Operational Risk Management in Indian Banks– the changing Paradigm

P.S.Subha Pradha,
Research Scholar, School of Management Studies, University of Hyderabad

&

Dr. P. Jyothi,
Professor, School of Management Studies, University of Hyderabad

Abstract
Rapid financial and technological innovations have transformed financial industry globally. On the one hand, these innovations have boosted rapid expansion and growth of the industry across frontiers, while on the other hand, it has brought with them many a risks of varied nature. Risks have taken many dimensions over the past few decades and are still evolving. Among many risks that contemporary banking is facing today credit, market, liquidity and operational risks are the major ones. While management of credit and market risk mitigation has developed substantially, operational risk management is still in a nascent stage. Operational Risk identification and its management is a critical and integral part of an overall risk management process in a bank. It is a double challenge as it requires a bank to mandatorily comply with the capital regulations of the Basel & RBI while ensuring that this does not adversely affect the business opportunities of the bank. The present paper attempts to give an overview of Operational Risk and its management in the Indian banking sector.

JEL Classification: E42, G32

Introduction
Operational Risk Management has gained significant concern in financial services. Even though business failure is a manifestation of many factors, people and processes involved in operations have been identified as considerable cause of risk. The organizational context in which people work and the processes that are followed highly influence the development of operational risks. This operational context is influenced by a combination of both exogenous and endogenous variables and the interactions among them. While the regulations of the government, industry, competition are some of the exogenous factors, the internal controls and government comprise the endogenous variables. It has been shown that the governance in an organization has a direct impact on the nature of its Risk Management.

Many financial losses across geographies have shown that most of the operational losses were consequences of internal frauds and failures, failed internal controls and audits. Basel Committee for Banking Supervision has reported some of the significant losses incurred because of operational risks in the past few years.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Financial Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>SocGen</td>
<td>4.9 billion Euros</td>
</tr>
<tr>
<td>Allied Irish</td>
<td>691 million dollars</td>
</tr>
<tr>
<td>Sumitomo</td>
<td>2.6 billion dollars</td>
</tr>
<tr>
<td>Barings Bank</td>
<td>1.3 billion dollars</td>
</tr>
</tbody>
</table>


Most of the above losses are the outcomes of a combination of market and operational risks. They were attributed to the deeds of overambitious traders who resorted to frauds for personal financial gains. The huge financial losses have left most of these organizations bankrupt. As a result, financial institutions have begun to create a formal structure for measurement and management of Operational Risk. They are in the process of defining Economic Capital that is required to cover operational risk. These estimates are quite high and occupy a significant percentage of total risk indicating the significance of operational risk.
Operational Risk Definition
Initially operational risk was not recognized as a separate category of risk and was identified to be residual risk. Anything that was not categorized as credit or market risk was treated as operational risk. However, due to the growing importance of operational risk, the Basel Committee in its Basel II guidelines has defined Operational Risk as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”
The Basel Committee has classified operational risk events into seven types - Internal Fraud; External Fraud; Employment Practices and Work Security; Clients, Products and Business Practices; Damage to Physical Assets; Business disruption and System Failures; Execution, Delivery and Process Management. These are classified across eight business lines – Corporate Finance; Trading and Sales; Retail Banking; Commercial Banking; Payment and Settlement; Agency services; Asset Management and Brokerage.
After several consultations, the Basel Committee has published the revised document -“Sound Principles for Management of Operational Risk, 2011” that clearly defines the measures that banks should adopt for effective management of Operational Risk. These principles are grouped as a. Fundamental Principles of Risk Management; b. Governance,c. Risk Management environment and d. Role of Disclosure. These principles aim at the creation of a robust operational risk management system across banks globally that is capable of averting catastrophic losses by identifying them before the damage is done. The following section describes the steps that are involved in developing operational risk management process.
Steps in an effective operational risk management process

1. **Formulating Policy**: Effective operational risk management policies specify clear guidelines for the organisation to follow. They aim at operational efficiency to reduce losses and are formulated for all aspects of business performance. The expectations of the stakeholders are kept in mind while formulating policies.

