Operational Risk Management: A Case Study Of An Indian Commercial Bank

Sartaj Hussain
Assistant Professor, Department of Business & Financial Studies, University of Kashmir Srinagar
Kashmir, India

Dr. Mohammad Shafi
Associate Professor, Department of Business & Financial Studies, University of Kashmir Srinagar
Kashmir, India
Abstract

Operational risk in ordinary sense is the risk of losses arising to us when we don’t perform our activities appropriately; rather conduct them in a bad or improper manner. Operational risk is not a recent phenomenon; it is being managed in the financial institutions since long by ensuring proper internal control and supervision, taking of safety measures and precautions, regular audits, and checks and balances, etc. Recently, in response to some disastrous operational loss events which shook the developed world and led to collapse of some financial giants, (Barings, LTCM and Daiwa) banking regulators have agreed to implement an explicit capital provision in the banks towards their exposure of operational risk. Across the world, banks are being now encouraged to develop operational risk management frameworks so that they are capable of measuring their operational risk exposure scientifically to determine the economic capital towards operational risk. In India also, since the onset of Basel II accord which pioneered the operational risk capital charge, hectic activity has been witnessed inside the banking industries towards setting up and development of operational risk management framework suitable to the new regulatory demands. On these lines, the current study attempts to understand the stage of development and preparedness of an Indian bank towards the operational risk management framework. The research findings given in the paper may have sensitivity and reputational implication for the concerned organisation, hence, name of the bank under study has been kept in anonymity.

Key Words: Operational Risk (OR), BCBS, BIA, TSA, AMA, ICAAP, RAROC

1. Introduction

Operational risk is the risk of some adverse outcome resulting from acts undertaken (or neglected) in carrying out business activities, inadequate or failed internal processes and information systems, misconduct by people or from external events and shocks. Operational risk is a generic risk present in operations which exists even before any deposit is accepted or a credit is granted by a bank. Unlike other banking risks, viz, credit and market risk which have a broader consensus on their conceptual understanding in the industry worldwide, operational risk is considered as a risk characterised by idiosyncrasy. Since last two decades, financial institutions worldwide have been seen placing increased emphasis on the management and measurement of operational risk. Modern approach of Operational Risk management which particularly stresses its measurement and linkage with the bank capital adequacy is considered as a new frontier of value creation and efficiency in banks. The need of an explicit capital charge to address a banks’ operational risk exposure has been felt by the Basel Committee of Banking Supervision (BCBS), as many banking institutions in the developed countries were shaken by mega operational failures emanating from events of fraud, technological...
failure or due to control breakdowns resulting in collapse of age old financial institutions like, Barings Bank of UK, Daiwa of Japan etc.

In response to these developments, Basel movement for explicit capital charge and emphasis on strong internal controls emerged in the early years of the last decade. Banks across the world by their local regulators have been stressed to invest in operational risk management function that aims at development of a framework intended to take care of operational risk exposure in a better scientific manner. Likewise, in India also, the local regulator, Reserve Bank of India, (RBI) after taking cue from the Basel guidelines has advised banks on how to create a sound operational risk management framework keeping in view the increased intensity of their operational risk exposure. Operational risks have in the recent past grown tremendously both in number as well as in intensity due to various developments like, massive investments in information systems & technology leading to shift from brick mortar branch banking to machine oriented ATM banking with less human intervention, transformation of manual processes to electronic and computerised systems leading to growth in electronic dealings, increased instances of mergers and acquisition leading to integration of complex business systems and processes and with the deregulation of financial markets leading to increase in complexity and sophistication of financial products. All these developments have given rise to new operational threats in the form of electronic and cyber thefts and frauds and also data security issues creating concerns for hacking and phishing threats. Traditionally, Operational Risk in banks was being managed by putting in place effective control systems, independent audit mechanism and corporate governance measures. Operational risk by its nature is unavoidable and to be borne by every business. Unlike credit and market risk, which arise due to exposure in credit and market tradable financial instruments, operational risk arises from a host of factors, like, people, technology, processes and external events.

Despite controversies that operational risk is not systemic, but more of idiosyncratic in nature, Basel Committee on Banking Supervision (BCBS) came out with an explicit capital charge to cover the operational risk exposure of the banks in the second Basel Accord in the year 2004. Initially banks in the developing countries like India were required to implement Basic Indicator Approach for estimation of operational risk capital charge. Thereafter, in a phased manner, banks like those in developing countries and their counterparts in the developed world were asked to develop operational risk management to the extent that operational risk exposure is measured from the actual operational loss experience of the bank with the help of internally developed risk measurement models. Operational risk management in essence is very difficult to measure as unlike credit ratings for credit risk and price volatility for market risk, it has to be understood from an institution’s historical loss experience across a host of operational risk events ranging from acts of fraud to technology failure and fire incidents, earthquakes to terrorist attacks and property damages caused by
vandalism due to public unrest. Banks in India face difficulties in implementation of a sound operational risk management framework primarily due to lack of conceptual understanding, inadequate expertise in modelling techniques and poor risk management culture.

