DUFAS

Dutch Fund and
Asset Management
Association

info@dufas.nl
www.dufas.nl

Response to the ESAs first batch of DORA policy products

To	European Supervisory Authorities
From	Dutch Fund and Asset Management Association (DUFAS)
Date	11 September 2023
Subject	**Response to the ESAs first 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 first batch of DORA policy products, consisting of:

- **RTS on ICT risk management framework (Art.15) and RTS on simplified ICT risk management framework (Art.16)**
- **RTS on criteria for the classification of ICT-related incidents (Art.18.3)**
- **ITS to establish the templates for the register of information (Art.28.9)**
- **RTS to specify the policy on ICT services performed by ICT third-party providers (Art.28.10)**

Main remarks

Proportionality

In general and applicable to each RTS and ITS of this first batch of DORA policy products, it should be noted that a large part of the guidance provided in the different RTS- and ITS documents presented by the ESA's effectively results in a translation of DORA Level I principle-based requirements into DORA Level II rule-based requirements and extend beyond DORA Level 1. These rule-based requirements are to a large extend based on existing requirements for a specific category of financial institutions (e.g. banks), where the requirements are not naturally also suitable for other financial institutions such as asset managers.

With the introduction of these more stringent rule-based requirements, the proportionality principle introduced in article 4 of DORA has been substantially limited, as the nature, scale and complexity of the services, activities and operations can no longer be effectively applied as a measure of proportionality. Instead, size effectively is the only remaining measure of proportionality, as a distinction is made between 'regular' financial entities, microenterprises and smaller financial entities.

As a result, a lot of the requirements of DORA Level I are translated into Level II implementation requirements that are more stringent than necessary for an asset manager to realize an acceptable level of digital operational resilience, and are most likely counterproductive in achieving operational resilience, given the great effort that must be put into Level II requirements, which, based on a risk analysis, potentially only involve insignificant risks. We

therefore argue for more discretion for the financial institutions that fall under DORA, whereby policies and processes can be designed on a risk-based basis.

An important point showing that proportionality has not been taken into account is that many obligations of the RTS- and ITS documents relate to 'all ICT assets'. We firmly believe that it is not in the spirit of DORA to classify all ICT assets or services that contain an IT component under DORA, which would mean that a caterer that uses a cash register system, or a coffee machine that contains software would be in scope. This can also be deduced from the fact that the definition of ICT services in DORA includes that it relates to digital and data services.

In addition, financial institutions work with parties to whom it is doubtful whether the DORA obligations should apply, such as the Dutch tax authorities, or even the national competent authorities. We therefore believe that certain counterparties should by definition fall outside the scope of DORA. In addition, on the basis of a risk analysis, DORA's obligations should be able to be applied to a very limited extent. This is the case, for example, with entities that qualify as CTPP and financial entities that themselves also fall under DORA and where (if necessary, based on a risk analysis) it can be determined, for example on the basis of an assurance report, that the obligations are being met.

Feedback period
Finally, we would like to mention that, although the consultations have been open for feedback for 3 months, it has been hard to collect sufficient input from the various members of DUFAS, due to the timing (holiday season), the size of (the questionnaires regarding) the various RTSs and ITSs, and of course the level of detail included in the documents.

Given that these policy documents give substance to Level 1 and given the level of detail of the documents, financial entities have an interest in responding carefully and comprehensively to the consultations. After all, the Level 2 texts have a major impact on the amount of work that each financial entity would have to carry out when implementing new rules before January 17, 2025. This should be taken more comprehensively into account when drafting provisions of the level 1 acts, as well as when scheduling future public consultations.

RTS on ICT risk management framework and RTS on simplified ICT risk management framework

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.

In general and applicable to each RTS and ITS of this first batch of DORA policy products, it should be noted that a large part of the guidance provided in the different RTS- and ITS documents presented by the ESA's effectively results in a translation of DORA Level I principle-based requirements into DORA Level II rule-based requirements. These rule-based requirements are to a large extend based on existing requirements for on specific category of financial institutions (e.g.

banks), where the requirements are not naturally also suitable for other financial institutions such as asset managers.

