08 January 2021
EBF_043690

EBF comments on the FSB Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships

EBF position:

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?

- Disparities amongst regulatory definitions and guidelines leads to significant complexity in implementing third-party risk management requirements in a global setting. Some examples of where there is a need for global consistency are:
    a. Clarity and consistency on key definitions across jurisdictions. e.g. "Outsourcing", "third-party relationships" and "criticality". Inconsistency of definitions makes it challenging for global organisations to apply a consistent global framework that provides the basis to obtain a consistent view of arrangements and risk across the firm. We note the general trend of regulators taking a more holistic approach to "third party relationships" and acknowledge that this may benefit through moving away from a prescriptive approach. However, we emphasise that in any framework that moves towards a holistic notion of "third-party relationships", it is important to take an outcomes-based approach with a focus on addressing risks. Furthermore, we note that to the extent existing regulated activity is captured within outsourcing and third-party regimes, this would arguably be seeking to mitigate risk that is therefore already addressed and creates a more complex regulatory landscape.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

b. Consistency in respect of Cloud Computing, e.g. "cloud computer services" should not automatically be deemed to be "Outsourcing", but an assessment should be undertaken to assess whether such services fall within the definition of "Outsourcing".
c. Intra-group differentiation: Regulators should acknowledge the differences between outsourcing and intra-group arrangements, including in relation to due diligence and ongoing monitoring expectations. It is the industry's view that intra-group arrangements contribute to sound risk management and to the overall resilience of the firm, including its subsidiaries.

- Regulatory/legislative fragmentation and localised focus of regulators in the context of a global marketplace can result in the localisation of systems, data and processes, preventing firms from achieving effective operational resilience and risk management. For example, global firms frequently rely on intra-group arrangements, which may in turn result in a supervisory response to bring that service back 'in-house' within geographic boundaries. Given that firms operate globally, the imposition of jurisdictional limitations may leave such firms exposed. Regulators can adopt an approach that allows for regulatory requirements to be applied on a proportionate basis to intra-group outsourcing arrangements.
- Current regulatory developments do not take a **risk and outcomes-based approach**, which significantly impacts existing review pipelines and capacities as well increasing efforts of any vendor contract negotiation plus management of existing portfolios. Prescriptive tick-in-the-box audit and inspection obligations, both on third-party and subcontractors, increase complexity and hamper financial institutions' capacity of providing innovative services. We believe greater emphasis should be placed on establishing the risks related to outsourcing and what governance and capabilities authorities require to ensure firms are able to remain within their risk appetite.
- The lack of a direct contractual relationship between the FI and the subcontractors limits the FIs influence and ability to directly supervise. This is more challenging when negotiating contractual provisions with unregulated entities. Some members have noted that, in some cases, service providers do not allow FIs to negotiate changes to their standard contract, do not allow site visits, or do not respond to a FI's due diligence questionnaire. In these situations, the FI is limited in its ability to conduct the type of due diligence, contract negotiation, and ongoing monitoring.
- Expectations of oversight of subcontracting chains for intragroup services, including where the subcontracting chain may lead to external providers, do not provide for situations where the subcontracting providers would already be subject to risk management processes.
- Some members have noted that highly standardized services and dominant market participants offer their services "as is" and expect that institutions have to adapt their available controls and risk mitigation policies to the service features offered by the vendor and not the other way around. This "take it or leave it" scenario requires a significantly higher effort to assess such services based on vendor documentation.
- Multiple regulatory initiatives arising at the same time increase the complexity of handling detected difficulties such as subcontracting, cross-border relationships, etc.
- As noted in the FSB discussion paper, one key issue is that some third-party providers are sometimes **unaware** of the fact that FIs are subject to **strict regulation and supervision requirements**. FIs have to meet certain requirements, such as identifying and managing potential risks, that can only be done if third parties share all the information/evidence they are requested, which is not always the case, e.g. for confidentiality reasons.

