RegCORE Client Alert

Financial Services: Catching up on the EU's proposal for a Directive for Resilience of Critical Entities

March 2022

Financial Services

Catching up on the EU's proposal for a Directive for Resilience of Critical Entities

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas
@pwc.com

Contact RegCORE Team
de_regcore@pwc.com

In addition to the proposal (published September 2020), aimed at regulated financial services providers, for an EU Regulation on digital operational resilience for financial services (**DORA**), the EC in December 2020 proposed an "all-hazards" framework with a Directive for Resilience of Critical Entities (the **RCE Directive**).[1] The RCE Directive is being introduced as part of a package of legislative measures to improve the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole in the field of cybersecurity and critical infrastructure protection. The RCE Directive equally expands the scope of existing EU rules on critical infrastructure.

The proposed RCE Directive expands the scope of the existing EU rules on critical infrastructure.[2] It also now covers ten sectors:

1. Energy (covered by existing rules);
2. Transport (covered by existing rules);
3. Banking (also caught by existing and new rules such as DORA);
4. Financial market infrastructure providers (**FMIPs**) (also caught by existing and new rules such as DORA and the European Central Bank's rules on resilience - CROE);
5. Health;
6. Drinking water;
7. Waste water;
8. Digital infrastructure;
9. Public administration; and
10. Space.

[1] Further details available here.
[2] Specifically, the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection available here.

On 17 January 2022 a revision to the "four-column document"[3] was published in the Council Register.[4] Equally, informal trialogue negotiations are ongoing[5]. This Client Alert assesses the state of play of the RCE Directive and its impact for financial services firms.

Aims of the RCE Directive and differences to DORA

While this new Directive does not purport to have extraterritorial effect nor be as fully advanced as DORA through the EU legislative process, it intends to ensure that critical entities, the reliable functioning of which are vital to the functioning of the internal market, are able to prevent, resist, absorb and recover from disruptive incidents, regardless of whether they are caused by natural hazards, accidents, terrorist attacks, insider threats or public health emergencies.

The RCE Directive will require Member States to have a strategy to ensure resilience of critical entities, carry out a national risk assessment and identify critical entities, which will then have to carry out own risk assessments and take appropriate technical and organisational measures as well as report disruptive incidents. In addition, the proposal includes the creation of an expert group, the **Critical Entities Resilience Group** to foster regular cross-border cooperation.

In contrast, DORA, which is advancing through the legislative process, and is which expected to become operational by 2024, builds on information and communications technology (**ICT**) risk management requirements for financial organisations and seeks to harmonise the currently fragmented rules on operational resilience across the EU. The proposal covers financial entities as well as ICT third-party service providers and introduces certain obligations, such as requiring financial institutions to maintain an ICT risk management framework, use updated ICT systems and introduce ICT security strategies and policies. In addition, financial entities must introduce an ICT-related incident management procedure and must report any major ICT-related incident to the competent Supervisory Authority.

Same aims yet differing details amongst EU co-legislators

The European co-legislators, i.e., the European Commission, the EP and the Council of the EU have provided their comments on the text of the RCE Directive. As a next step a draft agreement will need to be reached. Despite the co-legislators sharing consensus on the core aims of these reforms, the details and priorities are subject to differences and diverging views. This is to be expected – certainly at this stage of the proposal.

Importantly, the Council is proposing a number of amendments that maintain Member State autonomy and ability for national rules to co-exist and in certain instance trump the requirements set out in the RCE Directive. This could be problematic, certainly in terms of driving harmonisation ensuing that a Single Rulebook in this area is truly single both in which rules apply, when, where and to whom.

Where there is consensus, at least conceptually even though the drafting differs, is that:

- Broadening the focus of resilience of critical infrastructure and protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. This is important given the increasingly interconnected nature of operations using critical infrastructure. Critical entities themselves will be required to put in place resilience measures and how to recover from incidents that disrupt the provision of essential services.
- There is no single recognised list of critical infrastructure sectors and instead different legal acts create a fragmented set of requirements that require harmonisation. Crucially, while not mentioned

---

[3] This refers to working documents that are used as a basis for discussion during informal trialogues between the Council, European Commission and European Parliament (EP) on files under the ordinary legislative procedure (OLP). Often called four-column documents. Multi-column documents set out the positions of the three EU institutions depending on the stage of the OLP procedure (most often during first reading negotiations). The order and the number of columns may vary according to the political and negotiating circumstances relating to the file. Four-column documents, from left to right, will usually show the text of the Commission proposal, the EP and the Council positions on the text of the Commission proposal and finally, the compromise agreement on the text of the proposal resulting from these informal trialogue meetings. In five-column documents, the fourth column will reflect the Presidency observations, while the fifth column will present the compromise agreement on the text of the proposal resulting from these informal trialogue meetings.

