EFAMA
European Fund and Asset Management Association

# CONSULTATION RESPONSE

Brussels, 11 September 2023

## EFAMA RESPONSE TO THE CONSULTATION PAPER ON DRAFT REGULATORY TECHNICAL STANDARDS TO FURTHER HARMONISE ICT RISK MANAGEMENT TOOLS, METHODS, PROCESSES AND POLICIES AS MANDATED UNDER ARTICLE 15 AND 16(3) OF REGULATION (EU) 2022/2554.

### General remarks

EFAMA welcomes the launch by the ESAs of the first batch of public consultations on the level 2 legislation under DORA[1]. Due to their number and detailed scope they will be an important element of the new EU framework on digital operational resilience. They would also highly influence the amount of work that each financial entity would have to carry out while implementing new rules ahead of 17 January 2025.

While we also welcome that the authorities have envisaged a period of almost three months for market participants to submit their comments, we believe that the timing of the consultations will not work in favour of their outcome. The period of summer holidays is very challenging when it comes to gathering detailed feedback and analysis, in particular on topics as technical as these. Having four drafts simultaneously under consultation also impedes due consideration being given to all the details, in particular on drafts as elaborate as the ones concerning the risk management framework, or the register on contractual arrangements.

We are aware of the tight deadlines established in DORA for the submission of drafts by the ESAs to the European Commission. At the same time, we are of the opinion that it is in the common interest and power of those institutions to secure a timeframe which would favour best outcome of the process, including thought through views provided by all stakeholders. This should be taken more comprehensively into account when drafting provisions of the level 1 acts, as well as when scheduling future public consultations.

In reference to the 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[2] (Draft RTS), we would like to draw the ESAs attention in particular to the proper incorporation of the proportionality principle. As it is directly provided in DORA for the purposes of risk management framework,

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance).
[2] ESAs, 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.



Rue Marie-Thérèse 11 | B-1000 Bruxelles | T +32 2 513 39 69 | info@efama.org | www.efama.org | EU transparency register: 3373670692-24

we believe that it should be taken into account comprehensively not only as a general rule of the Draft RTS, but also be embedded in the detailed provisions on particular elements of the risk management framework and simplified risk management framework. Only under such circumstances can the Draft RTS be suitable for the wide range of entities that are in scope of art. 15 and 16 of DORA.

## Response to the ESAs' Questionnaire

### 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.**

EFAMA does not agree with the way the proportionality principle has been incorporated in the RTS based on art. 15 of DORA, as in our opinion it has not been taken into account comprehensively.

According to art. 4(1) of DORA on proportionality principle, rules on ICT risk management should be implemented considering the entity's "*(…) size and overall risk profile, and the nature, scale, and complexity of their services, activities and operations*." As DORA does not specify these considerations further, it could result both in the implementation of enhanced or simplified rules. On the contrary, art. 29 of the Draft RTS allows only for "*(…) elements of increased complexity or risk (…)*" to be taken into account. This does not address issues of smaller entities with a lower risk profile, where the nature, scale and complexity of their services, activities and operations would favour a less restrictive approach. Given the broad scope of DORA, which according to art. 2(1) includes entities ranging from credit and payment institutions to management companies and managers of alternative investment funds (AIFs), as well as others, a near "one size fits all" approach seems erroneous and excessive. Moreover, it does not take into account the risk assessment and appetite of the entity, which are also important elements of proportionality and risk management that should be acknowledged in the area of ICT services.

In particular, the level of control seems too high for management companies and managers of AIFs, as well as investment firms providing services such as portfolio management or investment advice which do not qualify as small-sized investment firms. These would not benefit from the simplified ICT risk management framework under art. 16(1) of DORA. These entities differ significantly from insurance companies or banks, which provide critical IT infrastructure and are subject to the NIS2 Directive[3] (whose standard of ICT risk management was clearly a benchmark for this Draft RTS). Asset managers do not require the same level of scrutiny, as currently their only requirements regarding ICT services derive from the ESMA Guidelines on outsourcing to cloud service providers (ESMA Guidelines)[4]. Moreover, also among asset managers, their structure, size and business models vary significantly, ranging from companies with a workforce of less than 50 employees to up to more than 1000. For most of them implementation of the Draft RTS in its current form would be excessively costly and burdensome, going beyond what is necessary according to their risk profile.

