DUFAS

Dutch Fund and
Asset Management
Association

Response to the ESAs second batch of DORA policy products

info@dufas.nl
www.dufas.nl

Date	4 March 2024
Subject	**Response to the ESAs second batch of DORA policy products**
Contact details	Manouk Fles, manager regulatory affairs, mf@dufas.nl

The Dutch Fund and Asset Management Association (DUFAS) welcomes the opportunity to respond to the public consultation of the ESA's second batch of DORA policy products. In our response we focus on the following policy documents:

- **RTS and ITS on content, timelines and templates on incident reporting**
- **GL on aggregated costs and losses from major incidents**
- **RTS on subcontracting of critical or important functions**
- **RTS on threat-led penetration testing (TLPT)**

Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat

Question 1. Do you agree with the proposed timelines for reporting of major incidents?

No

Additional comments, reasoning and suggested changes

In general, we would like to note that a lot of information is expected from financial entities within very short timelines, without also taking into account the size and importance of the financial entity, and the capacity the financial entity has to report an incident.

The ESAs have chosen to align with the timelines of the NIS2 Directive. However, the NIS2 Directive does not apply to all entities covered by DORA, as the NIS2 Directive covers essential and important entities. We are therefore of the opinion that is not proportionate to impose the timelines of the NIS 2 Directive on financial entities that are not in scope of the NIS2 Directive, as the entities in scope of DORA vary widely in size and importance. In the mandate to develop the draft RTS, the ESA's are also explicitly offered the opportunity to take into account different timelines that may reflect the specificities of financial sectors. Unfortunately, the ESAs have not opted for this in this draft RTS.

The amount of the information that needs to be provided, combined with the very short timeline, is undesirable. Especially when an incident just occurs or is just discovered, all resources and

expertise are needed to resolve the incident and/or limit its consequences. We would like to argue for limiting the scope of reporting and/or extending the timeline of the initial and intermediate report.

If it is not possible to use different timelines for different types of financial entities, then we would argue for a timeline of at least 48 hours after detection for the initial report (and no additional timeline for reporting after classification of an incident, as this can lead to unnecessary confusion). A longer deadline to submit the initial report should also impact the deadline for the intermediate report.

In addition, we believe that a financial entity should not only be able to submit an intermediate or final report the next working day when the deadline for submission falls on a weekend day or a bank holiday, but that this should also apply to the initial report. Submitting an initial report already has tight timelines, but these are certainly very difficult to meet if the deadline falls on a weekend day or bank holiday. It should be noted however that the timeline for submitting the report the next working day within one hour is unrealistic. For this addition to be useful, a longer time limit is therefore necessary.

Question 2. Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA?

No

Additional comments, reasoning and suggested changes

2.9 and 2.10 - in these data field a description of the impact of the incident on other financial entity or a TPP needs to be included. This information would be very subjective and in particular in case of the initial report financial entities would not have enough information to have definite opinion. We suggest removing these data fields.

2.12 and 2.13 - It is not entirely clear what the expectations are with regard to recurring incidents. Multiple or recurring incidents could lead to a major incident, which needs to be reported in accordance with the RTS. However, it is not clear what is meant by a 'recurring' incident in this RTS. Should be looked at the definition of recurring incident as meant in article 15 of RTS on criteria for classification of major incidents under DORA (instead of Article 16 which is now referred to in the draft RTS) , i.e. an incident that in itself does not constitute a major incident, but that must be reported because previous similar recurring incidents have already led to a major incident? Or is meant: an incident that is in itself a major incident, that occurs again?

2.15 - Including a description of the business continuity plan is too prescriptive, in particular for an initial report. We suggest removing this data field.

Question 3. Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA?

No

Additional comments, reasoning and suggested changes

Some questions are (potentially) too broad, for example as 3.16 (Information describing how the ICT related incident has affected or could affect the reputation of the financial entity) and 3.38 (Information on the involvement of CSIRTs in the handling of the incident, if applicable).

Also, all information of the initial report should also be updated by the financial entity. This means the intermediate report is extensive and therefore the timeline of 72 hours is too tight.

Question 4. Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA?

