9. DORA AND THIRD-PARTY RISKS: IS THE EU EXTENDING SUPERVISION TO (U.S.) BIG TECH?

Carolina Albuerne
Partner at Uría Menéndez

1. INTRODUCTION

During the last decades, financial entities in the European Union have been extensively using services rendered by third parties when conducting their business models. Outsourcing has been widely used in information and communication technologies (ICT), where financial entities have a long history of utilizing third-party services for the development and maintenance of their software, including data applications.

But during the last decade or so the use of the services of cloud computing providers has become more prominent. Financial entities have become dependent on a handful of ICT third-party service providers. The success of financial businesses, like many others, is reliant on their ability to process and manage large swaths of data in real-time to offer the best possible service to their clients. And doing it on a cost-effective basis. It is in this context when financial entities are taking advantage of the massive data-processing capabilities of cloud service providers. While the former may own their own data processing centers, they are increasingly likely to combine them with cloud services.

Moreover, many third-party service providers offer financial entities new software they can use in relations with their customers. This is a key aspect considering the unrelentless progress towards mobile and internet banking, where traditional physical banking channels through branches and direct interaction with customers are taking a back seat.

ICT relevance for financial businesses cannot be overstated, as evidenced by the growing share of intermediaries' overheads that is spent on the development and maintenance of their ICT frameworks. Even when entities require large numbers of IT specialists, they also need the support of specialized service providers, that have the scale and expertise to efficiently render their services to financial entities.

2. DORA: HARMONIZING ICT RISK STANDARDS THROUGHOUT THE FINANCIAL SECTOR BUT ALSO EXPANDING THE REGULATORY PERIMETER

Since the Global Financial Crisis, the prudential requirements applicable to regulated institutions, particularly to banks, have sharply increased, affecting all their activities. Financial institutions are required to operate with much higher levels of capital and liquidity, they are subject to very demanding internal governance and risk management standards, and they are continuously and intrusively inspected and supervised. In parallel with the digitization of financial business, authorities have expanded the regulatory and supervisory standards that address the ICT risks. For instance, they have set detailed and burdensome requirements for ICT risk management, including the use of third-party service providers.

Policymakers in the European Union have also widened the prudential regulatory perimeter. Nowadays, many more typologies of financial institutions are regulated in the European Union. For instance, payment institutions, crypto-services providers or trade repositories are subject to prudential regulation and supervision. And they are subject to rigorous standards on ICT risks.

In this context, the Digital Operational Resilience Act (hereinafter, DORA[1]) has been a new step ahead in expanding the extent and perimeter of prudential regulation. First, by harmonizing the standards on ICT risk management applicable to all EU financial entities, as they were subject to different, not entirely consistent requirements included in a patchwork of European regulations, national laws, European Agency's guidelines or supervisory recommendations. And, secondly, by establishing a new prudential supervisory framework for certain "critical" ICT third-party service providers, based on the extent and scope of their support for the critical or important functions of EU financial entities. It allocates the responsibilities of the new supervisory regime to a "Lead Overseer", one of the three European supervisory agencies (the European Banking Authority (EBA), the European Securities Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA)).

3. HARMONIZATION OF ICT STANDARDS ACROSS THE EUROPEAN FINANCIAL SYSTEM

Financial entities are making more use of the services by third party service providers as part of their ICT model, including those related to cloud computing (third-party risk). Entities that have always been outside of the perimeter for prudential supervision, until now.

[1] Regulation (EU) 2022/2554 of the European Parliament and the Council of 14 December 2022 on digital operational resilience for the financial sector and amending regulations (EC) No 1060/2009, (EU) No 680/2014, (EU) No 909/2014, and (EU) 2016/2011.

Policymakers and supervisors have been focusing on third-party risks for a long time. Authorities seek that regulated institutions, when using third-party services to perform their business, soundly manage their third-party risks. To this end, they have issued standards on third-party risk management, with the overarching goal that the internal controls for outsourced activities are equivalent to those applied to non-outsourced activities by the regulated entity. The regulated entity remains accountable for the outsourced activities, and contracts with third parties must acknowledge the supervisor's ability to access the outsourced activity to maintain adherence to the same prudential oversight regime.

The first milestone in setting outsourcing prudential standards happened in 2006, when EBA's predecessor, CEBS,[2] issued its Guidelines on Outsourcing, evidencing it was a broad-based trend that affected the European banking system,[3] and therefore deserved a European response. Supervisors have long been considering the assessment of third-party risks when reviewing a financial entity's operational risk profile, following the general mandate to assess outsourcing risk as part of the operational risk included in the CRDVI.[4] For instance, the EBA includes the third-party risk assessment in its Supervisory Review and Evaluation Process (SREP) approach,[5] and the European Central Bank (ECB) identifies this risk as one of the key subcategories of operational and ICT risks during its SREP assessment.[6]

But the increasing use of outsourcing, particularly in ICT services, has attracted closer scrutiny by policymakers and supervisors alike. EBA (and EIOPA and ESMA) issued new Guidelines on Outsourcing,[7] including on cloud computing, that set forth reinforced and granular standards on how banks and payment institutions are expected to manage and control their third-party risks[8]. Some of these recommendations have been included in DORA as binding rules. Likewise, the intensive usage that the largest banking groups in the Eurozone has been making of cloud computing services prompted the ECB to issue its own Guide on the use of cloud computing services in 2021.[9] Globally, policymakers and supervisors have also been taking steps towards ensuring closer

[2] Committee of European Banking Supervisors.