The Draft RTS does not incorporate the proportionality principle sufficiently also due to its prescriptiveness. The proposed provisions are so detailed that they do not leave any room for the entities to assess whether all elements of the framework should be implemented in their situation and according to their business model. This is contrary to what was prescribed in art. 7(a) of DORA which requires the ICT systems, protocols and tools to be "*appropriate to the magnitude of operations supporting the conduct of their*

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
[4] ESMA, Guidelines On outsourcing to cloud service providers, 10 May 2021.

*activities, in accordance with the proportionality principle as referred to in Article 4*". Examples of these excessive obligations are further discussed for example in answers to questions no. 4, 9, 13 and 15 below. The provisions of the Draft RTS are also too detailed to be implemented on a group level.

Therefore, we suggest that art. 29 of the Draft RTS should allow also for elements such as smaller size, decreased complexity, criticality of systems and functions, as well as the risk assessment and the entity's risk appetite to be taken into account when implementing the risk management framework.

We would also suggest reviewing the Draft RTS to assess whether all of the proposed rules are suitable for the wide variety of entities, with particular focus on those in need of a simplified approach like the asset management industry. This review should lead to introduction for such entities of further exemptions, less granular requirements, lower frequency of updates, trainings and reviews, as well as the exclusion from the scope services which do not support critical or important functions.

**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.**

The art. 16 of DORA does not include in its scope managers of AIFs and management companies, which will not be allowed to apply the simplified ICT risk management framework. However, EFAMA would like to highlight that what is prescribed in the Draft RTS based on art. 16 of DORA would suit more the operations, risks and complexity of those entities rather than provisions of the Draft RTS on art. 15 of DORA. We see the proposed simplified ICT risk management framework as more coherent, less burdensome and more cost efficient. As such, it will be better suited to the specificities of the asset management industry.

The simplified ICT risk management framework will, however, apply to small and non-interconnected investment firms. The entities listed under art. 16(1) of DORA are also a non-homogenous group, which should not be treated under a "one size fit all" approach. EFAMA is of the opinion that a separate, simplified ICT risk management framework in itself does not suffice for a proper application of the proportionality principle to the group of entities listed under art. 16(1) of DORA. As art. 4(1) of DORA addresses Chapter II in general, it does not distinguish the ICT risk management framework from the simplified ICT risk management framework. Therefore, the proportionality principle should be applied to the latter accordingly. In other terms, the Draft RTS should include a similar regulation to art. 29 of the Draft RTS (acknowledging issues mentioned above) in regards of the simplified ICT risk management framework and allow the entities to apply it with consideration of their size and overall risk profile, as well as the nature, scale and complexity of their services, activities and operations.

We would also like to highlight that entities entitled to apply a simplified ICT risk management framework, should not be deprived of the benefits of art. 16(1) of DORA if they are members of a group's capital structure. Therefore, it is important to reach a common understanding that the criteria determining the most appropriate framework should be analysed at the entity level.

## 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 would like to refer to the response to Question no. 1 and the need to thoroughly implement the principle of proportionality also regarding the ICT security policies, procedures, protocols and tools. These documents must not only be aligned with the characteristics of the particular entity and its business, but

also with what it is able to comply with and implement in daily operations. An overly developed and superfluous documentation, that the entity is not able to comply with, will not improve its ICT risk management. Therefore, we would suggest a principle-based approach like in the ESMA Guidelines.

Moreover, we would like to raise the issue of the ESAs not having a mandate to further specify tasks that should be assigned to the control function, as proposed in art. 2 of the Draft RTS. Article 15 of DORA does not refer to art. 6(4) of DORA and does not mention any right of the ESAs to further specify tasks and responsibilities of any function. Rather, it includes under point (a) further elements of ICT security policies, procedures, protocols and tools. Therefore, we would ask for the deletion of art. 2 from the Draft RTS.

