CLIFFORD

CHANCE

UK FINANCIAL SERVICES AND MARKETS BILL: NEW RULES FOR 'CRITICAL THIRD PARTIES'

UK FINANCIAL SERVICES AND MARKETS BILL: NEW RULES FOR 'CRITICAL THIRD PARTIES'

The UK Financial Services and Markets Bill includes proposals to regulate cloud service providers and other designated 'critical third parties' supplying services to UK regulated firms and financial market infrastructures. HM Treasury would have powers to designate service suppliers as 'critical' and the UK regulators would have new powers directly to oversee designated suppliers, which would be subject to new minimum resilience standards. The proposals are similar to but different from the planned EU Digital Operational Resilience Act.

What is the expected timing for the new rules?

The Bill was introduced into Parliament in July 2022. If enacted, it would make wide ranging to the UK financial services regulatory framework (see our briefing **here**), including the creation of a new regime for service suppliers designated by HM Treasury as 'critical third parties' (CTPs).

The legislative process will get under way in September and the Bill may be amended during the process. However, absent an intervening general election, the Bill should be passed and become law by the end of this Parliamentary session (expected to be in May 2023). Following this, HM Treasury would be able to bring its provisions into force on days to be appointed (to the extent not specified in the Bill) and the government and regulators could begin the process of adopting and implementing the regulations and rules contemplated by the new law.

The Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA) and the Bank of England (the Bank) published a joint discussion paper in July 2022 setting out how they could use their proposed powers under the Bill. The deadline for responses to the discussion paper is Friday 23 December 2022. Subject to the outcome of Parliamentary debates on the Bill, the regulators expect to consult on their requirements for CTPs in 2023.

Why are new rules being introduced for CTPs?

There is increasing regulatory focus on enhancing the operational resilience of regulated firms and financial market infrastructures (FMIs) given their perceived growing dependence on a limited number of cloud service providers and other technology suppliers, including data analytics suppliers. This is underlined by the findings by the Bank that over 65% of UK firms used the same four cloud providers for cloud infrastructure services in 2020. Regulators are concerned about the risks arising from a concentration in the provision of critical services by one third party to multiple firms and FMIs, as a failure or disruption of such a service provider could adversely affect the stability or integrity of the financial system or financial markets and the resilience of firms and FMIs.

What will be the framework for designating CTPs?

Under the Bill, HM Treasury would be able to designate a third party as 'critical' only if a failure in, or disruption to, the provision of its services to regulated firms and FMIs could threaten the stability of, or confidence in, the UK financial system. In making this assessment, HM Treasury would be required to have regard to the materiality of the services which the third party provides to the delivery of essential activities, services or operations and the number and type of firms and FMIs which use the third party.

Before a third party is designated as 'critical', HM Treasury would be required to give notice to the third party, to provide a reasonable period within which the third party may make representations and to have regard to any such representations. HM Treasury would also have to consult with the FCA, the PRA, the Bank and other appropriate bodies.

The July discussion paper sets out the UK regulators' initial thinking on the criteria they would take into account when considering whether to recommend designation of a service supplier. It also suggested that consultation and cooperation arrangements might involve a wide range of bodies including the Department of Digital, Culture, Media and Sport, the Information Commissioner's Office and the Competition and Markets Authority (CMA).

What powers will the UK regulators have over CTPs?

The Bill would give the UK regulators the power to make rules applying to CTPs when providing services to regulated firms and FMIs and to give directions to CTPs. Regulators would have the power to request information directly from CTPs and third parties, to commission an independent skilled person to report on CTPs' services, to appoint an investigator to review any potential breaches, to interview representatives of the CTPs and to enter the CTP's premises under warrant. They would also have powers to take disciplinary measures against CTPs if they contravene the requirements imposed on them, including powers to censure a CTP and to prohibit or restrict their services to regulated firms and FMIs.

What resilience standards will apply to CTPs?