2. Literature Review

Operational risk management is older than credit risk and market risk management as Buchelt and Unteregger (2004) argue that long before the advent of Basel II, financial institutions had put in place various control mechanisms and procedures. The process of managing operational risk is different from those of managing market risk and credit risk only in so far as operational risk is different from the other two kinds of risk. Kaiser and Kohne (2006) argue that the distinctive feature of operational risk may cause significant divergence of the individual steps of operational risk management from the corresponding steps of market and credit risk management. One important difference, however, is that it is much more difficult to implement operational risk management on different hierarchical levels than in the cases of market and credit risk management. Kaiser and Kohne attribute this difficulty to the absence of a portfolio concept for aggregating the individual risk categories that operational risk encompasses. Netter and Poulsen (2003) emphasis that either due to new regulations or the increasing level of operational risk in financial services, banks have to focus on development of sophisticated ways for measurement of operational risk, besides integration of market and credit risk into its analysis in the coming years. Kingsley et al. (1998) state the following objectives of operational risk management, (i) avoiding catastrophic losses, (ii) generating a broader understanding of operational risk issues, (iii) enabling the firm to anticipate risk more effectively, (iv) providing objective performance measurement, (v) changing behavior to reduce operational risk, (vi) providing objective information so that services offered by the firm take account of operational risk, (vii) ensuring that adequate due diligence is shown when carrying out mergers and acquisitions. All of these objectives, it seems, fall under the headings, “risk avoidance” and “risk reduction” but operational risk management is more than that as it encompasses risk transfer and risk financing.

Harris (2002a) provides a basic overview of what advanced financial organisations are doing to address operational risk that summarises the implementation of operational risk management. He identifies this pattern: recognising operational risk as a separate discipline, restructuring the organisational hierarchy, defining a management process, creating measurement tools, developing monitoring systems. Ford and Sundmacher (2004) argue it was unlikely that operational losses in the three banks Barings, AIB and NAB would have been recognised and consequently prevented under the revised capital standards for financial institutions suggested by the Basel Committee on Banking Supervision (BCBS). Accordingly, they identify some operational risk indicators like cost-to-income ratio, Ratio of Back Office to Front Office Staff, Number
of Daily Trades per Individual Trader, Expenditure on Training per staff member, proportion of incentive-based remuneration, that can be incorporated into a scorecard approach for use within institutions and, potentially, for external reporting purposes. Herring (2002) challenges the rationale for employing capital charge suggested by New Basel Capital Accord to mitigate operational risk. The argument is that operational risk unlike other risks is idiosyncratic, thereby involves less systemic implications. Tanase and Serbu (2010) suggest that banks with the help of technological advancements have been able to manage operational risk by offering innovative products like e-banking, which has been able to reduce a lot of their operational risk exposure by minimising the human intervention in their overall process. Martin (2009) argues that the culture of an organization is critical to its success in managing operational risk. Operational risk according to the author has two causes, an act of God (flood, earthquake and windstorm) and a person. People, who are at the heart of the culture of an organisation design and maintain processes and systems and cause operational risk events by either doing something they should not be doing or not doing something that they should be doing. He argues that the culture of an organisation is critical to its success in managing operational risk.

Grody and Hughes (2008) argue that a proper risk culture embedded in people and processes offers a financial institution greatest protection against failure as against its capital. At the core of any risk culture are the incentives for individual reward that balance risk and return with short-term self-interest and long-term stakeholder goals. Basel II presents an operational risk framework intended to foster a risk-adjusted performance culture that is hoped for preventing such crisis in the future. Dardac and Chiriac (2010) stress the role of effective corporate governance for management of operational risk in Romanian NBFS’s that will create solid ethical values, as well as a process control climate through the adoption of the best internal audit and control practices. Buchelt and Unteregger (2006) argue that Operational Risk management represents the next frontier in banks towards creation of higher risk awareness and transparency, the improvement of process quality and the significant reduction in the number of cases of damages or losses, besides enhancing bank’s profile and giving it competitive advantage among others.

Hiwatashi (2002) outlines several approaches to operational risk management in banks. He notes first that banks traditionally controlled operational risk based on qualitative risk management checklists and guidelines. This has become inadequate due to the increased complexity and speed of bank operations. Now, banks must first try to measure operational risk so that senior managers can establish objectives in “prioritising risk control among different business lines and risk categories, in order to supplement internal control in a more robust way”. Measurement also is necessary for the management to determine whether the banks have appropriate capital for their level of operational risk. In addition, measurement also enables the bank to tie performance to employees risk management effectiveness.
3. Objectives And Scope Of The Study

The present study was conducted with the following objectives:

1. To assess and analyse the present framework and management practices of the selected Bank towards operational risk and;
2. To examine and summarise the overall progress made by the Bank in the area of ORM at the Bank under study given the regulatory necessities.

The study remained restricted to the analysis of perception and framework of the management of Operational Risk at the Bank. Operational risk management, a new and emerging area in banks everywhere particularly in Indian Banks, the current study restricted its scope to survey top executives and the risk professionals of the bank only to assess the present status and framework of operational risk in the selected organisation.

