Digital Transformation: The impact of Operational Resilience on Digital Service Providers

David Shone	Hello and welcome to the Slaughter and May podcast. I'm David Shone. I'm a partner in the Financial Regulation Group here in London and I'm joined today by Martijn Stolze, an associate in our EU Financial Regulation practice. Martijn is based in Brussels and joins us down the line today and we have also got Tabitha Harris today, who is one of our Financial Regulation associates based in London. Hi guys, good to see you both. So in this very short podcast we are going to be discussing recent developments in the EU and UK regulatory regimes relating to operational resilience and the expansion of those regimes for the first time to cover technology service providers. Martijn – just to start with you. I think when people talk about this they often talk about operational resilience and DORA synonymously, DORA being the EU regulatory regime that has been introduced in the past few years to cover this off. So we'll start with a nice easy question – what is DORA?
Martijn Stolze	Well so DORA is the EU's Digital Operation Resilience Act, but it has a funky name. What DORA does is that it seeks to manage and mitigate the risks that providers of critical third party services to EU financial institutions could pose a risk to the financial stability in the case of a operational disruption. So, for example, if a key cloud or security service were to fail, DORA seeks to beef up EU financial institution's operational resilience and their internal functions and services, but it does that by regulating not just financial entities but their service providers as well. DORA is of course is one of these pieces of legislation that the EU has recently implemented to regulate big tech without actually implementing a specific big tech regulation framework. DORA is designed to address the supranational nature of large financial institutions and big tech and tries to subject both of these to what the EU perceives to be its own gold standard. We published a interesting Horizon Scanning article on both EU and UK operational resilience recently which you can find online.
David Shone	And its quite interesting, isn't it that the Commission is taking this dual-headed approach so that you cover the issue from both sides of the debate and of course we are doing that in the UK as well aren't we Tabs?
Tabitha Harris	We are indeed so its probably no surprise that we are also looking at the risk to financial stability from critical third party service providers in the UK. The way that that's being approached is slightly different to the EU though, so we've kind of adopted a two-pronged approach in the UK. The first approach is really through the imposition of rules on operational resilience that applies to regulated firms themselves. This requires firms to be thinking about their important business services, identifying them and setting impact tolerances that the firms have to remain within and then requiring the firms to implement strategies, processes and systems to help them stay within those impact tolerances. The second lens through which that's addressed in the UK is the introduction of the new oversight regime for regulators to designate and supervise critical third parties or as we will probably refer to during this podcast, CTPs and CTPs are those service providers that are really providing material services to regulated firms so it's coming at it from a kind of dual angle here.
David Shone	So we've got the same issue, two different jurisdictions, two different approaches. What would you say the major points of difference between the way that the UK's gone about this and the way that the EU's gone about it? Tabs, shall we start with you?
Tabitha Harris	I think the first thing you really have to draw out is DORA's focus on ICT risk. So the UK CTP regime would capture the same ICT service providers that would be in scope under DORA so if you think about the cloud-based service providers and possibly AI solutions that might fall within scope of DORA, we would expect those service providers to core in scope of the UK CTP regime as well. But there's also the potential at least in future for the UK regime to extend beyond that to perhaps claims management services that are provided to insurers so there's a real kind of potential for divergence there.

David Shone	And Martijn what about on the EU side? What would you say the key differences are?
Martijn Stolze	I would say the key difference mainly on the EU side is that is relatively prescriptive so DORA prescribes minimum contractual requirements that must be included in contractual arrangements between EU financial entities and ICT service providers. That may in the future include the use of standardised contractual provisions which they have not yet been published but we get the feeling that maybe they will in the future actually be encouraged. The UK operational resilience and CTP regime doesn't really impose equivalent requirements but works much more for a purposive position and overlaps with existing outsourcing rules. The designation system under the UK regime will in fact probably necessitate changes to the contractual arrangements but it won't be quite as prescriptive in how you actually achieve those minimum requirements but in our view, I think in many areas the UK and the EU financial entities will feel that there is a degree of similarity in the regimes both in terms of the application of testing, thread-led penetration testing, incident management requirements, as well as in position of rules on internal governance and control frameworks.
David Shone	I should say we're financial services lawyers, so obviously we are going to be approaching these regimes from that perspective but its right isn't it Martijn that DORA actually covers a broader range of services and sectors than just financial services, it's sort of sector agnostic in that respect.
Martijn Stolze	It is very much sector agnostic and it really covers the very broadest range of possible services as long as they are ICT services and financial entities are also very broadly defined in that context.
David Shone	That is something where the UK has taken a slightly different approach right because there are other sectors specific regimes that exist in the UK but when we talk about operational resilience in a financial services context it is a separate regime that's been devised by the UK regulators and applied to firms in that sector only. Do you think there's any potential read across there Tabs into the way that the UK Government may be thinking about this in future?
Tabitha Harris	I think it's a really good question. I think it's quite clear from the UK kind of regimes that have arisen to date, that the focus is kind of on financial regulators. So the kind of CTP regime is designed to have the financial regulators regulate the kind of service providers rather than anything else and in that respect there are some similarities with DORA because you've got the kind of European supervisory authorities who will be kind of overseeing your critical ICT service providers but it is definitely a kind of different way of looking at it I think.
David Shone	So if we're picking up on that theme of what's different here and I suppose one of the key differences is this idea of critical third parties and the designation and regulations to some extent of the firms that provide services to the financial services sector in the context of the UK regime and to a broader range of sectors in the context of DORA. When do you think we might start to see critical third parties being designated and what's the process around it?
Martijn Stolze	Well that's actually very interesting. So we are currently in the thick of these things and the ESAs have together announced that they will start designating from the second half of the year.
David Shone	And sorry Martijn, the ESAs that's the European Supervisory Authorities right?
Martijn Stolze	Yes that's correct.
David Shone	Great.
Martijn Stolze	So the European Supervisory Authorities which are ESMA, EBA and EIOPA, have announced that they expect their first designations to come through in the second half of the year (2025) though presumably that will be more towards the end of Q3 than at the beginning of Q3. They are currently waiting to receive information of registers from financial entities on which particular services they outsource and to which ICT service providers. However we are already hearing from the very largest ICT service providers, particularly those whose services are very, very important but not quite as well publicised as very, very largest entities getting a lot of information requests on exactly what they do. We are also seeing that everyone is running currently to try and make sure that they understand what a designation

