DORA's debut - the EU's Digital Operational Resilience Act

November 12, 2020

While operational resilience of financial services firms has been a long-standing supervisory priority, legislative action has to date been lagging. Rulemaking instruments have been put forward by various regulators, including the European Central Bank (**ECB**)[1], acting both in its central banking financial stability and markets oversight capacity as well as its Banking Union role at the helm of the Single Supervisory Mechanism (**SSM**). National level authorities, including Germany's Federal Financial Services Supervisory Authority (the **BaFin**)[2] have independently taken measures to update rules, guidance and supervisory expectations relating to digital operational resilience including elements beyond internet and communications technology (**ICT**).

In the face of continued client/counterparty-facing systems outages, cyber-risk and now COVID-19 have put operational resilience firmly on EU the priority list of financial services policymaking legislative proposals. An EU-harmonized approach to replace, what the EU sees[3] as "uncoordinated national initiatives" could lower the amount of administrative burdens that firms face when dealing with rules with "…overlaps, inconsistencies, duplicative needs and higher administrative and compliance expenditures." EU action in this area would promote legal certainty and level the playing field irrespective of how and when financial entities are not equally exposed to ICT risks.[4]

On September 24, 2020 as part of its "Digital Finance Strategy Package", the European Commission adopted:

- the MiCA proposal[5] including its Annexes[6] and an impact assessment[7];
- the Pilot DLT Market Infrastructure Regulation (**PDMIR**) proposal[8];
- the Digital Operational Resilience Regulation proposal (**DORA**); as supplemented by
- an EU directive introducing targeted amendments (the **Amending Directive**)[9] to existing financial services legislation [10] to accommodate the EU's MiCA regulatory regime. (collectively the **MiCA Regime**[11]).

This Client Alert assesses the aims, content and impact of the EU's DORA and the Amending Directive proposals as well as the differences to the UK's own efforts and should be read together with our Background Briefing " **Meet MiCA – The EU pushes forward its proposal for its Markets in Crypto-Assets Regulation plus a pilot regime for DLT infrastructure**"[12].

Both DORA and MiCA will be of relevance to financial services providers but equally those crypto-asset service providers (**CASP**s) that will be licensed under MiCA. In summary, those affected will want to take early action to prepare for each component of the new MiCA Regime. Even for a number of firms that are already subject to the ECB's supervisory expectations on cyber-risk and resilience, changes may be required to meet DORA's compliance obligations, even if DORA, in part, builds upon the ECB's rules. [13]

What does DORA aim to deliver?

DORA, as an EU Regulation, aims to establish a comprehensive and cross-sectoral EU-27 digital operational resilience framework with rules for all regulated financial institutions. The Amending Directive (as well as Chapter IX of DORA) introduces targeted changes to existing financial services rulemaking legislation by implementing DORA's obligations into those frameworks and MiCA requires CASPs to comply with DORA. Individually as well as when taken together, the requirements mark a quantum leap in policymaking in this area.

DORA's requirements go well beyond the Network Information Systems Directive (NIS-D) [14], that focused on a narrow set of firms, introducing a minimum standard on cyber-resilience introduced in other financial services rules as well as the EU's General Data Protection Regulation. DORA introduces much more prescriptive requirements to a much wider set of market participants. DORA does have some de minimis thresholds allowing microenterprises to apply DORA only in select instances. A proportionate approach to compliance effectively introduces a sliding scale of compliance with critical and significant firms having greater compliance obligations than others.

The current DORA text reflects responses to the European Commission's December 2019 inception impact assessment[15] that reflects specific aspects related to respondents' areas of activity along with feedback that the European Commission received following meetings with stakeholders, EU authorities and institutions.

By streamlining the existing set of differing, often fragmented rules, and by introducing new requirements where gaps exist, DORA and the Amending Directive aims to:

1. prompt firms to focus on improving the alignment of their business strategies, their conduct and their ICT risk management and thus strengthen the overall identification, mitigation and management of ICT risks including "ICT concentration risks"[16] and thus the overall effectiveness of their preventive and resilience measures while equally being proactive to identify and remedy vulnerabilities;
2. eliminate fragmentation, redundancies and barriers to prompt, simplified and efficient reporting of ICT-related incidents while concurrently increasing supervisors' threat knowledge and incident awareness by greater breadth and depth of (useful) data capture;
3. develop and deploy more resilient testing frameworks that are proportionate and tailored to the a firm's size, business strategy and risk profile;
4. increase the oversight and monitoring by firms of the risks and resilience measures employed by third-party ICT providers so as to better manage risks including on over-dependence on such firms; and
5. creating cooperation frameworks and encouraging linkages for firms to share information on cyber-threats and raise awareness on ICT risks generally so as to improve collective resilience.