The July discussion paper sets out the UK regulators' initial thinking on how they might use their new rule-making powers to set minimum resilience standards for CTPs. The paper envisages that a CTP should:

- **Identification and mapping:** identify and document all material services it provides to firms and FMIs and map the resources needed to deliver them (including processes, technology, facilities and information);
- **Risk management:** identify risks to its material services across the supply chain and implement appropriate controls, including in relation to cyber risks, environmental risks and legal and reputational risks;
- **Testing:** regularly test the resilience of its material services by performing its own internal tests as well as participating in tests convened by its regulators;
- **Engage with regulators:** proactively and promptly disclose information to regulators, particularly on incidents or threats that could have a systemic impact;

- **Financial sector continuity playbook:** maintain and submit to regulators a playbook documenting measures that it would take to mitigate the potential systemic impact that could arise from its failure or a severe but plausible disruption to its material services;
- **Post-incident communication:** develop a tailored communication plan to engage with all relevant stakeholders in the event of disruption to its material services; and
- **Learning and evolving:** regularly share with stakeholders lessons learnt from any disruption in the sector and the outcome of resilience tests it participated in.

What resilience testing will be required of CTPs?

The July discussion paper also sets out the UK regulators' initial thinking on how they might use their new rule-making powers to set resilience testing requirements for CTP to allow the regulators to assess whether the resilience standards are met in practice. The potential tools include the following:

- **Scenario testing:** CTPs would need to carry out regular scenario testing of their ability to continue providing material services in the event of their failure or severe but plausible disruption, and this scenario testing may need to take place in collaboration with firms, FMIs, industry groups and others.
- **Sector-wide exercises:** These tests would focus on the ability of the financial services sector as a whole to respond to operational incidents. They could be carried out on a cross-border basis, involving multiple firms and FMIs, and may require a significant level of coordination.
- **Cyber resilience:** At the end of each cyber resilience test, the CTP would agree a remediation plan with its supervisor to address any identified vulnerabilities.

How do the UK proposals compare to those in the EU?

In July 2020, the European Commission published its legislative proposal for an EU regulation - the Digital Operational Resilience Act (DORA). The proposed regulation sets out requirements for the security of information and communication technology (ICT) systems of firms operating in the financial sector as well as critical third parties which provide ICT-related services to them, such as cloud platforms or data analytics services. It also proposes an EU oversight framework which would apply to all critical ICT third-party providers (CTPPs), including cloud computing service providers. The co-legislators have reached agreement on an amended text of DORA, pending sign-off by the European Parliament and the Council of the EU.

The UK proposals under the Bill are similar to but differ from those under the amended text of DORA in a number of respects, including as set out in the table below.

	UK: the Bill	EU: DORA
Application to foreign suppliers	Non-UK firms may be designated as a CTP. The discussion paper does not envisage requirements for a local presence.	A third-country entity may be designated as a CTPP. However, the entity must establish a subsidiary in the EU within 12 months.
Responsibility for designation	HM Treasury, after consulting UK regulators and others.	Joint Committee of the European Supervisory Authorities (ESAs), upon the recommendation of an Oversight Forum comprising representatives of EU bodies and national supervisors.
Criteria for designating a supplier as critical	HM Treasury may designate a third party as 'critical' if a failure in, or disruption to, the provision of its services could threaten the stability of, or confidence in, the UK financial system.	The criteria for designating an entity as a CTPP include: • the systemic impact on the stability, continuity, or quality of the provision of financial services in case the entity faces a large-scale operational failure to provide its services; • the systemic importance of the financial entities that rely on the entity; • the criticality of the functions of the financial entities which rely on the same entity; • the degree of substitutability of the entity.
Supervisory responsibility over critical suppliers	The UK regulators which must coordinate the exercise of their powers.	The Lead Overseer for a CTPP will be one of the ESAs (the EBA, EIPOA and/or ESMA) in conjunction with a Joint Oversight Network of the ESAs and supported by the Oversight Forum.
Powers of regulators	UK regulators will have powers to make rules, give direction, require information, investigate and impose disciplinary measures on CTPs.	Lead Overseer will assess whether CTPP's have comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks they present and will have powers to adopt an oversight plan for CTPPs to request information, conduct inspections and issue recommendations.
Standards and testing of CTPs/CTPPs	The UK regulators will be able to use their powers to introduce minimum resilience standards and resilience testing to CTPs (as outlined above).	The Lead Overseer will perform an annual, tailored assessment of each CTPP based on standards set out in DORA.
Non-compliance consequences	A UK regulator may censure a CTP or prohibit or restrict its services to regulated firms and FMIs.	The Lead Overseer may impose fines of up to 1% of daily worldwide turnover in the preceding year in case of non-compliance or ask financial services firms to terminate their arrangement with the CTPP.

