STEPHENSON HARWOOD

Regulating critical third parties

The implications of DORA & FSMB on critical third parties in the financial services sector

Regulation of critical third parties

Current regulatory landscape

- Indirect regulation via regulated financial services entities
  - Local regulatory requirements: e.g. UK FCA cloud guidelines
  - EU & UK: EBA Guidelines

Pipeline regulatory landscape

- Indirect and direct regulation
  - EU: Digital Operational Resilience Act – likely to be enacted Q4 2022 and effective Q4 2024
  - UK: Financial Services and Markets Bill - possibly enacted in 2023 with effective date phased in, potentially end of 2024

EU: Digital Operational Resilience Act "DORA"

DORA: overview

The EU's most significant regulatory initiative on operational resilience and cyber security in the financial services sector

- Requirements to prevent sector disruption by cyber security attacks, outrages and other risks
- Directly regulates financial entities and designated critical ICT third party providers
- Additional requirements will apply when engaging non-critical ICT service providers
- Will build on current requirements - it will not repeal current requirements, e.g. under the EBA Guidelines, CRD, MiFID II and Solvency II frameworks

DORA: implications on critical ICT providers

Critical ICT third party providers (CITPPs) will be subject to direct oversight and regulation by applicable EU supervisory authorities, and additional obligations

- An obligation on CITPPs to form a subsidiary in the EU
- A lead supervisory authority will be appointed to directly supervise, investigate, inspect, request information and documents, and issue recommendations against CITTPs
- Powers to ask CITPPs to take specific IT security measures and change terms and conditions or subcontracting arrangements
- Powers to direct financial entities to suspend or cancel contracts with designated CITPPs
- Obligations around simplifying supply chains

DORA: Designation of critical ICT third party providers

DORA sets out a framework for the direct supervision of CITPPs which are to be designated by the EU supervisory authorities

The criteria for designation includes:

- the systemic impact on the stability, continuity or quality of the provision of financial services in case the relevant CITPP faced a large scale operational failure
- the systemic character or importance of the financial entities that rely on the relevant CITPP and the reliance of financial entities on the services provided
- the degree of substitutability of the CITPP
- the number of Member States in which CITPP provides services and the number of Member States in which financial entities using the relevant CITPP are operating

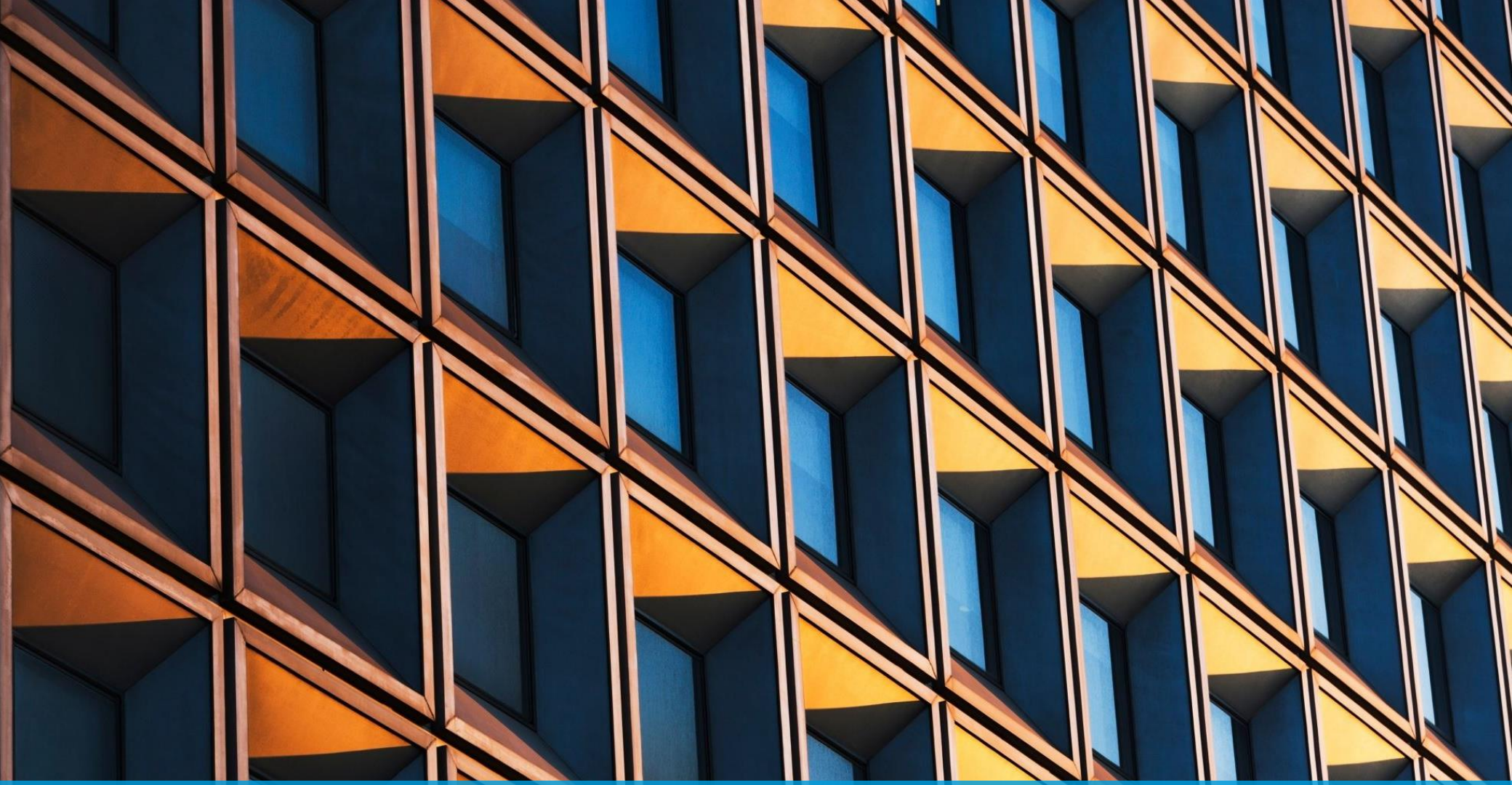
Supervisory authorities will publish the list of designated CITPPs 'at EU level' and update this on a yearly basis

