Betaalvereniging Nederland

Feedback on the draft Digital Operational Resilience Act

Introductory Remarks

The Dutch Payments Association (DPA) on behalf of its members welcomes the opportunity to share views on the Commission's proposal of a Regulation on Digital Operational Resilience for the financial sector (DORA). Based on the DPA key messages on DORA, the following positions and suggestions of amendments reflect the current understanding of our Dutch member banks. The DPA will continue position building, reflecting the discussions throughout the advancing EU legislative process.

As a central aspect, DORA should adopt a risk-based approach and follow the principle of proportionality. ICT incident reporting requires harmonization and EU-wide mutual recognition of digital operational testing should be facilitated. Information-sharing arrangements among trusted circles should be of voluntary nature. The upcoming various Regulatory Technical Standards (RTS) delegated to the ESAs should provide flexibility in the measures they adopt. When the European financial sector is regulated by DORA it should be tangible how the allocation of responsibilities among EU authorities and/or NCA's is organised so that they remain informed and feel themselves responsible for national financial entities.

Alignment of DORA's requirements for financial entities with existing supervisory guidance under the EBA guidelines on outsourcing and ICT and security risk management is necessary. Also a smooth introduction of DORA into the array of legislation with other reporting provisions (NIS2, PSD2, GDPR, RCE) is of great importance. An appropriately designed oversight framework for critical ICT third-party providers (CTPPs) should be of added value for CTPP-customers, while access to innovation must not be detrimentally limited due to disproportionate obligations and limits for the provider selection. And as a final point, we would like to see a unified EU lexicon for the definitions and terms used in DORA. To that end, the DPA offers constructive suggestions to the Commission to adjust details of the envisioned oversight.

1. Management of ICT risks; DORA sets out key principles around internal controls and governance structures.

1.1. Summary

The DPA calls for a risk-based approach and the consistent application of the proportionality principle in the ICT Risk Management provisions.

1.2. General commentary

If the European financial sector is regulated by a harmonised Single Rulebook and governed by a European system of financial supervision, how will the relationship and/or governance with national competent authorities be organised so that they remain informed about the national financial entities?
From a control perspective we think it is valuable to align with local governing bodies ('national initiatives') to incorporate best practices, supporting controls and removing ineffective controls. Also of great importance is to align with local ruling entities to define a smooth transition to a single standard framework.

In general, the proposed legislation is in line with the EBA guidelines and other regulation regarding ICT risk management. As for ICT governance, we think it is positive that DORA aims to streamline and upgrade the existing rulebooks. This creates one level playing field within financial system for all types of regulated EU financial entities. However, at this moment Dutch banks already comply with the EBA guidelines on ICT and security management (2019), Directive on Security of Network and Information Systems (2016/1148) and PSD2 (2018). It has taken time to implement this with the entities. If totally new regulatory technical standards are released, banks/FI's will need considerable time to comply with them. Therefore the ESAs and ECB, together with ENISA, should consider establishing an overall ICT risk management framework based on existing regulations while reusing earlier regulatory technical standards.

Furthermore we wonder whether it will be left up to the discretion of the Member states and national competent authorities to reach their own interpretation on ICT governance throughout the union. We would like to see some guidance in this matter.

For financial institutions it would be helpful if ESA's would be able to mark those parts of DORA that are new and those that are (partly) overlapping with parts that already exist in other regulations.

To help financial organizations become more agile and flexible, the burden of demonstrating operating effectiveness to multiple instances such as the Dutch Central Bank or ECB (JST) based on potentially deprecated frameworks should be eradicated. Another aspect is when it comes to defining new or improved requirements: it would be hugely beneficial when organizations are able to automate supporting controls.

1.3. Comments on specific Articles:

With reference to Article 5.9(g) we would like to point out that a multi-vendor strategy at entity level might be overly restrictive, more so considering that many outsourcing decisions are taken on a strategic level, including a concentration risk assessment and mitigation at group level. Moreover it is not easy to switch to multiple vendors as there aren't always enough qualitative alternatives for certain services in the market. Even the migration process toward another provider may take years and possesses risks on its own. Therefore we recommended that the requirement for a multi-vendor strategy is not mandatory, and that the use of multi-vendor strategies remains a risk-based business decision of financial entities.

