大成 DENTONS

European Commission offers further details on DORA and the wider efforts of global policymakers

DECEMBER 2020

Contents

The EU's proposal for an EU-Regulation on a Digital Operational Resilience Act (**DORA**) proposes to introduce an EU-wide harmonized rulebook for digital operational resilience, including identification, mitigation and management of cyber-risk, outsourcing and concentration risk. DORA will affect those firms that are defined as "financial entities", as well as those that are information and communications technology (**ICT**) third-party service providers[1]. Further rules apply to those that are defined as critical service providers.

DORA introduces a range of harmonized definitions. These aim to improve consistency and uniformity of principles and standards. Some firms may need to adapt their own existing use of definitions so as to strengthen compliance with what DORA expects of them under this new framework. DORA defines "digital operational resilience" as "...the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality". Moreover, DORA also introduces definitions for those affected to assess the extent of any "critical or important functions" and affected firms will want to periodically perform a stocktake of these. These are defined as those "... whose discontinued, defective or failed performance would materially impair the continuing compliance of a financial entity with conditions and obligations of its authorization, or with its other obligations under applicable financial services legislation, or its financial performance or the soundness or continuity of its services and activities". The latter part of that definition provides a catch-all to cover the core activity of a given firm as notably DORA does not "just" apply to those that are subject to financial services regulatory rules.

Ultimately, DORA will also, by introducing an EU-27 wide regime, replace what the EU describes as "uncoordinated national initiatives" and create one of the world's largest harmonized frameworks for supervision of ICT risks[2] and digital operational resilience more generally. This aims to reduce the administrative burdens that firms face when dealing with, as the EU states, "...overlaps, inconsistencies, duplicative needs and higher administrative and compliance expenditures". For many affected firms, it may be advisable to take early action, both with respect to their own systems as well as in relation to their contractual and outsourcing arrangements with ICT third-party service providers. Some firms may be more affected than others, given the breadth of changes to policies, processes and procedures, and the need to make non-document based workstreams comply with DORA, including the building of a "defense-in-depth" strategy[3] that will also need to be interoperable and support firms' wider enterprise-wide risk management and three lines of defense operating models.

This Client Alert assesses the further details of DORA and concurrent efforts by other global financial services policymakers that could impact the proposed EU-27 regime's evolution ahead of the EU's own efforts in revising the Directive on security of network and information systems (**NIS Directive**).[4] This Client Alert should be read in conjunction with "DORA's debut - the EU's Digital Operational Resilience Act", the first part in our dedicated series on DORA and the accompanying Amending Directive[5], which is available from our Eurozone Hub.

1 DORA defines a "ICT third-party service provider" as "...an undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services, data centers, but excluding providers of hardware components and undertakings authorized under Union law which provide electronic communication services..." as defined in the European Electronic Communications Code Directive] available here.

2 DORA defines "ICT risk" as "...any reasonably identifiable circumstance in relation to the use of network and information systems, - including a malfunction, capacity overrun, failure, disruption, impairment, misuse, loss or other type of malicious or non-malicious event - which, if materialized, may compromise the security of the network and information systems, of any technology-dependent tool or process, of the operation and process' running, or of the provision of services, thereby compromising the integrity or availability of data, software or any other component of ICT services and infrastructures, or causing a breach of confidentiality, a damage to physical ICT infrastructure or other adverse effects."

3 DORA defines a "defense-in-depth" strategy as "... an ICT-related strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the entity".

4 Details of which are available from the EU on the following landing page (at the time of writing hereof, last updated October 9, 2020). The NIS Directive revisions (**NIS-D2**) were subject to a consultation that opened on July 7, 2020, and closed on October 2, 2020. The DG-FISMA presentation made it clear that further impacts of NIS-D2 would flow into the future shape of the DORA framework. Further coverage of NIS-D2 will be made available on our Eurozone Hub.

5 The Amending Directive introduces targeted amendments and updates to existing financial services directives to introduce cross-references to DORA and relevant technical standards.