With the introduction of these more stringent rule-based requirements, the proportionality principle introduced in article 4 of DORA has been substantially limited, as the nature, scale and complexity of the services, activities and operations can no longer be effectively applied as a measure of proportionality. Instead, size effectively is the only remaining measure of proportionality, as a distinction is made between 'regular' financial entities, microenterprises and smaller financial entities.

As a result, a lot of the requirements of DORA Level I are translated into Level II implementation requirements that are more stringent than necessary for an asset manager to realize an acceptable level of digital operational resilience, and are possibly counterproductive in achieving operational resilience, given the great effort that must be put into Level 2 obligations, which, based on a risk analysis, potentially only involve minor risks.

An important point showing that proportionality has not been taken into account is that many obligations of the RTS- and ITS documents relate to 'all ICT assets'. We firmly believe that it is not in the spirit of DORA to classify all assets or services that contain an IT component under DORA, which would mean that a caterer that uses a cash register system, or a coffee machine that contains software would be in scope. This can also be deduced from the fact that the definition of ICT services in DORA includes that it relates to digital and data services.

In addition, financial institutions work with parties to whom it is doubtful whether the DORA obligations should apply, such as the Dutch tax authorities, or even the national competent authorities. We therefore believe that certain counterparties should by definition fall outside the scope of DORA. In addition, on the basis of a risk analysis, DORA's obligations should be able to be applied to a very limited extent. This is the case, for example, with financial institutions, entities that qualify as CTPP and financial entities that themselves also fall under DORA and where it can be determined, for example, on the basis of an assurance report, that the obligations are being met.

The articles below are other examples that show that proportionality has not been sufficiently taken into account. Due to lack of space to answer in full (character limitation in the survey), more examples are also given in the other answers to the questions of the consultation.

- Article 3 (2)(e) prescribes that 'any changes to their ICT landscape' should be monitored. This is unproportional and should only relate to significant changes.

- Article 10 (2)(b) prescribes that automated vulnerability scanning must be performed at least on a weekly basis. The frequency (and method) of a scan and assessment should depend on the specific circumstances.

- Article 10 (2)(c) prescribes that ICT third party service providers should report any vulnerability to the financial entity. This could lead to an overload of reports to the financial entity, which are costly to integrate in existing vulnerability management systems. The

financial entity and the ICT third party service provider should be able to agree on which vulnerabilities must be reported and which are not significant and therefore do not need to be reported.

- Article 17 (2) prescribes all changes to software, hardware, firmware components, systems or security parameters shall be included in the ICT change management procedure. In order to limit the scope and make the workload manageable, significant changes should be considered here only instead of all changes. A less stringent procedure could also apply to minor changes.

- Article 27 (2) lists the scenarios that must be taken into account as a minimum in the response and recovery plans. However, the financial entity itself will have to determine which scenarios are relevant to include.

- Article 29 seems to suggest that in the case of increased complexity or risk, the measures the financial entity takes should be intensified. While this should of course be taken into account, it should also work the other way around: it should also be possible to take 'decreased complexity or risk' into account. This is not apparent from the exact wording of the article. Proportionality should work both ways, and we therefore suggest to remover the wording 'increased'.

Q3: Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.

- Article 2 (1)(b) seems to imply the control function "manages" the financial entity's ICT risk. This should be clarified to avoid the suggestion that first and second line activities (as defined in the three lines of defense-model) spill over.

- Article 2 (1)(c) requires the financial entity to implement qualitative and quantitative measures, although article 6 (8) of DORA is not requiring to do so. In order for the financial entity to define suitable and proportionate ICT and information security measures based on identified risks, it should be up to the financial entity to select qualitative or qualitative measures, or both of them. We would suggest to remove the wording 'qualitative and quantitative'.

- Article 2 (1)(d) prescribes the control function should remain independent from the function or functions in charge of the ICT development, management, changes and operations. For firms with smaller ICT teams, the control function may not be completely separate, or may be assigned parttime to a person also performing other tasks within the ICT team. Article 6 (4) of DORA refers to an 'appropriate level of independence' which seems to leave more room to implement the control function, and would be more in line with the principle of proportionality.

