Frankfurt am Main,
11 September 2023

BVI[1] position on ESA's Consultation Paper on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of 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 further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554 (DORA Regulation).

General drafting principles

Q1: Do you agree with the approach followed to incorporate proportionality in the RTS based on Article 15 of DORA (Title I of the proposed RTS) and in particular its Article 29 (Complexity and risks considerations)? If not, please provide detailed justifications and alternative wording as needed.

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 taken from existing rules for insurance companies or 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, for example (cf., paragraph 3 of the consultation paper). Apart from the ESMA guidelines on outsourcing to cloud service providers, there are currently no further-reaching requirements or guidelines on ICT risk management for asset managers at European level. However, it must be noted that the applicable sector-specific requirements of asset managers set by the AIFMD and the UCITS Directive already contain overarching requirements on risk management that also cover ICT and cybersecurity risk (cf., outcome of the Joint Advice of the ESAs to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector). Moreover, BaFin published a circular with supervisory requirements for IT in German asset managers ('Kapitalverwaltungsaufsichtliche Anforderungen an die IT – KAIT') at the beginning of October 2019. The KAIT describe the principle-based minimum requirements which German asset managers have to meet. The processes established in the asset management sector as a result should therefore in principle also be taken into account in the future Level 2 measures and can continue to be used. **We therefore expressly 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.**

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) and business models. 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

[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

characteristics of their ICT structure and ICT 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 cannot make use of the simplified ICT risk management framework. This must be considered in the requirements for the respective internal processes in dealing with ICT and risk assessment.

We also support the approach that small and medium-sized enterprises must have minimum requirements for the operational resilience of their ICT systems. Nevertheless, there should be more flexibility in implementation of the Level 2 requirements, as is also provided for in Article 4(2) DORA Regulation. In particular, Article 7(a) of the DORA Regulation states that the ICT systems, protocols, and tools are appropriate to the magnitude of operations supporting the conduct of activities of the financial entities, in accordance with the proportionality principle as referred to in Article 4 of the DORA Regulation. Moreover, it must be considered that the DORA requirements on ICT governance and risk management are also part of the sector-specific organisation requirements of the AIFMD and UCITS Directive (cf., Articles 1 and 3 of the DORA Directive (EU) 2022/2556) which already set principle-based requirements (including applying the proportionality principle). This flexible approach should not be undermined by too high a level of detail at level 2. **Therefore, we call for a principle-based approach together with an amendment of the proposed Article 29 of the Draft RTS dealing with the principle of proportionality. 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.**

Proportionality can be implemented, for example, through the **granularity of requirements in guidelines**, 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. In Germany, the supervisory authority BaFin currently does not include specific criteria as to when a financial entity with a small number of employees or without a large IT infrastructure is deemed to exist. This should be retained. However, if it is nevertheless desired to apply concrete criteria for the proportionality principle, these could be derived from the ESMA Guidelines on Remuneration Practices (ESMA/2013/232) under the AIFMD for the establishment of a remuneration committee (see paragraph 53 et seq.).

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 economic damage that can occur due to ICT incidents**.

The proposed **Article 29 of the Draft RTS** does not do justice to the principle of proportionality because it only refers to elements of increased complexity or risk. We therefore suggest, at least, amending Chapter VI to the Draft RTS as follows:

‘CHAPTER VI
PROPORTIONALITY PRINCIPLE
Article 29
~~**Complexity and risk considerations**~~
Proportionality principle

Financial entities shall comply with the requirements of the Articles 1 to 28 to the extent that this appears necessary under the principle of proportionality in order to comply with the statutory obligations under Article 15 of Regulation (EU) 2022/2554. For the purposes of defining and implementing ICT risk management tools, methods, processes and policies referred to in Articles 1 to 28 elements of **the proportionality principle shall be taken into account, including the size, the nature, scale and complexity of services, activities and operations, the overall complexity of the ICT architecture, the share of the ICT services used,** increased complexity or risk ~~**shall be taken into account**~~, including elements relating to encryption and cryptography, ICT operations security, network security, ICT project and change management, and the potential impact of the ICT risk on confidentiality, integrity and availability of data, and **the number of material changes within the ICT environment over the last five years, and elements** of the disruptions on the continuity and availability of the financial entity’s activities **including the number of cyberattacks and related losses over the last five years**.’