DORA'S DEBUT AND CONCURRENT EFFORTS

DORA was published on September 24, 2020, and the European Parliament and the Council of the EU have now begun to consider the DORA legislative proposal.[6] Following DORA's adoption in its final format and entry into force, it will apply directly in EU-27 Member States after 12 months, with some final requirements applying after 36 months.[7]

On November 11, 2020, the European Commission's Directorate General for Financial Stability, Financial Services and Capital Markets Union (**DG-FISMA**)[8] held its first public webinar setting out further details of the DORA proposal. The webinar also used slides[9] that DG-FISMA, as the primary policymaker behind the DORA proposal, had previously presented to the First Council Working Party on October 30, 2020. The slides and the webinar present a number of further insights into DG-FISMA's expectations of how this new framework should be complied with.

It is conceivable that the evolution of DORA will also take note of work undertaken by global policymakers, notably that of the Financial Stability Board (**FSB**). This is especially likely to be the case given the FSB's own evolving policy on ICT concentration risk. While this has long been an FSB as well as an EU supervisory priority, the EU's Digital Finance Strategy, of which DORA forms a core deliverable, coupled with the impact of COVID-19 and a mass move to increased digitalization, have put this front and center for policymakers. DG-FISMA in its webinar also pointed to the recent increase in cyber-attacks[10] and systems outages, which also supports the need for DORA to be rolled out to regulated financial services firms and also for direct supervisory oversight of those critical ICT third-party service providers upon whom they rely.

ICT service providers operating in the EU-27 have generally previously only been subject to indirect supervisory oversight by financial services supervisory authorities through the supervision of outsourcing arrangements.[11] Consequently, direct supervisory oversight of ICT third-party services providers were largely beyond the direct supervisory scrutiny of European Supervisory Authorities (**ESA**s), let alone the national competent authorities (**NCA**s) of the EU-27 Member States.[12] DORA is set to change this and add direct supervisory oversight powers, thereby marking a paradigm shift in who is being supervised and how, but also in scrutiny of ICT concentration risk.[13] These direct powers would be introduced and co-exist next to those current powers of the ESAs as well as the European Central Bank (**ECB**), both in its Banking Union supervisory role in the context of the Single Supervisory Mechanism (**SSM**) and its central banking financial stability role in its payments systems oversight role.[14]

6 Details on DORA are set out inter alia in the European Parliament's legislative observatory – see here.

7 Notably the following Articles will apply after 36 months: Article 23 (Advanced testing of ICT tools, systems and processes based on threat-led penetration testing) and Article 24 (Requirements for testers).

8 See here.

9 Available here.

10 The EU estimates (see DG-FISMA slides) that during the pandemic, cyberattacks on financial institutions have risen by 38%.

11 Notably the European Banking Authority's (**EBA**) 2019 revised "Guidelines on outsourcing arrangements" (the **EBA 2019 Guidelines**) (available here), which applies to outsourcing more generally but were revised to include specific measures and expectations regarding cloud outsourcing. The EBA's 2019 Guidelines are in part being replaced by the harmonized measures brought in by DORA which, as an EU-27 wide applicable Regulation, sits as primary law, superordinate to the supervisory guidelines previously published by the EBA. Nevertheless, affected financial entities, notably those subject to Banking Union supervision, will still need to consider to what extent certain areas of the EBA 2019 Guidelines, or an updated format of them, still apply to them, given that some requirements, many of which will be driven by firm-specific facts, may continue to be relevant.

12 A notable exception is the National Bank of Belgium in its oversight of SWIFT in accordance with the CPMI-IOSCO Principles of Financial Market Infrastructures. The Bank of Italy has legal powers to obtain information and conduct inspections of service providers to which essential or important functions are outsourced.

13 DORA defines ICT concentration risk as "...an exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of the latter may potentially endanger the ability of a financial entity, and ultimately of the Union's financial systems as a whole, to deliver critical functions, or to suffer other type of adverse effects, including large losses".

14 ESMA notably has powers to conduct general investigations and on-site inspections in respect of central counterparties and trade repositories and their ICT service providers. The ECB-SSM can equally carry out on-site inspections on third parties to whom Banking Union supervised institutions have outsourced functions or activities. The ECB, in its payments systems oversight function, can request information and carry out on-site inspections of critical service providers of systemically important payment systems insofar as a contractual provision between the system and services provider permit this.