2. **Establishing the organisation**: An effective management structure and organization need to be in place for implementing the policy. Staff should be motivated and empowered to work as per the policy in the best interests of the firm. Effective staff involvement and communication makes employees to contribute significantly towards operational risk management. A strong risk management culture that shares a common understanding of the organization’s vision, value systems and beliefs towards risk is nurtured by active top management.

3. **Implementation**: There is a planned and systematic approach to implementing the operational risk management policy through an effective operational risk management system. The aim is to minimise risks. Risk assessment methods are used to decide on priorities and to set objectives for reducing risks. Risks are treated through selection and design of appropriate controls. If risks cannot be controlled internally then various risk transfer methods are considered. The overall capital adequacy is reviewed taking into account the overall operational risk profile of the firm. Performance indicators are established and used for measuring risk. Measures are undertaken to create a positive operational risk culture.

The Implementation Process - Strategic Initiatives
a. Define Risk Categories, Risks: The first step in the implementation process is to clearly define the various risk categories, risks and the interdependencies.

b. Assess Risks: All the risks are assessed based on the probability and the impact to identify the most common and significant risks. Risk maps are used for this.

c. Define Risk Strategy: Strategy is defined for the most significant risks based on the acceptable levels of risk.

d. Key Risk Indicators: KRIs are used to keep a track of risk levels. As the risks approach the acceptable levels and cross the thresholds, alerts are raised so that appropriate actions are taken.
e. Define Strategic Actions & Mitigation: In order to ensure that the KRI s do not cross the thresholds, strategic actions need to be defined for risk mitigation.

f. Monitor Risk Environment: Constantly monitoring KRI s helps in timely identification of threshold breaches and take appropriate action. Organizational self-assessment allows to detect changes in the environment.

The Implementation Process - Tactical Responses

The strategic initiatives should be supplemented by tactical activities for effective implementation.

a. Specify targets for KRI: The KRI s for a given business line or unit are identified and thresholds are set for KRI s to monitor any changes in the operating environment.

b. Monitor KRI s: Shorter time intervals for monitoring are set at the tactical levels while monitoring at top levels can be done at monthly or quarterly levels.

c. Take timely Actions: Monitoring the environment constantly allows the risks to be tackled at the business unit itself before the damage is done or needs to be escalated to the top management.

d. Escalate New Issues: Any changes in environment like new loss events, near miss events should be immediately escalated to top management through the risk management process.

4. Performance Measurement: Performance of Operational Risk Management is measured against standards to gauge the progress and areas of improvement. Risk Management needs to be both proactive and reactive. While constant monitoring of operational risk environment through internal controls helps to identify external and internal risk factors, any failure of controls can be handled by reactive risk management. Risk monitoring not only helps in early detection of underlying causes and their effects on the design and working of operational risk management.
5. **Auditing and reviewing:** There is a systematic review of performance based on data from monitoring activities and independent audits of the risk management system. These form the basis of self-regulation & regulatory compliance. Policies, systems and techniques of risk measurement and control are constantly monitored and improved. Performance is assessed by KRIs and comparative analysis. Feedback is an essential element of the entire system and constant improvement cycle is a critical aspect of risk management system.

**Operational Risk Regulatory Capital**

The Basel accord governing operational risk defines three approaches to the calculation of regulatory operational risk capital.

1. Basic Indicator approach
2. Standardized approach
3. Advanced Measurement approach (AMA)

The Basic Indicator and the standardized approaches require banks to allocate a fixed percentage of gross income as operational risk capital. Banks with limited exposure to operational risk can adopt any of these approaches. While the Basic Indicator approach requires a fixed 15% of three year average gross income to be allotted to operational risk capital, the Standardized approach categorises the banking activities into 8 business lines and allocates a percentage of 12 – 18% of three year average gross income as operational risk capital depending on the business line.

\[ K_{BIA} = GI \times \alpha, \]

where \( K_{BIA} = \) operational risk capital as per the Basic Indicator Approach,
GI = three year average Gross Income where positive and \( \alpha = 15\% \).

\[ K_{TSA} = \sum_{i=1}^{n} GI \beta_{1-8}, \]

where \( K_{TSA} = \) operational risk capital as per Standardized approach,
GI = three year average gross income across each business line,
\( \beta = \) percentage fixed for each business line varying from 12% - 18%. The \( \beta \) factors as per business lines are mentioned in the following table.