[3] The Guidelines were largely based on the Joint Forum 2005 Outsourcing Guidelines, that set the standards that both financial institutions and supervisors should apply when managing and/or supervising outsourcing. The EBA also consolidated in these Guidelines its Recommendations on outsourcing to cloud service providers (EBA-Rec-2017-003).

[4] Article 85 of Directive 2013/36/EU of the European Parliament and the Council of 26 of June 2013 on the access of activity of credit institutions and the prudential supervision of credit institutions.

[5] EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing under Directive 2013/36/EU (EBA/GL/2022/03).

[6] ECB operational risk methodology for SREP assessment.

[7] EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02), EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002), ESMA on outsourcing to cloud service providers (ESMA50-164-4285).

[8] Some standards on how banks should govern their risks were also included in the EBA Guidelines on internal governance under CRD (EBA/GL/2021/05), in the last reviewed version.

[9] ECB Guide on outsourcing cloud services to cloud service providers.

supervision of third-party risk management, as evidenced by the consultative document on the topic by the Basel Committee on Banking Supervision.[10]

Addressing third-party risks in operational continuity in resolution has also been a prominent aspect considered by resolution authorities during resolvability assessments.[11] Authorities are requesting banks to insert clauses in their contracts with third-party service providers that ensure they cannot suddenly stop the rendering of the services just because of the resolution or crisis situation of the institution.

DORA can be understood as one further step in the same direction. Many rules set out by DORA were already in force through recommendations, guidelines and other standards for most financial entities. But their relevance comes from their binding nature, as they are set out by European regulation and, therefore, directly applicable to EU financial entities.

4. DORA STANDARDS FOR ICT THIRD-PARTY RISK MANAGEMENT

4.1. BROAD SCOPE

The scope of application of DORA is very broad, as its main goal is to harmonize the standards for management ICT risks across the financial system, covering most financial intermediaries that operate in the European Union.[12] As such, most standards are not necessarily new for banks, insurance companies or securities companies. The rules covering third-party risk management are no exception to this.

It must be noted however that DORA's rules on third-party risk management only cover ICT services. DORA's rules are not directly applicable to other non-ICT third party services, that could be also very relevant in the business model of financial entities, including administrative, payment or other non-ICT services.[13]

[10] BCBS: Principles for the sound management of third-party risk. Consultative document. July 2024.

[11] Resolution authorities have been recommending banks to map their contracts with third-party service providers, to centralize their contracts with them and insert clauses that ensure that they cannot terminate unilaterally the services provided based on the resolution or crisis of the credit institution. See for instance, Single Resolution Board Operational guidance for operational continuity in resolution (November 2021). The guidelines were updated in January 2025.

[12] Article 2 of DORA includes a broad number of entities within its scope. They do not only include banks, payment institutions, investment entities, or insurance and reinsurance companies, but also other supervised entities in the European Union, such as credit rating agencies, or crypto-asset service providers, or the administrators of critical benchmarks.

[13] The guidelines or rules on outsourcing are applicable to the third-party provision of non-ICT services. For instance, banks and payment entities in the European Union are subject to the EBA Guidelines on Outsourcing.

4.2. GOVERNANCE REQUIREMENTS

DORA prescribes demanding governance and risk control requirements applicable to the outsourcing of ICT services. Beyond the general governance standards applicable for ICT risk management,[14] DORA requires financial entities to adopt and regularly update a strategy on ICT third-party risk, where they may consider a multi-vendor strategy. The strategy should consider the use of ICT third party service provider (TPSP) for supporting the performance of critical or important functions.[15] DORA seeks to ensure that the decision to use third-party services for ICT services is reasoned and thoroughly assessed, after fully considering its risks and benefits.

Financial entities should keep a comprehensive register of all their contractual arrangements with third party service providers for ICT services, distinguishing among those that support critical or important functions and those that do not. Financial entities should annually report to the relevant competent authority their new arrangements for ICT risks, including those that have been amended during the exercise. DORA seeks to ensure that financial entities store all relevant information in a centralized manner, so it can be easily controlled and monitored by them and by their supervisors. This is even more important in a context where financial institutions, when complex and sophisticated, may have hundreds, if not thousands, of relevant contracts with dozens of service providers.