DORA'S DESIGN AND DEMANDS

DORA's provisions aim to implement key interrelated principles and best practices that exist in EU and international guidance designed to enhance cyber and operational resilience for financial services firms. DORA demands a lot in terms of compliance and the following affected firms will want to begin preparing for compliance with DORA as soon as possible:

- credit institutions (i.e. banks);
- payment institutions and electronic money institutions;
- investment firms;
- crypto-asset service providers (CASPs);
- central counterparties (CCPs) and central securities depositories (CSDs);
- trading venues;
- trade repositories, data reporting service providers, securitization repositories;
- Alternative Investment Fund managers and UCITS management companies;
- institutions for occupational retirement pensions (IORPs);
- insurance and reinsurance undertakings;
- insurance intermediaries;
- credit rating agencies;
- administrators of critical benchmarks;
- crowdfunding service providers; and
- ICT third-party service providers, which does not distinguish between a cloud and non-cloud basis but does bring cloud service providers into DORA's scope. At present DORA unfortunately does not define whether an ICT service provider within the group of a financial entity, say for example a bank, would qualify as an ICT third-party service provider.

(collectively the persons above are defined in DORA as **financial entities**).

DORA's provisions, which aim to harmonize and replace all existing EU and national efforts that have existed and been applicable to financial entities to date, are based on the following core principles:

1. **ICT governance and risk.** All financial entities are subject to a principle and proportionate risk-based approach to compliance, with a detailed and prescriptive ICT governance and risk management framework. In particular, financial entities will need to set up an overall ICT risk management framework, with definitions, approval and control processes, as well as overall accountability and clear roles and responsibilities for all ICT-related functions. This includes full responsibility and accountability of the management body in terms of compliance but equally in terms of the setting of and performance within ICT-risk tolerance levels. Similar requirements apply to the approval, controls and review processes to implement ICT business continuity and disaster recovery plans, ICT audit plans and ICT third-party risk assessments, along with regular and periodic training, including also of the "management body"[15] of the financial entity;
2. **Uniform incident and information-sharing framework.** All financial entities are required to comply with an enhanced and extended reporting of "ICT-related incidents"[16], including for those sectors currently not covered by EU rules. Streamlined reporting processes are facilitated by common reporting templates and deadlines, as well as the designation of one competent authority to whom individual financial entities will report to. Equally, DORA introduces mandatory rules on financial entities having at least one person who is responsible for implementing a communication strategy for ICT-related incidents, as well as the maintenance of communication plans to clients, counterparties and the public. DORA, in addition to introducing mandatory rules on threat detection and training, promotes and supports voluntary schemes on threat intelligence sharing between financial institutions.[17] Proportionality of compliance also exists regarding reporting of "major" ICT-related

15 DORA's definition of management body cross-refers to such a term as used in a multitude of existing EU financial services legislative instruments but equally contains a catch-all reference to those "...equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national legislation ."

16 DORA defines an "ICT-related incident" as one that is "...an unforeseen identified occurrence in the network and information systems, whether resulting from malicious activity or not, which compromises the security of network and information systems, of the information that such systems process, store or transmit, or has adverse effects on the availability, confidentiality, continuity or authenticity of financial services provided by the financial entity".

17 DORA requires financial institutions individually to undertake the following tasks, but also encourages them to co-operate on, information gathering on vulnerabilities and cyber-threats, conducting post-incident reviews following significant ICT disruptions, cooperating on analyzing the causes of disruptions and raising ICT security awareness through training and other programs.

incidents. DORA defines this as "...those ICT-related incidents with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity". The precise definition of what constitutes a "major" incident may also be expanded in further detail in EU regulatory technical standards that have yet to be published.

3. **Harmonized digital operational resilience testing requirements.** All financial entities must conduct basic testing in line with requirements set in the DORA regime and those that qualify as "significant financial entities" must undertake advanced tests in line with the DORA regime. Testing results are shared with and recognized by competent authorities across the EU-27 Member States.
4. **Supervision of ICT third-party risk.** DORA introduces heightened outsourcing rules to be followed by all financial entities and greater oversight tools which are available to supervisors to gauge compliance and to achieve a "... complete monitoring of ICT third-party risk(s) in the conclusion, performance, termination and post-contractual stages of contractual arrangements" as well as to monitor "ICT concentration risk". Supervisors will also receive direct oversight powers in respect of those ICT third-party service providers that are deemed to be "critical".