Notwithstanding the above, the proposed art. 2(1) of the Draft RTS, includes under point (c) defining security objectives, setting measures, KPIs and key risk metrics which respond to what is usually understood as the first line of defense in the three lines of defense model. At the same time under point (d), it is required that this function would remain "*independent from the function or functions in charge of the ICT development, management, changes and operations*", which would suggest the second line of defense, which usually is an independent control function. This will be confusing for the financial entities and become a challenge when implementing the Draft RTS to their structures.

Therefore, in order to assist financial entities with implementing this element of the ICT risk management framework in a clear and effective manner, it should be coherent with the commonly used standards on good governance structure. As art. 6(4) of DORA requires to ensure an appropriate level of independence of such control function, with a clear indication to the three lines of defense model, it is clear to us that this role has been envisaged as the second line. Consequently, EFAMA proposes for point (c) to be removed from art. 2(1) of the Draft RTS.

**Q4: Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.**

In EFAMA's opinion, art. 3(1)(e) of the Draft RTS is a clear example of an insufficiently incorporated proportionality principle and excessively prescriptive provisions, as discussed in answer to question no. 1. It provides that ICT risk management policy and procedures shall include i.a. "*provisions on the monitoring of any changes to their ICT landscape, internal and external vulnerabilities and threats (…)*". Apart from it being disproportionate and burdensome, we believe that the monitoring of any changes is also not possible.

Therefore, we would suggest the following change to the wording of the first sentence in art. 3(1)(e) of the Draft RTS to "*provisions on the **monitoring of any significant change** to their ICT landscape, internal and external vulnerabilities and threats and of ICT risk to promptly detect changes that could affect the overall ICT risk profile.*"

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

EFAMA sees added value in the suggested approach to ICT asset management. It is important to avoid situations where cyber incidents/threats cascade from less valuable assets to the crucial ones. The identification of all ICT assets will be a helpful tool to prevent this from happening and it is also foreseen in art. 8(4) of DORA.

**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?**

According to the information gathered by EFAMA, keeping a record of the end-date of the provider's support, or the date of the extended support of ICT assets, is already an established market practice. In brings valuable information to the entities, as it indicates when patches should be used.

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

We would like to refer to the response to Question no. 1 and the need to thoroughly implement the principle of proportionality to the rules on encryption and cryptographic controls. The activities of asset managers differ significantly from those carried out by banks as, for example, they do not include open payment transactions. In our opinion, rules on encryption of internal network connections and traffic with external parties, as mentioned in art. 6(2)(b) of the Draft RTS, are too far-reaching and their application should be subject to the internal assessment of the entity.

On the other hand, EFAMA appreciates the possibility to adopt mitigation and monitoring measures, where a financial entity cannot adhere to the leading practices, or most reliable techniques under art. 6(3) of the Draft RTS, as well as when the entity cannot update or change the cryptography technology under art. 6(4) of the Draft RTS. We welcome the flexibility given to the financial entities by this element of the provisions.

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

EFAMA is of the opinion that some elements of Section V are important to be included in the policies and procedures managing operations of ICT assets, as for example art. 8(2)(b)(iii) of the draft RTS which addresses protocols for audit-trails and system log information.

On the other hand, there are also elements of the ICT operations security framework that are too prescriptive, as for example art. 8(2)(c) of the Draft RTS on "Error handling".

