IRSG

INTERNATIONAL REGULATORY STRATEGY GROUP

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland
(by email: fsb@fsb.org)

18 December 2020

OUTSOURCING AND THIRD-PARTY RELATIONSHIPS

Financial Stability Board Discussion Paper

Submission of the International Regulatory Strategy Group in relation to *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*

Dear Sir/Madam,

We are pleased to share with you a contribution to the public consultation on the discussion paper on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships. We submit this contribution on behalf of the International Regulatory Strategy Group (IRSG), an advisory body to both the City of London and TheCityUK.

The IRSG is a practitioner-led body comprising leading UK-based figures from the financial and related professional services industry. It provides a forum in which the whole industry can come together to discuss issues of public policy that are horizontal in nature. We chair the IRSG's Global Regulatory Coherence Standing Committee, looking at how global regulatory coherence can drive global competitiveness of UK financial and related professional services, and the IRSG's Data Workstream, which focuses on issues relating to financial services' use of data.

We welcome this discussion paper, exploring potential issues for supervisory authorities and financial stability arising from the significant scale of services provided via third-party outsourcing and the relatively small number of globally dominant players providing these services. We agree that a further discussion among supervisory and regulatory authorities on their approaches to outsourcing and third-party risks is needed, to address current cross-border supervisory challenges and potential financial stability issues.

With our submission, we call for the development of a global regulatory solution to tackle systemic risk challenges arising from concentration of outsourcing. Many challenges in this area will be new and time-sensitive, and this is an opportune time to achieve significant progress through this consultation process. There is a potential for systemic risk arising from the concentration of outsourcing to large technology vendors, which is especially pertinent now due to the increasing reliance on technological solutions post-pandemic and the rise of home working. In the context of operational resilience, policymakers and financial regulators need to co-ordinate their efforts to address such concentrated outsourcing. If one very large technology vendor were to fail or be disrupted over a prolonged period, this could have significant consequences for a high number of financial services firms around the world and could constitute a major systemic event. We outline our response to the specific consultation questions in more detail below.

1. What do you consider the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships, including risks in sub-contractors and the broader supply chain?

We are supportive of outsourcing in principle. Outsourcing enables firms to focus on the key business areas of the business and leverage the expertise and resources of third parties to support their shared services, technology and operational functions. It provides for a diverse business ecosystem. However, there is a potential systemic risk arising from the concentration of outsourcing to a limited number of large technology vendors in a single jurisdiction, and this is especially pertinent now due to the increasing reliance on technological solutions post-pandemic and the rise of home working. To that end, the current challenges that regulatory and supervisory bodies are facing on outsourcing are relatively new as well as time-sensitive in nature. Therefore, in identifying these emerging challenges, it will be important to do so in close collaboration with the industry, in a timely manner. When identifying and mitigating these risks, policymakers should consider the complexities of what are often global and complex supply chains and sub-contracting arrangements. Outsourcing may entail global risks, so policymakers, financial regulators and global standard setters should co-ordinate their efforts globally to address such concentrated outsourcing concerns. They should model their approach on lessons learnt from past crises where similar concentration posed systemic risk challenges. Ultimately, we welcome the development of a proportionate global regulatory solution that addresses the systemic risk challenges arising from concentration of outsourcing, while taking into account the regulatory and operational complexities of global supply chains and outsourcing arrangements, to avoid undue operational and regulatory compliance burdens.

Data localisation

The financial services industry is currently witnessing and responding to increasingly protectionist behaviours across the world in the form of data localisation. In recent years, the implementation of data localisation requirements within jurisdictions has increased, which has been driven by a number of concerns including the need for sufficient and timely access to data for regulators to effectively supervise regulated entities. The IRSG has recently produced a report entitled 'How the trend data localisation is impacting the financial services sector', which includes many of the following points.

Appropriate levels of supervisory access

One of the main risks and challenges associated with outsourcing in the financial services industry that relates to the concerns giving rise to data localisation is that of supervisory access. It is contended that outsourcing poses challenges to regulators and their ability to effectively regulate and supervise financial services companies. Amongst other things, one of the reasons for this relates to the perceived lack of control over the processes of, and data held by, the non-regulated outsourcing service provider. Such concerns have drawn the concept of data localisation into ongoing discussions surrounding regulating outsourcing. Regulators often require the financial services company to retain full regulatory responsibility for the outsourced services and some regulators have determined that the physical location of a financial service company's data can form such an unacceptable risk, as to warrant outsourcing restrictions that practically implement or mandate data localisation as a result. Outsourcing and the storing of data in a cloud may also be seen to increase risks which make the monitoring of, and reliance on outsourced tasks difficult. However, it is also the case that cloud service

IRSG Secretariat, City of London
PO Box 270, Guildhall, London, EC2P 2EJ
Email: IRSGsecretariat@cityoflondon.gov.uk

providers can also mitigate more prevalent data risks, enhancing the level of data security as they are often more aware of and are up to date with cyber-security issues *than local data centre providers or individual regulated entities.* Centralisation of data enables firms to focus their resources on ensuring appropriate security and ready access to all relevant data.