Q2: Do you agree with the approach followed for the RTS based on Article 16 of DORA (Title II of the proposed RTS)? If not, please provide an indication of further proportionality considerations, detailed justifications and alternative wording as needed.

In general, we miss a comparable Article which, as in Article 29 of the first title of the Draft RTS, emphasises the **principle of proportionality** also for the financial entities that are allowed to carry out simplified risk management. According to Article 29 of the Draft RTS, the proportionality principle should only apply to the first title (Articles 1 - 29), but not to the simplified set of rules set out in the second title (Articles 30 - 43). In particular, we do not share the ESAs' assessment during the public hearing that no further regulation would be needed for this because the simplified risk management already does not lay down such extensive rules and therefore already considers the proportionality principle.

According to **Article 4(1) of the DORA Regulation,** the proportionality principle also applies to the simplified risk management rules stated in Article 16 of the DORA Regulation. This means that also financial entities in the meaning of Article 16(1) of the DORA Regulation shall implement the simplified risk management rules in accordance with the principle of proportionality, considering their size and overall risk profile as well as the nature, scale and complexity of their services, activities and operations.

In particular, **small-sized investment firms** should not be treated equally across the board. Even the EBA regularly provides for special exceptions for investment firms with a licence for portfolio management, investment advice, reception and transmission of orders in relation to one or more financial instruments without a licence for client money access and dealing on own account under the investment firm framework (IFD/IFR). This principle should also be continued under DORA. For investment firms, the EBA has already published recommendations for a draft RTS that could be used. In it, the EBA proposes indicative measures to cover relevant ICT risks (see Art. 6(5)(b) draft RTS). The objective here relates to the assessment of when additional own capital should be held in order to reduce the likelihood of a default of an investment firm and the risk of its disorderly resolution. Nevertheless, there should be consistency in the question of when there is significant ICT risk and what kind of ICT risk management framework should be implemented.

We therefore suggest adding a new Chapter V to the Draft RTS as follows:

‘Chapter V
PROPORTIONALITY PRINCIPLE
Article 44
Proportionality Principle

Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall comply with the requirements of the Articles 30 to 43 to the extent that this appears necessary under the principle of proportionality in order to comply with the statutory obligations under Article 16 of Regulation (EU) 2022/2554. For the purposes of defining and implementing the simplified risk management framework referred to in Articles 30 to 43, elements of the proportionality principle shall be taken into account, including the size, the nature, scale and complexity of their services, activities and operations, the overall complexity of their ICT architecture, the share of their ICT services used, the potential impact of the ICT risk on confidentiality, integrity and availability of data, the number of material changes within the ICT environment over the last five years, any losses due to disruption due to incidents touching ICT services supporting critical and important functions of the financial entity over the last five years and the number of cyberattacks and related losses over the last five years.’

Moreover, clarification is needed on how to deal with **small and non-interconnected investment firms that qualify as microenterprises**. According to the general requirements of the DORA Regulation, microenterprises are exempt from the application of certain provisions of the ICT Risk Management Framework set out in Articles 6 - 11 of the DORA Regulation. However, in our view, as long as they qualify as small and non-interconnected investment firms, they should be limited to the application of the simplified risk management framework set out in Article 16 of the DORA Regulation.

Further harmonisation of ICT risk management tools, methods, processes and policies (Article 15)

ICT security policies, procedures, protocols and tools

Q3: Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.

We refer to our answer to Q1 regarding the **implementation of the proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in the ICT policies.

In particular, we believe that the requirements for ICT security policies, procedures, protocols and tools are too far-reaching for asset managers and investment firms affected. It will not be a problem to document all topics in an internal policy and guidelines. However, this must be at a scale that the financial entity can orientate itself on in its daily business and also comply with. In addition, internal resources must be created that can review the self-imposed guidelines. This does not include the annual compliance review by the internal audit. Many of the requirements that would be imposed on oneself in this context are beyond the scope of smaller financial entities or financial entities with limited ICT risks because, as mentioned in our answer to Q1, it is not classified as an entity providing critical IT infrastructure. For this reason, weakened Level 2 measures should be chosen for such entities, or the contents should be categorised by the ESAs, after which the requirements can be partially implemented by the financial entity on a voluntary basis.