Some other obligations raise the question of their necessity, or even their adherence to the objective of this regulation. For example, in art. 10(2)(c) of the Draft RTS the procedures on vulnerability management of the financial entities are required to "*ensure that ICT third-party service providers handle any vulnerabilities related to the ICT service provided to the financial entity and report them to the financial entity. (…)*". While we see merit in the ICT TPP handling the vulnerabilities, in practice financial entities are often in no position to ensure it. They can request the ICT TPP to investigate vulnerabilities, determine their root cause and implement appropriate solutions, although not every provider will be found compliant. There are providers that may not be willing to do so and due to their relative size, financial entities may not be in a position to negotiate. Moreover, we do not necessarily agree that all of the vulnerabilities, despite those of possibly lower importance, should be reported to the financial entity. This would be excessive and should be limited only to significant ones. Therefore, we would suggest the following change in the wording of art. 10(2)(c) of the Draft RTS: "*request that ICT third-party service providers handle any vulnerabilities related to the ICT service provided to the financial entity and report significant ones to the financial entity*".

The proposed art. 10(2)(d) of the Draft RTS requires the financial entity to track the usage of third-party libraries, including open source, monitoring versions and possible updates, which requires in fact evaluation of a software bill of materials (SBOM) and inventory all components and dependencies. EFAMA is of the opinion that responsibility for this should lie primarily with the manufacturers and ICT service providers, as

will be the case upon entry into force of the Cyber Resilience Act[5]. It should not be shifted to the financial entities, in particular those that do not belong to the critical IT structure like asset managers.

We also disagree with the concept that vulnerabilities could be disclosed to the public and that this should also be an element of the vulnerability management procedures, as prescribed under art. 10(2)(e) of the Draft RTS. Even though the provision requires "responsible disclosure" and one that is conducted "as appropriate", we would argue that the disclosure of vulnerabilities to the public might only increase the risk of these being used by cyber-criminals. Even disclosing them to clients, especially to a wide group, would raise serious questions and concerns. We would therefore suggest to include only the responsible disclosure of vulnerabilities to the counterparts, to be foreseen in the draft RTS.

Provisions of art. 10(4)(c) and art. 11(2)(i) of the Draft RTS also lack the inclusion of the proportionality principle, as they require from the financial entity to test and deploy software and hardware patches and updates in non-production environment, as well as identify and implement security measures to prevent data loss and leakage for systems and endpoint devices. These requirements should also be subject to the risk assessment.

**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.**

We understand that, despite what would now be prescribed in art. 10(2)(b) of the Draft RTS, which allows for the scanning and assessment to be commensurate to the classification and risk profile of the ICT asset, the ESAs are considering a broader scope of this obligation. EFAMA is of the opinion that automated vulnerability scans for all ICT assets would have a positive effect on limiting the risk of compromising high risk assets. This could be helpful in preventing the less critical ones being attacked to get through to those more critical. If the less critical assets were to come under attack because they were not scanned, it would prove difficult to separate them from others. Associated costs would in fact be higher than the *ex-ante* preventive scanning of everything.

We would however like to also highlight that weekly automated vulnerability scans for all ICT assets could be burdensome for smaller entities. Therefore, we would suggest for the ESAs to consider a monthly frequency of scanning that could be more proportionate.

**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.**

EFAMA agrees in principle with the requirements for cloud computing resources identified under art. 11(2)(k) of the Draft RTS. We would however like to highlight that this area has been comprehensively addressed for the vast part of financial entities by the ESMA Guidelines and therefore lacks a rationale for a separate regulation.

At the same time, we would like to bring attention to the fact that the training specific to the services used, which is required under point (i), will not always be available. Given the wording of this provision, it is understood that this would require the cloud computing services provider to conduct training for the individual in charge of using the cloud client interface. It is however common for the smaller SaaS providers

[5] European Commission, Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

not to offer training to their clients, which does not mean that the individual in charge will lack necessary competences to use the client interface with success. The lack of training should also not prevent such services from being used when they are non-critical services. We would therefore suggest that specific training be required only when cloud computing services are critical ones.

EFAMA would also suggest for the mandatory independent certification to be considered, however only for critical cloud computing services.