Many outsourcing guidelines, rules and regulations address these concerns by requiring the regulated entity to ensure that the regulators have certain levels of access to the data processed and stored by the outsourcing service provider including access to the outsourcing service providers premises and any other information on the outsourced service. In any approach taken, mandating data localisation within outsourcing should be avoided, as it would be severely disruptive to the financial services industry, is not the only mechanism to ensure regulatory access, and does not prevent third country regulatory or legal access to data.

2. What are possible ways to address these challenges and mitigate related risks? Are there any concerns with potential approaches that might increase risks, complexity or costs?

Responsibility for the data

It is the view of the IRSG that outsourcing regulations should seek only to ensure that such control of, access to, and ultimately the responsibility for the data remains that of the local regulated entity and that such is appropriately reflected in the relevant contract with the outsourcing provider. The data that is being accessed must actually be necessary to those authorities, statutorily. This may require technical focus and agreement within markets. Another avenue, as an alternative to formal regulation of access, is for access arrangements to be agreed through dialogue with regulators or even through contractual arrangements with internal and external service providers.

Focus on quality of solution, not location

We further advocate that an assessment operational resilience should focus on the quality of the outsourcing solution, not its location. Ultimately, an outsourcing service provider should not be deemed to be a threat to the operational resilience simply because it is providing the service from another jurisdiction. Guidance that encourages data localisation by implying that local data storage is more resilient should be avoided. In reality, the use of global data service providers often provides a greater degree of physical and virtual data protection.

These are legitimate issues that require a proportionate regulatory response, but that should not be a fig leaf for protectionist policies, whether directly, or indirectly, through localisation. It should be noted that cloud provision is arguably a distinct case in terms of the systemic risks challenges so any regulatory developments in this area should be appropriately attuned to what is being outsourced and what is the risk.

3. What are possible ways in which financial institutions, third-party service providers and supervisory authorities could collaborate to address these challenges on a cross-border basis?

International cooperation

The FSB should be a convenor of similarly minded jurisdictions that have significant market and regulatory power, creating opportunities to level up standards in a helpful way. Should governments

IRSG Secretariat, City of London
PO Box 270, Guildhall, London, EC2P 2EJ
Email: IRSGsecretariat@cityoflondon.gov.uk

choose to place requirements on virtual or physical infrastructure providers, any approach should be risk-based and proportionate, support international cooperation and avoid national variations in rules that undermine the efficiency gains of the Cloud.

In an increasingly digital world, there is a need to ensure the whole ecosystem is captured as firms rely on outsourced suppliers, experts, and infrastructure to operate. These all need to be within scope, not just “regulated” entities. For example, financial crime and cybersecurity are global issues with multi-tiered participants supporting the financial and broader business ecosystem.

4. What lessons have been learned from the COVID-19 pandemic regarding managing and mitigating risks relating to outsourcing and third-party relationships, including risks arising in sub-contractors and the broader supply chain?

Outsourcing to technology vendors has been a significant trend during the coronavirus pandemic. Covid-19 has shown that financial services can continue to operate efficiently as people can effectively work from home. This transition to remote work on such a massive and unprecedented scale has therefore accelerated the adoption of digital services by financial institutions. The proposal to address outsourcing risks is therefore timely, as such technological developments bring about an increased awareness to the level and nature of risk. Covid-19 continues to present unprecedented challenges and clearly underlines the necessity for a resilient financial services infrastructure, both physically in terms of adequate and stable access to the Internet, and the ability to leverage collaboration and communication tools. The IRSG supports the FSB’s aim of enhancing the resilience of the global financial services industry, and places the utmost value on risk management.

With recovery efforts from COVID-19 taking centre stage, support for global coherence remains critical, together with an enhanced commitment to solving issues with international co-operation. Global regulatory coherence and consistent implementation of global standards in a way that fosters cross-border activity, encourages fair and open competition, benefiting customers, firms and their regulators alike. This is good for economic growth and good for financial stability. The IRSG argues the case for a renewed commitment to international regulatory cooperation on outsourcing to avoid market fragmentation which may give rise to financial instability and other risks. Local and international bodies should ensure this principle remains central to their work on outsourcing, and this work should be rooted in principles of cooperation, communication, transparency and consultation.

We remain engaged actively in the discussion on outsourcing and if you would like to discuss this in further detail please do not hesitate to get in touch.

Yours sincerely,

Antony Manchester IRSG Global Regulatory Coherence Standing Committee Chair	Vivienne Artz IRSG Data Workstream Chair

IRSG Secretariat, City of London
PO Box 270, Guildhall, London, EC2P 2EJ
Email: IRSGsecretariat@cityoflondon.gov.uk