

Luxembourg, 8 September 2023

Subject: ALFI's response to the ESAs discussion on DORA: public consultation on the first batch of policy products

Introduction

The Association of the Luxembourg Fund Industry (ALFI) represents the face and voice of the Luxembourg asset management and investment fund community. The Association is committed to the development of the Luxembourg fund industry by striving to create new business opportunities, and through the exchange of information and knowledge.

Created in 1988, the Association today represents over 1,500 Luxembourg domiciled investment funds, asset management companies and a wide range of business that serve the sector. These include depositary banks, fund administrators, transfer agents, distributors, legal firms, consultants, tax advisory firms, auditors and accountants, specialised IT and communication companies. Luxembourg is the largest fund domicile in Europe and a worldwide leader in cross-border distribution of funds. Luxembourg domiciled investment funds are distributed in more than 70 countries around the world.

We thank the ESA for the opportunity to participate in this consultation on the first batch of policy products of DORA.

Our members appreciate the opportunity to share the views of the market practitioners in Luxembourg, with regards to ICT Risk Management in the context of DORA.

In order to provide evidence of the industry considerations with regards to those various topics in the context of DORA, answers will be given on a number of selected questions focusing on the high-level assessment and spotted industry-related consideration

Part I: RTS to further harmonise ICT risk management tools, methods, processes and policies

Question 3 *Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.*

ALFI welcomes the regulatory prescriptions of the RTS. Yet, although we see a convergence with the existing standards of the EBA guidelines, the industry assesses that the implementation workload would be highly significant (for all players in the investment funds value chain and for investment fund managers in particular as they are not directly in the scope of the EBA guidelines). In the interest of the implementation of the provisions, the industry would welcome a phasing of the expected implementation of the various provisions, with regards to the risk management framework, as well as the policy, the register of information and the operational processes, including the ICT contract review, the ICT service providers data collections.

ALFI agrees with the overall principles established in Article 2 which are in line with standard risk management practices. In order to acknowledge for the highly technical nature of ICT and for the operational models adopted by the investment fund manager industry, ALFI recommends providing further clarifications on:

- the split of responsibilities between the function in charge of ICT and the control function; and
- the flexibility to adopt a governance framework relying on intra-group coordination and resources;

promoting a consistent interpretation of the requirements and facilitating its implementation. The recommended clarifications are detailed below.

Split of responsibilities between the function in charge of ICT and the control function

Article 2 1.(d) – **Provision on governance** – establishes the requirement for the control function to remain independent from the functions in charge of ICT development, management, changes and operations. It is relevant to highlight that due to the technical nature of ICT topics, the in-depth expertise on the matter sits with a team specialised and dedicated to those topics. While the control functions rely on transversal governance and oversight capabilities, they might not necessarily have the specialist ICT expertise. In light of the above, a point of attention is highlighted in specific cases the team in charge of the second line of defense would be in a situation to make sure the controls were performed by the first line of defense. Nevertheless, they may not always have the full technical expertise to be in a position to re-perform the controls. This would most likely be the case for smaller size entities, applying a principle of proportionality.

Intra-group coordination and resources

The operational model of some financial entities, and industries at large, builds on the coordination and use of resources across group to deliver value to their clients at optimized costs and services level (i.e. economies of scale/scope, benefit of specialisation). In this respect, the center of expertise in ICT within a group might be located outside the supervised entity.

Against this background, it is recommended to clarify that the control function can maintain independence while relying on the technical expertise of the functions in charge of ICT and intra-group resources. In this context, the control function would maintain an oversight role while the ICT technical function would remain in charge of daily implementation of the ICT risk management policies (including controls). For example, instead of duplicating the controls, the control function reviews the appropriateness of the controls and ensures its appropriate execution. When appropriate, the control function could carry out additional control checks as justified per a risk-based approach.

Article 1.g provides the basis of such flexibility

*2. Financial entities shall ensure that the ICT security policies referred to in paragraph 1:
[...]*

(g) specify the segregation of duties arrangements to avoid conflicts of interest, in the context of the three lines of defense model or other internal risk management and control model, as applicable;
[...]

and it is recommended to clarify it in Article 2 as well. Similarly, this clarification should allow for intra-group entities

- to leverage on existing competences and capabilities within the group; and
- to acknowledge for the consistency of the framework (e.g. criticality of tools) globally across the group with local adjustments to specific requirements.

Question 4 *Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.*

Article 3 – **ICT risk management** – establishes the requirements pertaining to the risk management policy and procedures and its content. The principles introduced are in line with industry risk management practices.

Question 11 *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.*

It is critical to distinguish a) running automated scans from b) analysing the results of the scans. The Question 11 emphasises on the number (frequency) of scans rather than on the analysis of scans and the patching of material vulnerabilities.

In practice, scans can commonly generate output with hundreds of vulnerabilities. Analysing the results of scans is a time consuming and resource intensive exercise that goes beyond the simple automation of scans. In this regard, it is imperative to identify and segregate the type of vulnerabilities that involve a material risk and threat.