With reference to Article 8.3 *Protection and Prevention* we urgently request to remove 'state-of-the-art'. It might imply that mainframes or COBOL programmes are no longer allowed for banks? The requirements for ICT protection and prevention are at risk of becoming obsolete over time as new technologies emerge. Some terms, such as 'state of the art' should be reconsidered as they do not provide clear expectations to financial entities. We recommend that flexibility is provided to financial entities when performing protection and prevention activities to not impeded technology developments and adoption and ensure financial entities can adjust relevant controls.

With reference to Article 9.3 *Detection* it is currently unclear how financial institutions should evidence the devote sufficient resources and capability. We worry that it may lead to different interpretations of this by the NCA's in the EU member states and thus does not create one level playing field for all types of regulated EU financial entities.

1.4. Detailed comments on other relevant Articles

Article 2.(1): We recommend that with regard to the ESAs' designation of critical ICT third-party service providers (Art. 28) it is clarified that ICT providers that are part of a group, for example permanently affiliated to a central body as per Art. 10 or 113(6) CRR, are excluded by this mechanism.

Article 3.(1): The definition of digital operational resilience is not consistent with existing global definitions such as the Basel Committee for Banking Supervision (BCBS). Global consistency for definitions and terms applicable to operational resilience will provide clarity for financial entities, particularly for those operating cross-border. Any divergence will increase the burden on cross-border financial entities who will be required to reconcile different interpretations to meet similar regulatory expectations in different jurisdictions. We recommend that the definition of operational resilience is amended to be consistent with the BCBS definition.

Article 3.(2): Several other definitions are inconsistent in the proposal with globally recognised terms, such as in the FSB Cyber Lexicon. We recommend that these definitions are amended to be consistent globally with the FSB Cyber Lexicon. These include: network and information system (Art. 3.2); Information asset (Art. 3.5); ICT-related incident (Art. 3.6); Cyber threat (Art. 3.8); Cyber-attack (Art. 3.9); Threat intelligence (Art. 3.10); Defence-in-depth (Art. 3.11); Vulnerability (Art. 3.12); and Threat led penetration testing (Art. 3.13).

Article 3 (3–7): To be consistent in terminologies and their usage, rather use impact on critical business processes / services instead of critical functions since classification of business process is what financial entity does.

Article 3.(15): Article 3.(15): 'ICT third-party service provider', DORA defines the scope of third-party suppliers with a different logic than the European Banking Authority (EBA). According to the EBA, the ICT risks must be considered for all providers, in application of the guidelines on ICT risks and outsourcing. To ensure consistency with the existing EBA Guidelines on outsourcing arrangements, definitions such as 'ICT third-party service provider' (3.15), and 'ICT services' (3.16), should be aligned with the concept of outsourcing according to the EBA Guidelines (section 3). This should also include exceptions which would not be subject to the EBA Guidelines (paragraph 28).

Article 3 (18): The definition of critical third-party providers is an important gateway to target DORA's new regulatory safeguards (oversight) properly to those providers that currently are not addressed by EU level oversight. Where oversight or supervision already applies to entities via existing financial regulation, no duplicating requirements should be issued. This is the case for intra-group outsourcing of ICT services within financial groups meaning an ICT service provider that is part of a group of institutions permanently affiliated to a central body as per Art. 10 or 113(6) CRR or within the same institutional protection scheme as per Art. 113(7) CRR or where credit institutions are associated in a network in accordance with legal or statutory provisions as per Art. 400(2)(d) CRR. They should not be covered by DORA. Different from external third-party providers, these entities are already subject under the chain of financial regulation and respective supervision processes. Risks to operational resilience are therefore not unaddressed and – in turn – no gap needs to be closed by DORA. Banking groups already comply with EU regulation today, advancing operational resilience in line with EU law. An introduction of additional mandatory governance requirements for intra-group constellation does not add

additional security, but rather faces entities with more complexity, making the organization of resilience more difficult.

Article 4.2: We believe that financial entities should continue to have flexibility for the definition, approval, and overseeing of all arrangements related to the ICT risk management framework as is appropriate within existing governance models. The need for the management body of a financial entity to define and approve specific risk type policies is overly prescriptive as set out in the proposal. We recommend that flexibility is maintained for financial entities to perform these activities as appropriate to the risk and expertise required.
We believe that the scope of 'ICT Business Continuity policy' (Art. 4.2.d) should be defined in relation to existing Business Continuity Policies that already refer to Disaster Recovery Policies and Cyber Policies, and are specific components of Business Continuity Plans (e.g. Disaster Recovery Plan, Cyber-Attack Plan).

