Yaseen Anwar: Operational risk management in Pakistan – issues and challenges

Opening remarks by Mr Yaseen Anwar, Governor of the State Bank of Pakistan, at the SBP Conference on Operational Risk Management organised by the State Bank of Pakistan, Karachi, 7–8 February 2013.

* * *

Good morning ladies and gentlemen!

Thanks for participating in this well timed conference on operational risk. The conference is part of SBP's ongoing efforts to promote the culture of awareness on critical issues that demand the attention of the financial services industry.

In the local context, credit market and liquidity risks have been the subjects of much discussion. Financial institutions have made significant progress in the management of these risks and Pakistani banks have considerably improved their processes for identification and management of credit and market risk exposures. By contrast, it is relatively difficult to measure the level of operational risk exposures on an enterprise wide level. The global financial crisis has also demonstrated the cost of operational risk failures. It has been observed that in several instances, the mitigation or transfer of credit and market risks actually gives rise to operational risk.

Accordingly, operational risk is gaining prominence and coming close to credit risk as the foremost safety and soundness challenge to the financial institutions. It is imperative for our banks to develop requisite capacities to manage their operational risks, collect their loss data, implement risk indicators and set aside capital to cover potential operational risk losses.

Operational risk is about instilling proper risk behavior at each level of an organization. Informal operational risk management frameworks have been in place in our industry. However, these informal frameworks are undocumented, lack consistency and do not provide desired level of assurance to senior management or regulators. Thus, it is necessary for risk managers to develop awareness of operational risk and effectively use the emerging management techniques.

Under the traditional approach of managing operational risk, the focus has largely remained on protecting the risk of loss of capital through insurance. Banks have relied on internal controls and audit functions. The increased use of technology in executing transactions have necessitated banks to focus more on core banking solutions, IT security and business continuity programs. While the traditional approach has its own merits, there is a pressing need that banks modify their fragmented approach of operational risk management in favor of a much more comprehensive governance and management framework. A framework comprising of clearly defined roles and responsibilities along with reporting procedures. I hope that this conference will promote active discussions on this issue.

Against this background, I am pleased to deliver the opening address in which I will cover three main areas. First, I will begin by offering my view on operational risk management – the issues and challenges. Next, I will discuss Basel Accord treatment of operational risk and emergence of sound principles on the topic. Finally, I will talk about some of the regulatory developments & supervisory expectations to strengthen the operational risk management within our banking sector.

Operational risk has always existed as one of the core risks in banking. But what constituted operational risk was never agreed until the Basel Committee on Banking Supervision (BCBS) came up with a definition. For this reason, Basel Accord may rightly be credited for promoting

the discipline of operational risk which recognized it as a significant risk and prescribed capital charge to protect against operational risk losses.

The BCBS defined operational risk as – *"the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events".* While the definition has determined four sources of operational risk (i.e. people, processes, systems and external events), there are a number of ways in which operational risk can actually manifest itself. It could be a failure of control function, major system breakdown, rogue trading, accounting scam, regulatory penalties, internal/ external fraud, diminishing number of qualified staff, terrorist attack, floods, earth quakes etc.

Since the scope of operational risk encompasses the entire organization and covers several dimensions. We, as banking professionals, need to consider the following points in defining any strategy to manage and mitigate operational risk.

- The source of operational risk is from the day to day activities of a bank. For this reason, operational risk management must initiate from the business unit level.
- There is misconception that operational risk management is solely about internal controls. Banks are good in minimizing high frequency low severity risk events but it is often *low frequency high severity events* that can jeopardize the existence of a bank. Hence we need to identify and analyze predictive key risk indicators and use scenario analysis to simulate the impact of irregular events.
- Good operational risk management is about finding and correcting the real cause of the incidents and not about the effects or observed events. Thus, while maintaining the history of losses is important for capital modeling, we need to realize that two identical events may have entirely different underlying causes. As a result, every operational risk event requires deeper investigation.
- Operational risk management is all about instilling proper risk behaviors. Thus changes in culture and governance needs to be institutionalized.

I believe these challenges can be overcome if banks adopt a systematic approach like the one prescribed by the Basel Committee. Let me briefly talk about the spectrum of approaches offered by Basel Accord to calculate operational risk capital charge.

Under the two simple approaches (i.e. Basic Indicator and Standardized Approaches), gross income is used as a proxy for the scale of business operations. This suggests that banks with higher gross incomes are relatively bigger in size and have more operational risk exposure. However, it is often argued that gross income is not always a perfect proxy for operational risk since it may fluctuate with the business/ economic cycle. Nevertheless, in the absence of any other proxy, income is being used due to its simplicity, comparability and reduced capital arbitrage opportunity.