4.3. PRE-OUTSOURCING PROCESS

Financial entities are in principle free to decide whether to outsource or not their ICT services, including when the outsourcing affects or can affect the provision of critical or important services.[16] They are "only" required to apply sound standards and procedures before agreeing to any ICT outsourcing. Entities should assess the nature

[14] Article 5 of DORA.

[15] Critical or important functions are defined as a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorization, or with its other obligations under applicable financial services law. The definition of critical and important functions is aligned with the rules on banking resolution.

[16] A regulatory model whereby financial entities are required to request an authorization prior to any ICT outsourcing will not be desirable, as it has many shortcomings. First, financial entities may have hundreds of contracts with services providers, and therefore supervisors may need to have very large structures just to manage the file applications from supervised entities. The sheer number of applications may even put into question the ability of supervisor to process in time the applications. As a result, supervised entities may face significant delays, financial innovation may be curtailed for regulated institutions. Second, an authorization regime may create a false complacency on financial entities and service providers alike, as a supervisor's authorization may likely to be perceived as a "seal of approval" of the services provider.

of the activity to be outsourced (including whether it is a critical or important function) and conduct thorough due diligence on the service provider as part of the selection and review process. The vendor due diligence should check whether the third-party has the means to provide the agreed service under the agreed circumstances. The financial entity should also verify that the contractual standards include and meet all the legal and supervisory requirements, assess the risks that may stem from the contracts and identify any conflicts of interest arising from them.

4.4. INTERNAL CONTROLS

Financial entities shall determine the frequency of the audits and inspections, including the areas to be audited. DORA is very demanding with the involvement of the financial entity's internal audit services in the review of ICT risks. For all the outsourced services, financial entities must guarantee that the contracts enable the access of the entity, including the internal audit services, to the premises, information, and data managed by the service provider in relation to the services that are rendered to the financial entity.

4.5. CONTRACTUAL DOCUMENTATION

DORA[17] regulates the content that financial entities should insert in their contracts with service providers, prescribing the minimum contents of the clauses that the written contracts where ICT outsourcing are formalized should contain, including the service level agreements. Among other aspects, the law requires financial entities to include in the contract clauses that require the TPSP to cooperate with the supervisor and the resolution authority, termination rights in favor of the financial entity, and those that thoroughly regulate the location where the service is provided and include rigorous provisions on data security.

4.6. TERMINATION RIGHTS

Financial entities should insert clauses in their contracts that enable them to early terminate the contracts upon certain conditions. Entities[18] should be entitled to terminate the contract if the TPSP has breached the applicable contractual, legal or regulatory provisions, if a material change affecting the service provider has affected its capacity

[17] Article 30 of DORA.

[18] The inclusion of termination rights in the contracts is not new for banks and payment institutions. The section 13.4 of the EBA Guidelines on Outsourcing recommend entities to include clauses allowing the possibility to terminate the arrangement upon essentially the same circumstances foreseen by DORA.

to continue delivering the service, if the service provider has material weaknesses in its overall ICT risk management and particularly if its unable to ensure sound data authenticity, availability, integrity and confidentiality standards. Financial entities should also have the right to terminate the contract if the supervisor does not have the ability to effectively oversee the outsourced service.

4.7. REINFORCED STANDARDS FOR TPSP SUPPORTING CRITICAL OR IMPORTANT SERVICES

DORA[19] requires financial entities to apply more rigorous standards when employing service providers that support critical or important services. These standards cover three dimensions: (i) the requirement to define exit strategies for each individual contract, addressing the so-called lock-in risk (ii) the comprehensive assessment of concentration risks prior to deciding on outsourcing, and (iii) rules that prescribe in more detail the content of the contracts.

First, EU financial entities should define exit strategies for contracts supporting critical or important services and include contractual clauses that enable them to early terminate them. The exit strategies must be granular and contemplate mitigating actions to guarantee the quick replacement of the service provider. These contingency plans are not a novelty, as they were already recommended for banks and payment institutions by the EBA in its guidelines.[20]

Financial entities should assess the concentration risk that they may incur when outsourcing part of its critical or important functions to ICT TPSP. They must weigh whether they are exposed to high levels of concentration risk in one service provider or to closely linked service providers. Financial entities should define and implement, when appropriate, strategies to mitigate the concentration risk to ICT TPSP, to ensure that their ability to provide services and conduct their business model is not curtailed by any problems affecting the services provider.

Requesting financial entities to assess concentration risk with ICT TPSP is hardly something new. For instance, the ECB, in its Guide on cloud computing, recommends banks to go beyond assessing concentration risk prior to the decision to outsource, and continuously measuring this risk during the outsourcing lifetime. The ECB also expects that banks assess other concentration dimensions beyond single name, including the geographical location or deriving from a specific functionality or service. The EBA guidelines also recommend entities to assess the concentration risks associated with outsourcing.[21]

Financial entities must also include additional clauses in their contracts with service

[19] Article 28(8) for exit strategies, article 29 for assessing concentration risks prior to outsourcing article 30(3) for the additional information included in contracts.

