Managing Concentration Risk: Large Exposure Framework

Abstract

Regulators and central banks all over the world have highlighted the importance of monitoring exposures to one or more counterparties that are connected either financially or operationally. The connected counterparties usually exhibit very high degree of default correlation. The credit event taking place at one or more connected counterparties, can potentially impact the solvency of the bank having exposure to these counterparties.

This paper highlights the salient features of the Basel Committee on Banking Supervision (BCBS)’s Supervisory Framework for Measuring and Controlling Large Exposures regulation (BCBS 283) as applicable to the management of large exposures to connected counterparties. It also discusses its impact on banks, challenges in complying with the regulation, and suggests remediation measures.
BCBS 283: What and Why

Recent financial crises have demonstrated many shortcomings in the financial risk models in use today. One key loophole is the concentration of exposure to one or more related counterparties.

In the standard risk based capital framework, the risk mitigation measures are oriented toward individual counterparties. One of the key reasons for the 2008 global financial crisis was banks' failure to adequately measure and control their exposures to individual and connected counterparties. Concentrated exposures to individual or connected counterparties can threaten the solvency of banks leading to their failure, which in turn has a far-reaching impact on the financial services sector.

To address the potential threat to individual banks and the financial services sector as a whole, the Basel Committee on Banking Supervision (BCBS) published the Supervisory Framework for Measuring and Controlling Large Exposures in April 2014 for the identification, mitigation, and reporting of large exposures to related counterparties. The aim of the large exposure regime is to prevent banks and financial institutions from incurring disproportionately large losses as a result of failure of individual counterparties or a group of connected counterparties (see Figure 1).

### Figure 1: BCBS' Guidelines on Large Exposure Framework

- **Identification of connected counterparties**
  - Control relationship: When one counterparty directly or indirectly has control over the other(s).
  - Economic relationship: If financial difficulties related to funding and repayment experienced by one counterparty results in other counterparties facing problems.

- **Calculation and aggregation of large exposures and CRM**
  - Both on- and off-balance sheet exposures to be considered.
  - SA-CCR EAD risk measure to be used for the exposure calculation for all OTC derivatives transactions.
  - CCF method to be applied for off balance sheet exposure calculations for off balance sheet items.
  - Collaterals (such as cash, gold, debt securities with adequate level of credit rating, mutual funds and equities) that are recognized under Standardized Approach defined by BASEL II are eligible for risk mitigation.

- **Limit monitoring and reporting**
  - Total exposure values to a non-G-SIB counterparty or group of non-G-SIB counterparties must not exceed 25% of eligible tier 1 capital.
  - Total exposure values of a G-SIB entity to another G-SIB counterparties must not exceed 15% of eligible tier 1 capital.
  - Banks must report top 20 exposures to connected counterparties and all exposures equal to or above 10% of bank's eligible capital base.
Impact, Challenges, and Possible Remediation

Achieving compliance with the BCBS 283 regulation on large exposure frameworks will impact the existing counterparty credit risk framework. Banks must therefore evaluate the changes required, analyze the implementation challenges, and identify the remediation measures before embarking on a compliance program.

Operational impact

As specified in the regulations, banks must devise a stringent mechanism to identify and correlate counterparties. To efficiently track the connections among counterparties or groups of counterparties, banks must monitor managerial and operational details and track connections among counterparties. Certain exposures such as qualifying central counterparties (Q CCP) exposures and sovereign exposures need to be identified and reported separately in cases where exposure is more than 10% of the eligible capital base.

Financial impact

The BCBS has mandated the adoption of the Standardized Approach for Counterparty Credit Risk (SA-CCR) to measure the Exposure at Default (EAD). The SA-CCR methodology uses risk multipliers to calculate EAD resulting in elevated EAD values. In case the EAD values exceed the set limits, banks will need to make a provision for additional capital. This will have direct financial impact on the bank. Banks with significant concentrated exposures should make provisions for additional tier-1 capital or mitigate the exposure by means of hedging, collateralization, or securitization.

Implementation challenges

Global banks conduct a large number of transactions across various risk classes and typically deal with a large number of counterparties. To establish the relationship within the group of counterparties, banks have to process a huge amount of financial, legal, and operational information related to these counterparties. Setting up the infrastructure to handle the huge amount of information and complying with the requirements of large exposure identification and reporting within timelines can be a big challenge.
To establish a managerial relationship between two or more counterparties, banks need to scrutinize the complete legal information regarding the constitution of all the counterparties. The legal and managerial obligations of the key stakeholders in other counterparties also need to be scrutinized. For instance, when a person in a key managerial position at one of the corporate counterparties holds a controlling stake in another counterparty to which the bank has exposure. In this case, the bank needs to obtain the detailed legal information of both the counterparties to establish the relationship between the two.

Banks are required to source and process the historical transaction data to establish the economic interconnectedness between two counterparties. For instance, where a substantial portion of the income of one of the counterparties is sourced from the other counterparties, detailed financial and operational information of all the counterparties involved is required.

The SA-CCR approach for calculation of exposure is more complex compared to the Current Exposure Method (CEM), and could also result in higher exposure values. Implementing SA-CCR method for Over the Counter (OTC) derivatives transactions with a long maturity may be a complex and resource intensive process. Similarly, implementing the Look-through approach recommended for the structured product may also be a long and complex process and will put more pressure on the resources of the bank.

The regulation also specifies that only instruments with residual maturity of one or more years are eligible for hedging. All other hedge instruments with maturity of less than one year shall not qualify for risk mitigation. As a result, a significant proportion of the exposure may remain uncovered. This increase in exposure may require the bank to raise additional tier-1 capital.

**What Banks Must Do to Ensure Compliance**

With the growing systemic risk in financial services, the large exposures regulation will help banks to identify and mitigate concentration risk, and restrict the loss a bank is likely to face in case of counterparty failure. The provisions made in the BCBS 238 regulation will likely increase operational overheads for banks that are already burdened with ever-growing regulatory compliance costs. Banks will need to devise a process to identify the connected counterparties, which is a
resource-intensive process. Beside this, banks with significant exposure to connected groups of counterparties may likely have to make an additional provision for tier-1 capital if the exposures are not mitigated.

On the process front, banks will need to tighten the Know Your Customer (KYC) norms and make it mandatory for the counterparties to provide complete information on managerial and legal control as well as operational and financial matters. This will not only help banks to comply effectively with the regulation but also safeguard them from adverse credit events in the future. These aspects should be covered under the bilateral disclosure agreement, and periodically updated and audited.

Banks will also have to periodically conduct stress tests on the connected counterparties to assess the possible increase in the exposure to the related counterparties, and provide for regulatory capital, if required. Banks may hedge the exposures appropriately in order to keep the capital requirement at an optimum level. With adequate amount of eligible collateral and securitization, banks can protect themselves from the concentration risk resulting from large exposures to connected counterparties.

With the framework scheduled to take effect from January 2019, banks must put in place a comprehensive implementation roadmap rooted in the people-process-technology triad to achieve timely compliance.

References


About The Author
Ashutosh Bhure
Ashutosh is a Domain Consultant with the Risk Practice of TCS’ Banking and Financial Services (BFS) business unit. He holds a Master’s degree in Financial Management from Pune University, India, and has over 20 years of experience in the areas of trading, clearing and settlements, surveillance, capital markets, and risk management. Before joining TCS, Bhure was associated with a leading stock and commodities exchange in India.

Contact
Visit the Banking & Financial Services page on www.tcs.com
Email: bfs.marketing@tcs.com
Blog: Drive Governance

Subscribe to TCS White Papers
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)
Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com