DORA marks a turning point and while firms will most likely need to commit investment to meet compliance expectations, part of the success of this new regime depends on how EU authorities and institutions move forward. This applies irrespective of whether they are acting in their supervisory or financial regulatory policymaking capacity. DORA prompts these authorities (including ENISA)[18] to fully develop and deliver the technical areas from a "single reporting portal for ICT-related incidents", which will first be subject to a feasibility study, as well as the methodologies, standards, forms, templates and procedures for firms to use. Notably, this applies to prevention of ICT risks but also to specifying appropriate securities policies, protocols and components of ICT business continuity/disaster recovery plans.

Financial entities that need to comply with DORA will likely, as part of setting their ICT risk management framework, need to conduct a risk assessment and gap analysis both prior to transitioning to this new regime as well as periodically (ideally at least annually) thereafter. This includes taking a 360-degree approach to reviewing internal ICT arrangements, linkages to external ICT arrangements (both for documented and undocumented arrangements), as well as the business operating environment overall. It may also be worth firms considering how their ICT-specific

18 The European Union Agency for Cybersecurity, which has been fully operational since September 1, 2005, operating out of Athens as well as Heraklion, Greece.

arrangements interact with their management of the control functions of governance, compliance and risk and related internal control systems and testing programs, as well their internal and regulatory reporting framework more generally. Consequently, financial entities may want to consider for new as well as legacy systems[19] or any major changes:

1. The adequacy and resilience of ICT system configurations, both in terms of maintenance (patching/updates) and on-going assurance and governance (change management), as well as access control and tracking, including limits on physical and virtual access to ICT systems, and protocols on strong authentication;
2. Making an inventory of all ICT systems and accounts, all network resources and hardware equipment, including the critical nature of physical equipment;
3. Documented and undocumented interconnections with internal and external ICT systems, as well as making an inventory of all processes that are dependent on ICT third-party service providers;
4. Their dependency and degree of (over-)reliance by business as well as control functions and the management body on points 1, 2 and 3; and
5. The sources and drivers of ICT risk relating to points 1, 2, 3 and 4 and the setting of ICT risk tolerance levels, as well as how to identify single points of failure as well as anomalous activity more generally.

Both financial entities and ICT third-party service providers (regardless of whether they are deemed critical) might also need to review the adequacy of any existing as well as new contractual arrangements. In supervising firms' compliance with DORA, ESAs and NCAs will likely focus on the detail of the contractual arrangements and resilience measures, which are typically covered in the following types of contractual provisions setting out:

- Details of all functions and services provided and relevant service levels (including supply chain management (of service provider) and receipt of software/hardware during normal operating conditions, as well as prolonged pandemic preparedness);
- Descriptions of services to be outsourced;
- Specifics on location, processing and storage of data;
- Agreed standards on the accessibility, availability, integrity, security and protection of personal data (in addition to general GDPR matters);
- Notice periods and reporting obligations of the third-party service provider;
- Monitoring rights of the financial entity vis-à-vis the third-party service provider; and
- Termination and exit strategies, including porting to other providers and/or insourcing of previously outsourced services.

DORA's provisions, as with previous EU efforts and those of the FSB, require that financial entities ensure that their contracts enable firms as well as respective supervisory and resolution authorities to have appropriate rights to access, audit and obtain information from third parties. As noted by the FSB as well as earlier pre-DORA rulemaking and/or commentary, these rights can be challenging to negotiate let alone exercise, notably in a multi-jurisdictional context.

Financial entities will want to reflect the findings from their reviews both in targeted remedial measures, including contractual arrangements with third parties, but also by maintaining a comprehensive ICT Security Policy that includes key contractual arrangements. An ICT Security Policy should reflect best practices of improving resilience, ensuring governance and accountability. Such a policy should serve as a living document that supports other three lines of defense in an enterprise-wide risk model. Equally, an ICT Security Policy will, pursuant to DORA, need to be accompanied by an ICT Business Continuity Policy, an ICT Disaster Recovery Plan, policies on back-ups and possibly other key indicators that document the recovery methods and return to operations objectives of the financial entity as well as any third-party ICT provider it relies upon.

19 Microenterprises are not required to conduct a risk assessment upon major changes in the network and information system infrastructure, nor specific ICT risk assessments on legacy systems.

New direct supervisory focus on ICT third-party service providers and supervision through the Lead Overseer

DORA introduces a targeted supervisory regime for the direct oversight of those ICT third-party service providers that are designated individually and/or as a group as "critical", pursuant to Article 28 DORA, if the following characteristics and subjective criteria as described in the table are met. Further details on the criteria may be introduced under further regulatory technical standards.

