German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

Principles for the sound management of third-party risk (BCBS 577)

German Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Christina Pfaff
Telefon: +49 30 20225-5427
E-mail: christina.pfaff@dsgv.de

Berlin, October 08, 2024

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:
German Savings Banks Association
Charlottenstraße 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

General comments

The basic approach of the principles in adopting a holistic approach to assessing risks from arrangements with third-party service providers (TPSP) is understandable. However, we consider the requirements of the draft to be too broad and not sufficiently differentiated according to risk and materiality aspects of the arrangements commonly used by banks. Banks often have hundreds to thousands of contracts of various types and relevance. But the definition of "third party arrangements" would encompass almost all external services, which we regard as disproportionate. In addition to 'classic' outsourcing, there are generally numerous arrangements of a minor scope and/or with minor risks, as well as more or less 'no alternative' services. We would just like to mention a few examples:

- Contracts with municipal utilities (water, waste, etc.)
- One-off or temporary consultancy contracts
- Obtaining short-term support (temporary workers, temporary employment agencies)

In view of these circumstances, the level of requirements in the principles for the TPRM appears to us to be too high overall: according to the consultation paper, the vast majority of the requirements are intended for all arrangements, and in some places even go beyond what is currently only required for critical/material outsourcing (e.g., the requirement for exit strategies). Potential adverse effects of overly strict requirements for all types of TPSP arrangements should be considered when finalising the principles:

- Arrangements with smaller service providers and individuals could effectively be prevented because they are not in a position to fulfil all requirements. Larger service providers might not be willing to accept banking sector requirements and contractual conditions that are deemed too strict and/or unreasonable.
- The use of third-party services - which in themselves make sense - could be prevented altogether in certain areas. This would result in increasing concentrations (use of fewer providers) and higher costs and can also limit the innovative strength of banks.
- Competitive distortions can arise from corresponding disadvantages for banks compared to non-banks (e.g., insurance companies, NBFIs) to which these requirements do not apply. In addition, smaller regional banks may be at a disadvantage within the banking sector due to the comparatively higher fixed costs of the TPRM and lower negotiating power vis-à-vis service providers.

We consider a strong clarification of the proportionality principle to be necessary, in the sense that fulfilment of the requirements can be appropriately graded according to the risk content of the arrangement and that not all requirements need to be implemented for less risky and/or small-scale (non-material) TPSP arrangements. In addition, we believe that initial clarifications and restrictions to the scope of application are urgently required (see our specific comments).

Depending on the design of the final principles, extensive challenges will arise during their implementation: Legislators and supervisory authorities might have to adapt regulatory architectures geared towards 'traditional' outsourcing. Banks will have to review, evaluate, and renegotiate hundreds to thousands of existing arrangements, in addition to developing new strategies, guidelines, tools, etc. This would require a sufficient implementation period of several years.

Lastly, while the subject of this consultation intends to replace the 2005 Joint Forum Paper in respect of the banking sector, it should be specified how the Principles relate to the existing BCBS principles relevant to third-party risk management, such as Principles for operational resilience and the Principles for the sound management of operational risk. The reference to the Principles being "read in conjunction with" existing principles and guidance, could be interpreted differently: For example, it is not clear whether the Principles are intended to be an expansion of those existing principles and guidance or if the Principles are intended to define a separate and parallel rule, referring only the specific definitions and guidance expressly referenced.

Specific comments

Definitions (Para. 11)

TPSP
It would be difficult or impossible to apply many of the requirements formulated in the principles to individuals. These should be removed from the definition.

TPSP arrangement
From a risk perspective, many of the proposed principles are not necessary for all types of arrangements or, in some cases, could not be fully implemented. The following further exceptions should be integrated in the definition:

- one-off, occasional and/or minor services,
- statutory/regulatory or otherwise mandatory services (e.g., audits),
- services that banks typically do not (or cannot) provide themselves, such as facility management, utilities, goods purchasing.

We suggest developing a whitelist comprising services that do not relate to actual banking operations and are thus out of scope of TPRM.