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

We believe that the ICT risk management policy and procedures should be risk-based and more in line with the principle of proportionality. As risk is measured as a combination of likelihood and impact, non-critical systems have a lower impact value and therefore present a lower risk. For any lower risk ICT asset a less rigid approach should be expected.

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

We do not agree with the approach. Article 4 (2) relates to 'all ICT assets' and 'each ICT asset', from which it can be concluded that every ICT asset is in scope. The definition of an ICT asset is also very broad, which means that there is an enormous amount of work involved in creating and maintaining a record. From a proportionality point of view, a financial entity should be able to consider leaving certain ICT assets out of scope, or including limited information in the record, based on the risks identified. The RTS should be amended to either include a list of critical assets that need to be included in the register, or allow a financial entity to draw up a risk based ICT asset register.

It is unclear what is meant by 'authenticity' as referred to in article 5 (1) (also used in other articles of the RTS), as the CIA triad often only refers to availability, integrity and confidentiality.

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?

This could be included as a part of regular lifecycle management. However, that would also hinge on suppliers consistently sharing EOL/EOS dates in a manner that supports ICT asset and lifecycle management. If financial entities would be regulated on this aspect, it would be necessary to enforce consistent rules on all relevant soft- and hardware providers.

Also, this is only important for ICT assets supporting critical and important business functions, and even for critical and important business functions, not all ICT assets should be in scope of this recordkeeping of EOL/EOS dates. It should be left to the financial entity itself to determine (based on the risks involved) for which ICT assets this is relevant.

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

- Article 6 (2)(a) states 'data in use', but does not define what this entails. If this means adherence to (for instance) confidential computing (i.e. encrypting data in use in memory) the consequences could be significant and cost-prohibitive. The RTS should be amended to clarify the definition and scope of data in use. Also, we are wondering what is meant by a 'separate environment' (a separate environment per ICT asset, similarly classified set of data or general processing environment?).

- Article 6 (3) is referring to 'leading practices', where it is not entirely clear which leading practices are meant. We suggest removing this wording as it may be confusing and financial entities will always look at market standards and developments from a risk perspective. We've also noticed that some documents on the websites of what could be considered as parties providing guidance on 'leading practices' are outdated or publication is very infrequent.

- Article 7 (1) is referring to article 6 (2) point d, which doesn't exist. We suspect that article 6 (2) point c is meant.

- Article 7 prescribes that financial entities shall maintain a register of certificates and certificate storing devices. All endpoints (phone / laptop) and servers use several certificates. Aside from being a largely redundant form of registration, the point of the RTS is to aid certificate lifecycle management. This requires visibility – the current wording imposes the risk that the register would be drafted as a point in time register. We would recommend a different approach in which certificate lifecycle management is embedded through (for instance) CMDB-enforcement.

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

- In general we believe that the principle of proportionality hasn't been taken into account. Please see our answer to question 1.

- We are of the opinion that the obligations of article 8 should not relate to every ICT asset. Having to completely document and implement this end-to-end for each and every ICT asset would lead to an unacceptable additional workload and amount of documentation. We therefore believe a risk-based approach should be applicable. For further comments, please see our response to question 1.

- Article 8 (2)(b)(iv) contains requirements to ensure internal audits pose minimal disruptions. It is unclear what impact this clause has on existing codes imposed by auditing bodies, as it could be construed as a limitation in performing an audit.

- Article 8 (2)(b)(v) is very prescriptive regarding segregation of environments. This does not align with current software development methods (Agile / DevOps / DevSecOps) and poses restrictions which could decrease resilience as a result of longer time to market.

- Article 10 (2)(b): the RTS seems to hinge on two possibilities regarding vulnerability scanning. Either perform risk based scanning in accordance with internal assessments, of be fully prescriptive of scope, frequency and depth and breadth of scanning. The current clause does not provide the necessary clarity. We suggest to remove the sentence that prescribes the weekly scanning. DUFAS is not in favor of stringently prescribing a frequency and method for a vulnerability scan, because the financial entity must be able to determine this on the basis of the circumstances and the associated risks.