Characteristics	How DORA proposes that the characteristics are measured
a. The failure of the ICT third-party service provider would trigger a systemic impact (on the stability, continuity or quality of the provision of financial services)	• Number of financial entities to which the respective ICT third-party service provider delivers services
b. Systemic character (or importance) of the financial entities themselves	• Number of G-SIIs/O-SIIs relying on the respective ICT third-party service provider • Interdependence between G-SIIs or O-SIIs
c. Whether services received and which support critical or economic functions ultimately involve the same ICT third-party service provider (directly or indirectly)	• Degree of reliance and concentration
d. Degree of substitutability of the ICT third-party service provider	• Whether there is a lack of real alternatives, even partial, based on the limited number of providers, the relevant market share and/or technical complexity • Difficulties to partially or fully port/migrate data and/or workloads to another ICT third-party service provider due to costs, risks or other barriers
e. Number of Member States in which the relevant ICT third-party service provider provides services	• It is conceivable that this will also consider concentration by market segment across EU-27 Member States as well as geographical/regional concentrations
f. Number of Member States in which financial entities using the relevant ICT third-party service provider are operating	

Upon an ICT third-party service provider being categorized as critical, one ESA is appointed as "Lead Overseer". A Lead Overseer has powers to direct supervisory "Recommendations" i.e., instruments of EU law that allow EU institutions (such as the ESAs) to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed. Recommendations, while having no binding force, generally hold recipients to a comply or explain

approach. The fact that DORA focuses on using Recommendations as a means of rulemaking strikes a pragmatic balance. This approach generally facilitates the expanding of ESA's supervisory mandates in terms of adding a new thematic area but equally by facilitating direct supervisory oversight of ICT firms that have been beyond direct oversight of the ESAs, and notably all without the need for extensive changes to existing pillars of EU legislation.

The decision on which ESA will become the Lead Observer is, as per the DORA framework, dependent on the value of assets managed by the financial entity that is in the remit of the respective ESAs. As a result, this would suggest that the EBA may likely receive most of the roles of Lead Observers. It is conceivable that the EBA but equally ESMA will be in close cooperation with the ECB in its Banking Union role at the helm of the SSM but also as payment systems oversight supervisor.

DORA confers extensive supervisory powers upon the respective Lead Overseer. These shall be tasked with monitoring compliance of critical ICT third-party service providers. The Lead Observer will exercise direct powers, as assisted by national experts in examination teams and/or NCAs' assistance in follow-up and enforcement, and be empowered to request all relevant information and documentation, request reports, conduct general investigations and inspections and cause critical ICT third-party service providers to address its Recommendations. These powers also extend to reviewing and gauging the financial stability risks posed by subcontracting arrangements, including sub-outsourcing arrangements that the critical ICT third-party service provider undertakes or plans to undertake with other ICT third-party service providers or with ICT sub-contractors established in a third country i.e., outside of the EU.

Based on the current version of DORA, Art. 31(1)(iv) states that the Lead Observer may recommend that that further subcontracting arrangements are refrained from where the following cumulative conditions are met (i) the envisaged sub-contractor is an ICT third-party service provider or an ICT sub-contractor established in a third country; (ii) and the subcontracting concerns a critical or important function of the financial entity. Consequently, even if this provision stays as it is, financial entities (as well as critical and non-critical ICT third-party service providers) will want to assess the extent of relevant arrangements that could fall within those criteria. They will also want to assess what structural or documentary mitigants might be available to temper the regulatory impact of such a prohibition or, alternatively, any enhanced monitoring and reporting obligation that might be put in place.

Articles 29 to 39 of DORA also set out details on an "Oversight Forum", which would operate as a sub-committee of the existing Joint Committee of the ESAs. The Oversight Forum's composition is comprised of each of the chairs of the ESAs along with one high-level representative from each NCA, and observers such as executive directors from each ESA, and one representative each from the European Commission, the European Systemic Risk Board, the ECB-SSM and ENISA.

The Oversight Forum generally and the respective Lead Overseer will also be responsible for promoting international cooperation. This coordination channel exists independently of the broader international cooperation arrangements that DORA calls for in Articles 41 to 43, whereby the NCAs and NIS shall cooperate, conduct cross-sector exercises, improve communication, coordinate on administrative penalties and remedial measures, and goes beyond the voluntary information-sharing arrangements that may be set up by financial entities pursuant to Article 40 DORA.