	would mean for them and particularly because the designation provides more onerous requirements on contracting and the actual operation resilience of the ICT service provider itself.
David Shone	And so in the EU it's the ESAs who designate. Is that the same in the UK Tabs, is it the financial services regulators who designate, or does that power sit elsewhere?
Tabitha Harris	So the power sits with the Treasury but the way we expect that to work in practice is that there will be a dialogue between the financial services regulators so the FCA and the PRA feeding into Treasury, with Treasury making the kind of designations. I think what we don't quite have is the same level of clarity on timetable on the UK process at the moment. We expect this to run broadly in parallel with DORA given the overlap of who we expect to be designated and how we expect the regimes to run so we would again be expecting to see some activity on this in the second half of the year. But the process will allow kind of an opportunity for those designated to comment and respond to potential designation first so there will be an opportunity to, kind of if you like, oppose a potential designation before the final decision is made and we also know that there's going to be a transitional period for firms that are designated to come in and comply.
David Shone	And then back to the service recipient side of things. What do you think the key things that regulated firms should watch out for if these regimes continue to develop and firms have to implement their requirements?
Tabitha Harris	So I think from the kind of EU and UK side really for regulated firms it's about thinking more broadly about what information you might need to pass over to your service providers. The obligations under the kind of CTP regime in the UK aren't going to sit directly on regulated firms but there is going to need to be a degree of cooperation and obviously firms will remain responsible for ensuring compliance with the rules they are subject to under the operational resilience regime. So really what we're expecting to see is more of a natural alignment between kind of contracting service providers and regulated firms.
David Shone	Martijn, what about on the EU side of things? What should regulated firms be watching out for?
Martijn Stolze	I think what's important on both the EU and the UK side is that regulated firms should be aware of the fact that the parties they will be contracted with are now under supervision themselves. That may ultimately mean that where one of these large ICT service providers is acting in contravention of either the DORA or the UK CTP regime, they might actually be prohibited from providing these services going forward. That means that regulated firms need to have contingency plans in place and could actually be subject to penalties for non-compliance under DORA though not currently under the UK CTP regime as currently provided. And it should also be clear that the supervisory authority power for designated critical third party providers will actually be cross-border so even if you think you can mitigate any risks by perhaps contracting with US, Chinese or other third country ICT service providers the powers of the ESAs will actually extend beyond those borders and they will be quite, well in practice we'll have to find out of course how much they'll actually be applied that way but as they are drafted they are quite strong powers for EU ESAs. The UK regime does not have that focus on the actual location of service provisions and does not provide for extensive territorial powers in the same way that DORA does.
David Shone	That's great and look, this has been a bit of a whistle-stop tour and I think we are going to have to draw things to a close in a minute but before we wrap up can I ask you both what one key takeaway you think people should have when they are thinking about these two different approaches to operational resilience?
Tabitha Harris	I'll go first. I think actually the message from this side is actually it's never too early to start thinking about your contractual arrangements and revisiting them and making sure that they are compliant with, if it's in the UK existing operational resilience regime rules and future-proofing for potential impacts on service providers.
Martijn Stolze	And I think it is be aware of the fact that these large, big tech firms have previously almost entirely been unregulated and that life as a regulated entity will be very different for them but it may also impact your relationship with them.

David Shone	That's great. Well look thank you both very much for joining me and thanks to you all for listening. We are recording this on a very sunny Friday afternoon in London so hopefully it's like that with you in Brussels as well Martijn and you can get out there and enjoy the weekend.
Martijn Stolze	It's absolutely lovely, thank you.
David Shone	Brilliant. Thanks very much everyone and I should say for more information on this topic, or to hear our other podcasts, you can head to our website at www.slaughterandmay.com and I believe this podcast is also going to be available on iTunes, Google Play or wherever else you go to get your podcasts. Thank you very much.