[4] The current version of the four column file from 17 January 2022 is available here.

[5] Following the agreement by the European Council and EP on their negotiating positions on the proposal, informal trialogue negotiations can begin to reach an agreement on the final text at first reading. Then the proposed Directive will have to be formally adopted by the EP and Council. More details are available here.

specifically by the co-legislators, DORA also aims to foster such harmonisation and do so by way of a Regulation (thus directly effective) that will not, like a Directive, require implementation into the laws of individual Member States. Such fragmentation is also seen (at least by the European Parliament and Council) as a disincentive for critical infrastructure to operate across borders.

- Where there is a difference in approach between European Parliament and the Council position is that the latter is currently proposing that, where national rules already exist for critical infrastructures, then critical entities that satisfy those national rules should be deemed to satisfy the aims set out in the RCE Directive. While this may make sense from a pragmatic perspective, it may not serve to achieve the harmonisation aims of these reforms and thus allow fragmentation to continue, at least in certain sectors. Where there is consensus, where DORA applies, firms subject to compliance requirements therewith will be permitted to comply with those provisions as these are deemed equivalent. The Council is proposing that the RCE Directive be a minimum harmonisation Directive whereas the other co-legislators are proposing that the RCE Directive raises the bar in terms of standards.

In respect of the relevant sectors (introduced above) to which the RCE Directive will apply, Annex 1 to the proposal[6] sets out to what types of firms it will apply. Entities will need to ensure whether they are critical. For Banking this applies to credit institutions (but not systemic investment firms). This raises the question as to equal treatment but also what additional points the RCE Directive is supposed to cover if credit institutions are already subject to existing and future rules on digital and operational resilience in addition to how to deal with critical economic functions. The same applies with respect to FMIPs, which is to apply to operators of trading venues and central counterparties, which are again subject to similar rules and supervisory expectations, as well as further pending reforms being advanced by financial services regulatory policymakers, including at the global level.

The Council has proposed to exempt a number of entities from the RCE Directive. This includes the:

- entities that fall outside the scope of Union law and, in any event, entities that mainly carry out activities in the areas of defence, national security, public security or law enforcement, regardless of which entity is carrying out those activities and whether it is a public entity or a private entity;
- entities that carry out activities in the areas of the judiciary, parliaments, or central banks;
- activities of entities which fall outside the scope of Union law and, in any event, all activities concerning national security or defence, regardless of which entity is carrying out those activities and whether it is a public entity or a private entity.

Benchmarking RCE Directive's focus on FMIPs against international consultations

On 22 January 2022, the International Organisation of Securities Commissions (**IOSCO**) published its consultation on the resilience of trading venues and market intermediaries (the **IOSCO CP**) and thus FMIPs, which is set to run to 14 March 2022.[7] The IOSCO CP set out the following key summary of lessons learned on operational resilience during the pandemic. These extend to all financial services firms and thus also trading venues and market operators:

> "(a) *Operational resilience means more than just technological solutions* – the operational resilience of a regulated entity depends as much on the regulated entity's processes, premises and personnel as its technology when faced with a significant disruption.
>
> (b) *Consider dependencies and interconnectivity* – full business processes and all dependencies and interconnections are important to consider before and after a disruption to adequately assess potential risks and changes to controls. Critical to this is consideration of the role of service providers and off-shore services, whether intragroup or third parties.
>
> (c) *Review, update and test business continuity plans (BCP)* – BCP (including scenario planning) are important to review and consider whether updates are appropriate to reflect lessons learned from the pandemic. For example, pre-pandemic operations may not be restored for a prolonged period, a disruption may impact all or multiple locations at the same time and a broad range of scenarios (even those that are unlikely) may be appropriate to be tested.
>
> (d) *Effective governance frameworks* – the pandemic highlighted the importance of an entity's effective governance framework to facilitate and support operational resilience due to potentially novel

[6] Available in its original form here.
[7] Available here.

and fast-paced situations or changes that might arise. Decisions made under pressure may need to be revisited and tested if they impact the business beyond the period of disruption.

(e) *Compliance and supervisory processes* – greater automation and less dependence on physical documents and manual processes by regulated entities may better accommodate a remote workforce. A review of monitoring and supervision arrangements by regulated entities for remote workforces may be appropriate to help ensure continued effectiveness in a remote or hybrid environment.