Article 5.5: The DPA proposes to amend the definition of 'microenterprise' and align it to that of "small and non-complex institution" already enshrined in CRR2 (Art. 4 (145)). The wording 'microenterprise' should then be replaced throughout the legislative proposal (Recitals 34 and 35, Articles 4.3, 5.4, 5.5, 7.3, 7.7, 10.3, 10.5, 10.6, 10.9, 12.2). The EU definition of "microenterprises" (with a balance sheet total ≤ € 2 million according to EU Recommendation 2003/361) does not work for banks and especially not for small and medium sized co-operative banks, because neither the balance sheet total nor the number of staff is of sufficient importance to classify small or medium-sized banks.

Article 5.9: The need for an extensive range of additional governance and controls as part of the ICT risk management framework will lead to an additional administrative burden and increased inefficiencies for financial entities, providing limited value-add to financial entities in terms of risk mitigation. For example, the ICT risk management framework contains an information security management system, a digital resilience strategy, a ICT business continuity plan, an ICT disaster recovery plan, incident communication strategies, ICT reference architectures, mappings of ICT systems, and an information security policy. Each must be documented and collated under a single IT risk management framework. We recommend that greater flexibility is provided to financial entities in how the ICT risk management framework is developed and implemented, leveraging existing and mature governance structures, processes, documentation, and controls. This will reduce the compliance burden and duplication with financial entities existing arrangements.

5.9b: Terms such as 'impact tolerance' are provided without any definition and clarity is required.

5.9d: ICT risk management framework: is way too much content to include by a Risk department in a risk management framework. In a risk framework we would expect controls that there needs to be a ICT reference architecture. Large banks have many Enterprise Architects working on this daily.

Article 5.10: Does this mean that our IT risk framework needs to be approved by regulators? The DPA recommends amending an exemption for banking groups for which the competent authority may grant an approval for the whole group if the task is delegated to the same intra-group undertaking.

Article 6.2: We support regulators efforts to acknowledge the use of internationally recognised standards and industry leading practices on information security and ICT internal controls. To promote consistency across financial sector and reduce regulatory fragmentation, financial institutions from various jurisdictions along with other industry associations developed in 2018 the Cyber Risk Institute's (CRI) Cybersecurity Profile ("Profile"). The Profile is a globally recognised, scalable and extensible assessment tool. The list of questions is based on the intersection of global regulations and cyber standards, such as ISO and NIST that financial institutions of all types can use for internal and external (i.e., third-party) cyber risk management and as a mechanism to evidence compliance with various regulatory frameworks, globally. We recommend EU policymakers consider the Profile as an internationally recognized technical standard/industry leading practice on information security and ICT internal controls.

Article 7.1: Several terms proposed do not provide clarity on how to appropriately implement the requirements in line with current principles and risk-based practices. For example, how financial entities shall identify, classify, and adequately document all ICT-related business functions, and what constitutes a major change and an appropriate risk assessment (Art. 7.3).
Mappings contain highly sensitive information; therefore, appropriate safeguards should be in place to protect them. We recommend that a more proportionate approach to mapping requirements is proposed to address these challenges. In addition, we recommend that flexibility is provided to financial entities to determine what would be an adequate level of mapping to meet the intention of the requirements, especially where it is more appropriate for financial entities to continue performing these activities within existing operational resilience objectives (and aligned to the mapping requirements under the EBA ICT Guidelines).

Article 7.7: It needs to be more clear what is to be considered legacy and new technologies; no definition is included. This is subjective and could be different for each institution. We recommend that proportionality, and a risk-based approach, is provided regarding requirements for conducting specific ICT risk assessment on all legacy ICT system.

Article 15.1: The Financial Stability Board (FSB) published a toolkit on Cyber Incident Response and Recovery (CIRR) in October 2020. The toolkit provides best practices for incident reporting as part of cyber incident response and recovery.
It is unclear how the ICT-related incident management process proposed complements or overlaps with the FSB standard global approach. We recommend that the process is aligned with this global standard to reduce regulatory uncertainty and the regulatory burden for cyber incident responses for financial entities; especially those operating cross-border.

