IRSG

INTERNATIONAL REGULATORY STRATEGY GROUP

IRSG RESPONSE TO THE EUROPEAN COMMISSION'S LEGISLATIVE PROPOSAL FOR A DIGITAL OPERATIONAL RESILIENCE ACT ("DORA")

The International Regulatory Strategy Group ("IRSG") is pleased to respond to the European Commission's legislative proposal for a Digital Operational Resilience Act ("DORA", "the DORA proposal" or "the draft regulation").

This response groups its recommendations by the titles of the chapters in the legislative proposal.

The IRSG is a practitioner-led body of leading UK-based representatives from the financial and professional services industry. It is an advisory body to the City of London Corporation, and to TheCityUK. The IRSG develops its policy positions through a number of workstreams which comprise representatives from across the financial services industry to ensure a cross-sectoral response.

The financial services sector has long been a major user of information and communications technology (ICT), using it to become better, faster, more efficient, and more effective for the end customer. In recent years, established financial entities have overhauled their business models to better integrate technology and digitise finance. They have also used technology to become more secure and resilient, offering their customers new tools and the system new protections. Nevertheless, the current coronavirus pandemic is a stark reminder that the financial service sector cannot be complacent about the speed of digital adoption. Despite the financial services sector representing an important element of stability during the pandemic, Covid-19 continues to present unprecedented challenges and clearly underlines the necessity for a resilient financial services infrastructure.

Covid-19 has shown that people can work from home, and business can continue. This transition to remote work on such a massive scale has therefore accelerated the use of digital services by financial institutions. According to Gartner, cloud computing is now projected to make up 14.2% of the total

global enterprise IT spending market in 2024, up from 9.1% in 2020[1]. This proposal is therefore timely, as such technological developments bring about an increased awareness to the issues around cloud adoption.

The IRSG supports the Commission's aim of further enhancing the resilience of the European financial services industry, and places the utmost value on cyber security and risk management. Resilience is crucially important to the whole financial and professional services ecosystem, and the lack of financial services resilience has a detrimental impact on the wider economy. The EU economy must be strengthened in recovery phase and the financial services sector stands ready to support the efforts; through providing access to Environmental, Social and Governmental ("ESG") data, helping to fight financial crime and powering transparent and efficient financial markets. As such, we would like to share with you our initial high-level reaction to the European Commission's legislative proposal.

[1] https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021

PART 1: EXECUTIVE SUMMARY

Our key concerns and suggestions are summarised below. These concerns can broadly be split into three themes:

- Ensuring sufficient flexibility for requirements to be applied appropriately by each of the broad range of entities to which they apply;
- Avoiding overlap, duplication and contradictions caused by the application of the DORA requirements in conjunction with existing legislation / guidance; and
- Identifying practical issues arising from specific requirements in the draft proposal.

We have however split our comments into the core topics of the draft proposal for ease of reference.

ICT Risk Management

Whilst we recognise that ICT Risk Management is a core part of operational resilience, and that DORA is intended to be principle based it its approach, there are a number of cases (including in relation to required security measures) where the DORA proposal is overly prescriptive. We consider that there is a need to be less specific and more flexible given the wide range of entities caught, whose maturity will range from very low to highly sophisticated, particularly for SME's. The breadth of entities subject to DORA also needs to be reflected in the application in that some are indeed critical, while others play far less critical roles, or are currently explicitly carved out such as standardised services such as price feeds under MiFID II.

Additionally, the focus on legal entities is likely to lead to increased fragmentation, and does not recognise the realities of global organisations, where ICT Risk Management would usually apply at a group level.

Incident Reporting

Our key concerns in this regard are that it should clear when entities should make an incident report, that the mechanism for reporting should be practicable, and that the DORA requirements should not unnecessarily duplicate reporting obligations under other applicable legislation.

The threshold for reporting should be made clear, and should focus on major incidents to avoid regulators becoming overwhelmed. Group rather than entity reporting should be possible where an incident impacts more than a single entity, and reporting obligations under differing applicable laws should be aligned wherever possible to avoid duplication of reports. The timeline for reporting should be achievable and should take into account when the entity becomes aware of an incident.

The requirement to report costs and losses should be removed as it is impractical to make this calculation (certainly without further guidance) and not proportionate to do so, particularly in relation to small/low risk incidents. It is also likely to be inappropriate to report major vulnerabilities to the public, certainly prior to resolution of such incidents, given the increased level of risk associated with such disclosures. Any obligation to report incidents or vulnerabilities to clients and counterparts should be subject to appropriate confidentiality requirements.

Digital Operational Resilience Testing

Digital Operational Resilience Testing is clearly a vital part of ensuring operational resilience. However, requiring ICT providers to participate in financial entities' penetration testing will overburden suppliers, and will be particularly problematic for providers who supply multiple entities. Any testing scheme should be aligned with industry programmes, such as TIBER-EU, and should permit ICT providers to conduct their own testing and report to financial entities.

The definition of 'critical' ICT systems and applications should be clarified (currently such systems and applications are required to be tested annually), and the frequency of testing should be linked to risk rather than a fixed mandatory period.

Threat Led Penetration Testing

Clarity is required as to what constitutes 'critical functions and services' such that financial entities are clear where Threat Led Penetrating Testing ("TLPT") is required. As noted above, ICT providers should be required to conduct their own testing and report to financial entities, to avoid the need to participate in separate tests for each client.

Clarification is also needed in respect of the relationship between DORA's TLPT requirements and the TIBER EU framework. Finally, it would be helpful to clarify how mutual recognition of TLPT will be achieved both between Member States and with jurisdictions outside of the EU: international financial services groups operating around the world will be subject to different operational resilience and testing frameworks, and mutual recognition is vital to avoid regulatory fragmentation and unnecessary duplication of cost and resource.

ICT Third party risk

As per our comments regarding ICT risk management above, a key concern is that some provisions are overly prescriptive and disproportionate, for example, the requirement to apply the 'latest' information standards is unlikely to be possible, practical or appropriate in many cases.

The requirement for mandatory termination of contracts when certain conditions apply (such as a breach by the ICT third party service provider of applicable law, regulation or contractual terms) fails to consider that termination should be a last resort, and does not permit financial services entities to take into account other relevant factors when determining whether or not termination is the appropriate action. It may create operational risk, and can have significant unintended consequences for other group entities or reliant parties.

Designation of Critical Third-Party Service Providers

Given the intended timeline for agreeing Council Conclusions on DORA, it is important from an early stage to have as much transparency, clarity and consistency around the designation process as well as the criteria for designating ICT critical third-party service providers ("CTPPs") as is possible, to allow potentially designated firms a suitable timeframe for preparations to comply with the regulation. In particular, it would be helpful to have an idea of the quantitative thresholds referred to in the designation criteria (Article 28) so that appropriate preparations can be made.

Data localisation and onshoring

Although we understand this is not the intention of the European Commission, we consider that the proposed limitations on the use of third-country service providers, along with the desire to conduct

on-site inspections of premises (including data centres, which is somewhat impractical in relation to cloud services) could lead to the localisation of data in the EU, particularly in conjunction with the recent *Schrems II* judgment of the Court of Justice of the European Union ("CJEU").

