

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 the classification of ICT incidents, 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 II: RTS on specifying the criteria for the classification of ICT related incidents

Question 1 *Do you agree with the overall approach for classification of major incidents under DORA? If not, please provide your reasoning and alternative approach(es) you would suggest.*

ALFI agree with the global approach.

Yet, we would like to raise a concern with regards to the timing issue, in case of the occurrence of an incident, to qualify this incident: At a time of an incident or similar crisis, the focus of the operational teams would be concentrated on the resolution itself. Putting a regulatory constraint on an immediate and precise qualification exercise may take some scarce resources from the resolution itself. Delaying the complete qualification and corresponding reporting once the incident has been solved may result more efficient operationally.

Additionally, with regards to the data loss occurred at the time of an incident, performing a complete and precise assessment may take time and require substantial analysis.

We would be of the view that a delay should be allowed with regards to timing, to qualify the incident.

Question 2 *Do you agree with the specification and materiality thresholds of the criterion ‘Clients, financial counterparts and transactions affected’, as proposed in Articles 1 and 9 of the draft RTS? If not, please provide your reasoning and suggested changes*

As the guidelines suggest that “The relative threshold will have to ensure that the criterion is applied consistently by all FEs.”, ALFI is of the view that such criterion may lead to a large variety of interpretations among financial entities. As an illustration, an investment fund manager or management company may consider its “clients” are the investment funds or investment vehicles it manages, and therefore present a value for counting that criterion that is off-scale, as compared to a private bank dealing with individual clients’ deposits.

In the interest of comparability among players: Should this criterion be maintained in the RTS, we would welcome a further analysis of this requirement, as further clarification could come in the form of a standard, entity-type agnostic suggestion of a template register of “transactions and clients”, allowing to assess the potentially impacted clients and transactions on an unbiased basis.

Question 3a *Do you agree with the specification and thresholds of the criteria ‘Reputational impact’ as proposed in Articles 2 and 10 of the draft RTS? If not, please provide your reasoning and suggested changes*

With regards to Article 2:

On point a), ALFI would appreciate some quantitative guidance about the mentioned “reputational impact”. In particular, we consider it would be beneficial to bring clarification on the exact meaning of « attracted media attention ». e.g. The impact would differ substantially, should the financial entity be exposed on the front page of major financial media or on small local media.

On point b), we would like to highlight the fact that, the Regulator not being aware of the incident should not preclude that the incident will not have a reputational impact.

With regards to Article 10:

In order to allow for scoping the case, we would suggest a time range should be specified for this criterion, considering the fact that an incident could attract media attention or lead to resulting complaints long after the incident actually occurred.

In any cases, and with regards to question 2, ALFI is of the view that the preliminary assessment of the impact of the incident should be reassessed ex-post, to capture the impacts in a complete manner.

Question 3b *Do you agree with the specification and thresholds of the criteria ‘Duration and service downtime’ as proposed in Articles 3 and 11 of the draft RTS? If not, please provide your reasoning and suggested changes*

With regards to articles 3 and 11:

ALFI considers that the requirements specified in the articles 3 and 11 are consistent with the regulatory framework already in force, EBA guidelines and market practices.

This being said, ALFI would welcome precision on whether the two-hours threshold considered in the case of an incident affecting critical functions, is considered as a single two-hours block or if two blocks of one single hour during the recovery process, are also considered to this regard.

Question 3c *Do you agree with the specification and thresholds of the criteria ‘Geographical spread’ as proposed in Articles 4 and 12 of the draft RTS? If not, please provide your reasoning and suggested changes*

With regards to Articles 4 and 12:

ALFI is of the view that this criterion of an ‘Geographical spread’, being labelled such as “impact of the incident in the territories of at least two Member States”, could potentially create an unlevel playing field for financial centers which are positioned as hubs for cross-border distribution, as compared to those financial centers highly focused on their internal market. In particular, for a Luxembourg (and Ireland) based financial entity, the threshold of this criterion would likely be immediately reached, given the importance of cross-border transactions.

We would welcome an assessment of whether this criterion is creating a regulatory/strategic disadvantage for financial centers positioned as hubs for cross-border distribution, such as Luxembourg and Ireland.

In addition, we consider that point c) “Financial market infrastructures or third-party providers that may be common with other financial entities” would benefit from further clarification as the current wording may give way to individual interpretations.

Question 3d *Do you agree with the specification and thresholds of the criteria ‘Economic impact’ as proposed in Articles 7 and 15 of the draft RTS? If not, please provide your reasoning and suggested changes*

With regards to Article 7 and 15:

ALFI considers that the assessment of the “Economic impact” described in Articles 7 and 15 should be split into a two-steps process: while an initial, high level assessment of the economic impact could be performed during the occurrence of the incident, we consider it should be reassessed after the incident. This reassessment could take the form of a complete *post-mortem* analysis, and include the reiteration of the costs and losses impact analysis up to a few months after the actual occurrence of the incident. Consequently, we would welcome the definition of a timeframe as of when subsequent costs and losses should not be accounted anymore as a direct impact of an incident, in assessing whether the EUR 100 000 threshold is breached.

In any cases, the response and escalation may need to be reconsidered through time, as re-assessment of the impact is performed and the impact might change.