- Article 10 (2)(d) seems to require a 'software bill of materials'. This would be a significant undertaking if software developers do not regularly and clearly communicate software composition (for example due to legal considerations or a lack of software insight). Wording should be amended to less prescriptive terms (e.g. 'to the extent feasible or necessary to gain insight in material risks related to software components')

- Article 10 (2)(e) prescribes financial entities to establish procedures for responsible disclosure of vulnerabilities to clients and counterparts as well as to the public, as appropriate. It is unclear when it is appropriate to disclose a vulnerability, specifically to clients and the public, as it might lead to confusion, taking into account that only a vulnerability doesn't mean there is a data breach. It is also an additional administrative burden for firms to disclose vulnerabilities. We therefore suggest that disclosure of vulnerabilities should be done with great restraint.

- Article 11(2)(b): reference is made to international standards. It is unclear what exactly is meant by an international standard. For example, it is unclear whether this includes the current framework the Dutch Central Bank is using.

- Article 11(2)(d) should in the opinion of DUFAS be amended to focus on secure software development. Unintentional mistakes do not necessarily qualify as malicious code, but can create an attack vector using malicious code.

- Article 11(2)(f) regarding requirements to secure the use of portable endpoint devices and private non-portable endpoint devices is detailed and very prescriptive. Based on the circumstances and the risks, the financial entity should be able to make its own assessment, which would be in line with the principle of proportionality.

- Article 12 relates to logging. Logging should be done proportionate to the risk exposure. If there would be no room for proportionality, this would be a tremendous amount of work and strain on resources to develop, implement and maintain ICT assets in combination with significant operational costs.

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.

The impact on weekly vulnerability scans for all ICT assets will be gigantic and unmanageable. The definition of an ICT asset is very broad and the question is whether an automated vulnerability scan would even be possible for every ICT asset. DUFAS is not in favor of stringently prescribing a frequency and method for a vulnerability scan, because the financial entity must be able to determine this on the basis of the circumstances and the associated risks. Furthermore, considering the environmental impact of this frequent vulnerability scanning, this would negatively impact the financial sectors reputation, taking into account the amount of computing resources this would globally waste on a weekly basis.

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

- Article 13 (1)(a): whilst we see segregation/segmentation as a key measure to prevent lateral movement, segregation and segmentation of ICT systems and networks is not feasible for all systems and networks. For certain services, such as standard productivity tooling or data storage services, segregation and segmentation would be very costly to maintain, especially when used within a larger group structure. It is therefore important that proportionality is taken into account, which should be the case for entire article 13.

- Article 13(1)(c) should clarify what constitutes a separate network (different VLAN, different LAN, separate physical connection, etc.) Also, the RTS expects the use of a separate and dedicated network for the administration of ICT assets and prohibition of direct internet access. We believe that this obligation is excessive, mainly for smaller entities.

- Article 13(1)(e) seems to imply the encryption of all data on all networks. This should not be the case, but should be based on an own risk assessment by the financial entity.

- Article 13 (1)(h) also prescribes the minimum frequency for performing a review of firewall rules and connection filters for the ICT systems supporting critical or important functions. Here too, the financial entity should be able to apply proportionality to determine the most appropriate frequency.

- Article 14(1)(a) should be amended to include non-repudiation, in cases where the situation requires it.

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

- Article 16 (3): we are of the opinion that specific network, firewall and connectivity services should be excluded. There is, for example, typically no test network. And we assume that no entity would for instance have duplicated test network infrastructure SWIFT or Bloomberg in place. Having a complete duplicate test environment would have significant cost implications and is not needed with appropriate procedural safeguards.

- Article 16 (4) and (9): source code is typically seen as intellectual property and third party service providers will not want others to perform reviews/testing, rendering this article very hard or even impossible to comply with. Particularly ICT third party service providers who produce standardized (non-customised) software or deliver a SaaS will have already carried out extensive tests. The financial entity should be able to make agreements about this with the ICT third-party service providers, for example by receiving test reports or by relying on an assurance report. The manner and extent of the testing should depend on the specific circumstances.