4. Research Tool

To achieve the aforementioned objectives of the study, information was obtained by interviewing the respondents through a structured interview schedule. In order to make the interview schedule exhaustive and meaningful, both open ended and close ended questions have been included. Before the final administration, the interview schedule has been duly modified and improved after making it subject to opinion and advice of academic experts and risk professionals from the bank. Since, the research is a case study type, as such it may mainly rely on the primary data to be collected from the organisation itself. Convenience sampling technique is chosen to select the respondents keeping in view size and characteristics of the population. The interview schedule used in the research was constructed on the basis of various dimensions taken from the survey tool (Moody’s Analytical Framework for assessment of Operational Risk Management in Banks) used by a renowned rating agency, Moody’s for Operational Risk Rating of banks. The said assessment methodology of Moody’s has also been used by D Tripati Rao & Prodipta Ghosh for constructing a questionnaire used for conducting research about the preparedness of Indian Banks in managing operational risk in the year 2008.

The interview schedule investigates the problem on the basis of following operational risk management dimensions:

- **General Background of Operational Risk Function:** This dimension tries to investigate general level of understanding of the operational risk management and the key operational risks being faced by the bank
- **Organisational Structure:** Under this dimension, various questions have been raised to find out whether there is an adequate organisation framework suitable to the size and complexity of the bank to take care of its exposure of Operational Risk.
• **Systems and Procedures including Information Technology:** This dimension seeks to address the three fundamental questions; Does the bank have adequate and appropriate systems? Are they regularly and independently reviewed? In the event of failure, what would be the impact on the bank, its earnings and its reputation?

• **Data Quantification and Modeling:** This dimension assesses the current status and progress made by the bank in operational risk measurement. It also investigates whether the operational risk measurement models are put to proper periodic validation.

• **Contingency Planning:** Under this dimension, bank’s disaster management and recovery plans will be investigated to understand how well they work and how often are they subject to review?

The inputs of the interviews will be summarised to give a descriptive analysis of the current operational risk management framework of the bank.

5. **Results And Discussion**

The present research attempts to study and understand the operational risk management framework of the Bank. To achieve the said objective, respondents in the form of risk professionals from the bank’s integrated risk management department, information technology experts from the bank’s IT department, and executives working in the area of risk management were interviewed through a semi-structured interview schedule consisting of both open-ended and close-ended questions covering various dimensions of operational risk management framework, like, *General Background of Operational Risk Function, Organisational Structure, Systems and Procedures including Informational Technology, Data Quantification and Modeling; and Contingency Planning.* The research instrument comprising of these five dimensions was structured and designed after a thorough literature review on the subject as given in the chapter II of the current study.

Further, the survey instrument is the outcome of a rigorous exercise attempted to elicit the true state of affairs of Operational Risk Management in the organisation under study. Based on Moody’s assessment tool for rating of operational risk management in banks, the questionnaire was designed and customised after taking opinion from academicians and experts in the area of risk management to make it more appropriate to conduct the present study. The survey instrument contains eighty four (84) questions which are spread over to five (5) dimensions. The flexibility of open-ended and close-ended questions was purposely put to ensure that the respondents feel at ease and to remove monotony of the single-design questions. The dimension wise empirical analysis is put forth in the succeeding pages.
5.1 General Background of Operational Risk Function

This segment of the research interview posed thirty one (31) questions to the respondents, out of which almost half of the questions were close-ended and the other half were open-ended. As per survey, the bank has developed a definition of operational risk on the basis of Reserve Bank of India (RBI) guidelines. RBI’s definition on operational risk follows the same belief as given by Basel Committee for Banking Supervision, in their draft known as Basel Accord 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”. Almost all the banks in India unlike banks in the developed countries follow a common definition of operational risk which is the one provided by the local banking regulator, Reserve Bank of India. The respondents were of the opinion that the RBI definition on operational risk adopted by the bank is broader and exhaustive and covers all material operational risk exposure of the bank. The said definition is believed to be ideal for the bank considering that it covered peculiar operational risk exposure of the bank understood from its historical operational loss experience. One of the respondents agreed that RBI definition on operational risk which owes its origin to Basel Accord is a standard definition of operational risk and is being followed by almost all the banks operating in India. The other response about ‘what definition bank followed for operational risk and how was it developed?’ was that the definition of operational risk adopted by the bank is exhaustive and appropriate for measuring operational risk capital charge considering the present regulatory guidelines. The basic purpose of operational risk capital charge is to give a safety cover to a bank against any potential operational mishaps. Bank doesn’t realise any need to have a unique or specific definition of operational risk particularly due to lack of proper understanding of the operational risk and in general it follows a reactive approach towards operational risk. In essence, operational risk should be managed on proactive basis. Such attitude towards operational risk got rooted in the bank due to the fact that historically bank has been less vulnerable to the events of operational risk. This could have probably happened due to a limited operational canvas of the bank (both in terms of limited branch spread as well as limited financial products we had during pre-deregulation times) or due to an effective control mechanism bank had in place to monitor and minimise such risks.