<table>
<thead>
<tr>
<th>Business Line</th>
<th>( \beta ) coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Finance</td>
<td>18%</td>
</tr>
<tr>
<td>Trading &amp; Sales</td>
<td>18%</td>
</tr>
<tr>
<td>Retail Banking</td>
<td>12%</td>
</tr>
<tr>
<td>Commercial Banking</td>
<td>15%</td>
</tr>
<tr>
<td>Payment &amp; Settlement</td>
<td>18%</td>
</tr>
<tr>
<td>Agency Services</td>
<td>15%</td>
</tr>
<tr>
<td>Asset Management</td>
<td>12%</td>
</tr>
<tr>
<td>Retail Brokerage</td>
<td>12%</td>
</tr>
</tbody>
</table>

Source: BCBS document

---

**Fig 2:** The Operational Risk Management Process, Adapted from Peyman Mestchian, Advances in Operational Risk: Firm wide issues for Financial Institutions, 2005.
Banks that operate on a large scale and are exposed to substantial operational risk losses are required to move over to the Advanced Measurement Approach (AMA) over a period of time. Using the AMA, banks can calculate their own operational risk capital based on their internal models and business activities. As per Basel, banks should set aside an operational risk capital in-line with 99.9% or more confidence level over a one year holding period. The capital charge, $K$, can be defined as

$$K = \sum_{l=1}^{n} VaR^l_{\alpha},$$

where $VaR^l_{\alpha}$ represents Value at Risk (VaR) at confidence level $\alpha$ of a business line $l$. VaR values across different business lines and event types are added up to arrive at the aggregate VaR. VaR is a statistical estimation of a portfolio loss, which specifies that with a given very small probability of $1-\alpha$, there is a chance to incur that loss or more, over a given holding period.

The AMA is the most sophisticated approach that can be used for the quantification of operational risk. However, this requires a number of modelling assumptions to be satisfied. The accuracy of the predicted operational loss values depend on the quality of the historical data available. Banks need to use five year internal loss data for using AMA. However, banks using AMA for the first time can use three year historical data. AMA is likely to change the scenario of Operational Risk Management in the Indian context and bring a significant shift in the way operational risk is treated in banks.

**Causes of Operational Risk**

Huge losses do not occur in isolation. Operational Losses arise mainly because of the failure of internal controls. There are many factors contributing to these losses. Operational risk is said to be arising mainly because of

- People
- Processes
- Systems &
- External Controls

**People Risk:** Firms that value risk management establish an effective framework to maximise the contribution of employees. Operational risk objectives become part of the organizational culture. Support from top management, strong leadership and commitment of senior managers and directors are prerequisites to the success of operational risk management. Senior management communicate the beliefs underlying the policy through their management practices. It is also the responsibility of the Board of Directors to ensure co-ordination of effort. The whole organisation shares the management perception and beliefs about the importance of operational risk and the need to achieve the policy objectives.

Some of the human factors that influence operational risk are

**Organizational Factors:** These have a major influence on employee behaviour. These are ignored at times during the design of work and study of loss events. Organisations need to establish their own risk management culture that promotes employee involvement and commitment at all levels. This culture should establish standards and acceptable risk management practices. It should also reward professional and responsible behaviour.

**Job factors:** These directly influence employee performance and the control of risks. Mismatches between job requirements and individuals’ capabilities increase the potential for human error. Matching the job to the individual ensures consistent performance.