The Oversight Forum's mandate and rulemaking powers are split between individual supervisory matters and those that affect the market generally. In terms of individual supervision, the respective Lead Overseer consults the Oversight Forum before exercising any powers and before addressing any individual supervisory Recommendations to a critical ICT third-party service provider. Finally, the Oversight Forum acts as a standard setter and is responsible for the cross-sectorial coordination on ICT third-party risk and notably prepares draft joint positions and common acts of the Joint Committee of the ESAs.

Article 28 DORA also clarifies that those ICT third-party service providers that are already subject to oversight due to them providing services to the European System of Central Banks will be exempt from being defined as "critical" pursuant to DORA. Equally, Article 28 creates a voluntary opt-in regime for those ICT third-party services providers that do not qualify as critical but wish to become subject to the DORA Lead Observer framework.

THE FSB FURTHERS ITS OWN PRINCIPLES

On November 9, 2020, the FSB published a discussion paper "Regulatory and Supervisory Issues Relating to Outsourcing and Third-party Relationships"[20], which is open for public consultation until January 8, 2021. Responses to this consultation paper will shape the FSB's further efforts but will also likely impact the evolution of the EU's DORA regime. The same goes for some of the output from the FSB's "toolkit" on "Effective Practices for Cyber Incident and Recovery: Final Report"[21] and its proposed "Cyber Incident Response and Recovery (CIRR) framework.

This most recent FSB consultation for a new regime builds upon earlier work in December 2019 in the report "Third-party Dependencies in Cloud Services"[22], which also influenced the EBA's own rulemaking in respect of outsourcing generally and that of cloud computing, as well as those of EIOPA in its own cloud computing outsourcing guidelines. [23] The annex to the FSB's 2020 discussion paper in turn reviews and points to the positives that are present in the existing EU regulatory framework in this field. The FSB 2020 discussion paper does not discuss the future impact of DORA, yet, as shown below, the relationship between the two frameworks are likely to converge.

The FSB's focus in its review is to map whether the current rules remain fit for purpose given that technological developments, as accelerated by the COVID-19 pandemic, have pushed some financial institutions to rely even more on ICT service providers. Ultimately, the FSB, like the EU's efforts on DORA, are concerned with mitigating risks that arise due to concentration and/or over-reliance. The FSB frames this issue astutely in stating (our emphasis in bold): "There is a **common concern about the possibility of systemic risk arising from concentration in the provision of some outsourced and third-party services to financial institutions**. These **risks may become higher as the number of financial institutions receiving critical services from a given third party increases**. Where there is no appropriate mitigant in place, a major disruption, outage or failure at one of these third parties could create a single point of failure with potential adverse consequences for financial stability and/or the safety and soundness of multiple financial institutions. **Given the cross-border nature of this dependency, supervisory authorities and third parties could particularly benefit from enhanced dialogue on this issue**." This principle is echoed in EU publications on DORA as well as its recitals.

Welcomingly, the FSB also highlighted the difficulties (and thus supervisory concern) highlighted during the COVID-19 pandemic in terms of supply chains and the management of sub-contractors. The FSB points to the delays and logistical difficulties faced by many financial institutions in obtaining remote working equipment from third-party service providers due to their own respective disruptions in supply chains. The FSB states, "Even where contractual arrangements contain provisions and safeguards on the management of the third-party's sub-contractors and supply chain, these arrangements often do not bind those sub-contractors directly and it can be difficult for financial institutions and supervisory authorities to effectively identify and address risks across the supply chain." DORA does not currently aim to cover these types of concerns.

Similar deficiencies were described in relation to the failures of financial institutions and their ICT service providers to have effective business continuity plans and exist/wind-down plans in place that ensure a financial institution's recovery from an outage or failure at a service provider, and the exit options that might minimize potential disruption by an outage and/or service failure. This is particularly a problem if, according to the FSB a "...sufficiently large number of financial institutions (or a single systemic financial institution) became dependent on one or a small number of outsourced third-party service providers for the provision of critical services that were impossible or very difficult to substitute effectively and in an appropriate timeframe. Where there is no appropriate mitigant in place, a major disruption, outage or failure at one of these third parties could create a single point of failure with potential adverse consequences for financial stability and/or the safety and soundness of multiple financial institutions." These concerns are addressed in DORA and reflect global consensus on the need to tackle ICT concentration risk and mitigation.