Question 4 *Do you agree with the specification and threshold of the criterion ‘Data losses’, as proposed in Article 5 and 13? If not, please provide your reasoning and suggested changes.*

With regards to data losses, ALFI is of the view that the analysis should consist in a 2-step approach:

- (i) assessing the level of confidentiality of the data and
- (ii) whether confidentiality is breached

In addition to the assessment of compliance with GDPR, the level of confidentiality/sensitivity of data should be clarified in order to assess whether the data can be considered as being a “loss” in the sense that it is harmful for the financial entity.

In the present articles, sole reference to data is seen as insufficient and unclear, potentially leaving way to individual interpretations. Specific references to “critical data”, with thorough definition and reference to existing regulations on the matter, would be beneficial to enhance clarity, comparability and homogeneity among players.

Question 5 *Do you agree with the specification and threshold of the criterion ‘Critical services affected’, as proposed in Articles 6 and 14? If not, please provide your reasoning and suggested changes*

ALFI agrees with the general approach of the definition.

In the interest of clarity and consistency with other regulatory requirements, we would like to highlight the fact that the Luxembourg CSSF Circular 22/806, based on the requirements of the EBA Guidelines EBA/GL/2019/02, provides a definition of “Critical and important functions” which could be used as a reference in the present RTS.

This definition of “critical or important functions’ is based on the wording of MiFID II and the Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II. It is used only for the purpose of identifying ‘critical or important functions’ under outsourcing arrangements”:

The “Commission Delegated Regulation (EU) 2017/565 specifies, under Article 30, that ‘an operational function shall be regarded as critical or important where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its other obligations under Directive 2014/65/EU, or its financial performance, or the soundness or the continuity of its investment services and activities”.

With regards to the prescriptions of article 14, we would like to raise the concern that, internal escalation procedures are likely to vary from a financial entity to another depending on their individual risk appetite. While financial entities may have procedures in place to escalate incidents as part of their regular reporting, we would not consider escalation as a determining criterion for qualifying an incident as “major”. The decision to consider a reported incident as “major” should be left to the discretion and assessment of senior management, as the latest remain accountable for the incident classification and related action points. In all instances, we would be of the view that the assessment of the incident should be duly documented.

In any cases, ALFI understand that the definition of “critical functions” is aligned with the definition with the BRRD (Bank Recovery and Resolution Directive). We would welcome the clarification from the ESAs, as to precise the meaning of “important function”.

Question 6 *Do you agree with capturing recurring incidents with same apparent root cause, similar nature and impact, that in aggregate meet the classification criteria and thresholds as major incidents under DORA, as proposed in Article 16? If not, please provide your reasoning and suggested changes.*

With regards to the proposed approach of article 16, of regrouping incidents presenting a similar nature and impact, in the purpose of aggregating such incidents to assess their global impact, ALFI would like to raise the concern of the feasibility and applicability. Indeed, although a root cause analysis be performed for each incident, assessing that the root cause of various smaller incidents is the same with views to perform an aggregated impact assessment, could result both complex and subjective. To this respect, we would suggest this analysis of a similar root cause and subsequent aggregation of minor individual incidents be performed on a best effort basis. In any cases, we are supportive of the principle of implementation of systematic root cause analysis in case of major incidents.

This being said, and with regards to various distinct minor incidents with similar root cause occurring, especially in case of a centralised group reporting, we would like to raise concern around potential overreporting, considering that focusing the effort on reporting recurring minor incident could lead to unwanted simplification and not serving the purpose of performing proper root cause identification. Members underline the fact that, in their governance process and risk management framework, minor issues are handled in Problem Management (with a focus on root cause analysis) and should not systematically trigger incident reporting. (Please refer to our answer to Question 11 in the Consultation Part I: RTS to further harmonise ICT risk management tools, methods, processes and policies).

Question 7 *Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17? If not, please provide your reasoning and suggested changes.*

ALFI is of the view that the assessment of cyber threats should follow the same risk-based approach as applied to the assessment of the various risks of the financial entity's activity. In particular, the assessment of cyber threats should decompose into an inherent risk analysis, consisting in an identification of all cyber threats and potential vulnerability, and a risk mitigation techniques analysis, leading to the final assessment of the residual risk the financial entity is exposed to.

To this respect, we would appreciate clarification in the expected classification of cyber threats. Such clarification could, in particular, aim at making a distinction between detailing a complete inventory of all cyber threats, or highlighting those successful/ exploitable cyber threats, as well as precisising the scope of the classification being either on the inherent cyber threat risk, or rather the residual risk related to cyber threats.

In any cases, and with the aim of protecting the integrity of the financial entities and avoiding spreading the exploitability of potential cyber threats, we would be of the view that the assessment of cyber threats should remain strictly confidential within the financial entity and with the Regulators, and that any communication between Regulators should remain confidential.

Question 8 *Do you agree with the approach for assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities, as proposed in Articles 18 and 19? If not, please provide your reasoning and suggested changes*

ALFI agrees with the general approach, considering that information sharing among Regulators within Member States is in the best interest of an efficient supervision. In any cases, with regards to ICT incidents, cyber incidents and cyber threats, we would like to emphasize the industry critical requirement that communications with and among the Regulators should only be processed through secured communication channels, especially should the contents of the reports not be anonymized. The underlying rationale is to avoid, in all cases, the spread of information on vulnerabilities of a financial entity, as such a leak would substantially increase the risk of additional cyber threats and attacks.

With regards to these considerations on regulatory reporting and information sharing among Regulators, we would welcome joint initiatives from the Member States Regulators to align themselves on the concepts of significance/materiality/criticality.