We therefore suggest implementing a principle-based approach, for example as taken by ESMA in its guidelines on outsourcing to cloud service providers (cf. guideline 1 on governance, oversight and documentation).

Moreover, Article 2 of the Draft RTS should be deleted. Article 15 of the DORA Regulation does not mandate the ESAs to establish Level 2 requirements for the tasks and responsibilities of the control function referred to in Article 6(4) of the DORA Regulation. The mandate is limited to specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 9(2) of the DORA Regulation, with a view to ensuring the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delays. We therefore see Article 6(4) of the DORA Regulation as conclusive, so that financial entities are free to design their ICT risk management function within the framework of the requirements at Level 1 and are thus also subject to the proportionality principle.

In practice, this may also mean, for example, that '*appropriate segregation and independence*' according to the three lines of defence model or an internal risk management and control model (cf., Article 6(4) of the DORA Regulation) for smaller financial entities or financial entities with limited ICT risks is not to be interpreted so narrowly (e.g. that it could also be taken over by a managing director or another control function – e.g. risk controlling function – while respecting conflicts of interest).

Q4: Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.

We refer to our answers to Q1 and Q3 regarding the implementation of the **proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in the **ICT risk management** policy.

Q5: Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.

We refer to our answers to Q1 and Q3 regarding the implementation of the **proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in the **ICT asset management policy**.

Q6: Do you consider important for financial entities to keep record of the end date of the provider's support or the date of the extended support of ICT assets?

We refer to the ESMA's guidelines on outsourcing to cloud service providers (cf., guideline 1, paragraph 17, letter b) which require documentation of the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the cloud service provider and for the firm, only for arrangements which support critical or important functions. In view of the principle of proportionality, we therefore ask to limit such a documentation in the same manner for ICT assets.

Q7: Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

We refer to our answers to Q1 and Q3 regarding the implementation of the **proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in the **policy on encryption and cryptographic controls**. Asset managers, unlike the banking sector, do not have open

payment transactions, which is why further encryption is not necessary. Therefore, also in the case of group constellations, internal group communication could be exempt from possible encryption requirements (based on an internal assessment) which is why the requirements in Art. Article 6(2)(b) of the Draft RTS also seem too far-reaching to us.

Q8: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No. The control effort is already very extensive through DORA Level 1 and also addressed by the other RTS proposals. DORA's goal of strengthening the digital resilience of financial market participants should not be weakened by too high an implementation effort as well as too detailed requirements, which may provide further attack surfaces for cyber-attacks on IT systems. The proposals for a Draft RTS have a significant impact on the resources of financial entities, which are increasingly concerned with the implementation and monitoring of legal requirements, some of which offer no discernible added value.

Q9: Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.

We refer to our answers to Q1 and Q3 regarding the implementation of the **proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in the **ICT operation policies and procedures**. In particular, a distinction according to the criticality of the information to which access is available could be helpful.

Independently of this, we also have the following, not conclusive comments on the proposed Articles of the Draft RTS:

- **Article 10(2)(c) of the Draft RTS should be deleted**. According to this proposal, financial entities should ensure that ICT third-party service providers handle any vulnerabilities related to the ICT services provided to the financial entity and report them to the financial entity. In particular, financial entities shall request that ICT third-party service providers investigate the relevant vulnerabilities, determine the root cause and implement appropriate solutions. In reality, this is not possible with every service provider. Large US providers with corresponding market power are not very willing to negotiate. The companies concerned usually find out about weaknesses from the press (e.g. MSA Key Microsoft, Microsoft is not particularly transparent in its investigation). This is not necessarily reported directly by the ICT provider. We will not be able to negotiate this either.

- **Article 10(2)(d) of the Draft RTS** should be amended as follows:

  ‘(d) **~~track the usage of third-party libraries, including open source, monitoring the version and possible updates~~ include measures to adequately manage risks arising from the software supply chain;**

  The draft proposal requires a structured evaluation of a software bill of materials (SBOM) and inventory of all components and dependencies that are part of the development and delivery of software. The manufacturers/ICT service providers are already obliged to maintain an SBOM when the Cyber Resilience Act (CRA) comes into force. Accordingly, the responsibility for this should also remain with the respective manufacturers/ICT service providers and not be shifted to the users with this Article. In our view, this article is redundant with the entry into force of the CRA. Otherwise,

such requirements should only apply to companies that belong to the critical IT structure, which in any case does not include asset managers.