[20] Section 15 of the EBA Guidelines on Outsourcing.

[21] Paragraph 66 of the EBA Guidelines on Outsourcing.

providers that support the provision of critical or important services. Beyond the inclusion of further detailed information on the services to be provided, financial entities must insert in their contracts the following clauses:

- Transition periods linked to exit strategies. Transition periods seek to ensure that the provision of services is not suddenly interrupted by the TPSP when the financial entity decides to early terminate the contract. If that were to be the case, financial entities may be unable to exercise their termination rights in the contract, for fear of being unable to continue their operations (lock-in risk). Through sufficiently long transition periods[22] financial entities will be able to reintegrate the service in-house or replace the service provider in due time without affecting the performance of the service provided. This is very important, considering that many contracts with ICT TPSP are either difficult or impossible to replace.[23]

- The obligation of the service provider to participate and fully cooperate in the financial entity threat-led penetration test (TLPTs). These tests are a new requirement by DORA;[24] financial entities must engage "ethical hackers" to identify any vulnerabilities that can leave the entity exposed to risks to its operational continuity. These exercises must be undertaken at least every three years. With an increasing proportion of critical or important functions being reliant on ICT TPSP, together with the evidence that many cyber-attacks are exploiting financial entities' vulnerabilities by focusing on accessing the institution systems' through TPSP, the participation of service providers in these tests seems essential.[25] Financial entities are also expected to assess the risks related to the use of complex sub-outsourcing chains that can leave the financial entity unable to control the outsourced service.

- The inclusion in the contract of provisions that ensure full cooperation, including access rights, of the financial entity (including its audit services) and, particularly, of the supervisor, including the relevant competent authority and the Lead Overseer (see below). The inclusion of these clauses is expected to operate

[22] The law does not define the length of the transition period that financial entities must include in their contracts. Therefore, it is expected that it will be defined through the common practice.

[23] Banks and payments institutions were already recommended to include transition periods in their contracts. The paragraph 99 of the EBA Guidelines on Outsourcing recommends entities to set appropriate transition periods, and the obligation of the service provider to continue supporting the entity in the event of the termination of the outsourcing agreement.

[24] Articles 26 and 27 of DORA.

[25] See ECB IT and cybersecurity risk- key observations in 2024. The report pointed out to sharp increase in ransomware attacks on service providers, although it also indicates that none of the attacks resulted in a critical impact.

as an enabler for the new prudential oversight regime for "critical" ICT service providers.

5. NEW OVERSIGHT REGIME FOR TPSP

Besides from ensuring that financial entities apply sound standards to their outsourced activities, the legislator is aware that the concentration of the financial system in a few service providers can have systemic consequences. A failure of a relevant third-party service provider can result in multiple, interrelated impacts in the operational resilience of the European financial system or large parts of it, including entities belonging to different financial subsectors. In other words, an ICT TPSP that is suddenly unable to continue operating may trigger the inability or impaired ability of different banks, insurance companies, payment institutions, etc. to continue serving their retail and corporate clients.

In response, the European Union has adopted a policy seeking to expand the prudential supervision perimeter beyond financial organizations, covering unregulated ICT TPSPs that provide services to the former. The European Union considers that imposing requirements to financial entities on ICT third-party risk management may not be enough to address the risks that these entities pose to the continuity of critical services in the financial system. And therefore, a prudential authority must step in to directly oversee the activities of the ICT TPSP.

The regime is largely unprecedented. It articulates an architecture for the supervision for critical third-party service providers that gives European authorities ample powers to consistently review the operations of these entities that they use to render services to EU financial institutions. The framework creates obligations for TPSP to submit information, surrender to onsite or offsite inspections and responds to the recommendations issued by the relevant European authorities. This framework goes well beyond the existent regime in the United States, where the Bank Services Companies Act (BCSA)[26] enables certain supervisory authorities[27] to review the services provided by third-parties to banks.[28]

[26] A Law enacted in 1962 that facilitated the provision of services, not necessarily ICT, by TPSP to banks. The law has been subsequently amended in 1982, and is only applicable to services provided by third-parties to banks. The Act requires banks to apply the same standards to their outsourced activities to those that have not been outsourced.

[27] The Federal Reserve, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency.

[28] There are material differences between the European (DORA) and American (BSCA) frameworks. First, the scope of BSCA covers only banks (not even all deposit-taking entities in the US), whereas DORA covers most financial institutions in the EU. The covered services by DORA are exclusively ICT, whereas BSCA's scope is broader, covering mainly all services rendered by third-parties to banks, including others such as payment or lending services. But BSCA covers in principle more service providers than DORA, as it includes ICT and non-ICT services and does not restrict the supervision to only "critical" TPSP. Second, a

Having discussed the rationale of the regime, different questions of the new European regime shall be answered. Which ICT TPSPs will be subject to the oversight regime? Who will be the lead supervisor of these entities? Which powers does the lead supervisor have? How should the powers over institutions that are based in third countries outside of the European Union be exercised?