2. Classification and reporting of incidents; DORA proposes to harmonise incident reporting processes and documentation.

2.1. Summary

The DPA calls for a fully harmonised ICT- incident reporting framework without increasing the reporting burden for financial institutions which is already great at present.

2.2. General commentary

While we welcome the aim of DORA to create a consistent incident reporting mechanism and efforts towards centralization that will help reduce administrative burdens for financial entities, and strengthen supervisory effectiveness, we worry that in practice the many existing incident reporting frameworks will result in overlapping requirements and will increase the reporting

burden for financial institutions which is already great at present. It is therefore crucial to clarify how these guidelines will interact with DORA. We believe there is a need for harmonizing the cyber incident reporting mechanisms across EU legislation in the areas of timelines, thresholds, templates, type of information etc. Furthermore the intended distinction between ICT related incident reporting and non-ICT related incident reporting within DORA is difficult to uphold as nowadays most incidents are ICT driven. To ensure the necessary harmonization, we believe that DORA should be leading when it comes to incident reporting and other legislation, like Cybercrime, GDPR, NIS-Directive, PSD2, could refer to DORA. As such, alignment on reporting process, single point of contact, and templates should be aimed for.
With regards to standards to determine the materiality of incidents, the varying size of institutions should be taken into account. Therefore absolute thresholds should be avoided in the regulatory technical standards.

2.3. Comments on specific Articles

With reference to Article 10.7 we are interested in the objective of the requirement to record activities before disruptions? Without clear direction this means ALL activities, because you don't know upfront which activities are ultimately related to a disruption.

With reference to article 10.9 we strongly recommend to define a Cyber incident taxonomy. Organisations use (i) a pre-defined taxonomy for classifying cyber incidents according to, for example, the type of incident, threat actors, threat vectors and repercussions; and (ii) a pre-established severity assessment framework that takes into consideration criticality of systems or services to help gauge the severity of the cyber incident (FSB CIRR) In order to avoid that every simple internal IT incident (e.g. mouse broken) needs to reported due to this rule.

With reference to Article 11.2 regarding backup policies and recovery methods we believe this requirement might be effective in certain scenarios but not all (e.g. active-active or highly available architecture). We suggest to formulate this requirement in terms of objectives and not the "hows".

With reference to Article 11.3 we believe this requirement might be effective in certain scenarios but not all (e.g. an automatically fail-over to redundant infra-components). We suggest to formulate this requirement in terms of objectives and not the "hows". Furthermore "all transactions" needs scoping because this requirement will mean that all data is critical.

With reference to Article 11.4 we recommend that flexibility is provided for financial entities in managing redundant ICT capacity as part of a continuous evaluation of their Business Continuity capabilities (e.g. Recovery Sites, Business Continuity Plans, ICT capabilities).

With reference to Article 11.6 we would like a specification of "market efficiency"? Please note that efficiency is not part of operational risk - is this aligned with Basel IV?

With reference to Article 11.7 we are of the opinion this might be effective in certain scenarios but not all. We suggest to formulate this requirement in terms of objectives and not the "hows". Furthermore we would like to emphasize that having data consistent across the systems does not mean that data is accurate or complete.

With reference to Article 12.2 in which financial entities will be required to communicate changes to competent authorities following post ICT-related incident reviews after significant ICT disruptions of their core activities. We need further clarity on what information is required for

these communications. What are the exact reporting criteria for 'significant ICT disruptions' of their core activities as each bank, due to their different sizes, will have their own criticality levels. There is no one-size, fits-all criterium. We would like to know which changes should be reported to authorities

With reference to Article 12.4 in which financial entities will be required to map the evolution of ICT risks over time with a view to enhance their cyber maturity. We have concerns that this requirement will be overly complex and lacks precision in what is meant by 'evolution'. We need further clarity on the flexibility provided to financial entities when performing the activities listed.

With reference to Article 19.1 we would like to state we are supportive of the establishment of a single EU-hub for major ICT-related incident reporting. A single hub for incident reporting, if appropriately designed and implemented, could provide significant benefits to financial entities and regulators by increasing the efficiency of incident reporting. However, why a feasibility study first? Cross-border companies/groups of companies in scope of DORA may have great interest to benefit from a single reporting hub directly from the start.

