Comments

Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities - Consultative document

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Dr. Christoph Kunze
Telephone: +49 30 2021-2325
Telefax: +49 30 2021-192300
E-mail: c.kunze@bvr.de

Berlin, 18 August 2023

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

Chapter	Question No	Question	Proposed Answer
1	1	Are the definitions in the consultative document sufficiently clear and easily understood? Are there any important terms and definitions that should be included or amended?	Criteria of critical services or third parties: We suggest considering the methodology to assess the critical services/third parties aligned with the EBA guideline on outsourcing. There are also ongoing discussions on the definition of criticality within the amending DORA consultations to avoid unnecessary divergences, which could be considered here. Third-party definition: We support FSB in excluding the FMIs from the Third-party definition. To support consistency, back office of FMIs should not be part of the third-party definition and not part of the scope for holistic risk management, although your principle says to oversee engagements beyond outsourcing. We suggest consistent use of definition of service provider, as outlined in EBA's Outsourcing guidelines, which highlights the entity rather than individuals. (EBA definition: Service provider means a third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement.) Potentially the definition should be further clarified. We suggest to also exclude Third party relationships of minor extent, e. g. one-off or occasional purchases of goods and services.
2	2	Are the scope and general approaches of the toolkit appropriate?	To enhance risk orientation of the toolkit, section 3.4 should also be limited to critical services, or at least services of minor extent be excluded from extensive register requirements. In general, we agree with the principles of proportionality and holistic risk management. Yet, it should also be considered that the existing requirements for outsourcing arrangements have worked well. The definition of outsourcing and the focus of detailed regulatory requirements based on it already include a risk orientation that is fundamentally appropriate. In this respect, there is no need to extend outsourcing rules more or less to all third party services. An alternative approach would be to merely formulate some supplementary requirements for critical third party services that are not yet explicitly covered by existing regulatory requirements.

			It is unclear, whether we need to continue to monitor the FMIs, as they are suggested to be excluded from the Third-Party but the scope of monitoring is recommended beyond outsourcing. It is foreseen that intra-group service provider may also include a financial institution's branches amongst others. We recommend not to declare a financial institution's branch as an intra-group service provider. This should be considered as intra-bank services from a company law perspective and not as a third-party arrangement. A non independent branch of a financial institution is part of the same legal entity and therefore subject to all operational and organizational processes/procedure with no restrictions.
	3	Is the toolkit's focus on regulatory interoperability appropriate? Are there existing or potential issues of regulatory fragmentation that should be particularly addressed?	A common understanding of critical or important / material service definition across jurisdictions would be preferable. There are currently fragmented requirements in the measures where FSB is looking to assess the potential systemic risks and interdependencies. These include regulatory pre-notification on material outsourcing, Register and incident Reporting, where there are opportunities for consistency and harmonization for FIs to implement sustainable processes. For example, the incident reporting caused by third-parties are required to be reported via various channels depending on the nature of the incident (I.e. cyber incidents, PSD2 reporting, ECB IMAS reporting and upcoming DORA). There are also divergent requests on register and pre-notification requirement to be re-visited for standardization (wherever possible).
	4	Is the discussion on proportionality clear?	In relation to the intra-group services the paper says risk based approach may be leveraged. Please note that the risk based approach could be interpreted as a synonym of proportionality, in which case there would be no more differences between approaches to Third Party and intragroup arrangements. Given the above, instead of risk based approach we propose to say that companies may use effectively their internal group-wide policies and controls to manage intragroup arrangements risks.
3	5	Is the focus on critical services and critical service providers	Assessing the substitutability of a service and of possible actions (e.g. contingency and business continuity plans) is part of the risk management for critical services, but not necessarily of the initial criticality assessment.