5.1. WHICH ENTITIES CAN FALL WITHIN THE NEW SUPERVISORY PERIMETER?

An ICT TPSP designation as critical is the basis for being subject to the new oversight regime. But not all service providers that render ICT services to EU financial entities will be deemed critical. Not even all those that support EU financial entities in the provision of critical or important services will be critical. The "criticality" label is therefore a rather selected category, a "grand cru" standard that is reserved only to those service providers that can have "systemic" effects in the European Union due to their interconnections with financial entities.[29] The European Supervisory Agencies (ESAs), in the context of the Joint Forum, will be responsible for identifying these critical entities, a task they have already started. The first list of critical service providers is expected to be published during 2025 by the Joint Forum.[30]

Three features characterized the new supervisory framework: (i) its paneuropean dimension, as the rationale of the new oversight regime is the existence of entities that

critical difference is that enforcement provisions are very clear in DORA, whereas in BSCA are lacking, what significantly weakens the position of the supervisors, as makes oversight dependent on an entity willingness to cooperate. Third, DORA includes provisions that ensure that the public can know which are the critical third-party service providers that are subject to the oversight regime, as they will be disclosed, whereas BSCA does not include any provision on disclosing these elements. Overall, DORA is a much more ambitious approach than BSCA, as formalizes how the supervision of critical ICT services providers is expected to work, and creates prudential obligations for these entities.BSCA is a much less complete framework, where the powers of the supervisors are not underpinned by obligations of TPSPs.

[29] Indeed, this system may have some common features with the framework for designating systemically important institutions in the European Union. Designation is the key first step towards the application of a reinforced regulatory and supervisory framework. This risk-based approach intends to ensure that there is proportionality embedded in the new regime, the framework will only be expectedly applicable to a few, large and powerful service providers that may have the means and scale to meet the supervisory requirements and recommendations.

[30] Although the list is yet to be published, the ECB has published some aggregated data on ICT service providers to significant institutions that can give some hints on the process for the criticality designation. During the 2024 Outsourcing Register, the ECB concluded that around 50 percent of the total budget for critical services of significant institutions in the Eurozone was allocated to the top 20 TPSP. 90 percent of the total budget is allocated to top 300 service providers. It can be inferred from the data that banks in the Eurozone exhibit a large concentration in a few ICT TPSP, and that therefore this offers a blueprint for the identification of critical service providers. In the same vein, the report also identifies that most significant institutions are using third party cloud services, and identifies the top 6 cloud service providers (Microsoft, Amazon.com, Google LLC, Salesforce, Oracle Corporation and IBM Corporation).

can create systemic risks for the whole European Union, (ii) its cross-sectorial features, as critical TPSP provide services to a broad range of financial entities operating in diverse sectors and (iii) its collegiate nature, as many authorities (from different sectors, and from European and national levels) will be represented in the new joint examination teams supporting the deployment of the new powers of the Lead Overseer.

How and when this designation will happen are key questions hovering over the heads of many ICT service providers in the European Union. DORA[31] outlines several criteria that the ESAs should consider when assessing the criticality of TPSPs; only service providers that can have a serious impact on the EU financial stability will be identified as critical, based on the following criteria:

- The systemic impact on stability, continuity or quality in the provision of financial services if the ICT TPSP faces a large-scale operational failure. Authorities should consider the number of served financial entities and their total assets, to gauge the possible impact of the TPSPs on the operational resilience of the affected financial entities.

- The systemic relevance of the financial entities relying on the services provided by the ICT TPSP, by factoring in the number of global or domestic systemically important institutions served by the relevant entity. The law mandates ESAs to go beyond just measuring the size of the potentially directly affected financial entities and identify also the secondary impacts from the interconnections between these systemically important institutions and other financial entities to which they are subsequently rendering their services to.

- The reliance on the TPSP by financial entities for performing their critical or important services. In principle, if TPSP supports the provision of non-critical, non-important services, a sudden operational interruption of the service provider activities cannot trigger any significant impact on the citizens and corporates of the EU economy.

- The substitutability of the ICT TPSP, by gauging the availability of any realistic alternative providers. Authorities must consider whether there are service providers that can render comparable or similar services, and the complexities of the contract or services rendered, that can adversely affect their substitutability. Moreover, authorities should also assess that the ability to replace a TPSP may be affected by the difficulties migrating the relevant data to another service provider, due to either the high costs or the high operational risks involved in the migration (high switching costs). The limited substitutability of certain ICT TPSP is a well-known fact, especially for certain services, such as cloud computing.[32]

[31] Article 31(2) of DORA.