2.4. Detailed comments on the relevant Articles

Article 16.1: *Classification of ICT-related incidents*:
Regulators and financial entities would benefit from collaboration to promote standardisation and effective implementation for ICT-related incident criteria. For instance:

- How to assess reputational damage (Art. 16.1.a),
- When to consider that downtime has started (Art. 16.1.b), BTW Duration must be removed from impact; according to industry standard ITIL, impact is used together with urgency to determine the priority of the incident resolution process. Impact is determined at the beginning of the process, duration can be reported only after the incident has been resolved.
- Whether geographical spread should include EU Member States, or European countries or other jurisdictions with critical operations (Art. 16.1.(c)),
- How severity (Art 16.1.1) and criticality (Art. 16.1.(f) defined, and
- How to determine economic impact (Art. 16.1.(g). Is the Commission/the ESAs going to clarify the concept of "economic impact" listed in the Article?

Article 17.1: We welcome that the proposal provides flexibility to financial entities regarding the timing of reporting and the expected harmonisation of reporting templates (Art. 17.1, 17.2, 17.3). We note that the EBA and ECB have recently released a consultation on incident reporting under PSD2 in which they propose to raise the threshold for incidents reported explicitly to 'reduce the number of operational incidents that are required to be reported'. In that consultation they remark that 'a large number of reported operational incidents appear to have a very low impact on the institution, with most of them related to failure of less significant tasks and single processes.' Detailed ICT-related incident reporting requirements risk diverting financial entities resources from incident management. Also, financial entities may have to provide incomplete information to satisfy prescriptive reporting timeframes.
We recommend that the ESAs be given the role of defining incidents to ensure reporting requirements remain flexible and in line with the other RTS that the ESAs will produce, namely Art. 16.2(a).

Article 18: The DPA supports the proposal to harmonise incident reporting templates across regulations, industry sectors, and European Member States. We also support the need to define a single standard reporting for all competent authorities applicable to ICT and security incidents. The text introduces the harmonisation of cyber incident reporting, providing uniform criteria and materiality thresholds and for a common taxonomy, timeframes, data sets and templates, to be developed by the ESAs. However, harmonisation is envisaged only vis-à-vis the NIS Directive,

to which the proposed legislation functions as lex specialis, therefore removing the obligation of financial institutions to report twice (Recital 16). It does not entail complete harmonisation with regards to reporting obligations imposed in other EU legislation (e.g. GDPR, PSD2, eIDAS). We would like to continue to advocate towards this direction of full harmonisation.

Article 20.2: Could supervisory reports on anonymised and aggregated incident data be provided to financial entities more than once-yearly? It is doubtful how much value a yearly report would bring in terms of preparedness for future threats.

Article 41.(b): We are somewhat concerned that the reporting requirements might result in a more fragmented incident reporting framework regarding PSPs as non-ICT-incident reporting requirements remain under PSD 2.

3. Digital operational resilience testing; DORA will require financial entities to periodically test their ICT risk management frameworks.

3.1. Summary

The DPA calls for an EU-wide mutually recognized digital operational testing framework that is proportionate to the financial institutions' size and avoid additional testing load.

3.2. General commentary

How exactly will DORA be part of the One Rulebook? Will it be positioned "on top" of other legislation?
We support the harmonisation of operational resilience testing, thus currently existing frameworks such as (Tiber-EU) should be used when creating regulatory technical standards. It should be avoided to create an extra framework on top of the already existing frameworks that are being used.

Will Member states, national competent authorities, Dutch Payment Association, large banks be able to provide input for the standards (RTSs) which will be created by EBA, as commissioned by DORA (EC)?

How will relationship/governance with national competent authorities be organised so that they remain informed about the national financial entities?

In the current proposal financial entities shall test all critical ICT systems and applications at least yearly which is in our opinion too rigid and costly. For it is so that some ICT infrastructures span multiple regions and service centres (e.g. some cloud computing infrastructures are spread across multiple data centres). In such circumstances it would be extremely difficult, costly, and disruptive to test periodically the entire infrastructure. We recommend that the requirement is amended so that parts of the infrastructure can be tested at different stages over time, and that testing is proportionate based on different levels of risks.

We understand a new resilience testing framework will be implemented. Will the existing TIBER NL framework be leveraged and (re-)used as a basis and thereby avoiding multiple frameworks with the resulting misalignments? In addition, testing to one framework should be sufficient for the whole EU.