Aside from the economic damage caused by the increased costs associated with such data localisation, and the limits to EU firms' access to key services from providers of their choice, there is also a substantial risk that this would lead to other jurisdictions imitating the EU's actions, causing global fragmentation of operations and risk management, and ultimately potentially increasing operational resilience risks.

Oversight of CTPPs

We would like to better understand how the proposed novel oversight framework will function, given the novelty of shared responsibilities between European Supervisory Authorities ("ESAs") and National Competent Authorities ("NCAs"), as well as the choice of Lead Overseer based on the customers of the CTPP (which may not always produce the optional choice in terms of the expertise at hand). We would also like to see more clarity on the instances in which penalties will be imposed: these should be considered a last resort, with a view to ensuring DORA does not impose a disproportionate cost burden. There should also be a mechanism in place to ensure dialogue between the CTPP and Oversight Forum / Lead Overseer, in particular in relation to the Oversight plan to be produced annually by the Lead Overseer.

PART 2: DETAILED RESPONSE

CHAPTER I – General Provisions

1. Timing, scope of the regulation and proportionality of application of required measures

a. Timing for implementation

Article 56 of the draft regulation indicates that the majority of requirements will apply from 12 months after the date of entry into force, with Articles 23 and 24 (which deal with threat led penetration testing) having a slightly longer time frame for implementation of 36 months. In our experience, these deadlines will be difficult to meet: aside from the time it will take for entities to change internal technology, structures and procedures, the various regulatory technical standards ("RTS") will not be known until shortly before the entry into force of the regulation, and in some cases (e.g. Article 14) not for 12 months after DORA comes into force. We consider that 36 months from the date on which DORA comes into force would be a more realistic time period, or 24 months following the finalisation of the RTS, whichever is later.

b. Types of entity covered

i. List of covered entities

As noted in the explanatory memorandum accompanying the draft regulation[2], the list of covered entities in Article 2 is not exhaustive, and excludes for example payment system operators ("PSOs") and certain other Financial Market Infrastructure systems ("FMIs"). It is unclear given the materiality of PSOs why they are not included where some other firms are. It would be helpful to understand the basis on which certain entity types but not others are covered by the draft regulation (albeit we note that the Commission intends to continue assessing the necessity and impact of extending the scope of DORA to additional entities).

ii. Definitions of "ICT services" and "ICT Service Providers

The proposed definitions of "ICT services" and "ICT third-party service provider" do not allow us to be clear on the exact scope of what services (and, therefore, which businesses) are impacted, and would therefore benefit from refinement and further examples.

For example, Article 3(15) defines ICT third-party service provider as "an undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services, [and] data centres…" Although the provision of cloud services is clearly an in-scope activity, the general references to "digital and data services", "software" and "data analytics" could encompass a broad and indeterminate number of businesses and technologies.

This definition comingles materially different services with materially different operational resilience profiles, including in relation to the nature and extent of reliance placed on them by financial firms. Numerous businesses in this sector offer a range of modular services, which may include news, analysis, data, research, communication,

[2] See final paragraph of p.8 of DORA

as well as tools that support compliance with risk management, investor protection and market abuse regulatory requirements. Diluting oversight resources, by focusing on non-critical or core operations provided by software and data firms, is unlikely to achieve the stated objective of more effective operational resilience of the EU financial system.

Equally, any inclusion of regulated financial institutions in the category of third-party ICT service provider would further dilute resources and add significant complexity to the EU regulatory environment, while achieving little improvement in resilience given these firms' regulated status. Policy makers should consider an exemption for financial services from rules intended for third-party ICT providers in order to create regulatory certainty for financial institutions operating in the EU regarding the nature and level of supervision they will be subject to in the future.

As the proposed definition of "ICT third-party service provider" is very wide, we also recommend that "financial entity" is specifically carved out from the definition of "ICT third-party service provider", in order to reduce the potential for unintended overlap of definitions. Financial entities are already regulated entities, and it should be clear that financial entities are not expected to implement any requirements directly applicable to ICT third-party service providers (unless the requirement also applies to financial entities).

DORA should focus on core operational functions, which present objectively identifiable resilience risks. If co-legislators wish to proceed with capturing a broad range of products, technologies, services and solutions, a targeted and delineated approach should be followed, with regulatory obligations tailored to be proportionate to the differing service risk profiles. Any such delineation should take account of the criticality of the service, not merely the entity that provides it.

c. Proportionality

i. Financial Services entities: Exceptions for Microenterprises

The DORA proposal attempts to deal with the significant differences between covered financial entities (whether in terms of size, profile or exposure to digital risk) by exempting microenterprises from various requirements. We welcome this proposal. However, as a 'microenterprise' is defined[3] extremely narrowly as "an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million", there is still a huge variation between covered entities. In particular, small and medium-sized enterprises (SMEs) may not have the expertise and resources to, and may be overwhelmed by the requirements to, establish more complex governance arrangements, dedicated management functions, conduct regular risk assessments on ICT systems etc. We would propose re-considering whether any exemptions, whether partial or complete, should be extended to SMEs more broadly.

[3] Defined by reference to Article 2(3) of the Annex to Recommendation 2003/361/EC

ii. Application of requirements and controls

In various places, the DORA proposal seems to be disproportionality onerous, for example, suggesting that mapping should be applied to *all* ICT assets, processes and ICT third parties (Article 7(4)) irrespective of their significance. Other examples include: forced multi-vendor strategy (art 5.9); design network connection infrastructure (art 8.4); detection requirements (art 9); incident reporting (art 17); digital operational resilience testing (art 21); and key contractual arrangements (art 27.2).

We would encourage the Commission to consider whether the core requirements of DORA could be limited to ensure proportionality, for example by limiting their application to ICT assets, processes and ICT third parties which are used to support the regulated activities and other clearly defined "mission-critical" parts of financial firms, rather than *all* ICT. This reflects a more risk focussed approach, and would be better aligned to the Basel Committee on Banking Supervision ("BCBS") principles, for example, the concept of "critical operations" as set out in the BCBS Consultative Document on Principles for Operational Resilience (August 2020). A greater focus on criticality and outcomes would also allow for more tailoring to fit the size and risk of SMEs potentially presenting a solution to proportionality concerns in DORA.

d. Importance of alignment with existing regulation / other initiatives

i. Overlapping legislation and guidance

The firms falling within the wide scope of DORA are already subject to many other laws and regulations relating to information security and cyber and operational resilience both within and outside the European Union. Non-alignment of these requirements risks undermining the core objectives of DORA, by reducing resilience and security.