- Article 16 (6): In practice, using (some) production data for testing can be very valuable and is market practice. Systems in the financial services industry are heavily linked, and isolated non-production environments would be near-impossible to set up.
  Testing with production data mitigates the risk of implementing errors with large impact (especially to financial institutions), in specific cases outweighing confidentiality when it concerns non personally sensitive data, because of:
  - The ability to test system performance with production-like data;
  - The ability to compare results with other environments to which an interface exists or production systems;
  - Complex implementations impacting multiple systems require extensive testing. Doing this with production-like data increases reliability; and
  - It enables testing of the data quality of data retrieved from external data vendors

  Most products available in the market today do not offer options to generate randomized or anonymized data.

  The derogation in art. 16.7 does not provide workable situation (see above).
- Article 17 (2): firms should be able to make exceptions for elements that relate to changes of ICT assets form third party service providers. This should be done on a proportionate and risk based approach.

- Article 17(2)(b) prescribes a mandatory separation between the requestor and approver of a change. We understand that it is not always in line with current market practice. However, it is important that there is assurance in the change management chain, so we propose that the RTS focuses on this. For example, a requestor can request a change, where, for instance CI/CD automatically tests the code and then releases it. It's important that the RTS leaves room for these types of innovations.

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.

In general the RTS should provide mechanisms for micro third party service providers who would be severely impacted by DORA, such as organizations with only a few (<10 persons) software developers. These parties may not be able to meet all the requirements set by DORA but can deliver mission critical services in some cases. The RTS or DORA should provide means to ensure operational continuity in these cases.

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

There should be a clear exception for third party service providers, permitting oversight via assurance reports or specific certifications. For instance SaaS assets are hosted in data centers globally and third parties typically will not be provided much insight into the physical security measures.

Q20: Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.

Article 19(1) states that specific ICT security awareness programs and digital operational resilience training must include the elements mentioned. We believe that the term 'specific' is not needed, as article 13 of DORA already mentions ICT Security programs etc. It can be up to the financial entity whether to include this in regular or specific programs.

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.

- Article 20: Firms should be able to differentiate between own HR and HR at third party service providers. Aside from assuring that third parties have policies and access control in place (usually done via assurance reports, such as SOC reports), firms should not be required to validate third party service providers staff.

- Article 21 (3) (numbering is incorrect as paragraph 1 is missing): the elements of the identity management policy should be considered on the basis of risks involved. For a significant number of ICT systems, maintaining a record with all identity assignments is difficult and time consuming and outweighs the associated risk. This should be limited to ICT assets supporting critical and important functions. DORA provides for annual checks in article 22 (1)(e)(iv) on all ICT systems in any case.

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.

Yes. No further comment necessary.

Q24: Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.

Yes. No further comment necessary.

Q25: Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.

We suggest that article 25(2)(a) should clarify the legal definition of central counterparties and trading venues (by referring to legislation in which these definitions are already used).

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.

Article 28 includes a very prescriptive list of information to be included in the report. In particular article 28 (2)(h)(iii) that requires to include tools to be used and whether staff in charge to carry out the measures is internal/external lead, does not seem proportionate.

Developing and documenting this report would require tremendous resources. However, the information required would be available if needed, so we suggest that data should be provided to the competent authority on request, instead of drafting a report in advance.

RTS on criteria for the classification of ICT-related incidents

Q1. 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.

DUFAS is in favor of clarifying the classification of an '(major) incident', although the RTS contains a methodology which is very complex and burdensome. It would require monitoring of all the proposed criteria and gathering of evidence which in many cases will not result in detecting an incident.

The aim of the ESA's is a harmonized framework, but we agree with the ESA's: there are differences between sectors, business models and regulatory requirements, and proportionality needs to be observed. Additional testing of criteria and thresholds is therefore necessary.

Q2. 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.

A mechanism should be added to the RTS to separate major incidents at small financial entities, which have no further impact whatsoever. Based on the proposed wording, an interconnected asset manager with for example 10 customers needs to report every incident relating to a customer. This would create difficulties in drawing meaningful conclusions from incident reports on a national or EU level.

A suggestion for this requirement would be to introduce a consolidated approach for these cases, whereby the asset manager and its affiliated clients are considered one and the requirement is applied to the (end-)clients of the affiliated clients. Such an alternative approach could be structured as a counter evidence, whereby the asset manager and its affiliated clients can only apply this exception to the main rule if they can substantiate its effectiveness.