3.3. Comments on specific Articles

With reference to Article 23.2: To be consistent in terminologies and their usage, rather use impact on critical business processes and services instead of critical functions since classification of business process is what a financial entity does but not for functions. Furthermore "necessary measures" is too vague. If third parties are obliged to cooperate by the act, make it a legal obligation but not an action of the financial entities.

3.4. Detailed comments on the relevant Articles

Article 22.1: We recommend that flexibility is provided to allow financial institutions to use a risk-based approach when towards the performance and requirement for the testing activities listed.

Article 23.1: More information is needed about the principles for identification of financial entities that have to perform threat led pen testing.

Article 23.2: Will the overseeing function play a role in getting the participation from critical service providers?

4. **Managing third-party risk and regulating critical ICT service providers; DORA will require financial entities to monitor risks in connection with their use of ICT services provided by third parties.**

4.1. Summary

The DPA calls for alignment of DORA with the existing European supervisory framework, thus the delta between EBA GOA and DORA should be as small as possible,

4.2. General commentary

The Dutch Payment Association would like to emphasize that the RTS need to be available, before our members can adjust existing contracts.

Last year a lot of time was spent to become compliant with the EBA Guidelines on Outsourcing Agreements (GOA). A more in depth explanation of the delta with EBA GOA and possibly other existing regulation specific from EBA to DORA is required. This would avoid misinterpretation and focus on follow-up after the implementation of the cloud and outsourcing guidelines. Various elements are not specified as concrete as existing guidelines/regulation, so this makes it difficult to assess if there is a new (operational) requirement or not, and how to implement the requirements. It is therefore important that the new DORA requirements with regard to third party agreements remain largely the same, otherwise all agreements will have to be renegotiated.

Requirements for any immediate termination with a critical ICT third-party service providers could impact financial entities business and commercial decision-making (e.g. deterring investments in the EU) and potentially impact business continuity and financial stability. Any potential termination should be carefully considered as a final resort option only, providing due time and notice to financial entities to perform safe transitions, as required. Also, there is a risk of fragmentation if divergent approaches are implemented in each Member State, where National Competent Authorities may have their own approach on how to implement the findings of the Lead Overseer for designated critical ICT third-party service providers.

In the Netherlands audit departments of large banks worked together in order to obtain assurance from cloud providers such as Azure, AWS and Microsoft Office365. Can this continue or will a European/National competent authority play a role to obtain this assurance directly from the cloud providers?

Will the right to monitor on an ongoing basis the ICT third-party service provider's performance (rights of access, obligation to fully cooperate etc.) by competent authorities (EBA, ESMA, EIOPA) have to be arranged by large banks themselves by means of contractual arrangements with the Cloud Service Providers? Or will national or European competent authorities directly with the Cloud Service Providers handle this?

Will the recommendations to the third party service provider, resulting from the inspections be addressed to the Cloud Service providers? Or will it go to the large banks who will then have to take it up themselves with the Cloud Service Providers. The same question applies to following-up and verifying if the recommendations have been implemented.

4.3. Comments on specific Articles

With reference to Article 3.19 we wonder how in practice will critical third-party ICT providers "need to be established within the EU"? Does this mean the business activities or actual physical presence?

With reference to Article 25 we expect that the proposed Regulation, as part of the principle-based approach, introduces a catalogue of mandatory minimum content for the contractual agreement on the use of ICT services. Considering the relevance of legal certainty for this agreement, the proposed requirements appear challenging in parts.
We repeat our recommendation that the requirement for a multi-vendor strategy is not mandatory, and that the use of multi-vendor strategies remains a risk-based and business decision of financial entities.

With reference to Article 27.1 we note that a full contract, including service level agreements, documented in one written document, is potentially impractical for some outsourcing arrangements. This is because technology contracts often incorporate multiple documents by reference or have separate amendments. We suggest to align the key contractual provisions to the EBA Outsourcing Guidelines or that flexibility/voluntary application of the requirements is provided within this proposal.

4.4. Detailed comments on the relevant Articles

Article 25.3; 9(G); 29.2 From an information security perspective, there are limited viable alternatives for some specific critical service providers (e.g. for DDoS protection). This should be considered with regards to concentration risks across the industry. There will be a considerably negative impact when it would be prescribed which service providers we can and cannot contract because of concentration risk across the industry or even for multiple solutions.