We encourage the Commission to carefully consider overlapping requirements both within (for example the NIS Directive[4], PSD2[5], GDPR[6], MiFID II[7], the European Banking Association ("EBA") Outsourcing and ICT Risk Guidelines[8][9] and the Financial Stability Board's consultations on Effective Practices for Cyber Incident Response and Recovery and on Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships) and outside the European Union (for example the US NIST cyber security framework and the Bank of International Settlements' principles for operational resilience as set out in the BCBS Consultative Document on Principles for Operational Resilience) to ensure that the DORA requirements are fully aligned and only differ where there is objective justification and it is clearly proportionate and necessary to do so. In this regard we welcome the recent clarification provided in the recent

[4] EU Network and Information Security Directive (EU) 2016/1148 ("NIS Directive" or "NISD")
[5] Payment Services Directive (EU) 2015/2366 ("PSD2")
[6] General Data Protection Regulation (EU) 2016/679 ("GDPR")
[7] "MiFID II" is made up of Directive 2014/65/EU on Markets in Financial Instruments and Regulation (EU) No 600/2014 on Markets in Financial Instruments.
[8] EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02) ("EBA Outsourcing Guidelines")
[9] EBA Guidelines on ICT and security risk management ("EBA ICT Risk Guidelines")

Commission services non-paper on the Interaction between DORA and outsourcing rules in the Union legislation (the "Legislative Interactions non-paper") which sets out the interaction of DORA with specific provisions from a wide variety of sector-specific legislation.

By way of example, MiFID II explicitly carves out "the purchase of standardised services, including market information services and the provision of price feeds" as not critical (Article 30(2)(b) Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II). Furthermore, the EBA Outsourcing Guidelines state that, as a general principle, institutions and payment institutions should not consider market information services (e.g. provision of data) as outsourcing. These guidelines also have a markedly greater focus on critical and important functions in contrast to DORA's tendency to target "all".

ii. Definitions

We note that language used in the draft regulation is not always consistent with existing regulatory requirements or existing international standards and it is not always clear whether this is deliberate. Some definitions (such as "Information Asset" which is defined as "a collection of information…that is worth protecting") may as currently drafted lead to wide-spread uncertainty.

Clarification of scope and terms would be helpful: to avoid any regulatory uncertainty, we suggest that these definitions are amended to be consistent with international standards such as the FSB Cyber Lexicon definitions where possible.

While we fully support the need to define outcomes to support Operational Resilience, it is not helpful to be overly prescriptive in how this is achieved, for example in relation to impact tolerances. For example, there is a mention in Article 5(9)(b) to 'impact tolerance' for ICT disruptions. An outcomes-based approach would be preferable, such that assessment of impact tolerances is 'threat scenario' agnostic. Setting an expectation that firms consider tolerance for ICT disruptions in isolation would be onerous and unhelpful. Is the intention that an RTO (recovery time objective) should be set, as well as an MTPD (maximum period of tolerable disruption) for disruption to IT assets, as is typically done in more advanced business continuity analysis/planning? Impact tolerance is a separate, unresolved, topic and should be avoided in this context.

2. <u>Enforcement and Cooperation amongst competent authorities</u>

While we support the aim of harmonisation to ensure a coherent European framework in this area, there are a number of challenges with a centralised approach, including speed of regulatory action, a limited understanding of local business and operating requirements and conditions and a lack of appropriately skilled resources (particularly where existing institutions are taking on new roles). That said, a national approach also comes with its own issues such as a potentially inconsistent approach, the need for a separate consistency mechanism, varying skills between national

regulators, and challenges in consistent scalability. Visibility and the sharing of information is also critical in this respect.

Rather than centralising enforcement and supervision, there may be merit in supervision of national entities by national expert regulators, as in practice proximity is important to enforcement. Ultimately any enforcement should be consistent and deliver a timely result.

The proposed cooperation between competent authorities, and between the competent authorities and the ESA, will be helpful to ensure consistency of enforcement, but care should be taken that the rules supporting such cooperation do not create delays, particularly in respect of incidents where time is of the essence. A helpful demonstration of the issue is in relation to collaboration between data protection supervisory authorities, which can be extremely slow, and generates a very limited number of outcomes each year. Additional clarity is needed regarding supervisory co-operation for firms operating in multiple Member States.

Additionally, given that operational resilience is an international issue, it would be helpful to provide further information on international cooperation (the provisions in Article 39 which deal with this point being very high level). This is of particular importance for all firms regulated by, headquartered in, or operating from third countries to which those third country laws and regulations apply, and also for cloud providers (and financial entities using cloud solutions) given the cloud computing business is based on geographical diversification. A lack of international cooperation could have an adverse impact on inward investment to the EU. We are happy to further discuss what sort of structures would be optimal for effective international cooperation.

CHAPTER II - ICT Risk Management

3. ICT Risk Management Requirements

We agree that ICT Risk Management is a core part of operational resilience. We generally support the principles articulated in the DORA proposal, and we recognise the abilities the Commission is requiring firms to have (drawn from CPMI-IOSCO[10] and NIST[11]). However, despite the fact that the proposal is intended to be principle based in its approach, DORA includes a significant number of prescriptive requirements across each ICT risk management area for how firms should achieve these abilities. This risks becoming quickly outdated, is onerous on both small and large firms, and does not allow firms flexibility to achieve these outcomes in the way best for their firm and individual risk-profile. The various frameworks, strategies, business continuity management ("BCM") and disaster recovery plans required create a complex and confusing web for firms to comply with. Further, we do not believe these requirements are sufficiently understandable or differentiated for firms to comply with.

The scope of these Articles is extremely broad, and they will capture a very wide range of entities whose maturity will range from very low to highly sophisticated given the breadth of the scope of applicability, particularly in relation to previously unregulated firms. The implementation therefore

[10] International Organization of Securities Commissions - Committee on Payments and Market Infrastructures ("IOSCO-CPMI")
[11] National Institute of Standards and Technology ("NIST")

needs to be highly flexible to work across the sector so it applies in a more proportionate manner on firms in a way which better reflects whether they are key institutions and central players with systemic market risk versus periphery players, and also takes into account their size, i.e. SMEs. We do recognise that were multiple smaller firms to be impacted by a security incident that this may have a wider impact on the market. Nevertheless, the requirements set by these Articles are onerous and should only be applied where necessary and proportionate to ensure their effectiveness. The influx of regulations is causing a significant IT compliance overhead, and IT risk functions are typically experts on the technical detail rather than the compliance elements. Persons with a mix of these skill sets are rare and compliance with specific measures is expensive. It is therefore all the more important to ensure that requirements do not go beyond those necessary and proportionate to achieve the desired objective.

We believe that a principle/outcome-based approach is important, providing firms with the flexibility to achieve the desired outcomes through their own approach rather than setting out specific measures to be taken by firms.

a. ICT risk management framework / entity regulation

There is a risk that the proposed application of the DORA ICT risk management framework to individual legal entities within the same firm will *decrease* resilience and security by increasing complexity and driving a fragmentation of requirements.