[32] For instance, the banks surveyed by the ECB considered that less than 20 percent of their critical and

To avoid any regulatory arbitrage, the law requires the ESAs to conduct the assessment at group level, by considering together all the services that these TPSPs render to EU financial entities.[33]

The inclusion criteria are complemented by several exclusions of ICT TPSP which will not be subject to the prudential supervision framework. For instance the framework will not be applicable to supervised entities, either financial or non-financial, since their activities are already supervised.[34] The provision of intragroup services is also disregarded for these purposes. Finally, if the ICT TPSP provides services exclusively to financial entities that are only active in a Member State, the service provider will not be identified as critical, as their activities cannot raise paneuropean concerns.

DORA requires ICT TPSP considered "critical" to have at least one subsidiary in the European Union to render services to EU financial entities. This is a relevant requirement, as many large ICT TPSP are headquartered in third countries and may not have a direct subsidiary in the single market.[35] This rule evidences European Union's willingness to exert closer control on third-country critical TPSP.

DORA also foresees the possibility for an ICT TPSP to voluntarily request to be identified as critical, by submitting its application to one ESA. Despite its potential costs, some service providers might see the oversight framework as advantageous. Being listed as critical can make a provider appear safer behind clients and more relevant than other competitors not on the list, especially since the law mandates publishing the names of critical ICT TPSPs. Considering the current context, the possibility of a service provider willingly submitting to an administrative supervisory framework seems rather far-fetched.

5.2. ONE OF THE ESAS AS THE LEAD OVERSEER: A PRIMUS INTER PARES

The oversight regime for critical ICT TPSP is a collegiate, cooperative and essentially paneuropean undertaking. DORA determines that one of the ESAs (EBA, EIOPA or ESMA) should be appointed as "Lead Overseer",[36] effectively a *primus inter pares*.[37]

---

external contracts with third party service providers will be easy to substitute, with less than 10 percent being impossible to substitute. In 2022, the ECB singled out the six most relevant providers of cloud computing services, reflecting a low expected substitutability.

[33] Article 32(3) of DORA.

[34] For instance, a bank that provides software-as-a-service to other financial institutions will not be eligible as a critical TPSP, as it is already subject to a prudential supervisory framework that ensures that it manages the ICT risks relevant for the provision of services to any other financial entity.

[35] The rule does not explicitly require that the EU financial entity can only enter a contract with the EU subsidiary, nonetheless. It may therefore be possible that a critical TPSP to render services to an EU financial entity through a non-EU legal entity, if it has established a subsidiary in the EU.

[36] It is not the first time that the EU choses to allocate the responsibility of supervising financial institutions to ESAs. For instance, ESMA is responsible for the supervision of credit rating agencies, or trade repositories, for instance. The spirit is that issues with a European dimension require a European response.

[37] This is one of the key differences with the US BCSA, that confers inspection powers to three regulators

The designation is based on the total amount of the assets of the financial entities to which the services of the critical TPSP are rendered, broken down by sector (banking, insurance, or securities).[38] The chosen metric, in view of the larger size of the banking sector in the European Union makes the EBA the likely winning horse in the race to take over the leading role in the oversight of many of the critical TPSP across the European Union.[39]

The identification of critical ICT TPSP and other activities related to the prudential supervision regime will be undertaken in the Oversight Forum, a sub-committee of the Joint Forum. The Forum will have a harmonization mandate, to ensure the consistency of the emerging practices in the supervision of ICT TPSP. Its membership will be broad, with representatives from both European and national authorities involved in the oversight framework.

The Lead Overseer's main responsibility is assessing whether the critical ICT TPSP has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risk it may pose to European financial entities. The law clarifies that the assessment shall focus mainly on the services rendered by the ICT TPSP that support the performance of critical or important services by EU financial entities.[40] Based on this assessment, the Lead Overseer will prepare a draft oversight plan outlining the activities it intends to perform for the supervision of the critical ICT TPSP, that will be shared with the affected service provider.

5.3. POWERS OF THE LEAD OVERSEER

DORA gives the Lead Overseer relatively broad powers for supervising critical service providers. The oversight framework does not require critical TPSP to be licensed, and therefore a third-party service provider does not need to undergo any authorization process before starting the provision of critical or important services to a financial entity in the European Union. Nor will its directors or senior managers be required to be subject to a fit and proper assessment. In other words, providing critical services to

but fails to organize how supervision is expected to work, which significantly weakens supervisors' position and makes them contingent on the service provider willingness to cooperate.

[38] For instance, if the cumulative total assets of the served credit institutions are larger than the assets of insurance companies and securities entities, the EBA will be designated as the Lead Overseer.

[39] The criteria resemble the framework for identifying a lead supervisor of a financial conglomerate, in accordance with the Financial Conglomerates Directive (FICOD). Unlike a financial conglomerate, in the new supervisory framework there is no "parent entity", and therefore the criteria are only based on the size of the largest sector to which the TPSP provides services.