**Personal factors:** Employees bring with them their personal strengths, weaknesses, habits, attitudes, skills, etc., which are capable of affecting their behaviours significantly in organizations. Therefore, appropriate measures need to be taken to ensure awareness on ethical conduct and behaviour, and its impact on operational risk at all levels in the organization.
Technology Risk
Advances in risk and data management technologies have led to rapid development in the arena of risk management. Due to the dynamic nature of risk management, technology solutions should be flexible to fit in not only current requirements but also be scalable to meet future requirements of regulators, risk managers and top management.

Process Risk
Firms need to constantly reengineer their processes to meet the requirements of operational risk management. Firms must establish a link between qualitative and quantitative risk factors and build a process that can make use of established knowledge.

External Sourcing of Operational Risk
Apart from the internal controls over people, process and technology for management of operational risk, organizations can look at external sources for managing operational risks.

Organizations have allocated considerable resources for hedging of credit and market risks. However, operational risk was not given so much importance earlier. Experts on hedging have identified insurance as a key tool in this regard. Property coverage, fire, workers compensation, employer's liability and professional indemnity are used to cover the respective risks. Through insurance, organizations can take the risk away from the balance sheet and avoid the costs of capital associated with provisioning.

Multi-risk coverage programmes comprising of multi-billion currency limits have been developed. The market for alternative risk transfer has been growing in recent years. Multi-year, multi-line coverage where the various lines of coverage are bundled into one complete package and spread over five to ten years as opposed to the traditional annually renewable policy have become more popular. This gives both premium and transaction savings to the client as well as wider coverage.

Risk maps depicting loss severity and frequency are used as basis for making operational risk insurance decisions. Risks with low and medium severity, and, low, medium and high frequency must be retained through internal controls and capital provisions. Events with high severity and low and medium frequency can be insured either through self-insurance or through third-party insurance. However, high frequency-high severity risks should be avoided by changing business practices.

Another way of transferring risk to a third party is outsourcing. Functions that are non-core and involve high risk are usually targets for outsourcing. Sometimes, non-core back office functions are outsourced so that firms can focus on their core competencies. The third party passes on the benefits that it derives from the economies of scale and specialization to the clients. Apart from risk transfer, outsourcing also confers the benefits of cost-control, best practice methodologies, freeing-up capital to focus on core functions, reduction in administrative burden.

The Changing Dynamics of Operational Risk Management
Though operational risk management is relatively new to the banking and financial sectors, it has been a critical part of industries that have been safety centric like defence, energy, aviation and transportation for decades. The tools and methodologies that were developed in these industries could be adopted by the financial services sector.

Few of the leading tools that can be applied to operational risk management are Reliability based management; Behaviour based management; Knowledge Management and Activity based management.

Reliability Based Management: Organizations make use of failures associated with process, equipment and controls to develop robust operational maintenance and resilience.

Behaviour based Management: This combines the concepts of Total Quality Management, organizational behaviour and statistical techniques to address employee behaviour. This has been successfully applied in manufacturing and industrial sectors.
Knowledge based Management: Organizations have invested in latest systems and processes for managing their intangible assets. Individual and organizational knowledge can be used to create efficient and effective business processes. The same can be applied to operational risk management. The knowledge pool can be used to identify potential risks, risk avoidance and effective communication of risk management and best practices. The focus has recently been on text mining technology which is used to analyse unstructured data. As most of the organizational data is in unstructured form, this method can be used to identify operational risk events.

Activity-based management: From 1990s Activity-based costing and activity based management systems were commonly used for greater accuracy in cost allocation and providing true economic information to management for better profitability. This activity-based view of the business is highly relevant to operational risk management as it helps in decisions concerning pricing, product mix, cost reductions, process improvement, process or product redesign, and planning or managing activities. This approach can also be directly linked to the risk scorecard and key indicator approaches.

Another key driving force behind operational risk management is the mandatory regulatory requirement that aims at effective capital allocation and sound internal control system. However, implementing operational risk management only for regulatory compliance might not give the desired results of effective risk management as will the voluntary compliance. Adopting operational risk management beyond regulatory compliance will yield high return on investment from an effective operational risk management. This will pave way for further phases in operational risk management that will make it an integral part of everyday operations of financial institutions.

Bibliography