The reality in larger multinational firms is that operational resilience and security standards are set centrally by reference to many existing legal and regulatory requirements, security standards and guidance. They are not set at a local legal entity level. Similarly, risk assessments are typically undertaken centrally with firms applying a holistic view of risk across their operations. For example, it would be very unusual for a firm to set vendor selection, vetting and risk assessment strategies at a local entity level given that: (i) these strategies will interact and affect the group more broadly, and a local approach creates considerable risk, from a security perspective and more broadly, owing to conflicting measure and/or unforeseen interactions and dependencies; and (ii) this will involve duplication of effort, including in relation to strategy development and senior management approval. Flexibility should be provided to firms to allow them to determine the appropriate level at which the DORA ICT risk management framework should apply, which is unlikely to be at the legal entity level.

b. Security by design

We agree that appropriate security measures are a vital part of operational resilience, however certain aspects of the DORA proposal are very prescriptive. As recognised in Article 5(4) in relation to information security management systems, information security controls and processes should be designed using a risk-based approach and in line with published and already widely adopted industry standards (noting that it would be helpful if the EC were to refer to specific standards such as the International Organisation for Standardization (ISO) 27001, the National Institute of Standards and Technology – Cyber Security Framework, or the Cyber Risk Institute's Cybersecurity Profile[12]), and we consider that the Commission should focus on the required outcome rather than the specifics of how to achieve this.

[12] https://cyberriskinstitute.org/the-profile/

By way of example:

- security by design as a principle is to be encouraged, but including specific requirements as per the second sub-paragraph of Article 8 ("financial entities shall design the network connection infrastructure in a way that allows it to be instantaneously severed…") is too inflexible, especially given the wide range of different entities covered by the draft regulation. This requirement does not take into account the consequential impact on other areas where a connection is 'instantaneously severed'. It is also important to consider the impacts of a such a requirement, and the knock-on effect and unintended consequences for other group entities as a result of a connection severance, termination or other activity. This proposal is antithetical to the goals of resilience, incident response and threat intelligence gathering: inter-connectedness is a key feature of an efficient and collaborative operating model.

- Article 8(3) requires, inter alia, that, in order to achieve certain "objectives referred to in paragraph 2, financial entities shall use "state-of-the-art ICT technology and processes which (a) guarantee the security of the means of transfer of information…". The design, procurement and implementation of appropriate information security tools are done so as to mitigate the risks associated with a particular process but can never "guarantee" any aspect of security. Additionally, whilst "state-of-the-art" technology is something to take into account (as per Art. 32 GDPR), it will not always be appropriate (or indeed, particularly in respect of legacy systems, possible). Please also see comments in relation to "Managing ICT third party risk - Information Standards" in this regard.

- Article 5(9) mandates an ICT multi-vendor strategy at entity level: given the interdependencies between different entities in many groups, a local multi-vendor strategy will be inefficient, will significantly increase the duplication of work across an international organisation and indeed is likely to increase risk owing to conflicting approaches in differing jurisdictions and a lack of the 'big picture' overview.

Prescriptive requirements such as these will add complexity and cost but will not necessarily improve cyber resilience or help to deliver the underlying objectives of DORA. We respectfully request that the Commission removes this type of prescriptive requirement from the draft regulation and instead legislates for the desired outcomes only.

In this regard we note that, under Article 14(c), the ESAs are to develop draft regulatory technical standards to set out how to "establish a sound network and infrastructure management" (as required under Article 8(4)(b)). We consider that this approach again risks being too prescriptive, is unlikely to be technology neutral or future-proof, and would propose instead simply requiring systems to be designed to prevent and minimise infection (the desired objective) without prescribing the detailed measures to achieve this objective. We recognise of course that less sophisticated organisations may require more prescriptive guidance as to how to achieve the legislative objectives. However this could be achieved in non-legally binding

guidance which could evolve over time as cyber threats and the state of the art evolve, allowing for greater flexibility and impact and ensuring the longevity of DORA.

CHAPTER III – ICT Related Incidents

4. Triage and Incident Reporting

a. Triage / Threshold for reporting

Article 17(1) requires that financial entities report 'major ICT-related incidents' to the relevant competent authority, without delay (and usually on the same business day). Although Article 16 does set out various factors to be used to classify, and determine the impact of, ICT-related incidents, these do not themselves set the relevant reporting threshold.

In order to avoid similar uncertainty to that created by the breach reporting requirements of GDPR (where experience has demonstrated that the volume of such incidents is huge, but the criticality of the majority of such incidents is not), it is important that the draft regulatory technical standards to be developed by the Joint Committee of the ESAs both: (i) provide sufficient clarity (in particular as to what constitutes a "major" incident) to help firms determine whether or not an incident is reportable; and (ii) ensure appropriate prioritisation.

If every incident is reportable, the regulators will receive a huge volume of reports, which will overwhelm regulatory resources, complicating the ability of regulators to identify and triage the most serious incidents promptly. This issue has recently been acknowledged in the current EBA consultation on PSD2 incident reporting, where they are looking at raising the reporting threshold precisely because they have received a high volume of reports which are not material. It may be appropriate to differentiate between wholesale activity and retail activity regarding what constitutes a "major" incident, rather than applying the same thresholds for all types of financial services activity.

Generally, it would be helpful if the updated draft were to focus on major incident reporting: there are several instances in the text where all ICT incidents are covered, thereby expanding the scope of such reporting, such as Articles 15(3)(d), 16(2)(b) and 20(2).

b. Group vs Entity reporting

It is common for ICT incidents to impact a number of different legal entities within the same group, often across multiple jurisdictions. The precedent of the PSD2 incident reporting obligations and GDPR personal data breach notification demonstrates that this can result in incidents being double-counted, for example, where multiple group entities are affected by a single incident.

In order to streamline reporting (both for organisations and for the competent authorities) it would be helpful to permit firms to report an incident once on behalf of all affected entities within a group to a lead authority rather than having to address multiple slightly different reporting requirements which is often a distraction to the most important task of investigating, containing and remediating an incident. The Commission may find it helpful to consider the PSD2 Guidelines on major incident reporting which permit both delegation of reporting and co-ordination of reporting by affected payment service providers via a single service provider. This is also the approach taken by the ECB in their cyber incident reporting requirements.

Any solution should also consider the impact of the increasing number of reporting obligations to financial services regulators, privacy regulators, ICT regulators, all of which vary with different time limits, different criteria for reporting and different thresholds for reporting applying. The time and resources spent on dealing with such a wide and varying range of requirements reduce the resources available to deal with other requirements and issues, and the Commission should consider the extent to which alignment with existing standards is possible.

c. Multiple Reporting Requirements / Central Hub

Financial services entities are subject to a number of reporting requirements under different legislation, and in different jurisdictions. This duplication of reporting requirements to different regulators is unhelpful, and the requirements are frequently inconsistent for no reason other than they have been drafted by different legislatures or regulators in different jurisdictions. Given the very tight timescales typical for reporting requirements this can be a significant distraction to the task of investigating, containing and remediating an incident.

Although the proposed reporting template (to be produced by the ESAs) will go some way to deal with this issue, it is important that such template takes into account the information required to be reported under other legislation, such as NISD, PSD2, GDPR, and ideally would also be aligned with other reporting requirements such as timelines. We understand that the Commission is considering replacing the NIS Directive requirement for major incident reporting with the DORA requirement and that the Commission is also considering the overlap with PSD2 which we welcome. We would welcome a similar consideration of the overlap with GDPR reporting requirements.

We consider that the 'central hub' proposal could potentially greatly simplify reporting of incidents by impacted firms to help address the concerns raised above and speed up initial triage of incidents to avoid regulators becoming overwhelmed by the volume of reports (and so unable to effectively prioritise between minor issues and those with significant impact), particularly as a central hub would be able to establish a single standard notification template.