[40] DORA clarifies the aspects where the Lead Overseer should consider in its assessment of the critical ICT TPSP. Among others, the Lead Overseer will be expected to assess the requirements to ensure the availability, continuity, scalability and quality of services provided to financial entities, the physical security contributing to ensuring ICT security, the risk management processes, or the ability to identify, monitor and report any material ICT-related incidents and cyber-attacks, the governance arrangements, etc.

a regulated entity in the European Union is not a reserved activity, but it may trigger some prudential supervision. DORA gives the Lead Overseer information and inspection powers.

The Lead Overseer can request information and documents to the critical ICT TPSP including relevant business or operational documents, contracts, policies, etc. It will be able to examine records, data, procedures and any other material relevant to the execution of its responsibilities, obtain documents, including copies from the relevant materials by banks, or summon the representatives of the critical ICT TPSP. Moreover, the authority will be able to conduct onsite inspections on any business premises of the service provider.

The Lead Overseer will be assisted by a joint examination team to conduct inspections and other supervisory actions, in a structure that seems inspired by the Single Supervisory Mechanism's joint supervisory teams.[41] These teams will be set up individually for each critical ICT TPSP; there might be as many joint examination teams as supervised critical entities, each one with a different composition.

The composition of the joint examination team[42] will reflect, to the extent possible, the footprint of the critical service provider and of the financial entities served by it, seeking to combine and leverage the European and national expertise. It will be made up of representatives from the ESAs, the competent authorities for the supervision of the financial entities served by the ICT TPSP, and even a representative from the competent authority from the country where the service provider is established (on a voluntary basis). The joint examination team should have the expertise required to conduct the oversight of the ICT TPSP, particularly on ICT and operational risks. Considering that dozens, if not hundreds, of financial entities in the EU may be served by some large ICT TPSPs (particularly in cloud computing), the ESAs may need to cap the size of the joint examination team, as otherwise it can easily become unmanageable.

In the event of a critical ICT TPSP not complying with the recommendations or doing it unsatisfactorily[43] after receiving the requirement, the Lead Overseer may be able to impose serious sanctions on it. The Lead Overseer can apply a periodic penalty pay-

[41] The joint supervisory teams (JST) are made up of representatives from the ECB and from the local supervisory authorities from the countries in the Eurozone where the group operates. These structures leverage on the local knowledge and resources of the local authorities to ensure the effective supervision of significant institutions in the Eurozone.

[42] Joint draft Regulatory Technical Standards on the criteria for determining the composition of the joint examination team (JET), not yet applicable.

[43] The only punishable offenses by a critical ICT TPSP will be to fail to deliver the information or documentation required, failing to cooperate with the Lead Overseer during the general examinations or inspections, and failing to respond to the recommendations of the Lead Overseer or doing it so in an unsatisfying manner. The critical service provider will not be required to comply with the Lead Overseer's recommendations, as they are of a non-binding nature. Nevertheless, failing to comply with a supervisor's recommendations is rarely an option for a supervised entity, and even more when, in case of non-complying, the supervisor will disclose this fact publicly and may even result in a requirement to the financial entities that use its services to suspend or even terminate the services.

ment on the critical service provider. This fine will be imposed daily until compliance is achieved, but it will be capped to six months. The payment may be up to 1 percent of the daily worldwide turnover[44] of the critical ICT TPSP, potentially a very high amount that seeks to ensure that the service providers have legal incentives to cooperate with the Lead Overseer, and that the reflects these entities' global scale.[45] DORA also includes the requirement[46] to the Lead Overseer to disclose the periodic penalty, in a "name and shame" scheme.[47]

Power to issue recommendations. DORA gives the Lead Overseer the power to issue recommendations on certain areas of activity of the critical ICT TPSP, which may affect how it provides the ICT services that support critical or important services of financial entities. The Lead Overseer may recommend the use of specific ICT security and quality requirements or processes, or conditions and terms under which the critical ICT TPSP provide ICT services to financial entities.

The focus on subcontracting is notable due to potential risks it poses to financial entities receiving ICT services. The Lead Overseer may also issue recommendations to the critical service provider on refraining from entering into a further subcontracting agreement in cases where subcontracting may involve critical or important functions to the financial entities and the subcontracting party is located in a third country and the arrangement poses a clear and serious risk to the financial stability of the Union or to the served financial entities. Therefore, to limit the public intervention regime to the minimum possible the Lead Overseer can only issue recommendations for very specific topics under very determined circumstances.

The recommendations issued by the Lead Overseer do not have a binding nature; a critical ICT TPSP may decide to ignore them. Nonetheless, DORA contains different mechanisms of "moral suasion", that would compel the critical ICT TPSP to comply with the supervisory recommendations. First, the critical servicer will need to notify within 60 calendar days of its intention to follow the recommendations or the reasons

[44] The reference to the worldwide turnover of the critical service provider intends to ensure the relevance of the penalties. Many large ICT companies that provide services to the European financial entities are headquartered in third countries and only a fraction of their turnover comes from the European Union. For instance, the ECB in its outsourcing registry of 2024, has identified that significant institutions in the Eurozone has significant dependencies with many service providers (ICT and non-ICT) headquartered in the United Kingdom (53 significant institutions), USA (46), China (23), or India (16).