Article 25.4: "*Register of Information*" seems to have a similar function as the Outsourcing Register from EBA OGL and Cloud Register, but the scope of contracts is restricted to ICT services/products and at the same time expanded to contracts other than outsourcing/cloud. We would welcome a harmonized requirement that avoids the need to maintain multiple registers with (very) different data elements.

"*along with any information deemed necessary*": this reads as open-ended what information can be required to be reported in light of the Register of Information. Can this be clarified as 'any information from the register deemed necessary' with a defined set of information to be held in the register, as with the Outsourcing and Cloud guidelines?

Article 25.6: "*the latest information security standards*": seems open for interpretation? A referral to any standards would be preferable (and SMART).

Article 25.8: "*contractual arrangements on the use of ICT services are terminated at least under the following circumstances*": is this intended as an instruction to actually terminate these contracts, or is meant that financial institutions must have the ability to terminate in such circumstances through appropriate provisions in the contract? "*Breach of contract*" and "*circumstances deemed capable of altering the performance or functions*" can be in effect low risk, while terminating the contract would introduce far greater risks.

Articles 25.10+25.11: Since the specification of the *Register of Information* is going to be provided one year (?) after the regulation comes into force, what is the expectation on Article 25.4 until that time? Is maintaining existing Cloud and Outsourcing registers sufficient in line with those respective regulations?

Article 26.1.(b): "*closely connected ICT service providers*": guidance how to interpret closely connected would help make this requirement less open to own interpretation. Is this *connection* only meant as through subcontracting or group affiliation, or also in business partnerships, use of technology, etc.?

Article 28.9: How would a Financial Institution know this would be the case? The aggregated information to determine whether a provider qualifies under Article 28.2 may not be available to a financial entity (and probably not available at all)?

Article 29.2: This Article defines the scope of assessment undertaken under the Oversight Framework. For critical TPSPs, can financial entities rely on this assessment (and do no assessment themselves) as part of their risk control on these topics? *[Is the scope of the assessment set to be sufficient to fulfil assessment of the TPSP in compliance with the requirements of DORA itself?]*

Articles 30 – 35: while quite detailed on the interaction of Lead Overseer, Oversight Forum and TPSP, the approach doesn't go into information provision to or interaction with financial entities: who must consider for example internal mitigating measures or if there is any coordination/consultation on the intended recommendations, since these may impact different financial entities differently:

a) Does the Lead Overseer qualify arrangements and control of the TPSP as effective/ineffective, or is that qualification left to the financial entities based on their own risk appetite and usage of services from the TPSP?
b) How are financial entities informed on findings (does the Lead Overseer publish a report, or the TPSP? Is this communicated via the oversight dialogue of the respective ESA to the financial entity?)
c) How are risk responses coordinated, since the choice of risk response/mitigations may have different impacts on the different financial entities that receive services from the TPSP?

Article 30.1: Will the Lead Overseeing function also play a role in getting audit rights from critical service providers?

Article 31.1.d: To what extent will the advice of the Lead Overseer with regards to critical service providers be binding?

Article 31.1(d) (iii ;iv): With regards to third country subcontracting, the situation around UK leaving the EU should be considered.

Article 37.2: It is unclear how recommendations are communicated to the financial entity.

Article 37.3: This article grants the competence to National Competent Authorities to require a financial entity to terminate, in part or completely, the contractual arrangement. This option appears to insufficiently consider the detrimental effect that such termination can have on the business operation of the CTPP's customer. A termination of service provision by a CTPP is a complex endeavour, requiring a strategic retraction of data and shift towards in-house or alternative service providers so as not to disrupt the business operations in question. Business continuity is key. Considering the relevance of the CTTP's service an abrupt termination can carry significant risk to the operational resilience and business continuity of a financial entity. Termination and exit require security and control under a financial entity's exit strategy. In turn, it cannot become a standard enforcement tool, to be frivolously applied. Considering EBA Guidelines on outsourcing an outsourcing agreement may be terminated, only if necessary. Remedial actions and corrections shall be appropriate. Art. 37 (3) DORA should align with this evaluation of appropriateness prior to any consideration of termination. Therefore, we urge to explicitly include a reference under Art. 37 (3), outlining the right to call for (partial) termination only as an action of last resort.

Article about definitions:
Article 3.(15): Are companies that provide their software as a license (with maintenance) considered in scope (ISVs) or is an operational service aspect necessary to be in scope (SaaS is in scope, but ISVs would not be in scope)?