Q3. Do you agree with the specification and thresholds of the criteria 'Reputational impact', 'Duration and service downtime', 'Geographical spread' and 'Economic impact', as proposed in Articles 2, 3, 4, 7, 10, 11, 12 and 15 of the draft RTS? If not, please provide your reasoning and suggested changes.

<u>Reputational impact:</u>

The RTS relates to 'any impact', which could result in overreporting. This is also combined with a very broad definition of reputational impact in article 2, which for example speaks of "media attention".

Duration and service downtime:
The duration of an incident is irrelevant as long as sufficient good alternative measures have been taken; if the failure of a system is covered by adequate backups/workarounds, then this is not a factor for the materiality of the incident, as the service to the client may still be available.
We would also like to highlight that a downtime of 2 hours is too short, and could result in overreporting.

Geographical spread
This materiality threshold does not always seem to add value. For example the number of clients affected: many financial entities operate across borders, as intended by the capital market union. If two clients are affected, it shouldn't matter whether one of them is just within or just on the other side of any Member State's border.

Q4. 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.

We believe that with regard to inaccessibility or un-usability, the measurement of time (how long data was inaccessible or unusable) needs to be taken into account in order to be able to determine 'data loss'.

We also question how to differentiate between the trustworthiness and reliability of data and the integrity of data. The link with trustworthiness and reliability of the source of data does make sense.

Q5. 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.

It is not clear what is meant by 'services or activities which require authorization' in article 6. It would be preferable if no extra definitions would be created, and this criterium would only relate to the definition of major ICT-related incidents in article 3(10) of DORA.

With regard to the threshold: whether or not an incident is escalated to senior management is dependent on the financial entity's internal governance, rather than an indicator of the materiality of an incident. It could even provide an undesirable incentive not to escalate an incident internally (in order to avoid having to report to the NCA).

Q6. 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. Please also indicate how often you face recurring incidents, which in aggregate meet the materiality thresholds only over a period of 6 to 12 months based on

data from the previous two years (you may also indicate the number of these recurring incidents)

It seems logical to include these incidents, although it is administratively difficult to keep track of this and to report it in a timely manner. Secondly, for regulators to make effective use of this data it would require an international framework regarding root causes. Thirdly, a mechanism needs to be implemented to withdraw or amend incidents where a root cause is later to be found different than previously reported.

Q7. 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

The classification of a cyber threat in itself is clear. However, based on the obligation to report significant cyber threats to clients 'where applicable', as included in Level I of DORA, we would like to emphasize that not every significant cyber threat should be reported to the client. The financial entity would have to assess this based on the circumstances and the risks (this could link more explicitly to objective scoring frameworks (CVSS / ATT&CK / etc.). If there is a cyber threat, the risk has not yet materialized and informing clients can lead to unnecessary market turmoil. This could be further clarified in the RTS; only threats with significant impact and probable chance of occurring should be shared with the clients it concerns (i.e., a specific software vulnerability under active exploit is only shared with clients using the software package/version/configuration).

Q8. 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.

We see the added value of sharing this data between Member States. However, the sharing of data is extensive and not anonymized. This entails risks, for which the Member States must set up proper safeguards. Also, sharing this data should not have any consequences for the reporting financial entity and there should be no additional work for the reporting financial entity involved. Finally, ESA's should be aware of the risk of centralizing major incident information on an EU-level, its importance to (state) actors and their responsibility in managing and securing this information.

ITS to establish the templates for the register of information

Q1. Can you identify any significant operational obstacles to providing a Legal Entity Identifier (LEI) for third-party ICT service providers that are legal entities, excluding individuals acting in a business capacity?

LEI is used worldwide, so seems to be the most appropriate method. Not every provider may currently have an LEI, but applying for an LEI (at least in the Netherlands) is not difficult.

The disadvantage of LEI is that an LEI expires. Since the RTS prescribes an 'active' LEI, there will be a lot of maintenance involved in keeping track of the LEIs of service providers. The addition of 'active when entering into the contractual relationship' would mitigate this. Alternatively, a yearly review of the LEI being active should be sufficient.