DORA is structured around specific policy areas that the European Commission views as key interrelated pillars that exist in EU and international guidance as well as best practices aimed at enhancing cyber and operational resilience for financial services firms. DORA applies to:

- credit institutions (i.e. banks);
- payment institutions and electronic money institutions
- investment firms;
- 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[17] which does not distinguish between a cloud and non-cloud basis but does bring cloud service providers into DORA's scope.

(collectively **financial entities**)

DORA also seeks to promote convergence on supervisory approaches concerning ICT third-party risk in the financial sector by subjecting ICT third-party service providers that are critical for financial entities to an EU oversight framework. Under this framework, the relevant European Supervisory Authority (**ESA**) such as the European Banking Authority (EBA), European Securities and Markets Authority (ESMA) or the European Insurance and Occupational Pensions Authority (EIOPA) or the ECB-SSM designated as lead overseer for each such critical ICT third-party service provider has to assess whether that provider has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks that it may pose to financial entities. The ESAs will act as "Lead Overseers" and the national competent authorities (**NCA**s) as enforcers.

The oversight framework envisaged builds on the existing institutional architecture, whereby the Joint Committee of the ESAs ensures cross-sectoral coordination relating to all ICT risk matters, in accordance with its tasks on cybersecurity. The Joint Committee will establish a sub-committee, the Oversight Forum, to support its work in this area. The Oversight Framework will set up a designation mechanism applicable to critical ICT third-party service providers, taking into account the dimension and nature of the financial sector's reliance on services provided by ICT third-parties. Concretely, the designation will be based on a set of quantitative and qualitative criteria (some of which remain to be defined) setting out the parameters as a basis for inclusion into the oversight. The proposal will also foresee a voluntary opt-in for ICT third-party service providers that have not been designated on the basis of future criteria.

DORA allocates supervisory, investigatory and sanctioning power to both EU and national level competent authorities for them to fulfil their duties under DORA. Financial entities' compliance with substantive recommendations laid down by the Lead Overseers should be achieved mainly through the enforcement powers of national financial supervisors, including the possibility for third party providers to be fined. ESA's and NCA's powers, some of which they already have in relation to the financial entities (but not necessarily the ICT third party service providers) include that they may in respect of legal firms and/or individuals (limited to point (c) to (h)):

- have access to any document or data held in any form which the competent authority considers relevant for the performance of its duties and receive or take a copy of it;
- carry out on-site inspections or investigations – and we expect that a supervisory guide[18] will clarify how these powers are applied in practice;

- require corrective and remedial measures for breaches of DORA;
- issue an order requiring the natural or legal person to cease the conduct and to desist from a repetition of that conduct;
- require the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation and prevent repetition of that practice or conduct;
- adopt any type of measure, including of a pecuniary nature, to ensure that financial entities continue to comply with legal requirements;
- require, in so far as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of DORA and where such records may be relevant to an investigation into breaches of DORA; and
- issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach.

Member States may lay down rules on imposing criminal penalties.

What does DORA require of financial entities?

DORA requires financial entities to have internal governance and control frameworks that ensure an effective and prudent management of all ICT risks. The financial entity's management body will be required to define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework.

DORA will, among other things, set clear roles and responsibilities for all ICT-related functions, determine the appropriate risk tolerance level of the financial entity's ICT risk and agree the financial entity's policy on arrangements regarding the use of ICT services provided by third-party service providers. Equally, financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with high, appropriate and the latest information standards. This may require financial entities to work with counsel to validate the third-party provider. The same also applies in relation to verifying sub-contracting arrangements, notably when concluded with ICT third-party service providers established in a third-country.[19]

DORA requires financial entities to:

1. implement, maintain and periodically update:

- sound, comprehensive and well-documented ICT risk management frameworks that enable them to redress ICT risk quickly, efficiently and comprehensively, and to ensure a high level of digital operational resilience that matches their business needs, size and complexity;
- ICT systems, protocols and tools that are reliable and technologically resilient to deal with additional information processing needs as required under stressed market conditions or other adverse situations;
- a comprehensive digital operational resilience testing program as a core component of the firm’s ICT risk management framework, which includes a range of assessments, testing, methodologies, tools and an obligation to classify and annual test all ICT systems that are deemed critical;[20]
- plans and frameworks to carry out defined threat-led penetration testing at least every three years. This obligation

only applies to specific financial entities that are identified as significant and “cyber mature”;