Various regulatory risks, like credit, market and operational risk being faced by the bank are separately segregated in each category. At present, bank is confronted with no issues of double counting as it still follows income based method, which is the Basic Indicator Approach with parallel run of the Standardised Approach for operational risk capital charge measurement. Double counting issues (dual counting of a risk event as both market and operational risk or credit and operational risk) are expected to arise as the bank moves to advanced measurement approach for operational risk. This method will rely on bank’s internal operational risk loss data for modelling of operational risk capital charge and not the proxies like, gross
income used by the present adhoc methods. According to the respondents, under BIA, since operational risk events are not considered for risk measurement and setting capital adequacy requirements, the scope of double counting is not there. Therefore, there is a chance of misidentification of risk as operational risk, when it was some other risk or vice-versa. This problem can distort the overall capital estimations and consequently capital requirements of a bank. A risk wrongly taken as credit risk or market risk, when in real sense it was operational risk, can underestimate or overestimate capital requirements as risk differentiation in credit and market risk is possible since banks follow advanced measures in such cases, while as no such feature is present in respect of operational risk wherein estimations are crude and based upon some proxies, like, gross income or outstanding loans and advances of a bank. One of the respondents was of the opinion that double counting issue do exist presently, but under BIA, it was difficult to separate the overlapping of operational risk with other forms of risk, like credit and market risk. Once the bank moves into advanced approach of operational risk management, it has to spell out a policy to avoid overlapping of counting of risks. Operational risk has a disguising nature. Operational risk at times, overlaps with other banking risks, like credit and market risk. A credit given by a bank to one of its clients may default, the cause of the problem might be forgery of loan documents, prima facie bank would take it as default risk and create sufficient provisions and later on, it may take it as operational risk and go for additional capital provisions. In the same manner, market losses could happen because of usual market volatility, but the cause for such loss could be primarily the violation of trading limits by a bank trader, such problems create overlapping instances. The definition of operational risk adopted by the bank includes legal risk and fraud risk. The definition, however, excludes the strategic risk and reputational risk which are being separately dealt under bank’s ICAAP\(^1\) programme. Under ICAAP (Internal Capital Adequacy Assessment Process), financial institutions are required to demonstrate to the regulator that they have an internal risk assessment and management information systems in place to efficiently assess their economic capital requirements. The bank in line with the regulatory conditions is having expressive and formal support from the board of directors for operational risk management. Board of directors of the bank is also responsible for determining and approving the risk appetite of the overall bank.

The survey reveals that respondents on an average identified lower regulatory capital requirement, reduced losses, improved prioritisation and targeting of resources as highly significant objectives of bank’s operational risk management framework. While as, pricing improvement, lower insurance premiums, lower cost of finance were on an average identified by respondents as objectives with lowest significance. Similarly, according to the respondents, lower operating costs, improved quality and stability of earnings, enhanced competitive position were given on an average moderate significance as objectives of operational risk management framework of the bank.
The outcome of survey shows that respondents on an average ranked technology and infrastructure deficiencies, difficulty in demonstrating cost-benefit analysis, lack of skilled or professionally qualified people as highly significant limitations to the progress of operational risk management in the bank. Likewise, lack of senior management involvement, limited budget, and bureaucratic organisation structure are ranked as least significant limitations to the progress of operational risk management in the bank. Also, respondents on an average basis gave moderate significance rank to lack of common definition and categories, inappropriate approach by group risk and no clear group-wide approach as limitations to the progress of operational risk management in the bank. In addition to these, some respondents identified lack of general awareness about operational risk on bank-wide basis, inadequate management information systems, data inadequacy as the significant hurdles in the development of operational risk management function in the bank.
As per views of the respondents, the bank claims to have in place one of the best operational risk management systems fully in line with the regulatory guidelines. Some of the weaknesses in the current operational risk management framework adopted by the bank were observed during the interview with the respondents as internal control deficiencies for which bank has hired consultancy services and software solution is expected during the current year. Bank also has been facing issues in finalisation of an appropriate risk measurement model and such difficulties were affecting migration to the advanced measurement method of operational risk capital charge calculation, migration to which is expected to bring capital relief to the bank and hence help in improving the banks value.

One of the respondents asserted that the bank followed a top-down approach and ideally it should have had a bottom-up approach and switch over to such an approach was in progress and Request for Proposal (RFP) had been already floated by the bank and the responses generated were being considered. Another respondent identified data inadequacy as a main weakness in the current operational risk management framework of the bank and asserted that the bank was currently engaged in collection and development of an operational risk loss database which would help the bank in advancing towards AMA. One more opinion of the respondents identified lack of proper awareness and education of operational risk at the business unit level as the main weakness in the current operational risk management framework. Such a problem affected the adequate and smooth flow of operational loss data from the business units.

The respondents feel that though bank has made very good progress in development of operational risk management framework in line with the requirements of Basel guidelines, yet it lags behind its competitors who are mainly represented by Axis Bank, HDFC Bank, ICICI Bank and Punjab National Bank. The respondents were of the opinion that, bank lagged behind new generation private sector banks in the development of operational risk management framework as these banks were technologically ahead of it. These banks have the privilege of starting lately and starting all operations from the beginning on information technology platform, while as the bank being researched had to transform its operations from manual mode to the electronic mode involving much complexity and time. As such, these new generation private sector bank could take operational risk management initiative much earlier than the Bank under study. The respondents rate the bank on an average at ‘Good’ category against these competitors.
All the respondents affirm positively that the bank follows a regular practice of training its general level managers for improving their competence to deal with matters relating to day to day operational risk management. They are also of the opinion that the bank does provide specialised training to its managers responsible for the risk function for improving their competence in handing operational risk management.