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

We are of the opinion that some of the elements of Section VI on Network Security are excessive and do not take into account the proportionality principle sufficiently. Firstly, we would like to address the obligation under art. 13(1)(b) of the Draft RTS which requires for the policies, procedures, protocols and tools on network security management to include "*mapping and visual representation of all the financial entity' networks and data flows*". We are of the opinion that it is for the financial entity to decide on details such as this, with its obligation being primarily to be aware of its networks and data flows. However, as the introductory part to these provisions clearly states that all listed elements are obligatory, entities have no leeway in this regard. We are of the opinion that, as a minimum, this obligation should be limited to critical networks and data flows, if not removed entirely.

Secondly, under art. 13(1)(c) of the Draft RTS the use of a separate and dedicated network for the administration of ICT assets and prohibition of direct internet access is expected. In this regard we believe that this obligation is excessive for all entities. Especially that what we believe is to be achieved with this provision can be reached otherwise with for example IP access controls, access behavior monitoring, multifactor authentication. We are of the opinion that as a minimum, this obligation should be limited to critical assets and devices, if not removed entirely.

Finally, we do not agree with the six months frequency of reviews that have to be conducted on firewall rules and connections filters, under art. 13(1)(h) of the Draft RTS. According to art. 6(5) of DORA, the ICT risk management framework has to be reviewed "*at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT-related incident, and following supervisory instructions and conclusions derived from relevant digital operational resilience testing or audit processes.*" The rationale for the provisions on network security presented by the ESAs in the consultation paper do not provide any reasoning for the increased frequency of these reviews, and in particular, the paper does not mention any testing or audit outcome to justify such conclusion. EFAMA is of the opinion that the 6-month frequency of reviews for all ICT systems supporting critical of important functions is too cumbersome. In fact, taking also into account all elements that a review entails, this would lead to these functions being under constant evaluation. Therefore, we suggest that the need for a higher that annual frequency of the review should be assessed by the financial entity, according to its risk assessment and criticality of functions.

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

EFAMA supports the rationale behind Section VII: ICT project and change management as presented by the ESAs in the Consultation Paper. We agree on the importance of proper project management and change management in the area of ICT services in order to ensure their successful implementation and minimise the existence of loopholes. At the same time, we believe that some of the obligations could include a higher level of latitude, better suited for the wide diversity of financial entities that would be subject to these obligations. Examples of such provisions are presented below.

According to art. 15(3)(g) of the Draft RTS the ICT project management policy shall include "*testing of all requirements, including security requirements, and respective approval process when deploying an ICT system in the production environment*". We believe that testing of all requirements is excessive and should also be subject to an assessment of their criticality.

Obligations included in art. 15(4) and art. 17(2)(b) of the Draft RTS are in particular not suited for smaller entities, and therefore are other examples of the insufficient incorporation of the proportionality principle. The first one requires for each ICT project to include staff from business activities of functions impacted by the ICT project, whereas the second one for the independence between the functions that approve changes and those requesting or implementing them. In the case of smaller entities with limited staff such arrangements will often not be possible.

We also have strong reservations whether financial entities will be able to fulfill the obligations introduced under art. 16(9) of the Draft RTS which require them to analyse and test the source code and proprietary software provided by ICT TPPs or coming from open-source. In particular with open-source, but often also with proprietary software, the source code is not always available to the entity. We are of the opinion that this obligation should address TPPs, as they would have the best knowledge of the tools that they use, and this would allow them to protect their intellectual rights.

EFAMA is also of the opinion that obligations under art. 17(2)(d-e) of the Draft RTS are exaggerated and not suited for all developments. In particular in case of agile changes it will be impossible to document all the details, including purpose, scope, timeline and expected outcomes, as well as to identify fallback procedures and responsibilities, including those for aborting changes and recovering from them. There are cases when changes, in order to be successful, have to be implemented without any delay, which does not give room for such a detailed documentation and communication.

