CGAP | Empowering the Poor Through Financial Services

1818 H Street, NW, MSN F3K-306
Washington, DC 20433

CGAP comments on BCBS consultative documents on operational risk and operational resilience

The Consultative Group to Assist the Poor (CGAP) welcomes the opportunity to comment on the two sets of principles released in August 2020 for public consultation by the Basel Committee on Banking Supervision (BCBS):

1) Principles for the Sound Management of Operational Risk (PSMOR)
2) Principles for Operational Resilience (POR)

CGAP would like to contribute to the BCBS' important efforts to strengthen operational resilience and operational risk management, by sharing comments and recommendations that put special emphasis on recent market developments of high relevance to financial inclusion and innovation in emerging markets.

Overarching comments

Banking is going through fundamental transformations based on technological advancements and increased dynamism and competition. Two main developments behind such transformations are:

1) The fast growth in **cloud computing outsourcing** to cover an increasing range of activities and functions, including recovery strategies of banks.
2) The **modularization of banking** whereby banks become a piece of the whole banking services value chain, and set up outsourcing and partnership arrangements with third parties, unregulated nonbanks and non-financial companies that may control customer relationships, product design, or strategic decisions (eg Banking-as-a-Service (BaaS)).

In many emerging markets, these developments are fostering increased access and use of financial services by underserved and unserved consumers, while potentially increasing the complexity and risk profile of those services. These developments could impact the implementation of the PSMOR and POR. Thus, it will be important to provide supervisors with specific guidance on how to account for the effects of cloud computing outsourcing and modularization of banking on:

1) the effective implementation of the PSMOR and POR;
2) the need to adapt regulatory and supervisory frameworks;
3) the design and adoption of appropriate solutions for related cross-border issues; and
4) operational resilience, competition, innovation, and financial inclusion in the banking sector.

Supervisors in emerging markets that are aiming to enable financial inclusion and innovation while preserving stability will benefit from specific guidance by the Basel Committee. This guidance is needed as a complement to the Financial Stability Board's higher-level discussions on macroprudential and microprudential issues[1], and to regional initiatives like the guidance by the European Supervisory Authorities (EBA, EIOPA and ESMA) on cloud computing outsourcing arrangements. It is worth noting that these initiatives are already influencing emerging market authorities to adopt regulatory and supervisory reforms (eg requirements, guidance or supervisory expectations for cloud computing outsourcing in Brazil, Pakistan, South Africa).

General recommendations

The topics of cloud computing outsourcing and modularization of banking should be explicitly incorporated in different sections of PSMOR and POR:

1. **Introduction and Evolving Landscape**
   - The POR's introduction and section "An evolving operational risk landscape" should mention cloud computing outsourcing. For instance, one of the reasons why banks were able to rapidly adapt their operational posture in response to Covid-19 was their use of cloud computing.
   - The PSMOR should also have a section on evolving landscape (and be referenced in the POR, in case the two documents remain separate), which could address overarching issues that do not fit specific principles.
   - One topic that could be singled out is the need to explore solutions to the limits of the prevailing institution-based approach to regulation and supervision vis-à-vis the shifting allocation of responsibilities and accountability within cloud computing outsourcing and modularization arrangements. There is a need for a combination of regulation of institutions with regulation of infrastructure (eg cloud computing providers) and regulation of activities (eg "modules" of the banking value chain).[2]
   - Another topic is the complexity introduced by cross-border outsourcing arrangements in the assessment of risk management frameworks. For example, there is a risk of global and regional concentration of cloud computing outsourcing in a few cloud services providers (CSPs), most of them based in the US with data storage and processing centers spread over many countries. While this is key to realize some risk-mitigating benefits that enhance resilience, it leads to practical regulatory, supervisory and resolution challenges related to data protection, data sovereignty, access and audit rights by authorities, data portability, and jurisdiction over CSPs. Specific guidance and practical support (eg collection and dissemination at the global level of information about concentration in major CSPs) could be helpful for supervisors.

[1] In particular, "Third-party dependencies in cloud services: Considerations on financial stability implications", December 2019.

[2] There is ongoing discussion in Europe and the US on the merits of and potential approaches to regulating cloud services providers, which could have repercussions in emerging markets.

2. **Text of specific Principles**
   - PSMOR 9 (items 50-54), PSMOR 10 and PSMOR 11 should explicitly mention cloud computing outsourcing.
   - POR 5 should explicitly refer to modularization of banking.
   - See next section for specific recommendations.