That said, we consider that investigation and enforcement activities should be handed back to the relevant local supervisory authorities as required once triage is completed by the central hub, as local authorities are closer to the local market and to the entities they regulate which allows for increased understanding of local conditions, and their ability to quickly react to changing conditions and allow for local factors such as common business models, which allows responsiveness and flexibility.

Local regulators are also normally responsible for the stability of the markets in their jurisdiction, and so where an incident occurs in a branch, normally the local financial regulator would investigate. It would make sense for incident investigation and enforcement under DORA to follow the same approach. However, if the Commission determines that the central investigation and enforcement is more appropriate, it should be considered how financial regulators are able to ensure that their jurisdiction can continue to operate effectively if their existing powers are to be centralised.

Finally, safeguards and careful controls would need to be put in place by the Authorities before handling and sharing information on specific major ICT related incidents. Such reports can contain highly sensitive information related to the security of the firm which the firm should continue to control. Further, there is a risk of misunderstanding should only details of the full incident report be passed on by competent authorities as in Article 17(5). If the details are then further summarised and transmitted yet again as in Article 17(6), the risk of misunderstanding increases. Misunderstanding can lead not only to inappropriate regulatory actions with risks to firms, but also market risk should the information become public causing other market participants to react.

d. Requirement to report costs and losses due to ICT-related disruptions and incidents

The obligation at Article 10(9) for financial entities other than microenterprises to report to competent authorities "all costs and losses caused by ICT disruptions and ICT-related incidents" is impracticable and unworkable in practice. Firstly, this information (if known) will be extremely commercially sensitive; secondly, there is no 'de minimis' threshold, meaning that this reporting obligation is likely to apply to a vast number of events (even if it were practicable, it is unclear how the competent authorities would handle such a vast amount of data); and thirdly, calculating these figures is likely to be extremely complex, with a wide variation of calculation methods, meaning that comparisons will be of minimal value. It is also unclear whether there is any differentiation between direct and indirect costs and losses, or whether the knock-on cost to the customer should also be taken into account. We would propose that this requirement is removed.

e. Requirement to disclose ICT-related incidents and major vulnerabilities

Article 13 of the draft regulation requires that financial entities "have in place communication plans enabling a responsible disclosure of ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate". There is no allowance for the severity or criticality of ICT-related incidents: if it is anticipated that a "responsible disclosure" should take into account the level of risk associated with an incident, or that only incidents above a certain threshold should be disclosed, this should be made clear.

In any event we consider that it is unlikely to be appropriate to disclose major vulnerabilities to the public, certainly prior to such vulnerabilities being resolved, given the increased level of risk associated with such a disclosure. Accordingly. the requirement to make such disclosures should be removed. To the extent that the disclosure obligation remains in relation to clients and counterparts, this should be subject to appropriate confidentiality requirements.

f. Timeline for reporting (Article 17(2)

Whilst we recognise the desire for regulators to be provided with detailed information on incidents as soon as possible, the time limits for reporting major ICT-related incidents (as set out at Article 17(3)) within hours of the incident are impractical.

Many IT incidents are not discovered immediately, and there is no 'awareness' or 'knowledge' caveat in Article 17(3): accordingly, the proposed reporting deadlines are likely to be missed on a regular basis. Additionally, investigation of a major incident can take many weeks, and it is simply not practicable to assume that a full root cause analysis will have been completed and actual impact figures become available within one month of making the initial report.

We consider that it is of critical importance that firms have the flexibility to appropriately manage and respond to an incident, without having to divert critical time and resource to meet reporting requirements. The Commission should consider providing greater flexibility for firms in the timing of these reporting requirements.

g. Information Sharing

In order to remain effective, it is vital that information sharing remains voluntary. While we recognise that this is the European Commission's intention, there is no explicit acknowledgement of the principle of voluntary participation in the text. Further, the industry is concerned that the requirement to notify competent authorities of participation and cessation of membership in information sharing arrangements could be used to compel participation. We do not see the value in such notification being required in this legislation and believe that authorities can learn about firms' participation through already established supervisory relationships.

Voluntary participation is vital for several reasons. Most importantly, if firms are mandated to participate, there is a real risk that such forums will be flooded with information that is not useful for improving firms' knowledge of threats, thereby reducing the value added to those firms who choose to participate because of their ability to contribute and learn from the shared information. In addition, mandatory participation could erode the trusted relationship that exists between voluntary participants. Finally, we are of the view that participation by authorities in such groups will necessarily change the character of the groups. While in some situations the inclusion of competent authorities may be appropriate and helpful, the DORA text seems to assume such participation in Article 40(2).

CHAPTER IV – Digital Operational Resilience Testing

5. Digital Operational Resilience Testing

Article 21 requires that financial entities "shall establish, maintain and review, with due consideration to their size, business and risk profiles, a sound and comprehensive digital operational resilience testing programme…".

a. General requirements for the performance of digital operational resilience testing (Articles 21 & 22)

i. Definitions

Clarity is needed regarding the definition of testing. As currently drafted, it is unclear whether the list of techniques in Article 22(1) constitutes "testing" as required in Article 21(6). In particular, the text should be amended to make clear that the list is not exclusionary of other techniques which achieve the same result and that not every method listed in the relevant Article would be expected to be performed in each circumstance. The requirement to employ all of the methods listed in all cases would be beyond the capabilities of even the most advanced firms to comply with.

ii. Penetration Testing

Requiring ICT third-parties to participate in Financial Entity penetration testing could have serious negative impacts on resilience as ICT third-parties will likely have a continuous onslaught of scheduled attacks on their systems. Therefore, the proposed threat led penetration testing approach should align with industry threat led penetration testing programmes such as Threat Intelligence based Ethical Red Teaming ("TIBER-EU"), which was jointly developed by the ECB and the EU national central banks, and the CBEST framework in the UK

iii. Persons qualified to perform testing

We welcome the clarification in Article 21(4) that internal resources, when suitably independent, can be used for testing purposes. We recommend flexibility in the determination of independence to allow for different corporate and organisational structures.

iv. Frequency of testing / testing of critical systems

It must be for the firms to determine what constitutes critical for the purpose of testing. While critical ICT systems and applications as per Article 21(6) are important, testing prioritisation should ultimately be determined by the risk posed to the firm. Critical systems or applications that are externally facing will need to be prioritised over those with no external exposure. For the latter, less rigorous testing may be necessary in order to meet a firm's risk appetite.

Equally, not all issues identified will necessarily need to be addressed. A vulnerability may be discovered that is within risk appetite or which can be mitigated through compensating controls. In order to allow firms the flexibility they need, the text in Article 21(5) should be amended from "addressed" to "dispositioned". Further clarifications should be added to indicate that issues will be remedied "as necessary".

The specific frequency of the defined testing should be clarified throughout the rule. Instead of mandating a frequency for testing (e.g. Article 21(6) requires that financial entities test all critical ICT systems and applications at least yearly), in certain circumstances a level of risk assessment should drive the frequency of required testing.