20 Available here and in full here.
21 Full details of which are available from the FSB's following landing page.
22 Available here.
23 The EBA Guidelines available here and the EIOPA Guidelines available here.

The FSB notes that in some jurisdictions, supervisory authorities have legal powers, in addition to those conferred in contractual arrangements, that permit them access to third parties' data, personnel, premises and systems for the purposes of gathering information relevant to the exercise of their regulatory and supervisory powers, including on-site inspections. The FSB also addresses the issue that supervised financial institutions and supervisors face a shortage of relevant resources and ICT skills. The FSB also points out that "... third parties are sometimes unaware of the regulatory obligations of their financial institution clients or face difficulties in facilitating compliance with them. Imbalances in the respective negotiating power of financial institutions and third parties can also impact on the ability of financial institutions to exercise effective oversight." This issue is discussed in part in DORA, notably also in terms of the context presented in Recitals 27 to 29 of DORA, which state that:

> "(27) Despite some general rules on outsourcing in some of the Union's financial services pieces of legislation, the monitoring of the contractual dimension is not fully anchored into Union legislation. In the absence of clear and bespoke Union standards applying to the contractual arrangements concluded with ICT third-party service providers, the external source of ICT risk is not comprehensively addressed. Consequently, it is necessary to set out certain key principles to guide financial entities' management of ICT third-party risk, accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contracts with a view to enshrine certain minimum safeguards underpinning financial entities' ability to effectively monitor all risk emerging at ICT third-party level.
>
> (28) There exists a lack of homogeneity and convergence on ICT third-party risk and ICT third-party dependencies. Despite some efforts to tackle the specific area of outsourcing such as the 2017 recommendations on outsourcing to cloud service providers, the issue of systemic risk which may be triggered by the financial sector's exposure to a limited number of critical ICT third-party service providers is barely addressed in Union legislation. This lack at Union level is compounded by the absence of specific mandates and tools allowing national supervisors to acquire a good understanding of ICT third-party dependencies and adequately monitor risks arising from concentration of such ICT third-party dependencies.

> (29) Taking into account the potential systemic risks entailed by the increased outsourcing practices and by the ICT third-party concentration, and mindful of the insufficiency of national mechanisms enabling financial superiors to quantify, qualify and redress the consequences of ICT risks occurring at critical ICT third-party service providers, it is necessary to establish an appropriate Union oversight framework allowing for a continuous monitoring of the activities of ICT third-party service providers that are critical providers to financial entities."

Other areas that the FSB points to, and which DORA might look to improve on, are the FSB's concerns that may arise when third-party providers offer their own audit report on their own services to their financial institution clients. These are offered often in lieu of and to compensate for the on-site audits by their financial institution clients, but, depending on the content, the level of detail and quality of these reports, they may not always be sufficient to allow their financial institution clients to comply with their regulatory obligations in terms of third-party risk management. Moreover, the FSB also points to emerging best practice applied by groups of financial institutions sharing the same third-country service provider when auditing those providers (known as "pooled audits"). The FSB points to the advantages of pooled audits but cautions that senior management of individual financial institutions ought to assess whether the findings are suitable for an individual firm's needs. DORA, whether in any revisions or further rulemaking by way of regulatory technical standards, may in the future follow this same approach.

As in its work in 2019, the FSB 2020 discussion paper concludes that despite positive developments in domestic and regional frameworks and efforts, such as those of the EU, further supervisory alignment and dialogue would be welcome. In summary, the FSB's 2020 discussion paper will likely drive some parts of the debate and the direction of DORA in what is expected of supervised firms (including those operating from outside the EU-27 in "third countries") but equally for the competencies of supervisors.

OUTLOOK AND NEXT STEPS FOR DORA

DORA requires a lot from those that qualify as financial entities, inasmuch as it does for supervisors transitioning to this new regulatory and oversight regime and the identification, mitigation and management of a whole new taxonomy of risks. As dependency on ICT service providers is likely to grow, financial services providers and other firms will need to carefully consider what actions they can take to deal with ICT concentration risk. They will also need to ensure that their contractual arrangements with outsourcing service providers as well as ICT third-party service providers, and their internal policies and procedures are reflective of DORA's provisions and supervisory expectations.