Under finite resource and the limited gain from automation with regards to the analysis of the scans output, the effort should be focusing on the patching of truly material vulnerabilities instead. Accordingly, a balance should be struck between discovering new vulnerabilities and patching threatening vulnerabilities.

In view of the argument detailed, ALFI does not agree with extending the weekly automated vulnerability scans requirement to all ICT assets without considering their classification and overall risk profile.

Question 15 *Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.*

Article 15 – **ICT project management** – introduces a framework for change management through the documentation and implementation of an ICT change management policy.

Beyond the content of the policy outlined in paragraph 3, the requirements relative to the composition of the staff involved in the project are defined in paragraph 4. In this respect, a broad and business activities orientated composition is foreseen as per the following the paragraph

“Financial entities shall ensure that the staff dedicated to an ICT project includes staff from business activities or functions impacted by that ICT project and that it has the necessary knowledge to ensure the secure and successful project implementation.”

ALFI welcomes the opportunity to adopt a broad composition of the project management team, including internal teams and potentially qualified professional third parties, as required for each financial entity. This also offers the flexibility to involve and have a representative from the second line of defense as well as local entities at an early stage of the ICT project. Especially small and medium sized firms in the investment management sector may not always have the HR capacity and resource skills available inhouse to support a broad range of ICT projects as well as can benefit from the leverage and experiences gained from similar projects at other firms.

Article 16 – **ICT systems acquisition, development, and maintenance** – calls for some controls to be performed in the context of the acquisition, development, and maintenance of systems to preserve the availability, authenticity, integrity and confidentiality of data. In light of the diverse profiles of the entities captured by the broad scope of DORA, ALFI recommends to reinforce the proportionality and risk-based approach principles applicable to those controls and their implementation.

For instance, the control related to the source code review may require disproportionate resources for entities of medium size. This is particularly relevant considering that source code review requirement implies specific expertise not always available in-house depending on the entity. Accordingly, while the control is meaningful, flexibility should be provided on how to implement the review in proportionate manner.

In any cases, the term of “source code review” would need to be explained with regards to the underlying requirement and the limited feasibility in cases of software packages. More details would be appreciated with regards to the wording “source code review where feasible”.

We would also welcome a distinction between in-house developments and standard software packages: Since many tools are off-the-shelf software and software developed by external parties, contractual arrangements can foresee an in-depth quality assurance review, independent testing, by an external independent party, complemented with some pen tests performed by the entity if appropriate.

Question 23 *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.*

For incident detection, in the investment fund manager ecosystem, in order to benefit from expert knowledge many entities rely on a specialist department within the groups or on technical service providers. ALFI recommends the Article 23 and 24 to provide clarity on the flexibility to rely on different set-up and external resources as appropriately overseen.

The Article 24 – **Anomalous activities detection and criteria for ICT-related incidents detection and response** – paragraph 2.(c) states

To detect anomalous activities that can result in ICT network performance issues and ICT-related incidents in accordance with Article 10(1) of Regulation (EU) 2022/2554, financial entities shall implement detection mechanisms allowing them to:

[...]

(c) define the alerts referred to in point (b), to allow the detection of ICT-related incidents to be managed within the expected recovery time, both during and outside working hours

The last part of the sentence (“both during and outside working hours”) could imply a requirement to have human resource on duty (24/7). This requirement would be extremely burdensome for many entities. In this respect, ALFI recommends clarifying that the time requirement refers to the detection of incident – *incident alert* – to be performed outside working hours, while the “reaction” to the incident – *incident management* – can be performed within the expected recovery time within working hours, provided the urgency of the detected incident permits. For this purpose, performing a preliminary assessment of the criticality level of the incident at an early stage is required, in order to match the level of urgency / criticality of an incident and the respective anticipated response management time. Please refer to our response to the Consultation on Part II: RTS on specifying the criteria for the classification of ICT related incidents, for specific elements to this regard. The upcoming consultation in the pack II RTS on “Reporting of Major Incidents” could also bring useful clarification to this regard.

Question 26 *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.*

The format and content of the report is defined in Article 28 – **Report on the ICT risk management framework review** – which documents the review of the effectiveness of the process established in these RTS.

The current proposal leaves room for interpretation regarding the scope of this review. This materialises in the paragraph 2.(h) detailing the description of the measures to address identified weaknesses, deficiencies and gaps. Weaknesses, deficiencies and gaps can be either identified against a list of exhaustive risks or against established frameworks (such as Control Objectives for Information and Related Technologies COBIT) or regulatory frameworks (including the EBA guidelines on ICT and security risk management EBA/GL/2019/04). For consistency and ease of implementation purposes, it is argued that these established frameworks could form a relevant benchmark for this identification. We would also welcome a harmonized joint and common framework by the different ESAs.