Additionally, the definition of 'critical ICT systems and applications' needs to be clarified, as it is currently unclear, potentially creating significant compliance burden.

b. Threat Led Penetration Testing (Article 23)

We are concerned to see TLPT codified in 'level-1' text. TLPT is onerous and creates significant risk as has been acknowledged by EU authorities. BaFin recently stated the importance of robust risk management for TLPT noting that "such testing examines an entity's critical live production systems, which means that there is a risk of disruptions or outages in these systems".[13] While TLPT remains a valid tool for supervision, DORA should allow for the possibility that alternative methods such as active continuous monitoring may in the future be better able to provide the same assurance as TLPT while significantly reducing risk.

i. Critical functions and services

Article 23(2) requires that TLPT "shall cover at least the critical functions and services of a financial entity, and shall be performed on live production systems supporting such functions." What constitutes "critical functions and services" is to be determined by financial entities and validated by competent authorities. While a TLPT may be scoped from within critical and important systems, a test which was open to all of the firms' critical and important systems would represent a significant increase in risk by creating a wider channel for testers to access systems and data, the disruption of which results in outages. A narrower scope increases the chances for a controller environment where the necessary monitoring and risk management of the testing process can be achieved.

ii. TLPT for ICT providers

Where ICT third-party service providers are included in the remit of TLPT (i.e. where they are providing critical functions and services), the financial entity is currently required to take the necessary measures to ensure the participation of these providers.

We consider that it would be more appropriate for ICT providers to be required to conduct their own testing and report to financial entities. Otherwise, ICT providers will be required to participate in multiple TLPT for different clients, and this would also be extremely onerous for smaller ICT providers and favour the biggest tech companies.

iii. External testers

The language in Article 23(3) requiring financial entities to contract testers in accordance with Article 24 may be interpreted as suggesting that external testers are required. This is clearly not the intention given the recitals and the fact that certain provisions of Article 24(1) apply to external testers only, but it would be helpful to clarify that TLPT testing can be undertaken by internal testing teams, provided that they are independent.

iv. Interaction with TIBER-EU and mutual recognition

[13] BaFin Perspectives, Cyber Security, p.51, Issue 1, July 2020.

Regarding the requirements for firms to have TLPT on critical live ICT systems, there is no mention of the ECB's TIBER-EU testing framework. Policymakers should clarify how the requirements in the proposal relate and interact with the ECB's framework.

The objectives of the TIBER framework are to promote an adequate level of cyber resilience in order to ensure the proper functioning, stability and integrity of the financial system, and to enable the results of such penetration tests to be compared and mutually recognised in the European context.

v. Mutual Recognition

It would be helpful to clarify how mutual recognition of TLPT will be achieved between Member States. Although this is a clear aim of the legislation as indicated by the recitals (see for example recital 23), this is currently left to be determined by the ESAs as part of regulatory technical standards.

Additionally, DORA does not currently contain any provisions allowing recognition of TLPT test results undertaken in jurisdictions outside the EU, but international financial services groups operating around the world may be subject to different digital operational resilience and testing frameworks in different jurisdictions.

To avoid the risk of regulatory fragmentation and potentially costly requirements for separate tests to be undertaken in each jurisdiction, policymakers should include in the regulation a mutual recognition framework allowing TLPT tests undertaken in trusted third countries to be recognised under this framework.

CHAPTER V – Managing ICT Third-Party Risk

6. Managing ICT third-party Risk (Chapter V)

The overall principle that financial entities should manage ICT third-party risk as an integral component of ICT risk is not controversial: our concerns relate to the more specific requirements setting out "how" to implement this principle contained in this chapter of the draft regulation. Similar to the concerns raised above, a number of these requirements are unnecessarily prescriptive and disproportionate to achieving the stated objectives of DORA. Overly prescriptive requirements do not meet the objectives of technology neutrality, scalability and future proofing, nor are they universally applicable across different sizes and complexity of organisations.

a. Multi-vendor Strategy

Article 25(3) requires that, as part of their ICT risk management framework, financial entities "adopt and regularly review a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in [Article 5(9)(g)]", which requires that such strategy is prepared at entity level, "showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of third-party service providers".

In addition to the issues previously identified with having such a requirement apply at the entity level, there are some uncertainties as to what this 'multi-vendor strategy' requires in practice. For example, does this mean that services/data should be split between multiple vendors (e.g. some data hosted by AWS, some with Azure), or does it require duplication of services (e.g. should an entity have duplicate data feeds from two different providers)? Does the multi-vendor requirement apply at the legal entity level only, or should it be applied at the single application level (which would be inefficient and erode the business case for all but the most material cases)? It is also unclear as to whether this requirement includes services consumed within a particular business group (i.e. inter-affiliate).

We agree that using multiple vendors is a useful control, but it is only one of many to mitigate concentration risk and improve resilience. Rather than making this a blanket requirement, we would propose that firms are permitted to decide when and how this should be deployed appropriate to their structure, the outsourced function and the risk.

b. Register of information

The requirement at Article 25(4) for financial entities to maintain a Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers is likely to result in extremely long lists of providers capturing a large number of irrelevant relationships. This requirement is considerably broader than the EBA register requirement, both in terms of parties required to maintain a register and arrangements covered by such register.

In this regard, and more broadly, we note that many EU financial institutions are already required to comply with the EBA Outsourcing Guidelines when managing third party risk. We understand from the recent Legislative Interactions non-paper that the intention is for the EBA to perform a screening exercise in relation to the EBA Outsourcing Guidelines in relation to the final DORA text and to amend those Guidelines to bring them into line with DORA, and we would welcome this approach.

c. Information standards

The requirement at Article 25(6) for financial entities to only use ICT third-party service providers that comply with "high, appropriate and the latest information standards" is likely to be difficult to comply with.

Aside from the uncertainty as to what this means in practice, many organisations have legacy systems in relation to which it will not be possible to implement the "latest" information standards (for example, some systems cannot be encrypted and so other security measures are required), and it may not in fact be appropriate to always do so. We would propose that the latest information standards should simply be a factor to consider when determining whether the information standards in place are appropriate, i.e. moving towards the GDPR concept of "appropriate technical and organisational measures".

d. Termination of contracts

The requirement at Article 25(8) that contractual arrangements between financial entities and ICT third-party service providers are terminated under certain conditions (such as breach by the ICT third-party service provider of applicable laws, regulations or contractual terms) is very onerous and impractical, may create operational risk and can have significant unintended consequences for other group entities or reliant parties, including market uncertainty. Termination is a tool of final resort and should not be considered lightly. There are many other measures which may be more appropriate and less disruptive, including the competent authorities separately having the power to suspend financial entities' contracts with "critical" third party ICT providers as part of the oversight framework for these critical providers.

We note also that some of these specifically mandated termination rights differ from the equivalent in the EBA Outsourcing Guidelines (see section 13), in particular Articles 25(8)(b), (c) and (d) of the draft regulation. It would be helpful to align these requirements to the extent possible, particularly as the EBA Outsourcing Guidelines have already required a major repapering exercise throughout the supply chains of financial entities at a significant cost.