Other areas for consideration:

1. It is important to ensure that any attempts to oversee outsourcers/third parties directly is applied consistently with pre-existing regulations that may apply to the part, and interoperable globally. To the extent that this is not the case, this will arguably exacerbate the risk in relation to 'on-site audits' whereby time and resource of third parties are devoted to numerous audits, and in the case of any direct oversight, numerous regulators conducting fragmented supervision. This may present downstream risk to financial institutions where resources and capabilities are dedicated to this oversight by third parties (as opposed to the continued provision of safe and secure services to financial institutions).
2. Difficulties defining the time to implement exit plans and assessing appropriate interim steps before executing exit arrangements.
3. Concerns around perceptions on the cloud due to assumptions that the cloud is more susceptible to risk than services provisioned through traditional hardware models. However, the cloud does not necessarily carry greater risk and in fact has been recognised as an essential way to mitigate risks, particularly due to capacity limitations.

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?

- Further collaboration and alignment amongst regulatory authorities on outsourcing and third-party risk requirements, particularly with regards to common definitions and criteria for outsourcing, materiality, and criticality, and amongst interconnected topics such as recovery and resolution and operational resilience.
- As a way to ease the regulatory burden, existing upfront information and special termination rights of the institution should be considered as sufficient for subcontractor risks, in line with the principal vendor obligation to manage and control its own subcontractors in compliance with the contractual obligations, including those to ensure the location of and access to bank data as well as the general principle of unrestricted audit rights also applicable to (material) subcontractors. It should be enough for financial entities to have a guarantee of service fulfilment by their providers, leaving them to carry on their obligations to their subcontractors, unless there is sufficient evidence of a material risk that cannot be otherwise mitigated.
- A stronger alignment between international standards such as ISO, NIST and the Cybersecurity Profile and rules imposed on FI's will make it easier for both FI's as well as 3rd party providers to comply. Standardization reduces complexity and therefore drives down risk and costs. Driving (further) commoditization of products could reduce dependencies on specific 3rd parties.
- Supervisory authorities must acknowledge that it is possible to achieve compliance with third-party due diligence requirements through leveraging pooled audits and industry standard certifications. For subcontractor risk, supervisory authorities must acknowledge it is possible to leverage the third-party risk management processes in place with the primary third-party provider. General expectations on FIs for direct oversight of subcontractors leads to an oversaturation of assessments in the market (particularly with, but not limited to, cloud) and significantly increases costs of compliance, both from the perspective of providers in the chain and FIs who must adequately resource to address an exponential increase in assessments.

- An assessment of the contracting party's vendor risk management processes is currently part of most FI's vendor or third-party risk management processes which is extended to cover subcontracting risks.
- There are already certain back-up and BCM requirements in place that FIs adhere to. New technologies like cloud offer even higher resilience and stability of applications, but also require that FIs build up their own know-how and resources to use such platforms (partial insourcing of service management).
- A mandatory multi-vendor-strategy, such as the one currently proposed in the EU would significantly increase cost of innovation, complexity and the risk of operational disruption. In addition, it is based on the incorrect assumption that there are sufficiently interchangeable services available for all use cases which may be easier for cloud infrastructure platforms but would be a challenge for innovative or proprietary AI solutions.
- European entities are currently undertaking the implementation of the EBA Outsourcing Guidelines, while also reviewing those contained in the DORA proposal. Any further requirements should take into account and align with existing dispositions to prevent fragmentation, which could increase the workload without significant benefits.
- Facilitating the use of **licenses and pooled audits** would reduce operational effort for financial institutions and supervisors without compromising security. A globally recognized certification scheme may reinforce outsourcing supervision, establishing certain expectations on service providers and streamlining procedures for financial services participants.
- Raising awareness on FIs responsibilities. FSB mentions on page: 12: "third parties are sometimes unaware of the regulatory obligations of their FI clients".
- Outsourcing should take a risk and outcomes-based approach that focuses on the risk characteristics of third-party relationships. This approach should specify the regulatory outcomes that regulators seek to achieve and provide FIs with the ability to choose in a principled and disciplined way, how to deliver that outcome. This could include a focus on:
    - Core Business functions the Firm delivers.
    - Recognize and make provisions for FI's to address regulatory obligations, through external third-party procurement without considering outsourcing due to feasibility (not core business function and cost prohibitive to provide itself with an external third-party service) (i.e. Electronic and Physical storage facilities).