The bank as a whole doesn’t have any ‘whistle blowing system’ which could have been used to encourage disclosures about wrong doings threatening wider organisational interests. As per the information obtained during interview process, some cases of wrong doings on part of the constituents or information about operational loss events are reported, not openly but out of compulsion that such events are either too severe to be concealed or dressed up at the business unit level. Such a culture apart from affecting flow of information on the actual operational risk events is also impeding the availability of information on the ‘near-miss’ operational risk events happening in the bank. Operational risk events involving financial damages are widely publicised on the bank’s intranet site to create awareness among the stakeholders, involving mainly people working at different administrative levels and business units. Despite this, a culture of raising hands up at every fault doesn’t prop up in the whole institution for the fear of consequent disciplinary and reputational punishments. A whistle blowing system on the contrary, always requires incentives and motivations for encouraging confessions and disclosure about wrong doings and mistakes irrespective of their nature or potential threats.

Some respondents asserted that though there was no explicit whistle blowing system in place, and also operational risk policy of the bank also didn’t mention it, yet some inputs about the near miss events or materialised operational risk events flew to the global level through grapevine. Such flows of information from the individuals were usually motivated either due to realisation of moral obligation or were an outcome
of emotional attachment of the constituent (passing on that information) with their organisation. One of the respondents argued that audit in the bank worked as a whistle blower and alerts about violations were embedded in systems in certain cases to create such inputs.

The responses taken during the interview process reveal that the bank started to work on creation of operational risk management framework in line with new guidelines (post Basel Accord II) some five year ago, since the year 2007. However, humble efforts were made in loss data collection from the business units since the year 2010, where as such flow is being vigorously followed since last year only when bank issued a formal specimen instrument to be used by business units for loss data reporting. The said framework aimed to cover the exposure of operational risk across all the business lines of the bank. The president overlooking the Integrated Risk Management Department is also designated as the Chief Risk Officer of the Bank.

Response of the various interviewees regarding how they rated the level of progress made by the bank in various segments of operational risk, like risk identification, data collection and analysis, reporting, risk mitigation, risk modeling, and risk transfer is presented as below:

Diagram: 4 Level of Progress on various Operational Risk segments

The analysis of the data shows that the respondents have rated on an average the progress made by the bank in various layers of operational risk management function as ‘good’ in risk identification, data collection and analysis, risk mitigation and risk transfer, while as ‘reasonable’ in risk reporting and risk modelling activities. Progress in the areas of risk reporting and risk modelling has been reported as modest because of the reasons lack of preparedness and regulatory motivation in the implementation of operational risk management framework in Indian banking industry.
Operational Risk in banks started to attract explicit capital requirements after the announcement of Basel II Accord and its adoption by various countries, which include India as well. The accord suggests three different approaches of operational risk capital charge measurement viz, Basic Indicator Approach (BIA), The Standardised Approach (TSA) and Advanced Measurement Approach (AMA). These three different methods differ in terms of increasing complexity and requirement of capital produced by each of such methods. The banks have been suggested to begin with the simple one, i.e. Basic Indicator Approach and then after satisfying the supervisory conditions can move to advance measurement method, which is believed to align the regulatory and economic capital and bring a capital relief also in comparison to the simple Basic Indicator Approach. The Bank being researched in the present case is using BIA for measurement of operational risk capital charge. It is also following a parallel run of TSA to see how two approaches lead to variations in capital charge for operational risk, and in practice such variation between the estimates produced by two methods has been observed as insignificant. The process of moving to advance measurement method has already been undertaken and its progress is just waiting the finalisation of an appropriate operational risk model from the external vendors. The bank is yet to approach RBI with a proposal seeking approval of migration to AMA. In fact, a very few banks in India have so far sought approval for such scheme, however, RBI has set a timeline of September 2013 for granting of such approvals to the interested banks. The reason of slow progress in the development of operational risk measurement methodology based upon advanced or banks’ internal measurement models in case of bank being researched was attributed to banks’ lack of preparedness and also the lack of motivation from the local regulators’ side.

As a whole, the respondents are of unanimous opinion that the current guidelines which support practicing of income based methods of operational risk capital charge calculation, like BIA and TSA are faulty and produce misleading estimates as the proxy of operational risk (which in such cases is the gross income of the bank) has cyclical characteristics. In essence, a bank would need more operational risk capital during recessionary times as the incidence of operational risk events increases and less operational risk capital during normal times for lesser incidence of operational risk events. Empirical evidence supports that during recession, the incidence of credit card frauds increases which should lead to increase in operational risk capital requirements to support a bank’s solvency. Contrary to this, in recession, income comes down, so does capital given by BIA and TSA, as such leads to underestimation of operational risk capital requirements under these methods. Similarly, as income grows during boom periods, that is what would lead to overestimation of operational risk capital requirements under such methods during such times. These issues are expected to be resolved as soon a bank starts using AMA for measurement of its operational risk capital requirements. Some respondents argued that the current guideline were insufficient considering the subjective or institution specific nature of operational risk which makes it very complex for measurement. In addition to this, they also didn’t address
qualitative aspect of operational risk fully. However, in relation to AMA, the guidelines were thought to somewhat sufficient by some respondents.