- **Article 10(4)(c) of the Draft RTS** is also too broad (‘*test and deploy software and hardware patch and updates in an environment, which replicates the pro-duction one, to avoid adverse consequences and disruption before their deployment to production environments’*). Of course, as a rule, the financial entity should always deploy in staging first. However, all patches and updates are considered here. In our view, after weighing up the ICT risks, deployment in production is also possible if the ICT risk/impact is low.

- According to **Article 11(2)(i) of the Draft RTS,** the identification and implementation of security measures to prevent data loss and leakage for systems and endpoint devices will be mandatory in future. We also consider this to be too far-reaching. Rather, the application of the proportionality principle would be desirable here because the implementation effort and the costs for smaller financial entities are considerable.

Q10: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No. We refer to our answer to Q8.

Q11: What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.

For this question, it would first have to be clarified what automated vulnerability scans comprise and how far this obligation should go (we refer here to our answer to Q9 regarding the application of the proportionality principle). The frequency of such scans, if necessary, should be in line with the ICT infrastructure and ICT risk profile of the financial entity. In general, our members perform scans of their servers and clients (e.g., laptops). However, these scans include scans for known viruses and malware. For example, they have deployed an EDR, which also enables to automatically isolate clients/hosts that have been infected. However, they do not use specific vulnerability scanners like Burp Suite, Tenable etc. However, they check regularly for known vulnerabilities, but the process has not been automated to this extend.

In addition, automated scanning of ICT assets involves costs and (internal) effort that increase (almost linearly) with the number of assets scanned. On the other hand, separating assets into different scan tranches (weekly / monthly) is also time-consuming. In the practice of asset managers, we currently see no uniform implementation standards for the frequency of scan intervals for all assets. Equal scan intervals can be helpful if a vulnerability found on a less critical asset allows a ‘lateral movement’ to a critical asset after a successful attack. However, this also depends to a large extent on the ICT structure.

Therefore, the proposed approach is not necessarily suitable for all ICT assets. ICT assets which are already under strained resources and bear little risks, should not be included – as this might affect other ICT objectives. So, the impact of the proposed approach would be huge and might not even be possible to fully comply to. We propose to not be too specific with regard to vulnerability scanners. It is important that there are processes and measures in place to make sure, that financial entities regularly check for vulnerabilities. Nevertheless, it should be left to the supervised financial entities how they do this.

Q12: Do you agree with the requirements already identified for cloud computing resources? Is there any additional measure or control that should be considered specifically for cloud computing resources in the RTS, beyond those already identified in Article 11(2) point (k)? If yes, please explain and provide examples.

We refer to our answer to Q8. We do not see the need for additional requirements on cloud computing resources. In our view, the ESMA's approach taken in its guidelines on cloud outsourcing should be appropriate. Therefore, it could be sufficient to limit the Level 2 requirements to a general rule that financial entities will be required to allocate sufficient resources to ensure compliance with the DORA Regulation.

Q13: Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.

We refer to our answer to Q1 and Q3 regarding the implementation of the **proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in the **network security management**.

In this context, we suggest amending Article 13 of the Draft RTS as follows:

- **Article 13(1)(b) of the Draft RTS** should be limited to critical networks and data flows as follows:

  '(b) mapping and visual representation of all the financial entity' **critical** networks and data flows;'

- Article 13(1)(c) of the Draft RTS should be graded according to the need for protection as follows:

  '(c) use of a separate and dedicated network for the administration of **critical** ICT assets and prohibition of direct internet access from and to **critical** devices or servers used for information system administration **whose risk assessment resulted in high security requirements**;'

- The frequency of review required in **Article 13(1)(h) of the Draft RTS** is not appropriate, especially for smaller companies and those without a large IT structure. The provision should therefore be deleted or, at least, adapted as follows:

  '(h) identification of the roles and responsibilities for the definition, implementation, approval, change and review of firewall rules and connections filters. Financial entities shall perform the review on a regular basis according to the classification and overall risk profile of ICT systems involved. For the ICT systems supporting critical or important functions **and if relevant changes have been made**, the financial entities shall perform this review at least every ~~six~~ **twelve** months;

Q14: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No. We refer to our answer to Q8.

Q15: Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.