Q2. Do you agree with Article 4(1)b that reads 'the Register of Information includes information on all the material subcontractors when an ICT service provided by a direct ICT third-party service provider that is supporting a critical or important function of the financial entities.'? If not, could you please explain why you disagree and possible solutions, if available?

In order to determine which parties are in scope, the direct ICT third-party service provider supporting a critical or important function of the financial entity, must first be identified.

Subsequently, it must be determined which subcontractors of that ICT third-party service provider are material.

- The main question here is: who determines who is a material subcontractor? Is that the financial entity or is that the ICT third party service provider? The financial entity will have to be able to rely largely on what the ICT third party service provider indicates as an important subcontractor.

- Another relevant question is: should materiality of the subcontractor be determined from the point of view of the ICT third party service provider itself or from the point of view of the financial entity and the service used by the financial entity? An important subcontractor of the ICT provider isn't necessarily directly relevant for the ICT services provided and therefore relevant to the financial entity.

More fundamentally, smaller ICT third party service providers may not be able or willing to comply with DORA, causing them to exit the market. This might inadvertently result in a larger concentration risk. Proportionality in laying through the terms of DORA would help to mitigate this risk and could counter inadvertent concentration risk.

RT.05.01 and RT.05.02 and the explanation to it in Annex I do not deviate between material and other subcontractors of the TPSP. All subcontractors of the direct third party service provider should be listed (supply chain). What exact information is meant here as a 'top-up' on 'material subcontractors' to the generic info produced on subcontractors in general? Does article 4 (1)(b) imply requirements for material subcontractors additional to the general RT.05.02 requirements that apply to all subcontractors?

Q3. When implementing the Register of Information for the first time:

- **What would be the concrete necessary tasks and processes for the financial entities?**
- **Are there any significant operational issues to consider?**

Please elaborate.

The register must be completed by 17 January 2025, also for existing contracts. Given that the definition of ICT third party provider is extremely broad, the size of the register is potentially also enormous. Given the large amount of data per ICT third party provider, it becomes very challenging to have all this information ready. Please note the comments that we provided about the scope of ICT assets and services in question 1 regarding the RTS on ICT risk management tools methods processes and policies.

We also want to emphasize that the template differs from the standard that is now used for outsourcing. We would like to insist that the template is in line with the standard in the context of outsourcing, or both registers should be even combined in one.

Q4. Have you identified any significant operational obstacles for keeping information regarding contractual arrangements that have been terminated for five years in the Register of Information?

With regards to the amount of work required to implement the register, it would be disproportionate to include contracts that have been terminated for five years, in the second year of the register. The RTS should be amended to reflect that, until 2030, financial entities should indicate, each year, which contracts are being terminated. By 2030, the register would then contain a five-year history of terminated contracts, and going forward will be maintained as currently intended by the RTS.

As the aim of DORA is to make sure that 'digital operational resilience' is sufficiently met by financial entities, we wonder what is the objective of keeping information on terminated contracts for 5 years after the relation with the supplier has ended.

Q6. Do you see significant operational issues to consider when each financial entity shall maintain and update the registers of information at sub-consolidated and consolidated level in addition to the register of information at entity level?

We are of the opinion that the obligation that each entity apart from its own register would also maintain and update the register on sub-consolidated and consolidated level is highly excessive and will lead to duplication of work.

Also, different entities can rate third party service providers differently, which could lead to issues when a group has multiple contracts with the same third party provider (i.e. one third party service provider providing BPO and IT support to two in-group FE's).

Q7. Do you agree with the inclusion of columns RT.02.01.0041 (Annual expense or estimated cost of the contractual arrangement for the past year) and RT.02.01.0042 (Budget of the contractual arrangement for the upcoming year) in the template RT.02.01 on general information on the contractual arrangements? If not, could you please provide a clear rationale and suggest any alternatives if available?

We believe that this information is commercially sensitive and we do not see the rationale behind this obligation. We also foresee some practical issues, such as the enforcement of Chinese walls between in-group entities. We would suggest to have these costs paragraphs deleted.

