



Operational Risk Management in Banking Sector: An overview

KEYWORDS

Rakesh Chutia

Assistant, State Bank of India Margheita-786181 Dist.-Tinsukia Assam

ABSTRACT Operational risk is inherent in all banking products, activities and processes and systems and the effective management of operational risk is of paramount importance for every bank's board and senior management. With globalization and deregulation of financial markets, increased competition combined with the advent of high-end, innovative, sophisticated technology tremendous changes have taken place in the products distribution channels and service delivery mechanism of the banking sector. These have introduced more complexities into the banking operations and consequently the risk patterns and profiles of the industry have also become complex, diverse and catastrophic. The New Capital Adequacy Framework of the Reserve Bank of India requires bank to maintain capital explicitly towards operational risk. This paper tries to study the various methodologies used by the banks in their operational risk management activity and to study the regulatory framework related to operational risk management.

Introduction

Since the late 1990s, globalization, deregulation, consolidation, outsourcing, breaking of geographical barriers by use of sophisticated technology, growth of e-commerce etc. have significantly changed the business, economic and regulatory climate of the banking sector. These developments introduced more complexities into the activities of banks and their risk profiles. Consequently a series of high profile operational loss events at Societe Generale, UBS, AIB, and National Australia Bank etc. have led banks and their managements world over to increasingly view operational risk management as an integral part of their risk management activity like the management of market risk and credit risk. The identification and measurement of operational risk is a significant issue for modern-day banks, particularly since the decision by the Basel Committee on Banking Supervision (BCBS) to introduce a capital charge for this risk as part of the new capital adequacy framework (Basel II).

Operational risk has been defined by the Basel Committee on Banking Supervision as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition is based on the underlying causes of operational risk. It seeks to identify the causes of a loss event and at the broadest level includes the breakdown by four causes: people, processes, systems and external factors. Operational risk may materialise directly, e.g., in electronic fund transfer (transfer of funds to the wrong person) or could result indirectly as a credit or market loss. Since there is a close linkage of operational risk with other types of risks, it is very important for banks to first have a clear understanding of the concept of operational risk before designing the appropriate operational risk measurement and management framework.

Different types of operational risk in Banking Sector

The Basel Committee has identified the following types of operational risk events as having the potential to result in substantial losses for banks:

- Internal fraud. For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.
- External fraud. For example, robbery, forgery, cheque kiting, and damage from computer hacking.
- Employment practices and workplace safety. For example, workers compensation claims, violation of employee health and safety rules, organised labour activities, discrimination claims, and general liability.
- Clients, products and business practices. For example,

fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorized products.

- Damage to physical assets. For example, terrorism, vandalism, earthquakes, fires and floods.
- Business disruption and system failures. For example, hardware and software failures, telecommunication problems, and utility outages.
- Execution, delivery and process management. For example: data entry errors, collateral management failures, incomplete legal documentation, and unauthorized access given to client accounts, non-client counterparty misperformance, and vendor disputes.

OPERATIONAL RISK MANAGEMENT PROCESS:

Operational Risk management generally encompasses the process of identifying risks to the bank, measuring exposures to those risks), ensuring that an effective capital planning and monitoring programme is in place, monitoring risk exposures and corresponding capital needs on an ongoing basis, taking steps to control or mitigate risk exposures.

- Identification of operational risk. Banks should identify and assess the operational risk inherent in all products, services, activities, processes and systems. Effective risk identification should consider both internal factors (such as the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organizational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.
- Assessment of Operational Risk. In addition to identifying the risk events, banks should assess their vulnerability to these risk events. Effective risk assessment allows a bank to

better understand its risk profile and most effectively target risk management resources.

Amongst the possible tools that may be used by banks for assessing operational risk are:

- **Self Risk Assessment:** A bank assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment.

- **Risk Mapping:** In this process, various business units, organizational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management action.
- **Key Risk Indicators:** Key risk indicators are statistics and/or metrics, often financial, which can provide insight into a bank's risk position. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.
- **Measurement.** A key element of risk management is measuring the size and scope of the bank's risk exposures. However, there is no clearly established, single method to measure operational risk on a bank-wide basis. Banks may develop risk assessment techniques that are appropriate to the size and complexities of their portfolio, their resources and data availability. A good assessment model must cover certain standard features. An example is the "matrix" approach in which losses are categorized according to the type of event and the business line in which the event occurred. Banks may quantify their exposure to operational risk using a variety of approaches. For example, data on a bank's historical loss experience could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control the risk.
- **Monitoring of Operational Risk.** An effective monitoring process is essential for adequately managing operational risk. Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. In addition to monitoring operational loss events, banks should identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, and so on. There should be regular reporting of pertinent information to senior management and the Board of Directors that supports the proactive management of operational risk.
- **Controls / Mitigation of Operational Risk.** With regard to operational risk, several methods may be adopted for mitigating the risk. For example, losses that might arise on account of natural disasters can be insured against. Losses that might arise from business disruptions due to telecommunication or electrical failures can be mitigated by establishing redundant backup facilities. Loss due to internal factors, like employee fraud or product flaws, which may be difficult to identify and insure against, can be mitigated through strong internal auditing procedures. The Board of Directors and senior management must make efforts for establishing a strong internal control culture in which control activities are an integral part of the regular activities of a bank. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile. Investment in appropriate processing technology and information technology security are also important for risk mitigation. Banks should also have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