Article 3.(19): Please clarify "*has not set up business/presence in the Union*" what is and what is not considered presence: is selling your services via an EU reseller considered business in the Union, for example? If the TPSP has an EU-region website?

Impact of Articles in other sections (from procurement perspective):
Article 4.2.h seems to be a heavier requirement than before, this was only for large outsourcing of critical and important functions.

Article 5.9.g.: "*ICT multi-vendor strategy at entity level*" phrasing seems to carry the intent that a financial entity must have or be able to shift between vendors for any key dependency?

Article 7.5: mapping these dependencies and interconnections is new and seems to require a level of detailed mappings we do not currently have.

Article 10.4: "*outsourced or contracted*" is a very clear indication that DORA seems to extend the scope of contractual arrangements beyond outsourcing and cloud contracts.

Article 23.2: This requirement may impact contracts to ensure we have provisions to allow pen-testing and get the required cooperation. (To my knowledge) this is not common practice today to scope in the ICT domains of TPSPs in such tests.

Article 24: These would be contracting requirements, the procurement consultant must be aware of.

5. Information sharing; DORA will facilitate arrangements between financial entities to exchange cyber threat information and intelligence amongst themselves.

5.1. Summary

The DPA calls for enabling the establishment of meaningful and voluntary cyber threat information-sharing arrangements among trusted circles.

5.2. General commentary

In general we support the efforts towards information sharing and we see the value of it for the ecosystem as a whole. However, due to the sensitivity of the information, we do see some challenges in sharing information. It would be helpful if the ESA's and the National Competent Authorities could enable sharing information by taking some of the roadblocks away and harmonizing the process. E.g. by creating standards for information sharing that are in line with privacy regulations and best practices that are currently used. Will there be feedback, advice, threat and incident Intelligence sharing, potentially complemented with information from other large banks in order to have an improved defence and response?
For the development of crisis management and contingency exercises, existing frameworks and best practices should be used.

Large banks could benefit from learning from the security incidents of other banks, if the national competent authority (CERT, CSIRT) would share this information in an anonymized way. We would welcome sharing information from security incidents in order to prevent incidents.

We support the introduction of a standardized way for submission of incident reports (structured data like STIX, TAXI) in order to have harmonized content and a consistent format for reporting, thus a standard template and taxonomy.

Information sharing in the Netherlands is already in place within the financial sector via an ISAC-structure. Does this structure align with ENISA initiatives in this area? In addition, other initiatives in this area are underway with the 4 Horizon 2020 Pilot programmes (such as with Concordia).

Will this information sharing initiative be useful for incident reporting? Will NCAs reuse the information obtained from incident reporting? For example, share cyber incident information and threat intelligence from other companies.

5.3. Detailed comments on the relevant Articles

Article 17.5: We support efforts to increase information sharing between public sector authorities and reduce the need for financial entities to report to multiple stakeholders when a critical incident takes place. We believe further action should be taken to encourage information sharing between the public and the private sector. Public sector authorities can aggregate and gather reported information from financial entities and provide anonymised feedback to support sector preparedness and response. However, because critical-incident reporting contains sensitive data, we recommend a considered approach is taken on how incident reporting information is shared between stakeholders. Given the intention in the proposals to share summaries, it will be important that necessary safeguards are put in place to prevent confusion or misunderstanding from authorities when receiving reports second hand.

Article 28-39: Since the advocacy from one of our members has not been followed (they encouraged a certification scheme, leaving the institutions themselves responsible for their third party risk), we would like to see if and how the FI's will be informed on the supervisory observations and recommendations of the critical ICT third-party service provider. The proposal provides for a limited space for financial institutions to leverage gathered information under the oversight framework from critical TPPs. Information sharing on the Lead Overseer's findings and actions is focused on the relationship within the supervisory structure (EU and national level). While this enhances inter-authority coordination, it does not offer the information for use by financial institutions, for example when assessing details under Art. 25 (5) c).

Article 40.1: Dutch financial institutions are already sharing threat intelligence. Due to privacy regulations, it does remain a challenge however. Standards on information sharing in line with privacy regulation can help to move this forward.

Article 40.1.c: The flow of information should be bi-directional and we would appreciate facilitation for the information sharing process.

Article 43.1: Further clarification of the to be established mechanisms is needed.