Q8. Do you agree that template RT.05.02 on ICT service supply chain enables financial entities and supervisors to properly capture the full (material) ICT value chain? If not, which aspects are missing?

Please see the answer to question 2.

Q9. Do you support the proposed taxonomy for ICT services in Annex IV? If not, please explain and provide alternative suggestions, if available?

We support a taxonomy to be in place. We firmly believe that it is not in the spirit of DORA to classify all assets or services that contain an IT component under DORA, which would mean that a caterer that uses a cash register system, or a coffee machine that contains software would be in scope. This can also be deduced from the fact that the definition of ICT services in DORA includes that it relates to digital and data services.

In addition, financial institutions work with parties to whom it is doubtful whether the DORA obligations should apply, such as the Dutch tax authorities, or even the national competent authorities. We therefore believe that certain counterparties should by definition fall outside the scope of DORA. In addition, on the basis of a risk analysis, DORA's obligations should be able to apply to a very limited extent. This is the case, for example, with financial institutions, entities that qualify as CTPP and financial entities that themselves also fall under DORA and where it can be determined, for example, on the basis of an assurance report, that the obligations are being met.

Q10. Do you agree with the instructions provided in Annex V on how to report the total value of assets and the value of other financial indicator for each type of financial entity? If not, please explain and provide alternative suggestions?

Yes.

We would like to ask for confirmation that an AIF with a permit to provide MiFID-services (top-up) falls under the category sub (k).

Q11. Is the structure of the Register of Information clear? If not, please explain what aspects are unclear and suggest any alternatives, if available?

The register holds a lot of different types of information, and has a lot of cross references in it. Both aspects add to the complexity of the register. We doubt whether all information provided via the register is indeed that important (for the regulator) to have a full overview to make sure that the 'digital operational resilience' of EU financial entities is guaranteed. We would like to propose to create a more workable register.

Q12. Do you agree with the level of information requested in the Register of Information templates? Do you think that the minimum level of information requested is sufficient to fulfill the three purposes of the Register of Information, while also considering the varying levels of granularity and maturity among different financial entities?

Please see the answer to question 11. We would also like to stress that the time for financial entities to implement the register is very short.

Q13. Do you agree with the principle of used to draft the ITS? If not, please explain why you disagree and which alternative approach you would suggest.

We are not sure what the question is, it seems the wording of the question is not complete.

RTS to specify the policy on ICT services performed by ICT third-party providers

Q1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?

In general, the text of the articles is clear. However, we believe that the principle of proportionality has not been taken into account in the entire RTS. More specifically, the following articles are examples that show that proportionality has not been sufficiently taken into account:

- Article 2 prescribes that the parent undertaking is responsible for ensuring that the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as referred to in Article 28 (2) of DORA, is implemented consistently in their subsidiaries and is adequate for the effective application of this Regulation at all relevant levels. There is no room for another (perhaps more appropriate) way of allocating responsibilities.

- Article 3 prescribes that the financial entity assesses that the ICT third party service provider has sufficient resources to ensure that the financial entity complies with all its legal and regulatory requirements. There is no room for proportionality.

Also, article 1 specifies that 'elements of increased complexity or risk' must be taken into account. The article seems to suggest that in the case of increased complexity or risk, the measures the financial entity takes should be intensified. While this should of course be taken into account, it should also work the other way around: it should also be possible to take 'reduced complexity or risk' into account. This is not apparent from the exact wording of the article. Proportionality should work both ways, and we therefore suggest to remover the wording ‘increased’.

Q5: Are articles 6 and 7 appropriate and sufficiently clear?

Article 7 (1)(e) is noteworthy because it anchors social and environmental responsibility with third party service providers. Currently, some of the measures suggested in other RTS’s have a significant environmental impact.

Although we believe these are important elements in due diligence on suppliers (in general, not only related to ICT services) we wonder if DORA is the right place to address this, as it’s already part of other extensive legislative packages.

Q9: Is article 11 appropriate and sufficiently clear?

Article 11 should be amended to reflect that it is not feasible to draw up a realistic and manageable exit plan during contracting. A exit strategy (more abstract) should suffice, if legally binding and providing adequate assurances to all parties that the exit strategy is feasible, realistic and effective.

***

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.