No

Additional comments, reasoning and suggested changes

4.23 and 4.25: This data will already be included in the costs and losses report, so it seems repetitive to include this data also in this incident report.

Question 5. Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA?

Yes

Additional comments, reasoning and suggested changes

No comments

Question 6. Do you agree with the proposed reporting requirements set out in the draft ITS?

No

Additional comments, reasoning and suggested changes

We prefer standardized specifications for the formats and interfaces to be established on EU level, as this may make reporting easier for financial entities providing cross-border services.

Question 7. Do you have any further comment you would like to share?

It is also important to note that the incident reporting environment should be set up based on principle of cooperation between financial entities and competent authorities, with a common goal to protect the resilience of the financial sector. The reporting of incidents takes place in circumstances of higher pressure, caused by the incident itself and the importance of it being quickly resolved, as well as time available to submit the reports. It is, therefore, crucial that financial entities do not fear being penalised for mistakes in reporting or reclassifying major incidents as non-major if the conditions change. In addition, the NCA's use of the information that

is included in the reports must be limited to the referenced common goal and should not be used as a source of information for the ongoing supervision over the reporting entity.

Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents

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?

No

Additional comments, reasoning and suggested changes

In general, we believe that the administrative burden it entails to provide such detailed insight into the costs and losses (gross and net) is disproportionate to the intended objective. Because often it's not clear in advance when a major incident will occur, a detailed overview of the costs incurred should be kept for each incident. This means that people who work in the field of IT within a financial entity have to deal with a (extensive) administrative task. Experience shows that IT people do not always appreciate this type of work as it distracts them from their core tasks. It could even lead to IT people preferring to choose another sector, where such far-reaching administrative work is not part of the job description. This could cause the financial sector to lose important talent.

We do not see a rationale for reporting both net costs and losses and gross costs and losses, each aggregated on an annual basis, as well as broken down by incident. We are of the opinion that gross costs should be sufficient for the purposes of this reporting.

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?

Yes

Additional comments, reasoning and suggested changes

No comments

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?

No

Additional comments, reasoning and suggested changes

We disagree with the statement that the requirement to report also costs and losses individually for each major ICT-related incident would not pose an inappropriate burden. As the calculations for reporting, subject to this draft guidelines, are to be based on amounts reflected in the financial

statements such as profit and loss account, they would already be aggregated. To break them down by incident, would require separate calculations to be made. We therefore propose to only include aggregated gross costs and losses.

Question 4. Do you have any further comment you would like to share?

No

Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554

Question 1. Are articles 1 and 2 appropriate and sufficiently clear?

No

Additional comments, reasoning and suggested changes

In general, we assume that whenever this RTS refers to subcontractors, this only concerns subcontractors who provide ICT services that support a critical and important function of the financial entity. In other words, a financial entity must first determine whether the 'first' ICT TPP provides a service that that supports a critical and important function of the financial entity. If that is the case, only subcontractors that (indirectly) support a critical and important function of the financial entity are in scope of the requirements set out in this RTS.

This could be clarified in more detail in the RTS, so it is clear not all subcontractors of a ICT TPP that support a critical or important function are in scope, but only those supporting (indirectly) critical or important functions of the financial entity. This also seems to be intended in recital 4 *([...] to identify and monitor all the subcontractors that effectively provide the ICT service supporting critical or important functions*.)

DORA is based on the principle of proportionality (Article 4 DORA)Although article 1 of this RTS provides financial entities with the possibility to take into account increased or reduced risks, this does not always appear to have been clearly applied in Articles 2 to 7 of the draft RTS. In our opinion the analysis conducted by the financial entity in accordance with article 1 of the draft RTS should have a much broader impact, allowing entities for which it is justified to adhere to simplified rules or to limit the scope of obligations to the elements that are relevant to their particular situation.

Question 2. Is article 3 appropriate and sufficiently clear?

No

Additional comments, reasoning and suggested changes

Please refer to the response to question 1 regarding proportionality. All elements listed in article 3 should be assessed in accordance with this proportionality principle. The fulfillment of particular obligations should be subject to the risk assessment of the financial entity and should therefore apply 'where appropriate'.