To assess the operational risks in all of its material activities, bank in the past, though not exactly as per regulatory guidelines has undergone a Risk Control Self Assessment exercise (RCSA). The research suggests that the events of fraud, acts of burglary, system connectivity in remote areas, technological failures, skill deficiencies, political instability as the key operational risks being faced by the bank presently. People, which include both internal (employees) and external (clients and vendors), represent the categories due to which bank has faced huge operational losses in the past. Internal and external fraud according to respondents represents the operational risk event type implicating the bank with huge operational losses in the past. The biggest operational risk threats being faced by the bank and their solutions according to the respondents are enumerated below:

<table>
<thead>
<tr>
<th>Operational Risk threat</th>
<th>Respondent suggested measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology failures</td>
<td>Contingency planning, maintenance of backups.</td>
</tr>
<tr>
<td>People failures</td>
<td>Internal control and operational risk awareness.</td>
</tr>
<tr>
<td>Frauds</td>
<td>Adherence to Standard Operating Procedures (SOP).</td>
</tr>
<tr>
<td>Internal frauds</td>
<td>Making use of control and putting in place best checks and balances.</td>
</tr>
<tr>
<td>Absence of well defined processes</td>
<td>Setting up of Standard Operating Procedure (SOP) for various activities.</td>
</tr>
</tbody>
</table>

Through the feedback made by the respondents, it was observed that the Bank in the present case does not follow any practice of operational risk loss provisioning as a whole, however, in compliance to the regulatory guidelines, provision on frauds was being maintained by the bank since very long times. Apart from this, damage to physical property was being covered through property insurance. The bank has a formal operational risk policy document and it has been there in existence since the year 2007. The said policy document has the privilege of being approved by the board of directors of the bank. The policy documents are reviewed and updated every year to make it more appropriate to the changing profile of bank’s operational risk exposure and to incorporate new regulatory requirements. Bank’s Chief Risk Officer (CRO), is being briefed by the group risk function (operating in the bank’s integrated risk management department) with the operational risk reports on every half monthly basis, however, formal reports are submitted to the CRO on monthly basis. Such reports are also brought into the knowledge of the board of directors of the bank. However, they are made aware about such information on quarterly basis.
The bank prepares almost all the operational risk related reports as have been enquired through the interview. However, the reports which are prepared through risk management function include, chief risk officer’s report to the board, KRI’s report, and the reports which are prepared by other entities like, Human Resource Wing, Customer Care Division, Board Secretariat and audit wing etc. include reports like corporate governance report, audit report, IT report, key employee report, customer complaints report, and errors and escalation report. Reports from other entities are not presently being used by operational risk management function to assess associated operational risk dimension as could have been given by such reports.

Bank is not following the score card method to measure qualitative aspect of operational risk, however, risk based rating system through risk based internal audit is practiced since last two to three years. This method rates the business units for their risk management quality taking into account various parameters like control weaknesses and number of fraud cases occurred and reported in a given year. Key performance indicators report is not being prepared by the Risk Management function, however, key risk indicators report specific to fraud risk is being prepared since last four years. In order to prepare for various requirements of qualifying criteria set for adoption of AMA, bank has started collection of operational risk loss data and its analysis since last five years.

However, in absence of a proper sophisticated software solution to accomplish the task of loss data collection and analysis, bank has been doing such exercise currently in the Microsoft excel programme. Operational risk Value at Risk (OPVaR), Extreme Value Theory (EVT) and Risk Adjusted Return on Capital (RAROC) are not used currently, however, preparations to use such techniques are underway, subject bank’s attainment of qualifying criteria for AMA and its subsequent approval by the local regulator. Qualifying criteria for AMA requires among many things, a bank has to have sound and robust operational risk framework, rich operational risk loss data of at least five years, and board approved policy of operational risk management etc. Due to these reasons, economic capital for operational risk is not currently measured, leading to the main impediment in measurement of RAROC.

There was a mixed opinion about whether bank did obtain feedback of customers particularly distracting ones and was it being used for improving operational risk management of the bank. Some respondents agreed that it happened only to some extent, while others said that it was done only in respect of high net worth customers. A respondent asserted that such reports were regularly being obtained from concerned departments formally on quarterly basis to include them in assessment of operational risk exposure of the bank. Apart from this, number of customer complaints received in a given year is being considered an important indicator for operational risk assessment.
5.2 Organisational Structure

This section of the research comprises of thirteen (13) questions, out of which 23% questions were close ended while the rest 77% represented open ended questions. As per the respondents interviewed, about 90%, (i.e. seven out of the total of eight of the board members) of the board composition is represented by the independent non-executive members which is a strong qualitative indicator of good operational risk management framework currently installed in the bank. In response to a question whether any board member is well conversant with ORM, it was observed that one of the members among its board of directors is having expertise in the area of risk management who can provide the board an independent oversight in the matters concerning risk management including operational risk (Bank’s Annual Report 2013). At the board level, bank has constituted a committee known as Integrated Risk Management Committee (IRMC) with the specific responsibility of overlooking the management of market risk, credit risk and operational risk in an integrated and efficient manner. The various functions which the committee has been entrusted with to perform include, identification, monitoring and measurement of the risk profile of the bank, development of policies and procedures, verifying the models that are used for pricing complex products and also identification of new risks, development of policies that clearly spell out the quantitative prudential limits on various segments of bank’s operations and effectively communicating the risk strategy and policies throughout the organisation.