(f) *Information security risk* – Decentralized and remote work may increase the importance of monitoring processes to help ensure information security, and in particular, to prevent cyber-attacks."

Importantly, and rather welcomingly, the IOSCO CP discusses what should constitute "critical operations", which in turn include critical functions. The latter is already defined at the Financial Stability Board level globally as well as at EU level. They typically extend to include those functions and services performed for counterparts, clients and consumers by a financial services firm (and thus trading venue and/or market operator) where a failure would lead to the lead to the disruption of services that are vital for the functioning of the real economy and for financial stability. Examples include payments, custody, certain lending and deposit-taking activities in the commercial or retail sector, clearing and settling, limited segments of wholesale markets, market-making in certain securities and highly concentrated specialist lending sectors.

In contrast, the IOSCO CP states that "Critical operations include activities, processes, services and their relevant supporting assets, the disruption of which would be material to the continued operation of the regulated entity." In differentiating that definition as to how it is applied by the Basel Committee on Banking Supervision, and considering that the identification of critical operations will vary depending on the profile of the entity, such critical operations may include but not be limited to:

- access to services for clients or participants;
- accepting orders and executing trades for clients or participants in agreed asset classes during trading hours;
- efficient and accurate documentation and record keeping requirements;
- providing and meeting settlement and clearing processes and requirements;
- ability to facilitate capital raising services, as appropriate; and
- where appropriate, the ability to transfer trading to other trading venues if there is a system outage or other possible failures.

The IOSCO CP goes on to state that:

"**For trading venues**, these may include systems and processes relating to order entry, order routing execution systems, data dissemination, network infrastructure, market regulation, risk management systems, surveillance and the like to help ensure critical operations are provided.

For market intermediaries, there is more diversity in what the critical operations may be, again depending on the nature of the products and services being provided, the client base and regulatory requirements (e.g., a market maker has some very different critical operations compared to a retail stockbroker)."

The IOSCO CP certainly makes for a welcome contribution to debate and insight into global policymakers' thinking. It also covers a lot of the best practices that have emerged across global trading venues in the transition from an office-centric to remote working operating environment (but not location independent working arrangements – a consideration that also the RCE Directive misses) in particular during a prolonged pandemic and rapidly changing set of restrictions. However, there are some areas where the IOSCO CP does not address developments of risks and responses in full or inasmuch detail as it could.

Specifically, given the number of outages, especially during 2020, across trading venues and FMIPs and despite these largely being down to a single point of failure[8] , the IOSCO CP is largely silent on how to improve measures in their own operations as well as the third-party service providers upon which they rely. Accordingly, this should be a priority not only for on-going resilience in pandemic and/or extraordinary operating conditions (including in light of potential geostrategic tensions directly or indirectly affecting the orderly functioning of financial services firms and their counterparties) but also how to prevent and/or react to the risks of shutdowns - howsoever caused. If policymakers fail to act, this might be a missed opportunity. EU policymakers will likely have to redress such shortcomings as part of revisions to the drafts of the RCE Directive and/or DORA.

[8] In most instances related to digital (cyber) and operational (technical as well as power supply) resilience failures.

Outlook

Given the state of play on both the RCE Directive, DORA and the IOSCO CP, financial services firms affected directly by these reforms in terms of compliance with the rules and supervisory expectations but equally the counterparts, clients and also other stakeholders that are users of such financial services firms' services and products, may wish to consider forward-planning their options. This might include modelling the impact of such changes as well as how to participate in the dialogue with policymakers. The shared goal amongst policymakers and market participants is to of course improve digital and operational resilience in light of a whole new risk paradigm affecting a market operating environment that has changed rapidly over the past years and will continue to do so beyond the present pandemic. Such new rules however need to be pragmatic in how firms can reach the goals that are set out in these new legislative instruments.

Ultimately, while the RCE Directive is a welcome development for markets as a whole, some of what it aims to achieve and how it does it, is perhaps already addressed (more fully) in other EU regulatory reform initiatives. This includes those reform efforts where the views of the co-legislators may be somewhat more aligned. Affected firms will want to map where there are overlaps and conflicting obligations and consider how to raise this with policymakers as well as their own preparatory actions.

As the RCE Directive continues its path down the legislative process, further Client Alerts may supplement coverage herein as well as set out actions that firms may want to consider.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from these proposals.

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas@pwc.com

www.pwclegal.de