Question 3. Is article 4 appropriate and sufficiently clear?

No

Additional comments, reasoning and suggested changes

We would like to comment in particular on the Art. 4(f) of the draft RTS, which regards the obligation of the ICT TPP to ensure the continuous provision of ICT services, even in case of failure by the subcontractor, to meet its service levels or any other contractual obligations. We believe that such guarantees cannot reasonably be offered by ICT TPP. However, we understand that business continuity is important, and therefore propose to replace this text with the obligation to make agreements on continuity measures to be taken by the ICT TPP.

Question 4. Is article 5 appropriate and sufficiently clear?

No

Additional comments, reasoning and suggested changes

First of all it should be clarified that the obligation only concerns subcontractors supporting (indirectly) critical or important functions of the financial entity (as is indicated already in the policy considerations). Monitoring (if any in the first place) should be based on materiality, which does not necessarily means monitoring the whole chain.

Secondly, we consider it to be too far-reaching to review all contractual documentation between the ICT TPP and the subcontractor, as it may also contain commercially sensitive information. We assume sub processors will not cooperate with full-fledged monitoring of these subcontractors, since there is no direct legal relationship between the subcontractor and the financial entity. We are in favor of being able to rely on the monitoring and reporting by the ICT TPP as referred to in Article 4. This is option C of the policy considerations. This option was not chosen with the following consideration: "Delegation of the monitoring of the ICT service third party providers (Option C) is not in line with the DORA framework." We wonder why this is considered not in line with the DORA framework. The details of this monitoring and reporting should be part of the contractual agreement between the financial entity and the ICT TPP, so the financial entity is able to thoroughly assess the risks involved with the subcontracting.

Finally, we wonder whether establishing this monitoring obligation of subcontractors falls within the mandate of the ESAs, since the mandate relates to developing a draft RTS to further specify elements referred to in article 30(2)(a). Article 30(2) of DORA specifies elements of contractual arrangement on the use of ICT services, with the letter (a) concentrating on the description of those services, whether they can be subcontracted, and the conditions of said subcontracting.

Article 5 of the draft RTS introduces a completely new monitoring obligation. For this reason, we propose to delete Article 5 of the draft RTS in its entirety.

Question 5. Are articles 6 and 7 appropriate and sufficiently clear?

No

Additional comments, reasoning and suggested changes

We believe article 6(2) should be deleted as it is repetitive with Article 6(4). We see no need to share the results of the risk assessment, as prescribed in Article 6(2), as Article 6(4) already provides the right to request adjustments if a new subcontractor conflicts with the risk appetite of the financial institutions. If this risk does not exist, we see no reason why the results of the risk analysis should be shared.

Question 6. Do you have any further comment you would like to share?

We would like to share our impression that the limitation of the draft RTS to cases of subcontracting of ICT critical or important functions is not comprehensively embedded in the entire document.

In addition, we do not agree with the cost estimate made by the ESAs. The estimate is that the costs would be low, but carrying out risk assessments, making new agreements with counterparties, the proposed monitoring obligation and the general effort to continue to comply with the extensive obligations regarding ICT TPP and subcontractors are very extensive. activities that will lead to high costs.

Draft regulatory technical standards on specifying elements related to threat led penetration tests

Question 1. Do you agree with the proposed cross-sectoral approach?

Yes

Additional comments, reasoning and suggested changes

We agree using TIBER as a standard is logical, as there is already experience in the market with this methodology, and many financial entities already use the framework.

Question 2. Do you agree with the proposed approach on proportionality?

Yes

Additional comments, reasoning and suggested changes

We understand that parties enlisted as entities that must perform TLPT under art. 2(1) all have a similar degree of system relevance. Fund and asset managers are not included in art. 2(1).

However, the TLPT authority could determine an asset manager is obliged to carry out a TLPT. We would like to note that the criteria used to determine whether a financial entity must conduct a TLPT are not entirely clear. Although relevant descriptive/qualitative criteria are mentioned, no thresholds or other quantitative criteria are included, which can hinder harmonized application in the EU. Although the impact assessment shows that some consideration has been given to setting absolute thresholds (but this was not chosen as this should require regular updates), we believe that financial entities should be given more certainty. For example, some guidance for the TLPT authorities on how these criteria should be interpreted could ensure more harmonized application.