Firms, whether they are ICT third-party firms or any of the other types of financial entities more generally, will want to take preparatory action now, regardless of DORA's final legislative drafting, given the potentially short timelines to introduction and the budget allocations that will need to be committed. This includes them:

1. **Conducting a comprehensive stocktake.** This should be done on a 360-degree basis, as to their ICT risk drivers due to internal and external arrangements (including contractual relationships), across silos, whether in respect of business lines and/or control functions in individual firms or, if a group exists, across such a group. Firms will want to document findings both in terms of what works well and where vulnerabilities exist. This exercise should be a prerequisite for implementing remedial and/or preventive measures and for creating a comprehensive ICT Risk Strategy. These tasks will also require the respective policy documents discussed above, along with a robust "defense-in-depth" approach that also complements and supports firms' general enterprise-wide risk management and a three-lines of defense model and thus the respective control functions (governance, risk, compliance, legal and audit).
2. **Setting ICT risk appetite and risk tolerance levels along with remedial action.** This will tie in the ICT risk appetite and tolerance levels into firms' overall risk appetite frameworks (RAFs) and risk tolerance levels. In addition, it may help force firms, whether due to financial services legislation or otherwise, to replace existing and/or introduce wholly new ICT systems to increase capacity, redress and reduce known dependencies and/or overreliance and/or ICT concentration risk within their organization, and, possibly, where negotiating power exists, address the same issues within an ICT third-party service provider.
3. **Focusing on DORA, FSB and other global principles on digital operational resilience**. Firms can take appropriate steps so that the outcomes of bullets 1 and 2 are interoperable with efforts beyond the EU-27, even if these are prescriptive. Firms will want to undertake a periodic review of these considerations along with periodic reviews of findings and measures undertaken in points 1 and 2 to ensure these remain fit for purpose and remain robust and efficient. These qualitative review measures should also be complemented by fire drill testing and penetration testing, fully cognizant of the fact that rules and supervisory expectations in that area, notably of the ECB, are possibly set to change (see our series on this from our Eurozone Hub).
4. **Making use of the voluntary information sharing networks. This should be done** well prior to DORA's full finalization, across borders and with relevant regulatory and supervisory authorities and/or policymakers. This may also mean learning and borrowing from best practices that exist in other jurisdictions and/or market segments that could benefit a given firm.

In short, there is a lot that firms will need to consider and comply with as the general supervisory priority shifts to how firms identify, mitigate and manage ICT risks as they move to much more digitized operating models.

Our Eurozone Hub lawyers are assisting a number of firms with ICT risk gap analysis, as well as updating of their digital operational and cyber-resilience policies and the relevant supervisory dialogue, including how to operationalize the relevant desired outcomes in documentation and non-documentation workstreams. If you would like to discuss any of the items mentioned above, in particular how to forward plan and benefit from changes that are being proposed, as well as how these developments fit into the 2021 supervisory priorities of the ECB-SSM, EBA, ESMA and other ESAs and NCAs, or how they may affect your business more generally, please contact any of our key contacts or the wider team from our Eurozone Hub.

Key contacts

Dr. Michael Huertas
Partner, Co-Head Financial Institutions Regulatory Europe
D +49 69 45 00 12 330
M +49 162 2997 674
michael.huertas@dentons.com

Dr. Holger Schelling
Partner
D +49 69 45 00 12 295
M +49 162 1041 413
holger.schelling@dentons.com

Michael Wainwright
Partner
D +44 20 7246 7735
M +44 7811 330 585
michael.wainwright@dentons.com

Jonathan Garforth
Partner
D +44 20 7320 3743
M +44 7747 585 358
jonathan.garforth@dentons.com

Arno Voerman
Partner
D +31 20 795 30 62
M +31 61 138 85 38
arno.voerman@dentons.com

ABOUT DENTONS

Dentons is the world's largest law firm, connecting talent to the world's challenges and opportunities in more than 75 countries. Dentons' legal and business solutions benefit from deep roots in our communities and award-winning advancements in client service, including Nextlaw, Dentons' innovation and strategic advisory services. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and world-class talent challenge the status quo to advance client and community interests in the New Dynamic.

dentons.com

 CSBrand-43339-Client Alert-DORA-2-02 — 03/12/2020