DORA: implications on non-critical ICT providers

Obligations largely aligned to EBA Guidelines, but with additional requirements

Including:

- Contracts must be in writing and available as “one written document”
- Providers to assist when an ICT-related incident occurs “at no additional cost or at a cost that is determined ex-ante”
- Providers to further participate in the financial entities' ICT security awareness programs and digital operational resilience trainings
- Contracts must specify whether subcontracting is permitted, the conditions of subcontracting and the relevant locations
- Additional requirements for outsourced critical or important functions



UK: Financial Services and Markets Bill "FSMB"

FSMB: overview

Status

- FSMB currently before parliament, and includes powers to extend regulatory remit and oversight
- HM Treasury Policy Statement and Bank of England, Prudential Regulation Authority and Financial Conduct Authority joint Discussion Paper on proposals under FSMB for regulating and mitigating risks from critical ICT third parties
- Consultation on the Discussion Paper closes on 23 December 2022

Key rationale

- "*The increasing criticality of the services that critical third parties provide, alongside concentration in a small number of providers, pose a threat to financial stability in the absence of greater direct regulatory oversight*"

FSMB: implications on critical third parties

The main focus areas outlined in the Discussion Paper are to increase minimum resilience standards and impose tools for testing resilience

Proposed powers include:

- to request information from CTPs and to investigate concerns
- to conduct skilled person reviews of CTP activities
- to interview a representative of the CTP
- to issue directions requiring action, such as to implement recommendations, remediate issues or implement conditions or restrictions on services
- powers to publish details of breaches
- prohibiting a CTP from providing future services to a financial entity, or prohibiting financial entities from receiving certain CTPs services

FSMB: designation of critical third parties

HM Treasury will be able to designate certain third parties as CTPs, and supervisory authorities (BoE, FCA, PRA) will also be consulted and may proactively recommend designations

The assessment criteria will be based on:

- materiality of the services provided
- nature of the concentration of firms and institutions to which they provide services
- the overall potential systemic impact that disruption to the services could have on the financial sector supervisory authorities' resilience objectives

FSMB: implications on non-critical third parties

Whilst the Discussion Paper concentrates on additional resilience requirements on financial entities, and directly regulating CTPs, non-critical third party supplies will also come under the spotlight

- Additional due diligence on technical and operational measures
- Increased scrutiny on operational resilience
- Analysis of the concentrated risks of overreliance on a relatively small number of key providers
- Diligence beyond the immediate outsourced suppliers to cover the sub-sourcing supply chain
- Pressures to provide multiple sub-sourcing options (e.g. multiple hosting providers)

There is (and has been for some time) increasing concern that a failure of one individual provider could take out controls, functions, and services of the regulated entity, and also their underlying supply and sub-supply chain.

Our concluding thoughts

The direction of travel

- The concentration risk has been a prominent concern in the financial services sector for some time, and many regulated entities have failed to adequately address it
- The risk of single-points-of-failure is a key driver in the scope of the proposals, and financial entities and potential CITPPs/CTPs should plan-ahead to understand their own risks and those arising through their interconnected supply chains
- Given the investment in the use of cloud products/services over recent years, these issues should now feed into long term plans
- CITPPs/CTPs have been keen to show willingness to engage with regulators and to demonstrate resilience. However, the pressures will intensify, and any arrangements will need to be formally adopted in anticipation of direct regulatory oversight
- The proposed measures, and ultimate outcomes, could also have an impact on competition around service providers, which need to be factored into business plans and development roadmaps

Key actions for ICT suppliers

Suppliers into the financial services industry must analyse their own operational resilience, and that of their supply chains

- Ensure you have relevant terms in place with your subcontractors that meet current EBA Guidelines – e.g. FS Addendums with hosting suppliers
- Consider whether long or complex chains of sub-contracting affect your ability to effectively monitor them
- Review your tech stack and the downstream elements of subcontracted services and considering whether they could be adjusted to accommodate regulatory requirements and customer pressure to diversify suppliers to dissipate risk
- Ask subcontractors that are like to be designated as critical third parties to explain what measures they are implementing to comply with the new requirements
- Keep under review your risk of being designated as a critical third party under the direct oversight of an applicable regulator

Key Contact

Simon Bollans
Partner, Technology

T: +44 20 7809 2668
E: simon.bollans@shlegal.com

STEPHENSON HARWOOD

#techintelligence
breaking down the issues

#techintelligence **is Stephenson Harwood's knowledge centre, focused on breaking down the legal issues and providing market insights on the development and use of technology and data.**

October 2022

STEPHENSON HARWOOD