Challenges in supervising banks' large exposures[1]

Executive summary

Recent failures to manage counterparty risk serve as a reminder of the need to control and limit risk concentrations. The origin of the failure of Archegos Capital Management, a family office of a former hedge fund manager, can be found in the concentrated risk exposures that it built up and mismanaged. Archegos built large and highly leveraged equity positions through total return equity swaps with several banks who were unaware of its overall positions and had also, in the case of Credit Suisse in particular, insufficiently collateralised their exposure to the family office. When the value of these positions contracted sharply, Archegos defaulted on its margin calls, with several of the exposed banks suffering large losses.

Regulators have long recognised the need to prevent banks from becoming overexposed to a single counterparty. This is because such a concentration exposes a bank to disproportionately large losses should this counterparty fail. Accordingly, the need to limit the size of these exposures is a fundamental principle of prudential regulation and ensuring that banks abide by such regulation is a core component of banking supervision. This principle forms the basis of the large exposures (LEX) standard issued by the Basel Committee on Banking Supervision (BCBS), which complements the risk-based capital standards.

Multiple supervisory challenges make this standard difficult to enforce and partly explain the wide ranges of jurisdictional practices. These challenges, difficulties and ranges of practices relate to the supervisory authority's ability to conduct case by case assessments and use its supervisory judgment as such assessments are needed throughout the standard. Challenges include those related to the ability to determine whether exposures are connected or not; whether exposures fall within the scope of the standard or constitute special cases that warrant specific treatments or exemptions; whether and to what extent exposures are mitigated; and how to treat breaches. These challenges, and how supervisory authorities have sought to overcome them, are discussed in this paper.

The first set of challenges is to identify and assess groups of connected counterparties. Connected counterparties are those that have relationships such that, should one of the counterparties fail, the others would very likely fail. Establishing interconnectedness generates an assumption that exposures to these counterparties constitute a single risk. To determine whether counterparties are connected, banks must use control relationship criteria and economic dependence criteria. In practice, establishing interconnectedness does not always lead to aggregating the exposures. This is because the criteria may not be sufficient to establish a connection between the counterparties or because the connection is not sufficiently strong to consider that the exposures constitute a single risk. When this takes place, the supervisor determines whether the exposures constitute a single risk or not based on the bank's analysis.

Another set of challenges is the lack of common criteria applicable to all exposures. There are various approaches that are specific to certain exposures under the LEX standard, and specific approaches may need to be designed to address jurisdictional challenges. Examples of specific treatments include the valuation of trading book positions. Exemptions include entities connected with sovereigns or intraday bank exposures. Examples of jurisdiction-specific treatments relate to intra-banking group

[1] Vasily Pozdyshev (Vasily.Pozdyshev@bis.org), Jean-Philippe Svoronos (Jean-Philippe.Svoronos@bis.org), Bank for International Settlements, and Rize-Mari van Zyl (Rize-Mari.vanZyl@resbank.co.za), South African Reserve Bank Prudential Authority. The authors are grateful to Rodrigo Coelho and Jatin Taneja for helpful comments. We are also grateful to Anna Henzmann and Marie-Christine Drexler for valuable administrative support with this paper.

exposures or to supervisory carve-outs which may be temporarily granted in special situations such as mergers and acquisitions and resolution.

The complexity involved in assessing credit risk mitigation (CRM) techniques is an additional challenge for supervisors. While the LEX standard requires that banks report both gross and net large exposures, additional information is necessary to enable a supervisor to check the effectiveness of CRM instruments. To ensure that the instruments provide sufficient legal certainty to be eligible as CRM techniques, the supervisor would need to review all relevant contractual documentation for all instruments used. For financial collateral, this would include verifying the collateral's existence, that it is effectively available and unpledged, and that it is prudently valued. For guarantees, this would imply the ability to assess the credit quality and financial position of the guarantor and, for credit derivatives, the need to verify and ensure that the underlying reference entity and default events are such that the protection would effectively be triggered, and the pay-out would take place should the bank's counterparty default.

The treatment of breaches constitutes a final set of challenges. While limit breaches are meant to be exceptional and should be reported and addressed immediately, this is not always the case in practice. A supervisor typically becomes aware of a breach when it is informed by the bank. Force majeure and unpredictability may qualify a breach as exceptional because it was caused by reasons beyond the bank's control or because it was unforeseeable by the bank. However, there are also breaches caused by risk management deficiencies, faulty controls, or poor governance. Although contents vary, remediation plans typically include three types of measures. These are measures to reduce the size of the exposure or increase the bank's capital position, ones to reinforce the bank's risk management and internal controls, and ones to ensure the plan's execution. For non-exceptional breaches, remediation plans are combined with corrective measures, more intensive supervision, possible downgrades of the supervisory rating and fines.

Automated tools could increase the efficiency of supervisory oversight. The supervisory challenges associated with the standard's implementation are such that supervisory authorities do not have the resources to ensure that all large exposures at all reporting banks are comprehensively controlled. Several jurisdictions are therefore considering or developing automated tools to address these limitations. Tools include automated cross-checks across banks to compare groups of interconnected exposures declared by banks. A supervisory database containing groups of connected counterparties could constitute a common supervisory tool that would help to ensure consistent reporting across banks and jurisdictions. Another type of tool would be one allowing a supervisory authority to identify exposures and situations that may lead to breaches.

International cooperation and guidance could promote the sharing and development of common supervisory practices. This could include sharing interconnectedness case studies and additional interconnectedness criteria based on supervisory practices. International guidance could be useful for harmonising practices related to the detection, analysis and resolution of limit breaches and harmonising reporting requirements for periodic reporting and breach reporting. There could also be value in developing common reporting templates and guidelines that would lay out how the standard should be enforced by supervisory authorities.