We refer to our answers to Q1 and Q3 regarding the implementation of the **proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in the I**CT project and change management.**

In this context, we suggest amending Article 16 of the Draft RTS as follows:

- **Sentence 2 of Article 16(6) of the Draft RTS** should be deleted. According to this proposal, financial entities shall protect the integrity and confidentiality of data in non-production environments. However, **non-production environments** shall only store anonymised, pseudonymised or randomised production data. The latter cannot be implemented for all systems. In view of the fact that non-production environments are not publicly accessible and are secured separately, this is also not necessary. In any case, the exemption should be made if anonymised, pseudonymised or randomised data are not sufficient for testing purposes.

- According to **Article 16(9) of the Draft RTS**, the **source code** and proprietary software provided by ICT third-party service providers or coming from **open-source projects** shall be analysed and tested for vulnerabilities and for absence of malicious codes in accordance with paragraph 4 prior to the deployment in the production environment. However, the source code is usually not made available for proprietary software, so no verification can take place here. Developers regularly create forks in open-source projects. It would be much more important to implement preventive measures (such as against fork bombs and malicious forks). Therefore, Article 16(9) of the Draft RTS should be amended as follows:

  > '(9) The source code**, where available,** and proprietary software provided by ICT third-party service providers or coming from open-source projects shall be analysed and tested for vulnerabilities and for absence of malicious codes in accordance with paragraph 4 prior to the deployment in the production environment. **For open-source projects other appropriate mitigating and preventative measures could be taken into account.**'

Q16: Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.

No.

Q17: Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.

Not applicable.

Q18: Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.

We refer to our answers to Q1 and Q3 regarding the implementation of the **proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in the **physical and environmental security policy**.

Q19: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No. We refer to our answer to Q8.

Q20: Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.

We refer to our answer to Q1 regarding the implementation of the **proportionality principle** and ask for a more tailored approach, in particular, with regard to the **frequency of the programs and training**. It should be left to the companies' own decision how often they train their employees. According to the sector-specific requirements, asset managers are already required to employ sufficient personnel with the skills, knowledge and expertise necessary for discharging the responsibilities allocated to them. This also involves internal programs and training. Any kind of double regulation should be avoided.

Human resources policy and access control

Q21: Do you agree with the suggested approach on Chapter II - Human resources policy and access control? If not, please explain and provide alternative suggestion.

We refer to our answer to Q1 regarding the **implementation of the proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in the **human resources policy**.

In addition, the control effort is already very extensive through DORA Level 1 and also addressed by the Draft RTS proposals. In this context, also the proposed **Article 22(1)(e)(iv) of the Draft RTS** will have a significant impact on the resources of smaller financial entities and those without a large structure. In particular, the frequency of the review of access rights should be part of the decision of the financial entity. However, in any case, the proposed frequency of at least every six months for ITC systems supporting critical or important functions should be deleted.

Q22: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No. We refer to our answer to Q8.

ICT-related incident detection and response

Q23: Do you agree with the suggested approach regarding ICT-related incidents detection and response, in particular with respect to the criteria to trigger ICT-related incident detection and response process referred to in Article 24(5) of the proposed RTS? If not, please explain and provide alternative suggestion.

Central logging is important. However, we understand **Article 24(2) of the Draft RTS** – also in conjunction with **Article 12 of the Draft RTS** – in such a way that the use of a **SIEM/SOC solution** would be mandatory in the future. We strongly disagree with introducing mandatory requirements for the implementation and use of these special solutions such as **SIEM or SOC**. Especially for smaller companies or companies without a distinct IT structure, the effort for implementation is far too high. The running costs of a SIEM alone are >100,000 € per year. Exceptions/further gradations should also be created here. It must continue to be at the discretion of the financial entity which solutions can be used in

practice, measured against its own ICT risks profile. The Level 2 measures should therefore only prescribe the principles, but not concrete measures.

ICT business continuity management

Q24: Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.

We refer to our answer to Q1 regarding the **implementation of the proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in **the business continuity policy**.

Article 57(3) of the Delegated Regulation (EU) 231/2013 and Article 4(3) of the Delegated Directive 2010/43/EU already contain general requirements for emergency plans of asset managers. Therefore, contingency plans are already comprehensively established in practice and are geared to individual needs and business areas. The level of detail of the contents of the **business continuity policy** should therefore not go too deep, but rather be designed in a principle-based manner (e.g., at most only specify keywords for contents that should be mapped). A differentiation according to the criticality of the business processes could also be helpful.