There are also questions arising from the provisions of art. 16(6) of the Draft RTS which addresses data stored in a non-production environment. We understand the rationale behind this, mentioned by the ESAs during the public hearing on 13 July, that the need to protect data also in a non-production environment allows to prevent from risks being transferred also to the production environment. However, if the entity has in place protective measures for the non-production environment that are similar to those suitable for the production environment, would it be understood as meeting the requirements of art. 16(6) of the Draft RTS? In particular, the requirement to store only anonymised, pseudonymised or randomised production data will not always be possible. Given that non-production environments are not publicly accessible and are secured separately, we are of the opinion that anonymisation is not necessary. The priority should be to secure the non-production environment properly. What is also important and should be taken into account is that overburdensome provisions will make the testing much more difficult for the entities.

**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.**

EFAMA is against such inclusion, as the supply-chain should be mainly the responsibility of the ICT TPP.

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

We would like to refer to the response to Question no. 1 and the need to thoroughly implement the principle of proportionality to the rules on physical and environmental security, in particular, the granularity of the relevant provisions.

**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 would like to refer to the response to Question no. 1 and the need to thoroughly implement the principle of proportionality to the rules on ICT and information security awareness training. EFAMA is of the opinion that the frequency of the programmes and training should be subject to the assessment and decision of the financial entity. Bearing also in mind that the requirement to employ sufficient personnel is already addressed within the sector-specific regulations for asset managers.

### 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.**

EFAMA agrees with the obligations provided in art. 20 and 21 of the Draft RTS as they include elements that should be at the core of any human resources policy and access control.

On the other hand, we do not support how some of the obligations under art. 22 of the Draft RTS have been calibrated. According to art. 22(1)(e)(iv) of the Draft RTS, the review of access rights should be conducted at least once a year for all ICT systems, and for those supporting critical or important functions at least every six months. We believe that the six months frequency is too high and financial entities would struggle to comply with it. The yearly frequency seems to be better suited, regardless of the service being critical/important or not. Were the ESAs do not agree on such homogenous frequency, an acceptable solution could also be for the management body of the entity to decide on the appropriate review frequency according to its risk assessment.

Moreover, we do not believe that strong authentication, mentioned in art. 22(1)(f)(ii) of the Draft RTS, is relevant for publicly accessible functions that are not important.

### 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.**

EFAMA partially agrees with the approach regarding ICT-related incidents detection and response. In particular we agree with the criteria listed under art. 24(5) of the Draft RTS.

However, we would like to draw attention to the provision of art. 24(2) of the Draft RTS on detection mechanisms, which should be analysed in conjunction with art. 12 of the Draft RTS which elaborates on logging. The scope of logging foreseen in these provisions might not be possible to achieve by smaller companies, as it would require the use of large tracking systems (e.g. SIEM or SOC). These are very specific and costly solutions, which should not be mandatory. It should be the decision of the financial entity, based on its own ICT risk assessment, what scope of logging is essential for them to track anomalous activities and what solutions would be best to achieve it. We are of the opinion that logging tailored to catch events important from the perspective of entity's activities, business model and solutions used, may in many cases be more effective than logging everything.

Moreover, we would like to question art. 24(3) of the Draft RTS which requires protection from tampering and unauthorised access at rest and in use and where relevant in transit of any recording of anomalous

activities. We are of the opinion that the implementation of this obligation will be expensive and the volume of the recording that would have to be protected in such manner would be high due to false positives.

We would also like to highlight that art. 23(1)(f) of the Draft RTS seems superfluous, as ICT response and recovery plans are already comprehensively regulated under art. 27 of the Draft RTS.

### 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 would like to refer to the response to Question no. 1 and the need to thoroughly implement the principle of proportionality to the rules on ICT business continuity management. EFAMA would like to highlight that general requirements for the emergency plans of asset managers are included in sector-specific regulations of art. 57(3) of the Delegated Regulation 213/2013[6] and art. 4(3) of the Delegated Directive 2010/43/EU[7]. This area is already comprehensively addressed and implemented in the business activities of asset managers, as is most likely also the case for other financial entities. The provisions of the Draft RTS in the area of business continuity management should be designed in a principle-based manner, to supplement what has already been foreseen in sector-specific regulations. In particular, art. 26 of the Draft RTS on testing of the ICT business continuity plans seems very prescriptive and too detailed. In the case of small and medium-sized companies it will cause a high implementation, and thus disproportionate, effort.