Similar concerns also arise in relation to the proposed powers of national competent authorities to require firms to temporarily suspend or terminate the use of services from a critical third-party provider. This could have a significant impact on firm's service delivery and operational resilience, and should be again considered only as a last resort. In the event of termination, sufficient time should be provided to permit transition to alternative providers.

e. Contractual clauses

In general, the proposed clauses contain reasonable provisions, although it remains to be seen whether ICT third party service providers will agree to such terms (as Article 27 does not currently specify whether financial services entities or ICT third-party service providers (or both) are responsible for ensuring that the required clauses are in place).

i. Single contract

Irrespective of whether the mandated clauses are appropriate, and whether vendors will in fact agree to them, the requirement at Article 27(1) that the full contract, including the service level agreements, should be documented in one written

document is unhelpful and impractical. In reality, technology contracts often incorporate multiple documents by reference and / or links, and it is common to have amendments and/or renewals and/or statements of work (SoW) made in separate documents. Additionally, this requirement seems impractical where an ICT provider offers a number of modular services. We would propose that this requirement is removed.

ii. Audit

In relation to audit, the requirement that all customers have the right to carry out ongoing monitoring of ICT third-party service providers, including on-site audits of their proprietary data centres would effectively undermine the safety and security of the systems DORA aims to protect. Article 27 permits every customer of an ICT third-party service provider or an appointed third party to exercise these rights (Art. 27(h)(i)).

Firstly, access and audit rights should be limited to objectively identified critical services rather than entities given that a single ICT third-party service provider may provider multiple services, some of which are critical and others of which are not. It is disproportionate to extend this audit requirement to all service.

Secondly, CTPPs should be encouraged to obtain and make available (at their own expense) trusted third party inspection reports (e.g., the US framework for System and Organisational Controls (SOC) reporting). CTPPs should be able to provide these reports to customers and regulators in lieu of a direct on-site audit. Not only will this shift audit expense to the provider, but the use of recognized standards like SOC reporting will ensure that consistent, validated principles and standards are applied.

Additionally, allowing Financial Entities or third-party auditors to remove potentially sensitive documentation (e.g. policies, security reports) from an ICT third party's premises without proper controls could cause undue risk and harm to the ICT third party.

7. Designation of CTPPs

In light of the intended timeline for agreeing Council Conclusions on DORA, it is important from an early stage to have as much transparency, clarity and consistency around the designation process as well as the criteria for designating ICT providers as "critical third-party service providers" (CTPPs) as is possible, to allow *potentially* designated firms a suitable timeframe for preparations to comply with the regulation.

a. Transparency of Designation Process

The current criteria for designation of critical ICT third-party providers (Article 28) currently does not provide sufficient clarity to determine third-party providers designated as CTPPs. For example, Article 28(2)(b) states that third-party providers may be designated as critical based on "the number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider". In this case, as in others, it would be helpful to have an idea of the quantitative thresholds

referred to in the designation criteria as soon as possible so that the appropriate preparations for compliance with the regulation can be made.

b. Notion of Criticality in Relation to Other Regulations

It is equally not straightforward for a firm to assess whether they will be considered critical based on previous European Union regulations. A data company may serve globally systemic institutions as referenced in the criteria, but does not provide services that were deemed "critical or important functions" under MiFID II. In fact, MiFID II explicitly carves out "the purchase of standardised services, including market information services and the provision of price feeds" as not critical (Article 30(2)(b) Delegated Regulation 2017/565). On this basis, it has been commonly understood that firms which aggregate publicly available data to provide enhanced market data and analytics as a commercial service are not critical to the continuity of investment services or their clients' ability to serve their customers. If it is the case that the Commission's understanding of outsourcing criticality has changed, and it now considers such firms as posing risks of "large scale operational failure" (Article 28(1)), it would be helpful to have clear criteria that set out the rationale and hence allow firms in this space to have a better idea of whether they need to prepare to comply with DORA as CTPPs.

c. Preparation Time for Compliance

Especially due to the pace at which DORA is expected to move through the EU's legislative process, greater transparency from the outset regarding the designation process would be highly beneficial so that those firms which are to be designated as critical ICT third-party providers have preparation time for compliance with the regulation. Certainty is important for regulated firms, which tend to plan on a three-year, as opposed to one-year, cycle.

Furthermore, many of the companies which could feasibly be regulated as CTPPs under DORA are not currently directly supervised across large parts or the entirety of their business. Accordingly, they might need to hire new compliance staff in order to implement and comply with the regulation. In a time of significant instability and change, when firms are already making reassessments, restructuring and reallocating capital, it is key that DORA does not cause any unnecessary instability in the industry and hence counteract its intended purpose.

As previously noted, the application of the DORA requirements 12 months after the entry into force of the regulation is an unrealistically short timeframe for implementation. It is also not clear if there is an implementation period from when a CTPP is designated as such and when it must start to comply with the requirements of DORA. Ultimately any time frames need to provide sufficient time to make changes to systems, controls, testing, staffing, contracting and other processes in order to ensure smooth implementation. Please see Part 1 of this response for our proposals regarding workable time frames for implementation.

8. <u>Data localisation and onshoring</u>

We are also concerned that the lack of clarity in the definition of third-country service providers and the proposed limitations on the use of those providers, as well as the desire to conduct onsite inspections of premises including data centres, which echo a trend towards data localisation and onshoring which the Commission itself has previously indicated is not its objective.

The financial services industry is currently witnessing and responding to increasingly protectionist behaviours in various jurisdictions in the form of data localisation. We urge the Commission to continue to resist this alarming trend which is detrimental to the economy. In a study commissioned by the European Centre for International Political Economy ("ECIPE") the cost of compliance with existing data localisation measures in EU Member States is costing the EU economy $52bn per year whilst the removal of the existing regulations would generate GDP gains of $8bn per year[14].

The IRSG has recently published a report, alongside DAC Beachcroft, outlining the negative impacts of data localisation on the financial services sector. The IRSG does not consider that measures requiring, or that have as their effect, data localisation are an effective solution to 21st century problems. The report can be accessed here.

Whilst we understand that the intention from the Commission is to introduce enforcement and oversight powers from the EU, by requiring critical ICT Service Providers to establish a local entity in the EU, we are concerned that the impact of the restrictions on third-country ICT service providers may end up introducing data localisation by the back door. This risk has been exacerbated where personal data are processed by the recent *Schrems II* judgment of the CJEU which although not banning international transfers of personal data to third countries has without doubt made such transfers much more challenging for firms in financial services and the rest of the economy. We risk inadvertently creating a European data silo which will result in more fragmented data, duplicated data, create additional cost and administrative requirements for firms, adversely impact the timely actions to combat financial crime and cybercrime, limit EU firms' access to key services from the providers of their choice, adversely impact inward investment into the EU, and raise the cost of doing business in the EU. This outcome would also be inconsistent with the objective of developing open and globally interconnected capital markets in the EU,

There is also a substantial risk that taking this approach would embolden and encourage other jurisdictions to imitate the EU's actions thereby causing global fragmentation of operations and risk management frameworks, as well as uncoordinated and inconsistent regulatory interventions/recommendations. Mandated subsidiarisation of CTPPs might, therefore, inadvertently increase operational resilience risks and would be counter-productive to the EU's broader trade objectives, especially in connection with market-opening goals for other jurisdictions.