2. identify, classify and adequately document all ICT-related business functions, identify on a continuous basis all sources of ICT risk, and assess cyber threats and ICT vulnerabilities relevant to their ICT-related business functions;

3. carry out on-going monitoring and control the functioning of the ICT systems and tools and minimize the impact of risks through the use of appropriate ICT security tools, policies and procedures;

4. maintain mechanisms to promptly detect anomalous activities, including ICT network performance issues and ICT-related incidents, and to identify all potential material single points of failure;

5. maintain and update a dedicated and comprehensive ICT business continuity policy as an integral part of their operational business continuity policy;

6. embed a back-up policy specifying the scope of the data that is subject to the back-up and the minimum frequency of the back-up, and recovery methods;

7. ensure the firm has sufficient capabilities and staff to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks as well as to analyze their likely impacts on their digital operational resilience;

8. carry out reviews following significant ICT disruptions of the firm’s core activities, analyzing the causes of disruption and identifying required improvements;

9. implement dedicated:

- ICT-related incident management processes to identify, manage and notify ICT-related incidents as well as to introduce early warning indicators as alerts;
- measures to categorize ICT-related incidents on the basis of their impact following a disruption on the firm, customers and other criteria in relation to the immediate incident, its duration, severity and geographical spread;
- systems to report ICT-related incidents to the relevant competent authority within the prescribed timeframes;
- communication plans that facilitate a prompt but responsible disclosure of ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate.

While much of the above might be easier for existing regulated financial services firms to achieve, ICT third-party service providers will need to first assess whether they are likely to be deemed “critical”. Those who are may need to establish new regulatory teams and assess how they comply with DORA’s oversight framework. Larger firms will want to keep tabs on the ESA’s work on finalizing threat-led penetration i.e., ethical hacking. Even for those firms who are already subject to existing requirements that DORA looks to build on, they may still need to consider whether their current i.e. pre-DORA response and recovery strategies/plans correspond to the compliance and supervisory expectations that ESAs and NCAs will set as DORA enters into force and is operationalized.

A look across to the UK

Just prior to lockdown the UK’s Financial Conduct Authority (**FCA**) and Prudential Regulatory Authority (**PRA**) published Consultation Papers[21] proposing measures to improve resilience of the UK’s financial sector. Similar yet slightly different to DORA, the UK’s authorities aim to bolster operational resilience and the ability of firms and the financial sector more generally to prevent, adapt, respond to, recover and learn from operational disruptions. Unlike

DORA, the UK's approach does not apply to ICT service providers and the UK's approach (perhaps correctly) focuses on operational resilience more generally whereas DORA's narrower focus is on digital operational resilience. If adopted, the UK's proposals could be implemented in 2022 as the original 3Q 2021 implementation date seems likely to be delayed due to COVID-19.

The UK's approach also proposes that firms, unlike DORA, assess the impact tolerance for disruption for each important business service and ensure firms can continue to deliver their important business services during severe but plausible scenarios. The UK's approach also proposes requirements for firms to map and test important business services to identify vulnerabilities in their operational resilience and drive change where it is needed.

Unlike DORA, the UK's approach requires that certain pre-approved control functions – in the UK this includes the Chief Operations Function (SMF 24) under the Senior Managers & Certification Regime – are required to have responsibility for managing the internal operations or technology of the firm (or of a part of the firm) including responsibility for areas such as business continuity, internal operations, operational continuity, resilience and strategy. It is likely that in EU Member States that have similar pre-approved control function regimes (and not all do – certainly not as of yet) they may have to implement a similar approach. In any event, there is possibly quite a lot that firms complying with DORA can learn from the UK's regime and vice versa as ICT risks know no borders.

Outlook and next steps for DORA

The European Parliament and the Council of the EU will now consider the DORA legislative proposal.[22] After it has been adopted and has entered into force, it will apply directly in EU-27 Member States after 12 months, except for Article 23 (Advanced testing of ICT tools, systems and processes based on threat led penetration testing) and Article 24 (Requirements for testers), which will apply after 36 months.

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)[23] to fully develop and deliver the technical areas from a "single reporting portal for ICT-related incidents", that will first be subject to a feasibility study, but equally 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 an ICT business continuity/disaster recovery plans. The same situation and prerequisites for success also apply to the breadth of work being prompted by the MiCA Regime more generally.

As with the MiCA Regime more generally, ESAs will need to step up their staffing, and resources and the impact assessment proposes that the EBA, ESMA an EIOPA may each receive six new full time equivalent positions and a proposal of 30 million euro budget for the expansion of their respective supervisory mandates. We anticipate that the ECB(-SSM) will also publish and fill its needs soon.