Do the proposals have competition law implications?

As already noted, the UK regulators may consult and cooperate with other authorities such as the CMA in relation to the designation of a service supplier as a CTP under the new powers in the Bill. In addition, designation as a CTP could support an argument that a service supplier has a dominant position or, conversely, a finding of dominance by the CMA could support the designation of a third party as a CTP.

There may also be interplays with other recent competition law developments. Various competition authorities, including the Japanese Fair Trade Commission, the French Competition Authority and the Dutch Authority for Consumers and Markets, have launched market studies into cloud services. A finding in such a market study report that a company has market power in the cloud or IT services sector could support the designation of that company as a CTP.

In addition, a new Digital Markets Unit in the UK may be able to designate a company as having 'strategic market status' (SMS) if the government's planned Digital Markets, Competition and Consumer Bill is introduced and enacted. It has been proposed that SMS designation will be applied to a limited number of firms which have a substantial and entrenched market power in at least one digital activity that provides them with a strategic position. Designation as having SMS may also be relevant to HM Treasury when considering designation of a service supplier as a CTP.

What is the impact on service users?

The new regime may provide assurance to UK regulated firms and FMIs that CTPs are subject to appropriate resilience standards, which may help them with their own risk assessments on outsourcing to CTPs. However, the new regime might also increase 'CTPs' costs which they may seek to pass on to service users or even (depending on how the regime operates) cause some service providers to consider the extent to which they provide services in the UK. Regulated and firms and FMIs may also be asked to participate in the resilience testing programmes for CTPs and may need to adapt their contingency plans to address the risk of regulatory action prohibiting or restricting the provision of services by CTPs.

CONTACTS

Monica Sah
Partner
London
T: +44 207006 1041
E: monica.sah@cliffordchance.com

Caroline Dawson
Partner
London
T: +44 207006 4355
E: caroline.dawson@cliffordchance.com

Simon Crown
Partner
London
T: +44 207006 2944
E: simon.crown@cliffordchance.com

Paul Ellison
Partner
London
T: +44 207006 3207
E: paul.ellison@cliffordchance.com

Simon Gleeson
Partner
London
T: +44 207006 4979
E: simon.gleeson@cliffordchance.com

Nelson Jung
Partner
London
T: +44 207006 6675
E: nelson.jung@cliffordchance.com

Caroline Meinertz
Partner
London
T: +44 207006 4253
E: caroline.meinertz@cliffordchance.com

Ashley Prebble
Partner
London
T: +44 207006 3058
E: ashley.prebble@cliffordchance.com

Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@cliffordchance.com

Christopher Bates
Special Counsel
London
T: +44 207006 1041
E: chris.bates@cliffordchance.com

Diego Ballon Ossio
Senior Associate
London
T: +44 207006 3425
E: diego.ballonossio@cliffordchance.com

Laura Douglas
Senior Associate
London
T: +44 207006 1113
E: laura.douglas@cliffordchance.com

Shruti Hiremath
Senior Associate
London
T: +44 207006 3075
E: shruti.hiremath@cliffordchance.com

Nancy Li
Senior Associate
London
T: +44 207006 6047
E: nancy.li@cliffordchance.com

Stephanie Peacock
Senior Associate
London
T: +44 207006 4387
E: stephanie.peacock@cliffordchance.com

Meera Ragha
Senior Associate
London
T: +44 207006 5421
E: meera.ragha@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2209-002469