a. Definition of Third-Country ICT Service Provider

In the DORA proposal (Article 3(19)), "'ICT third-party service provider established in a third country' is defined as "an ICT third-party service provider that is a legal person established in a third-country, has not set up business/presence in the Union, and has entered into a contractual arrangement with a financial entity for the provision of ICT services". We assume this requirement is similar to GDPR requirement to have a representative or representative office within the EU? Understanding the expectation and obligations of the presence in the EU

[14] ECPE, Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in EU Member States, 2016, accessible at https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu/

is something that should be clarified as soon as possible so that firms can plan accordingly, or set up an entity if required.

b. Use of Third-Country ICT Service Providers

The statement (Article 28(9)) that "financial entities shall not make use of an ICT third-party service provider established in a third country that would be designated as critical" raises questions as to what is designated as critical. A lack of clarity as to the designation criteria may lead to an inconsistent approach, and will inhibit the ability of financial institutions to make decisions based on a range of relevant existing factors (including from an operational resilience perspective) of using a particular provider, which would create operational complexity for firms who need to amend their supplier agreements, and would ultimately be to the detriment of market efficiency without necessarily furthering the objectives of DORA.

Article 28(9), if maintained, also risks creating barriers for third-country firms such that they might choose to exit the European market. This could be disadvantageous to the international and internal competitiveness of the European financial services industry and may also be counterproductive in terms of its ability to manage cyber risks, both by reducing access to advanced technology and services that support firms' resilience, and because mature market participants (e.g. large cloud service providers), many of which are from third countries, often have the most sophisticated cyber risk management frameworks in place.

c. Intention to Conduct Onsite Inspections

The Commission's intention (Article 34(4)) for the Lead Overseer to conduct on-site inspections covering "the full range of relevant ICT systems, networks, devices, information and data either used for, or contributing to, the provision of services to financial entities", does not necessarily align with or recognise the way in which ICT companies operate today. Many firms use cloud storage to reduce costs by accessing flexible computing power that is commensurate with their business needs rather than committing massive investment to on-premise hardware and infrastructure. This type of technology is innately borderless, and it is therefore difficult to see how such on-site inspections would be conducted without requiring firms to set up data centres in the European Union.

Not only would this be less cost efficient, obstruct this competitiveness, hamper innovation and curb the use of big data, it would also risk counteracting effective risk management. Indeed, firms that operate in multiple jurisdictions need to be able to track their operations to manage risks consistently and comprehensively, using data from multiple sources. Onshoring of data centres would limit their ability to do so.

It would also be helpful to add some sensible limitations on the Lead Overseer's right to audit, including requirements to: (i) provide notice of audit, and cause minimal disruption when carrying out an audit, wherever possible; and (ii) considering the circumstances and operational resilience risks to a CTPP when determining whether it is necessary to seal any business premises. Similar clauses exist in other recent financial services outsourcing regulation, and are not understood to represent a limitation to the authorities' rights, but rather to provide assurance to market participants.

d. International Precedent for Data Localisation

We have strongly supported the Commission's past assertions which targeted data localisation requirements both by Member States within the single market and criticised similar efforts in other countries such as India. It is a major concern, therefore, that some elements of DORA could not only lead to data localisation within the EU, but could also set an international precedent for other similar legislation in other jurisdictions to be used to serve existing data localisation agendas. This broader trend poses a particular challenge to the fight against financial crime, which is significantly hindered by restrictive data localisation rules due to the necessity of sharing data to combat complex criminal networks. Again, while the intentions of this proposal are clearly well intentioned, it is important to set the right direction of travel at an early stage to ensure it does not increase risks in one area while attempting to manage them in another. Furthermore, free trade agreements negotiated in recent years are increasingly requiring that data localisation requirements should not be permitted between the parties to the relevant free trade agreement.

9. <u>Novel oversight framework for CTPPs</u>

We would like to understand better how the oversight framework will function given the novelty of shared responsibility between ESAs and NCAs as well as the choice of Lead Overseer based on the customers of the CTPP, and would like to see more clarity on the instances in which penalty fees will be imposed, with a view to ensuring DORA does not impose a disproportionate cost burden.

a. Selection of Lead Overseer Based on Customers

The proposal states (Article 28(1)(b)) that the Joint Committee will "appoint either EBA, ESMA or EIOPA as Lead Overseer for each critical ICT third-party service provider, depending on whether the total value of assets of financial entities making use of the services of that critical ICT third-party service provider and which are covered by one of the Regulations". The appointment of the lead overseer based on the customers of the CTPP as opposed to the operations of the CTPP itself may not produce the optimal choice in terms of the expertise at hand. For example, market data company's clients might be predominantly large banks, hence leading to its overseer being the EBA, when in reality, ESMA may have a better understanding of financial market infrastructures, the services data and infrastructure companies provide, and the risks associated with them.

b. Level at which Oversight Will Take Place

The framework does not clearly state the level at which the oversight will take place – i.e. whether it will take place at group level (the entire firm receiving oversight) or subgroup level (the specific services that the company provides that are deemed critical). This is an important distinction, as oversight conducted at group level could risk creating an uneven playing field at the sub-group level if one entity designated as critical and therefore bearing the costs of oversight is competing with another which is not.

c. Imposition of Penalty Fees

Whilst, as previously stated, we fully support the aim of enhancing resilience in financial services, imposing direct oversight on CTPPs will inevitably be costly and onerous for the companies designated, and the costs are likely to be passed on to financial institutions. As such,

we propose a recital to Article 31(7) that clearly states *Lead Overseers shall only impose penalty payments as a last resort in the event that the ICT third-party provider fails to comply despite other reasonable measures being taken*.

d. *Lack of Mechanisms for Dialogue between CTPP and Overseers*

Given the novelty of the framework's structure and, in particular, the shared responsibility of the ESAs and the NCAs, there should be a mechanism in place to ensure dialogue between the CTPP and Oversight Forum/Lead Overseer is always possible. Article 30(3) states that "Lead Overseer shall adopt a clear, detailed and reasoned individual Oversight plan for each critical ICT third party service provider. That plan shall be communicated each year to the critical ICT third-party service provider." We propose adding that "*The critical ICT third-party service provider shall be able to raise queries about the Oversight plan at the beginning of the year and throughout the year on an ad hoc basis".*

PART 3: CONCLUDING COMMENTS AND MEMBERSHIP

We stand ready and willing to continue to engage with the European Commission on this important project and look forward to opportunities to exchange more detail in the future.

The IRSG organised two workshops on DORA, in October and November 2020, with interested Members. The IRSG wishes to thank those who have overseen production of this response, in particular DLA Piper.

We thank you for considering this submission.

Contact address:
IRSGSecretariat@cityoflondon.gov.uk

ABI
Accenture
AFME
AIG
Barclays
Blackrock
Bloomberg
BNY Mellon
Citi
CME Group
DLA Piper
Eversheds Sutherland
EY
Fidelity
HSBC
Investment Association
JP Morgan
KPMG
London Stock Exchange Group
Moody's
PwC
Refinitiv
Schroders
Simmons & Simmons
Standard Chartered
State Street
techUK
UK Finance