### 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.**

EFAMA agrees partially with the content of the report on the ICT risk management framework review. We do not agree with the scope of art. 28(2)(h) of the Draft RTS which includes the description of the measures to address identified weaknesses, deficiencies, and gaps. While we understand in general the need of the competent authorities to know how the financial entity conducts its reviews and addresses identified weaknesses, deficiencies, and gaps, we are of the opinion that including in the report all elements listed under point (h) in relation to all of those events is too detailed and excessive. This would lead to a report which will be highly elaborate, to the extent that could make it challenging for any analysis. Therefore, we are of the opinion that in the event of identified weaknesses, deficiencies, and gaps it should include a description limited only to the main and critical ones.

Moreover, we would like to highlight that our understanding of art. 6(5) of DORA is that the report will be prepared by a financial entity and submitted only upon request to the competent authority. In other cases, the financial entity will first document the ICT risk management framework, then review it according to art. 6(5) of DORA, and if necessary, make changes to it. It will not, however, prepare a report after each of these reviews. Otherwise, the extent of the report provided in art. 28 of the Draft RTS would be too

[6] Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision

[7] Commission Directive 2010/43/EU of 1 July 2010 implementing Directive 2009/65/EC of the European Parliament and of the Council as regards organisational requirements, conflicts of interest, conduct of business, risk management and content of the agreement between a depositary and a management company

excessive for such frequent reviews. This will lead to a bureaucratic burden that will not bring added value to the operational resilience of the entity.

### 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.**

EFAMA would like to refer to the response to Question no. 2 and the need to thoroughly implement the principle of proportionality that would comprehensively address the whole scope or the simplified ICT risk management framework.

Moreover, we would like to highlight that art. 30(4) of the Draft RTS should be removed. It requests financial entities to ensure "*appropriate segregation and independence of control functions and internal audit functions*" which is an obligation not included in art. 16 of DORA. It is provided for in art. 6(6) of DORA which does not apply to a simplified ICT risk management framework. In view of sectoral regulations which apply to investment firms, i.e.: art. 24 of Delegated Regulation 2017/565[8] and art. 16(5) od MiFID II[9], they are not obliged to implement a segregated and independent internal audit function.

Similarly, art. 16 of DORA does not include an obligation, comparable to art. 6(8)(b) of DORA, to establish a risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity and analyzing the impact tolerance for ICT disruptions. Therefore, mitigation strategies should be defined according to art. 33(1)(c) of the Draft RTS only for major ICT risks and only when necessary.

### 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.**

EFAMA would like to refer to our response to Question no. 26 and issues mentioned therein.

We would also like to highlight that the list of changes which were done in the reported area, included in art. 43(2)(a)(iv) of the Draft RTS as a part of the report, should be limited to major changes. This is the case for the corresponding part of report requested under ICT risk management framework, according to art. 28(2)(f) of the Draft RTS. This is by all means unjustified that the report under the simplified ICT risk management framework would be more detailed in this regard than the non-simplified one.

*****

[8] Commission delegated regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.

[9] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) Text with EEA relevance.

## ABOUT EFAMA

EFAMA is the voice of the European investment management industry, which manages EUR 28.5 trillion of assets on behalf of its clients in Europe and around the world. We advocate for a regulatory environment that supports our industry's crucial role in steering capital towards investments for a sustainable future and providing long-term value for investors.

Besides fostering a Capital Markets Union, consumer empowerment and sustainable finance in Europe, we also support open and well-functioning global capital markets and engage with international standard setters and relevant third-country authorities. EFAMA is a primary source of industry statistical data and issues regular publications, including Market Insights and the EFAMA Fact Book. More information is available at www.efama.org

**Contact:**

**Zuzanna Bogusz**
Regulatory Policy Advisor
zuzanna.bogusz@efama.org | +32 2 548 26 69