OPERATIONAL RISK MANAGEMENT APPROACHES IN BASEL II

The Basel framework (2004) proposes a range of approaches for setting aside regulatory capital for operational risk under Pillar 1: The Basic Indicator Approach (BIA), The Standardised Approach (TSA) and the Advanced Measurement Approach (AMA). All the three approaches differ in their complexity and the banks are encouraged to move along the spectrum of approaches as they obtain more sophistication in their risk management practices. The Basic Indicator Approach is the simplest approach for estimating regulatory capital, wherein

banks are required to set apart an amount equal to the average over the previous three years of 15% of positive annual gross income. In The Standardised Approach, banks' activities are divided into eight business lines: Corporate finance, Trading & Sales, Retail Banking, Commercial Banking, Payment & Settlement, Agency Services, Asset Management and Retail Brokerage. While gross income continues to be the main indicator of operational risk as under the Basic Indicator Approach, the specific amount to be set apart as a percentage of the gross income varies between business lines, ranging from 12 to 18% , as compared to the 15% overall under the Basic Indicator Approach. This approach is more refined than the Basic Indicator Approach as it takes into the account the fact that some business lines are riskier than others and therefore a higher proportion of capital has to be set apart for those business lines. The Advanced Measurement Approach (AMA) is based on the banks' internal models to quantify operational risk. The framework gives flexibility to the banks in the characteristics of the choice of internal models, though it requires banks to demonstrate that the operational risk measures meet a soundness standard comparable to a one-year holding period and a 99.9% confidence level, which means that a bank's capital charge should be equal to at least 99.9% quantile of their annual aggregate loss distribution. Banks are required to factor in four key elements in designing their Advanced Measurement Approach framework: internal loss data, external loss data, scenario analysis and bank specific business environmental and internal control factors. The methodologies under the advanced approach are evolving and there are a range of methods in practice in banks internationally.

OPERATIONAL RISK MANAGEMENT IN THE CONTEXT OF INDIAN BANKING SECTOR:

The Reserve Bank of India is the regulator and supervisor of the banking system in India and is entrusted with the task of framing the capital adequacy guidelines for banks in India under Basel II. Public sector banks, where the Government of India is the major shareholder, dominate the Indian banking system, accounting for nearly three-fourths of total assets and income. These banks are large and very old banks, operating through thousands of branches spread all over the country. The new private sector banks are fully automated from day-one and operate like other high-tech foreign banks. The private sector banks have grown rapidly since the onset of reforms and have increased their share in total assets of the banking industry, whereas the public sector banks have witnessed shrinkage in their market share. The public sector banks have only recently started automating their processes and operations. This transition has posed significant challenges in the management of operational risk to the banks as introduction of new technology and complete overhauling of the existing systems requires a re-engineering of business processes, training of manpower, audit in a computerized environment and other related operational risk challenges. The new generation private sector banks on the other hand have to deal with the risks arising from growth at a scorching pace. With the reforms in the Indian banking sector and banks being allowed to access new markets and sophisticated products, the Reserve Bank of India has also been repeatedly advising the banks to have in place an effective and resilient control framework in place to manage operational risks. Specific guidance on management of operational risk has also been issued as per which some banks; especially the larger and internationally active banks are expected to move along the range towards more sophisticated approaches as they develop more sophisticated operational risk management systems and practices which meet the prescribed qualifying criteria.

Conclusion:

Managing Operational Risk is emerging as an important element of sound risk management practice in modern day banks in the wake of phenomenal increase in volume of transactions, high degree of structural changes and complex technological support systems. RBI expects all Indian banks to strengthen their operation risk management system and to

be in readiness to graduate to more sophisticated approaches of operational risk management under Basel norms. In order to derive maximum gains banks need to gear up efforts for speedy and effective implementation of comprehensive

operational risk management frameworks and thereby bring more efficiency, transparency, profitability and sustainability into their operations.

REFERENCE

Reserve Bank of India, Department of Banking Operations and Development, Central Office, Mumbai, (2005), "Draft guidance note on management of operational risk", 2. Basel Committee on Banking Supervision (August, 2003) "The Joint Forum Operational risk transfer across financial sectors", 3. Usha, Janaki, Raman, (2008) "Operational Risk Management in Indian Banks in the Context of Basel II: A Survey of the State of Preparedness and Challenges in Developing the Framework", 4. Rao, D, Tripathi and Ghosh, Prodipta, (2008) "Preparedness of Indian Banks in Managing Operational Risk", 5. Kale, Ketan and Agarwal, Mohit, Marsh India, (2011) "Operational Risk Mitigation & Basel II Accord - Challenges & Opportunities".