The said committee is headed by the chairman of the bank and includes three independent non-executive members from the board of directors. This committee, according to the respondents has been in existence since the year 2007 and it reports directly to the overall board on the matters of risk exposure of the bank. Bank has a specific operational risk management committee at the executive level, which is represented by the chief risk officer of the bank, heads of various functions like, business support division, strategy and business development, human resources wing, treasury, law, information technology, besides all executive presidents of the bank. This committee is also represented by members from other committees like, credit risk committee, market risk committee, and asset-liability management committee to ensure coherence and coordination among them. This is to address the requirements which arise due to specific nature of operational risk having overlapping relation with other forms of the banking risks, like credit and market risk.

Operational risk loss data aggregation followed a sequential process and flow in the bank. At the business unit level, loss data aggregation was entrusted with the designated operational risk manager. Thereafter, from individual branches such aggregated loss data went to the concerned zonal offices, where at respective zonal level operational risk managers consolidated the loss data coming from various business units. Each zonal level operational risk management function forwards the aggregate zonal level data to the Integrated Risk
Management Department (IRMD) of the bank, where finally whole loss data of the bank gets consolidated for development of loss database purpose. The respondents on an average basis rate the bank’s overall organisational structure for operational risk management as ‘competitive’.

**Diagram: 5 Organisation Structure of ORM**

### 5.3 Systems And Procedures Including Information Technology

This part of the research is based on sixteen (16) questions, most of which were open ended and the responses generated during the interview are summarised in the below. The survey interview reveals that the bank has a comprehensive set of policies, procedures, systems fully documented and has been placed on the organisation’s intranet website for the availability of users. However, as per one of the respondents, there is no thrust from bank for the users to understand the same. The various departments which are taken on board for preparation and approval of policies and procedures include external auditors, internal auditors, people from operational risk function, compliance, information technology, security and legal functions. The policies and procedures according to one of the respondents are active documents and as such, are reviewed by the information technology department of the bank on ongoing basis as and when there is a new development either on technology or regulatory front. The bank according to the respondents has a fully automated, centralised and integrated reporting system in place to cater to information reporting requirements. A respondent, however, disagreed and expressed that such reporting capability was only partially centralised and work on the residual centralisation was in progress. The data resides at the central data centre and the adequacy and integrity issues are ensured by application of various checks and balances by central data centre of the bank. Another view was that data adequacy and integrity was maintained by making IT systems subject to the checks by internal and external audit. All the respondents agreed that IT systems of the bank are sufficiently flexible towards reporting capabilities.
The bank, according to the respondents outsourced some of its IT activities, like network links, ATM switch, e-payment gateway etc. However, no core function of the bank was being outsourced. While outsourcing any activities, bank took care of due diligence measures by ensuring compliance to RBI’s guidelines regarding outsourcing to ensure that operational risks are kept under control. The bank has all of its business units on the Core Banking Solution\(^4\) (CBS) platform. Almost all the branches were being covered under the concurrent audit scheme of the bank. Concurrent audit mainly covers and attempts to identify and plug revenue leakages (like under charging of interest, fee, commission on loan accounts or overcharging of interest, etc on deposit liabilities) which could particularly happen because of any system malfunctions of inadequacies. Such audit was independently being performed by the supervision and control function of the bank.

Security violation reports which form an essential input for operational risk assessment in IT systems were being created by systems on ongoing basis but were being produced and investigated on daily basis. One of the respondents expressed that triggers were set in the firewalls\(^5\) and any alerts generated by them were being investigated very promptly. There were mixed responses from the respondents about whether the bank was having any IT audit and how often was such audit conducted, however, all respondents affirmed that such audit was suitably done in the bank. An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization’s goals or objectives. The responses supported that it was done on ongoing basis, (as systems have to comply every regulatory requirement soon they are imposed), and also on half yearly basis and yearly basis. All the respondents agreed that IT auditing in the bank was being exercised as an independent function.