3. **Role of supervisors**
   - The relevant section at the end of PSMOR should incorporate additional guidance for supervisors on cloud computing outsourcing and modularization of banking.
   - The POR should add a section on this topic that includes guidance for supervisors on cloud computing outsourcing and modularization of banking and how they impact assessment of operational resilience at banks.
   - Supervisors should adopt approaches that balance the potential benefits (eg competition, innovation, inclusion, efficiency) and risks of modularization of banking. Such approaches may include "modularization" of regulation, by incorporating an activity-based perspective as a complement to the prevailing institutional focus. Such an approach could require revision to the legal liabilities before consumers and responsibilities for regulatory compliance, which today rest solely on the bank. It would require the establishment of a supervisory framework for at least major nonbanks active in modular banking value chains.

An alternative to the above suggestions would be an annex, or an independent publication that deals with these market developments. This would allow a more extensive discussion of the issues, challenges and opportunities brought by these developments to the implementation of the PSMOR and POR. However, we still see value in making explicit mention to such developments in the PSMOR and POR.

Specific recommendations

The PSMOR and POR should address the following key points[3]:

1. **Banks that implement material cloud computing outsourcing may suffer profound, impactful changes, and would benefit from a cloud strategy and management framework, rather than relying solely on general outsourcing policies. Experience has shown[4] that lack of dedicated planning and attention to material cloud outsourcing can increase risks. Specialized skills and knowledge are needed at both the bank and the supervisory agency.**

[3] The intent is not to be comprehensive. There are many areas not covered in the comments that may be relevant in the implementation of PSMOR and POR when cloud computing outsourcing and modularization are present, for instance, the issues related to cyber-security.

[4] Eg "Outsourcing involving cloud computing services". Information Paper, Australian Prudential Regulation Authority, 24 September, 2018.

- Add to PSMOR 4, 5, 6 and POR 1, 2:
  - *Banks should have an appropriate governance and risk management framework for cloud computing outsourcing, as well as specialized skills to assess, monitor and mitigate the risks of outsourcing and the controls put in place by cloud service providers (CSPs). Cloud computing risks must be specifically addressed in a bank's operational risk management framework and risk governance structure.*
- Add to Role of supervisors:
  - *Supervisors may need to invest in specialized expertise to adequately assess banks' governance of cloud computing outsourcing.*

2. **There could be strategic and operational risks, including to operational resilience, in not shifting to cloud computing and relying on outdated legacy systems.**
   - Add to Role of supervisors:
     - *Supervisors should assess such risks at least in the largest institutions, particularly when considering measures that limit or delay adoption of cloud computing outsourcing in their jurisdictions.*
   - Add to PSMOR 2, 4, 5, 6, 7 and POR 1, 2:
     - *Banks should incorporate the analysis of risks specific to cloud computing outsourcing in their risk appetite and tolerance statements, as well as their operational risk framework and governance structure, including their policies and procedures for approving and implementing changes to processes and systems. A bank's risk investments in cloud outsourcing should result from the intersection of risk management, business and IT strategies.*
   - Add to PSMOR 4, 5 and POR 2, 3, 4:
     - *Banks' scenario and stress testing to identify events that may push them outside risk appetite and tolerance limits should specifically consider cloud computing outsourcing risks.*
   - Add to PSMOR 5, 6, 7 and POR 2, 3, 4, 5:
     - *Banks should have enterprise-wide policies and processes for engaging in, and managing risks of, cloud computing outsourcing. Banks should ensure that staff charged with identifying and evaluating cloud outsourcing risks have the necessary experience and expertise.*
   - Add to PSMOR 7 and POR 2, 3, 4, 5:
     - *Banks planning or implementing a total or material shift from legacy data architecture to cloud infrastructure should do a thorough analysis of the risks involved.*
   - Add to PSMOR 7 (37) and POR 2:
     - *The three lines of defense should be engaged in changes of data architecture and even minor outsourcing to cloud applications.*

3. **There are concentration, vendor lock-in and CSP dependency risks in cloud computing outsourcing. The levels of dependency and vendor lock-in risks increase as outsourcing**

moves from IaaS to SaaS, and due to the parallel provision of non-cloud services (eg big data analytics, machine learning). Interconnectedness of banks could increase through concentration in a few CSPs. The lack of data interoperability across CSPs and between the cloud and in-premise architectures can limit the resilience-enhancing benefits of cloud computing outsourcing, increase lock-in risk and limit exit strategies.