Another approach offered under Basel II is the Advanced Measurement Approach (AMA), wherein banks can develop their own internal assessment techniques. Unfortunately, the quantitative techniques for measuring operational risk are evolving and there is no broad consensus on the modeling methodologies of operational risk.

Thus, it can be said that the quantitative approaches offered under Basel Accord are still in the process of refinement. However, this is all the more reason for banks to focus on qualitative requirements depending on the regulatory approach they intend to follow. In the past one decade, the awareness of operational risk has improved and resultantly the principles for sound management of operational risk have emerged. Banks need to incorporate these internationally agreed principles while implementing any operational risk management framework. These principles mainly focus on the Governance, Risk management environment, role of supervisors and business resilience.

I will now outline SBP's expectation on the integrated components of the overall framework for managing operational risk across the enterprise.

Sound internal governance forms the foundation of an effective operational risk management Framework. It is necessary that those at the top of the organization should take the lead in establishing a strong risk management culture. The board of directors needs to regularly review the framework and ensure that senior management is actively monitoring the effectiveness of risk management and controls. For this purpose, the board should establish a management structure based on clear lines of responsibility, accountability and reporting. The board should set the bank's risk appetite through the approval of operational risk management policy. SBP expects that boards should seek periodic reports from management to the monitor the operational risk profile of the bank in a proactive manner.

The role of senior management is to implement the operational risk management framework as approved by the board. Senior management must ensure that all its business activities are adequately staffed having necessary experience and technical skills. The remuneration policies should also be consistent with the approved risk appetite. Managers should not be rewarded solely on the basis of profits, but audit findings and compliance status should also be considered while deciding bonuses and compensations.

Sound operational risk governance practices rely mainly on the following lines of defense:

i. Business line management is the first line of defense against operational risk. Business line management is responsible for identifying and managing risks in the products, activities, processes and systems for which they are accountable. It is important that clearly documented and regularly updated operating manuals are readily available to all employees. Segregation of duties needs to be ensured. It is also necessary that operational staff must have necessary skills and training so that they can fulfill their duties.

ii. A separate independent operational risk management function is the second line of defense and has become a good practice. Independent operational risk management function would assist management to understand and manage operational risk. The function should be responsible to assist in establishing policies & standards and coordinate with various businesses/ risk management activities. The function assesses, monitors, and reports operational risks as a whole, and ensures that the management of operational risk in the bank is as per approved strategy/ policies.

iii. Independent validation and verification is the third line of defense in the governance structure. It serves as a challenge function to the other two lines of defense. Internal audit or any independent group of qualified staff may conduct these independent reviews. Since internal audit reports to the board audit committee therefore the audit function should also provide assurance to the board regarding effectiveness of the operational risk management framework. Senior management should seriously investigate the findings of audit to set up a risk culture in the bank.

The next principles focus on *Risk management environment*, it outlines the bank's approach to the identification, assessment, monitoring, control and mitigation of risk. Banks need to use various tools for proactive operational risk management. These tools include audit findings, analysis of internal and external loss data, risk control and self assessments, key risk indicators, scenario analysis, comparative analysis etc. I am pleased to know that lively discussions on these tools will follow in the coming sessions.

SBP is cognizant of its responsibilities with regard to sound operational risk management frameworks in banks. SBP will continue to play its role in ensuring effectiveness of established frameworks in banks. We expect each bank to develop and continuously improve its risk management and control framework depending on nature, location, size, sophistication, complexity of business operations and approved risk appetite.

In order to have comprehensive and current information on operational risk, SBP will expand its existing reporting mechanism. SBP is working on a *two prong strategy*; one is to update the *existing instructions on frauds & forgeries* with the purpose to further strengthen the fraud risk management and monitoring in banks. On the second front, Guidelines *on operational risk data collection* will be issued to enhance the scope of loss data gathering in line with Basel II requirements and to provide the industry a minimum set of instructions for consistent recognition of losses and their reporting to a centralized data consortium. These projects are at an advanced stage of consultation with the industry. These guidelines/ instructions will help banks improve their operational risk management processes.

Information security and business continuity are becoming the top supervisory concerns. Banks need to monitor IT security risks and respond to security breaches in a timely manner. Banks need to devise and test their business continuity plans to ensure they are able to operate on an ongoing basis in the event of severe business disruption. The plans must be based on different types of worst case scenarios like inaccessibility of bank's facilities, IT infrastructure or a pandemic event.

Let me sum up the key message of this address. For sound management of operational risk, we need to inculcate a risk culture within the organization with open communication channels between business lines and control functions. There is a need for close cooperation between banks and SBP. We are all on the learning curve; therefore exchange of ideas is very important in capacity building for operational risk management. I hope this conference will provide a good opportunity to exchange our thoughts on the subject and learn from each other's experiences.

Thank you very much for your attention.