but the policy ‘may’ (but does not have to) provide rules on this. This would also be in line with the ESMA guidelines on cloud outsourcing.

Q8: Is article 10 appropriate and sufficiently clear?

☐ Yes
☒ No

Here too, we consider the requirements in **Article 10 of the Draft RTS on monitoring of the contractual arrangements for the use of ICT services supporting critical or important functions** to be far too detailed and no longer compatible with the principle of proportionality. In particular, the requirements for the monitoring process are already comprehensively set out in Article 30(3)(e) of the DORA Regulation. Here it should be sufficient to refer to this provision than to redefine these processes with different wording and content.

Q9: Is article 11 appropriate and sufficiently clear?

☐ Yes
☒ No

Here too, we consider the requirements in **Article 11 of the Draft RTS on exit and termination of contractual arrangements for the use of ICT services supporting critical or important functions** to be far too detailed and no longer compatible with the principle of proportionality. In particular, the requirements for the exit-strategies are already comprehensively set out in Article 30(3)(f) of the DORA Regulation. Here it should be sufficient to refer to this provision than to redefine these processes with different wording and content.

****