- Add to Role of supervisors:
  - *Supervisors should collect information on cloud computing outsourcing arrangements, possibly keeping a database with the main CSPs, key sub-contractors (whenever possible), mapped to current material/strategic outsourcing at least at the largest banks. Such mapping could identify the cloud outsourcing models and services involved.*
  - *Supervisors should monitor concentration risk and interconnectedness related to cloud computing outsourcing in their jurisdictions, from a microprudential and a macroprudential perspective.*
  - *Supervisors should consider solutions to address concentration risk, including negotiating with systemic banks, when appropriate, the adoption of hybrid and multi-cloud models, or even imposing certain requirements (eg redundancy). Supervisors may consider the need to impose requirements or oversight directly on systemic CSPs.*
  - *Supervisors should encourage or require the banking industry to develop technical solutions for data/cloud interoperability.*
- Add to PSMOR 4, 5, 6, 9 and POR 2, 3, 4, 5:
  - *Banks should assess concentration, vendor lock-in and CSP dependency risks in cloud computing outsourcing, including by analyzing the nature and relevance of the outsourced services/activities, and sub-outsourcing conducted by CSPs.*
- Add to PSMOR 9, 11 and POR 2, 3, 4, 5:
  - *Banks should have appropriate risk mitigation and transfer strategies vis-à-vis cloud computing outsourcing, including potential risks of vendor lock-in, high dependency on CSPs, non-substitutability of CSPs, and interconnectedness to other banks through CSPs. The potential unviability of terminating or transferring a CSP contract without major disruption should also be considered in a bank's business continuity plan and contingency arrangements.*

4. **Certain aspects of the current regulatory and supervisory framework for outsourcing (eg concept of materiality, limitations, requirements for prior approval) may not be appropriate for all cloud computing outsourcing and sub-outsourcing.**
   - Add to Role of supervisors:
     - *Supervisors should assess the need to update their regulation and supervisory procedures and expectations to address cloud computing outsourcing and sub-outsourcing (eg authorization requirements).*

5. **Cross-border cloud outsourcing may face legal inconsistencies that create challenges for data flows and increase legal risks for banks. Obstacles to data flows could also reduce the risk mitigation and resilience benefits of using the cloud.**
   - Add to Role of supervisors:
     - *Supervisors should be cognizant of the risks faced by banks engaging in cross-border cloud computing outsourcing, and consider specific measures to address risks, including adjustments to requirements pertaining to business continuity and contingency arrangements.*
     - *Supervisors should carefully weigh the potential benefits and downsides of data localization and location requirements before imposing them.*

6. **Geographically dispersed data management and multi-tenant cloud infrastructure pose challenges to audit and risk assessment methods traditionally deployed by banks, the exercise of supervisors' and resolution authorities' audit and access rights, and business continuity testing, regardless of the criticality of the services provided by a CSP to a bank.**
   - Add to PSMOR 9, 11 and POR 2:
     - *Banks could be allowed to use credible alternatives to current audit and assessment methods (eg specialized audits and certification). Banks should ensure that their methods to assess and audit CSPs are effective, regardless of the service types and models adopted in each cloud outsourcing arrangement.*
   - Add to Role of supervisors:
     - *Supervisors should coordinate and collaborate with authorities in countries where systemic CSPs are based or data is stored/processed, to ensure that the mandate of supervisors and resolution authorities can be effectively discharged, including timely access to data, and to set up a framework to deal with operational disruptions and cyber incidents at CSPs.*

7. **With modularization of banking, aspects of risk management may be totally or partially conducted by several third parties under a complex web of commercial relationships. This complexity may hinder banks' ability to implement a comprehensive operational risk management framework and increase their reputational -and other- risks, while keeping them liable for the whole banking value chain.**
   - Add to Role of supervisors:
     - *Supervisors should monitor the emergence or increase in the use of BaaS or similar business models in their jurisdictions, to assess whether the regulatory and supervisory frameworks need to be updated.*
   - Add to PSMOR 2, 4, 5, 6 and POR 2,3:
     - *Bank's boards and senior management should articulate how adoption of modularization impacts the effectiveness of the operational risk management framework, clearly identifying the responsibilities of different parties in the value chain in managing risks that can impact the bank.*
     - *Banks should have a clear view of how modularization may impact risk assessment and monitoring, control activities, information and communication.*