[45] Article 35(8) of DORA lays down the criteria that the Lead Overseer should use when graduating the periodic penalty payment against the critical ICT service provider. Among other aspects, it should assess the gravity and duration of the non-compliance, whether the non-compliance was committed intentionally or negligently, and the level of cooperation of the services provider. Article 35(9) states that the amount of the periodic penalty payments will be allocated to the general budget of the European Union.

[46] DORA does not include, however, other sanctions that are usually applicable to supervised entities or their managers. A critical service provider cannot have its license revoked, as it does not have one. There is no accountability framework for the administrators or the senior managers of the affected banks, as there is no fit and proper regime applicable to them.

[47] Article 35(10) of DORA, that also recognizes that if the disclosure can jeopardize the financial markets or cause disproportionate impact to the parties involved, the Lead Overseer may decide against disclosure.

for not doing so.[48] Second, the Lead Overseer must disclose to the public if the critical ICT TPSP does not notify the supervisor within the required period, or when the explanations provided by the entity to not follow the recommendations have not been deemed sufficient by the supervisor. This disclosure is intended to work as a mechanism to pressure the service provider into complying with the recommendations. Third, DORA also foresees that as a last resort, and after having received the assessment by the Lead Overseer, the competent authority[49] (for instance, the banking supervisor for a bank) can force the financial entity to temporarily suspend or to terminate the use of the services of the ICT TPSP. This will be close to a "nuclear option" by the Lead Overseer and by the banking supervisor and may have huge business and reputational effects for the third-party service provider.[50]

5.4. EXERCISE OF THE SUPERVISORY POWERS IN THIRD COUNTRIES

DORA also enables the Lead Overseer to exercise its powers (mainly information requirements and the power to conduct general investigations and inspections) outside of the European Union, on a subsidiarity basis when the objectives of the supervision regime cannot be achieved by applying them to the European subsidiary critical TPSP. To implement its powers in a third country, the law requires the explicit consent of the critical ICT TPSP, the notification to the relevant competent authority in the third country and be justified by the inability to achieve the desired outcome by applying the powers to the EU subsidiary of the TPSP. It is not clear whether the critical TPSP and the relevant authorities in the third country would authorize an inspection or any other supervisory activity in the service provider's premises in that country. The Lead Overseer might be compelled to conduct its supervisory activities in a third country if, for instance, if the TPSP manages or processes data using in that country.

5.5. WHO WILL PAY THE COSTS OF SUPERVISION?

As DORA lays out a new regime for the prudential supervision of critical ICT TPSP, a relevant question is how the costs incurred by the authorities in charge of supervision will be funded. The exercise of the new supervisory powers will result in human and

[48] Failing to communicate the willingness to comply or the reasons for not complying may be considered a breach of the obligations required by DORA to the critical third-party servicer and therefore may result in a penalty against the entity.

[49] The reference to the competent authority instead of the Lead Overseer is explained by the lack of power of the latter with regard to regulated financial entities. As the Lead Overseer does not have any enforcement powers over a financial entity, the restriction or mandate should be enforced by the financial entity's competent authority.

[50] DORA has not given the Lead Overseer the power to force the TPSP to terminate the contract with the relevant financial entity.

technical costs by the relevant authorities (mainly but not limited to ESAs). DORA has clarified the financing model by imposing the costs of supervision directly on critical ICT TPSP.

6. CONCLUSIONS

DORA toolkit for addressing the micro and macro impacts of ICT third-party risks may give the European authorities the required comfort that there are good chances that their recommendations will be followed by the critical ICT TPSP. Nonetheless, the oversight framework is new and unprecedented; and its main elements must be tested. For instance, the ESAs are yet to make the first designation of critical providers,[51] and therefore nowadays there is still significant uncertainty about which third parties may end up falling within the new supervisory perimeter. Similarly, there are still unresolved issues regarding the organization of prudential supervision. How will supervision focus solely on services to financial entities without impacting third-party providers' services to other clients? How will the Lead Overseer manage the supervision of these complex groups involving close interconnections of large number of legal entities? How will the composition of the joint examination teams be?

In any case, European financial entities may have yet another source of regulatory costs that other international competitors-notably financial entities from the United States of America are not subject to. When it comes to the provision of ICT TPSP, EU financial entities will incur significant costs related to the amendment of contracts, the maintenance of a centralized register with all the data points for the covered contracts, etc. They may also face an increase in their operating costs, as TPSP may pass the costs of compliance through them. Depending on how ESAs decide to use their newly granted powers, EU financial entities may face higher costs linked to their operational models, that can affect their competitiveness in international markets and, in some cases, may also dent their ability to innovate.

[51] Although they have already started the information collection process required to identify the critical third-party service providers in 2024, with a view of making the first designation by 2025.