Equally, it is quite conceivable that DORA's framework may be replicated to EU firms operating outside of the financial services sector on digital operational resilience framework as well as regulation of digital business offering more generally. Crucially, financial services firms will want to actively benchmark how they can balance the need to meet DORA and the UK's own framework as well as others around the globe. Some affected stakeholders may wish to engage in a legislative review as well as lobbying more generally as DORA progresses down the path of legislative adoption.

The lawyers of our financial institutions regulatory team are assisting a number of banks and other regulated firms on regulatory matters. If you would like to discuss any of the items mentioned, or how they may affect

your business more generally, please contact any of our key contacts or the wider team of our financial institutions regulatory team.

---

1. See coverage available here.
2. See coverage as to the BaFin's change to its supervisory guidance on supervisory requirements for IT in financial institutions available here, which updates coverage from July 2018 available here.
3. As set out in the DORA's legislative proposal documentation.
4. ICT risks are dependent on the size, functions and business profiles of the firms and their ICT arrangements. ICT risk, as used in DORA, means "…any reasonably identifiable circumstance in relation to the use of network and information systems 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."
5. For the main legislative text the final legislative proposal is available here.
6. The Annexes 1 to 6 to MiCA are available here.
7. Available here.
8. Available here.
9. Available here.
10. The European Commission consulted on the possibility of an EU framework for crypto-assets in December 2019 and the feedback to that consultation is set out in part 2 of the final legislative proposal. In part, MiCA builds upon the work of the European Supervisory Authorities (**ESA**s), in particular the European Banking Authority (**EBA**), the European Securities and Markets Authority (**ESMA**) and to a lesser degree the European Insurance and Occupational Pensions Authority (**EIOPA**) as well as the European Central Bank (**ECB**) in its role at the head of the Banking Union's Single Supervisory Mechanism (**SSM**). This includes notably ESMA's advice on initial coin offerings and crypto-assets – see here as well as the EBA's report with advice for the European Commission on crypto assets – see here as well as our analysis here.
11. A link to the legislative procedure file (and supporting documents) are available here.
12. Available here.
13. Please see our forthcoming analysis, which will be available once DORA's text is closer to finalization, that benchmarks the ECB's rules (TIBER, Cyber-Resilience Oversight Expectations as well as penetration testing) with DORA. Please see our existing coverage on:
    a. "Setting the controllers' conduct expectations during cyber-resilience exercises", June 14, 2019;
    b. "New Cyber-resilience Oversight Expectations may carry compliance challenges", December 2018;
    c. "ECB releases procurement guidelines for selecting service providers in cyber-resilience testing", September 2018; and
    d. "Central Bank of Cyber? ECB releases first new framework on testing cyber-resilience and combatting digital financial crime", July 2018.
14. Available here.
15. Available here.
16. Defined as follows: "'ICT concentration risk' means 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 system as a whole, to deliver critical functions, or to suffer other type of adverse effects, including large losses."
17. DORA defines this 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." The term electronic

communication services is defined in EU Regulation 2019/881 on the European Union Agency for Cybersecurity (**ENISA**) and on information and communications technology cybersecurity certification.

18. In a similar fashion to that of the ECB-SSM's guide – see our analysis here.
19. Which DORA states "means an ICT third-party service provider that is a legal person established in a third-country, has not set up business/presence in the Union, and has entered into a contractual arrangement with a financial entity for the provision of ICT services."
20. A critical or important function is defined in DORA as "…a function whose discontinued, defective or failed performance 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 legislation, or its financial performance or the soundness or continuity of its services and activities."
21. See FCA Consultation Paper 19/32: available here and PRA Consultation paper 29/19 and Discussion Paper 1/18 – see the landing page here.
22. Details on DORA are set out inter alia in the European Parliament's legislative observatory – see here.
23. The European Union Agency for Cybersecurity, which has been fully operational since September 1, 2005 operating out of Athens as well as Heraklion, Greece.

Your Key Contacts

Dr. Holger Schelling
Partner, Co-Head Financial Institutions Regulatory Europe, Frankfurt
D +49 69 45 00 12 345
holger.schelling@dentons.com

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

Jonathan Garforth
Partner, London
D +44 20 7320 3743
M +44 7769 551399
jonathan.garforth@dentons.com

Arno Voerman
Partner, Amsterdam
D +31 20 795 30 62
M +31 6 11 38 85 38
arno.voerman@dentons.com