Critical TPSP arrangement
For a categorisation as a 'critical' TPSP arrangement and the associated application of extended requirements, a certain materiality should be given, not just any (possibly only indirect) reference to critical services. Please clarify this.

Key nth party
When determining 'key' nth parties, the categorisation should not have to be based on a minor contribution to the provision of a critical service. As well, the access of an nth party to confidential information should also not automatically result in categorisation as a 'key'. We ask for clarification that the circumstances and significance of the nth party for the provision of critical services by the TPSP should be considered as a whole.

Third-party risk management principles

Para. 15 (Key concepts)
The options for a proportional design of the TPRM should be further clarified. For example, it could be added that significantly simplified approaches are permissible for certain types/classes of low-risk arrangements, such as summarised brief assessments. See also our general comments and notes on the overly broad definitions.

Para. 22 (Risk management)
The requirement to map dependencies and links between arrangements should not be interpreted as requiring the use of special tools for this purpose. Proportional solutions should be possible. This should also be clarified in the wording of paragraphs 45 and 49.

Para. 23 (Risk management)
The requirements partially overlap with BCM and could therefore be streamlined. At least, the example ('eg testing at more frequent intervals') in the third sentence should be omitted, as it is not clear how this could reduce concentration risks.

Para. 24 (Strategy)
Strategic determinations on the use of TPSP can also be part of the business strategy. We suggest the following rewording:
„The board of directors should approve a third-party strategy (which could also be part of the bank's overall business and/or risk management strategy and should be consistent with these strategies). ~~It should be consistent with the bank's overall business strategy, risk appetite and tolerance for disruption.~~ …"

In addition, the 2nd bullet point should refer to TPSPs, not to a single provider.

Para. 32 (Risk assessment)
Ongoing assessments are neither necessary nor useful. The wording should be changed to „… regularly and ad hoc in case of relevant events …".

Para. 38 (Relative benefits and costs)
In our opinion, banks should not be subject to regulatory requirements in terms of business considerations; an assessment (does the proposed TPSP arrangement make sense overall?) will be carried out in their own interest. We suggest deleting the section and, if necessary, integrating individual risk-relevant aspects into the corresponding section (paragraph 37).

Para. 41 (Contracting)
In order to clarify the proportionality more clearly, we suggest the following addition:
„Banks' contracts governing TPSP arrangements should consider, where relevant and appropriate: …"

Para. 42 (Contracting / critical TPSP arrangements)
The requirement in the last bullet point to prescribe insurance for all insurable risks for the TPSP is too far-reaching. We suggest the following wording: „TPSPs' obligation to take out insurance against material insurable risks"

Para. 44 (Onboarding)
The wording of this requirement is unclear. As the core points should already be covered by paragraph 26, we suggest deleting it.

Para. 49 (Ongoing monitoring)
Performance indicators cannot and need not be collected and monitored for all types of TPSP arrangements (see our general comments and notes on the overly broad definitions). This should be clarified.

Para. 58 and 59 (Business continuity management)
From a proportionality perspective, it should be considered whether these requirements should only apply to critical TPSP arrangements or arrangements that support essential time-critical processes

Para. 63 - 65 (planned termination)
Many TPSP arrangements of banks are designed for a permanent division of responsibilities. Detailed steps for termination are defined there on an ad hoc basis, i.e. when the termination of a specific arrangement is actively planned. Creating extensive termination plans for hundreds to thousands of arrangements, keeping them up to date and testing them regularly would create an unreasonable amount of additional bureaucratic burden. For the sake of risk-adequacy and efficiency, we suggest limiting the requirement to have exit plans to critical TPSPs in the first place. Also, detailed plans should only be required in the event of a specific intended termination.

Para. 66 and 67 (unplanned termination)
Overall, the requirements for exit strategies should only relate to critical TPSP arrangements. Disruptions or interruptions at other non-critical service providers are covered by BCM where necessary. Intragroup TPSP arrangements should generally be excluded from exit strategy requirements, in order to avoid unnecessary bureaucratic burden. Due to the mutual knowledge and influence within groups and financial networks, it seems very unlikely that such arrangements will be terminated unilaterally and unexpectedly.