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?

- **Public-Private Forum**: We encourage industry and policymaker collaboration to support help to identify potential risks and gaps in relations to outsourcing and third-party risk management, particularly given sector-wide interdependencies. This could assist with a number of the practical challenges identified in the FSB paper, particularly in relation to ensuring that third parties are aware of the regulatory environment in which financial institutions operate, and therefore help to combat common issues among both financial institutions and third parties. Further collaboration with FIs and supervisory authorities to agree practical and scalable approaches to new and evolving concepts, such as subcontracting, data protection, register usage, cloud, concentration risk, and criteria for definitions/classifications.

- **Exercises to address concentration risk**: In the event of a disruption at a major provider it is vital that the financial industry, including its regulators, have rehearsed some of the potential scenarios and steps required. Exercises that help all market participants better understand the actions they would need to take and pre-identify risks that could arise as a result would therefore be a useful initial step toward addressing concerns related to systemic concentration. Given the cross-border nature of the IT services provided it is likely that for a major failure of a provider such as a CSP, coordination between authorities would be necessary.
- **Supervisory information sharing and collaboration**: To contribute to globally consistent regulatory and supervisory approaches to outsourcing and third parties, we encourage establishing a mechanism for supervisory information sharing and collaboration. This could help to combat issues in relation to common terminologies, scope, standards, measurement of cross-border concentration risk and data access.
- Align policies and standards with internationally accepted standards. As there is strong concentration on the Cloud providers (Amazon, Google, Microsoft), coordinating audits and/or prudential oversight including adherence to regulatory compliance and European law on these providers on their offering to European FI's could benefit all European FI's and their customers. Dependency on those -even as an n-th party- is unavoidable.
- To achieve this objective, it might be useful to have a harmonized set of criteria and definitions for terminology (such as 'critical/essential process'), along with some kind of international register standard.
- Better and more consistent usage of pooled audits to broaden their coverage. This requires a reliable framework and consistent expectations from the supervisory authorities. Work should not start from scratch, but build on existing initiatives, such as the Collaborative Cloud Audit Group (CCAG).
- Promote developing and leveraging the third-party utilities platform through published minimum standards and allowing FI's time to implement e.g. KY3P, TruSight or use pooled audit reports which are audits paid for by a group of FIs that use the same third party for similar products or services.

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?

Responding quickly and providing the necessary investment during the pandemic ensured that operational resilience was maintained, despite increased pressure on the organisation. The rapid response to the pandemic and the enhanced collaboration with the Banks regulators made effective risk management possible.

Overall, critical suppliers have performed well during the pandemic, with a limited number of real issues outside of temporary breaks in service delivery or reduced SLAs. Regular interactions and check-ins have been key, particularly around topics such as home working, the effectiveness of business continuity plans, and financial stability.

The implementation of reinforced monitoring processes dedicated to the most significant services has made it possible to mobilize the outsourcing actors, and to constantly verify that the suppliers have remained able to deliver the expected services. The COVID-19 crisis therefore made it possible to verify that the system put in place had a real added value in terms of risk control and operational continuity.

There is an increased risk posed by the financial resilience of smaller third parties post COVID-19, with a difficulty in managing this risk being that a large amount of the data used to establish the financial resilience of third parties being publicly available information, is historic and not live nature means it is difficult to have an up-to-date view of third parties financial resilience.

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Blazej Blasikiewicz
Director
b.blasikiewicz@ebf.eu
+32 2 508 37 32