Moreover, we are very concerned about the scope of the proposed **test of the ICT business continuity plans** in **Article 26 of the Draft RTS**. Here we see a very high implementation effort that cannot be provided with the existing manpower, especially in small and medium-sized companies.

Moreover, it is not only small and medium-sized companies that face major challenges in forcing ICT third party providers to comply with DORA. The implementation of emergency tests with SaaS providers is organisationally complex and usually not covered by old contracts, which means high costs. Facilitation (applicability, frequency, ...) would be desirable here. The testing rhythm should be based on the criticality of individual indicators. In the case of IT systems, on the need to protect information; in the case of people and buildings, on risk indicators; and likewise for service providers.

Moreover, it would be desirable to clarify the relationship between the general tests to be carried out annually under **Article 25 of the DORA Regulation** and the tests to be carried out annually under **Article 11(6) of the DORA Regulation.** Level 2 measures are to be adopted only for the latter test. For example, Article 10(1) of the DORA Regulation refers to the general tests in Article 25 of the DORA Regulation for the detection of incidents and problems, whereas Article 11(6) of the DORA Regulation does not contain a corresponding reference. In our understanding, the tests mentioned in Art. 11(6) DORA Regulation would already be the subject of the general tests in Art. 25 DORA Regulation.

Q25: Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.

Not applicable.

Report on the ICT risk management framework review

Q26: Do you agree with the suggested approach on the format and content of the report on the ICT risk management framework review? If not, please explain and provide alternative suggestion.

We refer to our answer to Q1 regarding the **implementation of the proportionality principle** and ask for a more tailored approach with regard to the granularity of requirements in **the report on the review of the ICT risk management framework**. In particular, the content of the report should be based on the company's individual processes and business activities and, at most, only provide keywords for the content to be mapped.

Moreover, it should be clarified that a report on the review of the ICT risk management framework should not be documented on a regularly basis. Hence, we understand the requirements in Article 6(5) of the DORA Regulation in such a way that the ICT risk management framework referred to in sentence 1 of Article 6(5) of the DORA Regulation shall be documented and reviewed periodically and upon the occurrence of major ICT-related incidents in compliance with supervisory instructions. However, a report only needs to be prepared if requested by the supervisory authority based on the content provided in Article 28 of the Draft RTS. Otherwise, this will lead to a bureaucratic burden without added value. This is all the more true as the Draft RTS already provides for separate review clauses for the individual rules in many places.

Moreover, Article 6(5) of the DORA Regulation does not require that the financial entity itself shall develop and provide the report to the competent authority. It is common practise that also external auditors of the annual financial statements provide reports to competent authorities to demonstrate that the legal requirements are met. Therefore, it should be also possible that the report will be established and provided by such an external auditor.

In this context, at least paragraph 1 and the introductory part of paragraph 2 of Article 28 of the Draft RTS should be amended as follows:

‘CHAPTER V
REPORT ON THE ICT RISK MANAGEMENT FRAMEWORK REVIEW
Article 28
Format and content

1. ~~**Financial entities shall develop and document the**~~ **The** report referred to in Article 6(5) **sentence 3** of Regulation (EU) 2022/2554 **shall be developed upon request of the competent authority and documented** in a searchable electronic format.
2. ~~**Financial entities**~~ **The report referred to in paragraph 1** shall include all of the following information in the report: […]’

Simplified ICT risk management framework

Simplified ICT risk management framework

Q27: Do you agree with the suggested approach regarding the simplified ICT risk management framework? If not, please explain and provide alternative drafting as necessary.

In principle, we agree with the proposed approach, provided that a new Article on the **principle of proportionality** is added. We refer to our proposal and answer to Q2.

Moreover, we see a particular need for additional improvement to the following aspects:

- **Segregated and independent internal audit function (cf. Article 30(4) of the Draft RTS)**

Article 30(4) of the Draft RTS which requires an appropriate segregation and independence of control functions and internal audit functions 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. 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. Such an obligation should therefore not be introduced under DORA Level 2 either.