It is also important that (in accordance with recital 56 of DORA and recital 4 of the RTS) that the organization is sufficiently mature to be able to carry out a TLPT. The TLPT authority must also sufficiently take into account (as part of the maturity test, or in addition to it) the organization's IT capacity, so that the impact of a TLPT on daily operations is limited.

If these conditions are met, we agree that the principle of proportionality is applied in the way that a TLPT is only mandatory for a financial entity that meets the criteria, and that there will not be a proportionate application of the TLPT itself.

Question 3. Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT?

No

Additional comments, reasoning and suggested changes

We are not against a two-layered approach in itself. We agree with a set list of entities required to perform TLPT, and we understand that there should be an option to include other entities as well (or exclude entities). However, as mentioned in the answer to question 2: there are no absolute criteria or thresholds included in article 2(3), which could lead to different interpretation between member states.

Also the preparation phase of three months is very short, specifically for entities that are obliged to carry out the TLPT based on article 2(3). After all, they do not necessarily have to be prepared for a TLPT and therefore might need longer to prepare for a TLPT.

We therefore would like to propose that a period of at least 9 months will be used for the group of entities designated on the basis of Article 2(2) to submit the initiation documents to the TLPT authority. Given the requirements for (external) TLPT testers, it is also important to take into account that not too many financial entities have to perform a TLPT at the same time, given the availability of (qualified) testers in the market.

Question 4. Do you agree with the proposed quantitative criteria and thresholds in Article 2(1) of the draft RTS to identify financial entities required to perform TLPT?

Yes

Additional comments, reasoning and suggested changes

No comment. Fund and asset managers are not included in the list, which we agree upon. We have no comments on the criteria mentioned for other type of entities.

Question 5. Do you consider that the RTS should include additional aspects of the TIBER-EU process?

No

Additional comments, reasoning and suggested changes

No comments

Question 6. Do you agree with the approach followed for financial entities to assess the risks stemming from the conduct of testing by means of TLPT?

Yes

Additional comments, reasoning and suggested changes

No comments

Question 7. Do you consider the proposed additional requirements for external testers and threat intelligence providers are appropriate?

Yes

Additional comments, reasoning and suggested changes

We do believe that the requirements are appropriate. However, it is now entirely the responsibility of the financial entity to verify that the requirements are met. This also requires the necessary capacity of the organization, in addition to the already extensive work in the context of the TLPT. That is why, for example, a register of qualified testers would be of added value.

Question 8. Do you think that the specified number of years of experience for threat intelligence providers and external testers is an appropriate measure to ensure external testers and threat intelligence providers of highest suitability and reputability and the appropriate knowledge and skills?

Yes

Additional comments, reasoning and suggested changes

No comments

Question 9. Do you consider the proposed testing process is appropriate?

Yes

Additional comments, reasoning and suggested changes

No comments

Question 10. Do you consider the proposed requirements for pooled testing are appropriate?

Yes

Additional comments, reasoning and suggested changes

No comments

Question 11. Do you agree with the proposed requirements on the use of internal testers?

Yes

Additional comments, reasoning and suggested changes

No comments

Question 12. Do you consider the proposed requirements on supervisory cooperation are appropriate?

Yes

Additional comments, reasoning and suggested changes

No comments

Question 13. Do you have any other comment or suggestion to make in relation to the proposed draft RTS?

No

***

More information
Would you like to respond, or should you have any questions? I would be pleased to hear from you. Please feel welcome to e-mail Manouk Fles, DUFAS manager regulatory affairs, at mf@dufas.nl.

DUFAS: Dutch Fund and Asset Management Association

Since 2003, DUFAS has been committed to a healthy asset management sector in the Netherlands. DUFAS has more than 50 members: from large asset managers who invest Dutch pension and insurance assets to smaller, specialist asset managers. DUFAS increases awareness of the social relevance of investing, helps to develop sector standards and represents the sector in the implementation of new laws and regulations. In addition, DUFAS is committed to a single European market with equal regulations.