RESPONSE TO CONSULTATIONS

DIGITAL OPERATIONAL RESILIENCE ACT

Aggregated costs & losses from major ICT-related incidents (Guidelines)

association of the luxembourg fund industry

Luxembourg, 1 March 2024

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 European Supervisory Authorities (ESAs) for the opportunity to participate in this consultation on the second batch of policy products of DORA.

Our members appreciate the opportunity to share the views of the market practitioners in Luxembourg, with regards to aggregated costs and losses from major ICT-related 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 priorities stemming from industry-related consideration and impact assessment.

I. AGGREGATED COSTS AND LOSSES FROM MAJOR ICT-RELATED INCIDENTS (GUIDELINES)

Important considerations

ALFI's main advocacy points in this consultation are as follows:

1. "**Upon request" reporting**: ALFI would welcome the guidelines to confirm the non-periodic (i.e. ad-hoc) characteristic of the report, upon request from the NCA, and to limit the timeframe the requested report could cover (e.g. up to 3 years backwards).
2. **Treatment of exceptional costs**: we would appreciate clarification and guidance with regards to exceptional costs, such as consulting expenses involved in the resolution of the incident or in the implementation of measures to avoid recurrence of incidents.
3. **No mandatory external validation**: being based on actual audited accounting figures, external validation of this report should not be implemented.

Response to consultation

Question 1 – Do you agree with paragraph 7 and 9 of the Guidelines on the assessment of gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

With regards to the reference period being proposed in the draft guidelines, ALFI agree with the reference period being the accounting year of the FE.
Yet, the guidelines do not precise any prescribed timeframe or deadline, further to the closing of the financial year to make the reporting. To this regard, we would like to highlight that the closer to the closing date of the financial year, the higher the risk that reported data would consist in a large share of estimates, rather than actual data.

Considering that the National Competent Authorities (NCA) would be doing an open request for the reporting, we acknowledge this is not a periodic reporting and therefore, the deadline for this report is not specified. Yet, ALFI would welcome the guidelines to confirm the non-periodic (i.e. ad-hoc) characteristic of the report, upon request from the NCA. We would also consider appropriate to have a limit timeframe set for the NCA to request this yearly reporting and would suggest a maximum period of three years after the year end closing of a given financial year.

This being said, we would like to raise concerns with the fact that, in global group structures, many costs may be mutualised at group level and the local FE may be charged a pro-rata for internalised group-wide costs. Such costs may include, but not be limited to, IT and support staff costs, internal communication, and advisory costs. Particular care should be given when allocating such mutualised cost to the incident's costs and losses, as the accounting pro-rata share may not accurately reflect the potential exceptional cost related to the incident. For this, we advise that the Guidelines should differentiate between external and internal costs, focusing only on external or extraordinary costs that are beyond normal operational functioning.

In any cases, we are in favour of the proportionality principle applied and excluding the micro-enterprises.

An incident might be closed, yet updates to the impact could be evidenced a few months / years after the occurrence of the initial incident. We agree with the proposal of Article 9 to include such adjustments in the reporting of the relevant accounting year in which the adjustments are made if impacts of an incident are identified after a few years.

Question 2 – Do you agree with paragraphs 5, 6 and 8 of the Guidelines on the specification of the one-year period, the incidents to include in the aggregation and the base of information for the estimation of the aggregated annual gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

ALFI agree with the proposed reference to the financial year.
With regards to the content of the reporting and the principles defining the costs, losses and financial recoveries to include in the report, we agree with the inclusion of the costs, losses and financial recoveries that are reflected in their financial statements. This alignment with the accounting principles facilitate the identification and calculation, while avoiding interpretation or uncertainty. We are also in favour of including adjustments performed, on the impact of incidents occurred on the previous years and accounted for in the current financial year. We understand this view excludes implicit or indirect costs (such as opportunity costs) and we agree with this approach for the financial entity.
Nevertheless, we would appreciate clarification and guidance with regards to exceptional costs, such as consulting expenses involved in the resolution of the incident or in the implementation of measures to avoid recurrence of incidents. To this respect, clarity would be appreciated, to avoid interpretation and vagueness.

In addition, we would like to raise a concern regarding the inclusion of incidents that do not trigger the economic impact criterion but are still classified as major due to other factors, such as a data breach with significant media coverage across multiple countries (European or wider) triggering a reputational impact. While the classification of an incident as major is crucial for operational and reputational risk management, the aggregation of costs and losses for incidents without a direct economic impact could lead to a misrepresentation of the financial entity's risk profile and operational resilience.
To address this concern, we suggest a distinction in the reporting template between incidents that have triggered the economic impact criterion and those that have not. This would allow competent authorities to better understand the nature of the incidents and the actual financial impact on the entity.

Question 3 - Do you agree with paragraph 10 and 11 and the annex of the Guidelines on the reporting of annual costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

We would like to reiterate the point made in question 2, with regards to the guidelines providing precise specification on the side costs and expenses that should or should not be included in the reporting (e.g. consulting cost, exceptional costs of personnel…).

With regards to the point on external validation of the report, we would raise concerns, with views to avoid having the FE incurring additional and unnecessary costs solely related to the reporting process. For this, we would be of the view that external validation of this report should not be implemented. Since this report makes use of costs, expenses and financial recoveries figures as presented in the financial statements, which are audited, we consider this second layer of external validation is not bringing additional value.

About ALFI

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.