- **ICT risk mitigation strategies** (cf. Article 33(1)(c) of the Draft RTS)

We ask that Article 33(1)(c) of the Draft RTS be amended as follows:

> ‘c) define mitigation strategies at least for ~~**the**~~ **major** ICT risk**, where necessary** ~~**that are not within the risk tolerance levels of the financial entity**~~;’

The simplified ICT risk management framework set out in Article 16 of the DORA regulation does not contain an obligation comparable to Article 6(8)(b) of the DORA Regulation applying to all other financial entities to establish a risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity and analysing the impact tolerance for ICT disruptions. Therefore, mitigation strategies of financial entities in the meaning of Article 16(1) of the DORA Regulation should be limited to major ICT risk, where necessary in view of the proportionality principle.

Further elements of systems, protocols, and tools to minimise the impact of ICT risk

Q28: Do you agree with the suggested approach regarding the further elements of systems, protocols, and tools to minimise the impact of ICT risk under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.

In principle, we agree with the proposed approach, provided that a new Article on the **principle of proportionality** is added. We refer to our proposal and answer to Q2.

Q29: What would be the impact for financial entities to expand the ICT operation security requirements for all ICT assets? Please provide details and if possible, quantitative data.

We request the ESAs to adhere to the principle of proportionality. This is not satisfied, if the ICT operation security requirements are extended to all ICT assets. We recommend to take into account classification and risk profile.

Q30: Are there any additional measures or control that should be considered specifically for cloud resources in the draft RTS, beyond those already identified in Article 37(2)(h) of the proposed draft RTS? If yes, please explain and provide examples.

We do not see the need for further requirements on cloud computing resources. In our view, the proposal is in line with the ESMA cloud outsourcing guidelines (cf. guideline 4, paragraph 30 letter b) which state that strong authentication mechanisms (for example multi-factor authentication) and access controls are in place with a view to prevent unauthorised access to the firm's data and back-end cloud resources.

ICT business continuity management

Q31: Do you agree with the suggested approach regarding ICT business continuity management under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.

In principle, we agree with the proposed approach, provided that a new Article on the **principle of proportionality** is added. We refer to our proposal and answer to Q2.

Report on the ICT risk management framework review

Q32: Do you agree with the suggested approach regarding the article on Format and content of the report on the simplified ICT risk management review? If not, please explain and provide alternative suggestion as necessary.

First of all, it should be clarified that a **report on the review of the simplified ICT risk management framework should not be documented on a regularly basis**. Hence, we understand the requirements in Article 16(2) of the DORA Regulation in such a way that the ICT risk management framework referred to in paragraph 1, second subparagraph, point (a) of Article 16 of the DORA Regulation shall be documented and reviewed periodically and upon the occurrence of major ICT-related incidents in compliance with supervisory instructions. However, a report only needs to be prepared if requested by the supervisory authority based on the content provided in Article 43 of the Draft RTS. Otherwise, this will lead to a bureaucratic burden without added value.

Moreover, Article 16(2) of the DORA Regulation does not require that the financial entity in the meaning of Article 16(1) of the DORA Regulation shall develop and provide the report to the competent authority. It is common practise that also **external auditors of the annual financial statements** provide reports to competent authorities to demonstrate that the legal requirements are met. Therefore, it should be also possible that the report will be established and provided by such an external auditor.

Furthermore, in view of the principle of proportionality, the **list of changes** which were done in the reported area should be limited to major changes (cf. **Article 43(2)(a)(iv) of the Draft RTS**). It is not appropriate that the requirements for simplified ICT risk management are more stringent than in the report for the other financial undertakings, which are only required to document major changes in the report (cf. Article 28(2)(f) of the Draft RTS).

In this context, we ask that paragraph 1, the introductory part of paragraph 2 and point (iv) of letter (a) of paragraph 2 of Article 43 of the Draft RTS be amended as follows:

‘CHAPTER IV
REPORT ON THE REVIEW OF THE ICT RMF
Article 43
Format and content

1. ~~**Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop and document t**~~**T**he report referred to in Article 16(2) **sentence 2** of Regulation (EU) 2022/2554 **shall be developed upon request of the competent authority and documented** in a searchable electronic format.

2. ~~**Financial entities**~~ **The report** referred to in paragraph 1 shall include the following information ~~**in the report**~~:

(a) […]
(i) […]
(iv) provides list of **major** changes which were done in the reported area;
(v) […]

****