		appropriate and useful? Does the toolkit provide sufficient tools for financial institutions to identify critical services? Do these tools rightly balance consistency and flexibility?	We suggest that no risk assessment is required if "non-outsourcing" providers, are not seen as a provider for critical services.
	7	What are the potential merits, challenges and practical feasibility of greater harmonisation of the data in financial institutions' registers of third-party service relationships?	On one hand it could support globally active financial institutions to create a common, jurisdiction agnostic register, however on the other hand there is a risk that very detailed information about Third Party relationships will need to be applied. We observe multiple initiatives globally. However, what should be highlighted is that there are types of data not required in other jurisdictions or that are limited to material outsourcing, whereas EU regulation (i. e. draft ITS on DORA) requires very detailed information. Greater harmonization, in form of a restriction to essential information, would generate cost and process efficiencies. It will help with common terms and definitions across the third-party life cycle. To enhance risk orientation of the toolkit, extensive register information requirements (if kept) should be limited to critical services, or at least services of minor extent should be excluded. FSB asks for regular update on new/planned material arrangements or significant changes to existing services. The criteria seem more appropriate for the pre-notification (an event driven report) before the contracts are signed off. Clarification would be helpful whether FSB is looking for a pre-notification or the post reporting to clearly assess the implications of this requirement.
	8	Are the tools appropriate and proportionate to manage supply chain risks? Are there any other actionable, effective and	In general, the expectations should focus on supply chains for critical services and relevant nth-party service providers for these services. Whilst obtaining transparency of the nth supply chain is understandable, the risk should be managed on proportionate basis, focusing on the material sub-contractors.

		proportionate tools based on best practices that financial institutions could leverage? Are there any other challenges not identified in the toolkit?	
	9	What do effective business continuity plans for critical services look like? Are there any best practices in the development and testing of these plans that could be included as tools? Are there any additional challenges or barriers not covered in the toolkit?	Extensive expectations on business continuity planning should be focussed on time-critical services. The toolkit covers all material aspects of effective BCM planning and testing, additional tools are not necessary in our view.
	10	How can financial institutions effectively identify and manage concentration and related risks at the individual institution level? Are there any additional tools or effective practices that the toolkit could consider?	We favour that no prescriptive approach should be specified. The indications under sections 3.8.1 and 3.8.2 are sufficient. To consider concentration risks on broader supply chain, fourth party/supply chain dependencies, in addition, to consider the risk aggregation including the non-critical services, which may also have systemic interdependences as accumulated effect in the financial market
4	12	Is the concept of "systemic third-party dependencies" readily understood? Is the scope of this term	The concept is clear, however the scope of the term may be narrowed to financial sector critical service providers.

		appropriate or should it be amended?	
	13	How can proportionality be achieved with financial authorities' identification of systemic third-party dependencies?	Supervisors already collect information, especially on critical and/or material outsourcing arrangements across financial institutions, which may be used to determine which service providers are sector critical service providers. Imposing new reporting obligations to financial institutions is not necessary from our point of view. If this is nevertheless planned, requirements should be limited to information that is essential for risk assessment.
	14	Are there any thoughts on financial authorities' identification/designation of service providers as critical from a financial stability perspective?	The Third Parties in relation to which any incident or disruption may severely impact a significant portion of market participants and consequently the global and local financial markets may be indicated as critical from a financial stability perspective.
	15	Should direct reporting of incidents by third-party service providers within systemic third-party dependencies to financial authorities be considered? If so, what potential forms could this reporting take?	Third Parties may be required to report incidents to their service recipients instead of direct reporting. Usually, they are obliged to do so by contract. We would suggest more holistic approach by harmonizing the existing incident reporting framework, define roles and responsibilities with clear objectives on the reporting. Without such baseline, it would create confusion and inefficiencies. There is significant resource implications expected both from FIs and third parties for your consideration. Such direct reporting, however, should be limited to serious incidents affecting critical services heavily.
	16	What are the challenges and barriers to effective cross-border cooperation and information sharing among financial authorities? How do these	Challenges: different timelines and requirements re: incident notification, different scope of information gathered by supervisors around the world, different regulatory structures, interoperability in the resolution planning, level of due diligence as of local regulators' requirement, operational resilience, harmonization of the data.

		challenges impact financial institutions or service providers?	
	17	Are there any views on (i) cross border information sharing among financial authorities on the areas covered in this toolkit (ii) including [certain third-party service providers] in cross-border resilience testing and exercises, including participation in pooled audits and?	We observe already existing network for sharing the information across the jurisdictions, however, the requirement should be more specific on what kind of information is being shared by supervisors (some information related to third-party providers might be highly sensitive and may expose financial authorities, financial institutions or the service providers to legal and reputation risks).
	18	Are there specific forms of cross-border cooperation that financial authorities should consider to address the challenges faced by financial institutions or service providers?	Greater convergence of regulatory and supervisory frameworks around systemic third-party dependencies is seen beneficial. Potential requirements on information sharing should be more specific.

***