Bank as a whole faced system disruptions very rarely once a year for a maximum of thirty (30) minutes of time due to hardware or communication failure, such disruptions were rare as bank had a strong redundancy link (buffer in the shape of second or multiple lines of defence) which are kept in high availability mode to cater to any potential technology or systems disruptions or failures. One of the respondents expressed that system disruptions happened historically for about 0.20% of the times and 99.8% of the times systems operations were smooth. One other respondent affirmed that few disruptions were due to the fact that bank has a state-of-art disaster recovery systems in place to take care of such future contingencies. Since disruptions in information technology systems witnessed were negligible, there was no formal practice of measuring impact of such failures on bank’s earnings. Similarly, no measurements of downtime costs, transaction failures were being assessed by the bank. The bank under survey had faced no hacking attacks on
its databases in the past. As such, the respondents as a whole felt that technology risk was not so significantly present in the bank. The customers were being sensitised about the possibility of ‘phishing attacks’ and their adverse consequence through mobile text messages and other modes. According to respondents, various IT codes and guidelines which the bank complied included ISO 27001, PCI-DSS, BS 7799, IT Act, Data Protection Act to ensure system safety and security. Beyond these safeguard measures, bank is also compliant towards RBI’s regulations on IT e-governance. Similarly, access to bank’s data warehouse was strictly restricted and only concerned IT people were allowed to access the said facility. Restriction to the free entry was being maintained by imposition of biometric and logical barriers at such installations.

5.4 Data Quantification And Modeling

This segment of the research was conducted with the help of nine (9) questions, most of which were open-ended. The response of the interviewees shows that loss data collection about operational risk has been in exercise in the bank since last five years. The threshold for an operational loss event has been set by the bank at Rs 10,000 which was determined in accordance with the regulatory guidelines and also the operational risk policy of the bank. The threshold of the loss among various things depends mainly on the size of the institution. According to RBI guidelines, banks in India have been asked to determine their threshold for operational risk loss events for data collection and its subsequent risk modelling purposes subject to a maximum ceiling of Rs 50,000. As such, there is no ceiling on the lower floor of the operational risk loss events threshold, only upper cap is maintained by the RBI. The underlying principle is also that the branch can handle a loss itself which is less than the threshold level, however, all losses irrespective of their size are generally reported for data collection and aggregation. The bank considered in the present study collects data about all operational risk loss events irrespective of the threshold and their size. One of the respondents expressed that threshold for operational losses for the purpose of reporting was determined on the basis of analysis of bank’s historical operational losses and the risk bearing capacity of each branch. Another respondent suggested that threshold of operational losses for the sake of reporting was worked out on judgmental basis. One more response from the interviewees revealed that such threshold was set as per the RBI guidelines.

The loss data so collected is drawn separately from each business line and segregated into various event types as per Basel II guidelines. Presently, the bank is not using any external data for operational risk modelling for the reason that operational risk loss modelling is yet at a nascent stage in the bank. One of the respondents affirmed that some consortium data is availed by the bank occasionally from RBI and IBA, but it is not being used by the bank for any risk measurement presently.
All the respondents expressed that though bank was yet to start modeling of operational risk, yet they followed the practice of collecting operational risk loss data for future use from the media reports. Banks have been asked to use external loss data for scenario building after properly scaling such external data to their requirements. External loss data obtained from vendors or loss data consortiums is widely used by the banks in the developed countries to supplement their internal loss data or in case of insufficiency of internal proprietary loss data. Indian Banks’ Association (IBA) took an initiative to create a loss data consortium which was named as Credit Operational Risk Data Exchange (CORDEX). The Bank being researched also gave its consent to participate in the said consortium, however, the consortium could not take off practically until date. The respondents favored that the current regulatory guidelines are sufficient to guide the bank in development of loss data and its quantification which would ultimately end up in migration towards AMA. The bank does track 'near misses'. However, since it is a bottom up exercise, as such, much data doesn’t flow from the business units for the fear of reprimand and follow up actions from various controlling entities. One more respondent favored that near-misses were reported partially by the designated operational risk managers. The bank plans to use in future both Extreme Value Theory (EVT) as well as operational risk VaR as methods for quantification of operational risk economic capital. The respondents belonging to the risk management group believe that the existing technology is not sufficient to support loss data collection of the bank. To address this problem, bank is currently consulting the vendors and software solution would be acquired very soon. The bank has so far not done any exercise of evaluating the estimated cost of expenditure for switching to AMA. However, cost of software solution and consultancy charges have already been worked out.

5.5 Contingency Planning
This segment of the research interviewed the respondents with fifteen open-ended questions which were aimed at capturing the contingency planning aspect of the operational risk management framework existing in the bank. According to respondents’ views, bank’s contingency plans are very robust and cover all its critical and essential facilities. The whole facilities being operated by the bank can be bifurcated into three categories like, critical, essential and desirable with varying degrees of significance. For example, core banking systems, ATM services and e-banking are among the facilities categorised as critical. Critical facilities are the ones which need to be restored without much time lag while the essential and desirable can afford some lag time. The bank has three data centers located at different seismic zones in Gurgaon, Noida and Mumbai. Bank’s data centers as per respondents are equipped with one of the state-of- art technology and are best among banks operating in India. The main data center operating at Gurgaon is housed in a premise which has been designed to be disaster free. These data centers house mirror records of data which a bank can use in the times of a natural disaster or technological failure. Every year, bank conducts two technology drills as
a contingency measure. Besides this, evacuation and fire exit drills are also carried out at the large establishments like corporate office, zonal offices and the business units having heavy foot fall.

Almost all the facilities/business units are equipped with CCTV surveillance, however, in certain units, such measures have been taken at critical places like locker room only. A respondent was of this opinion that such measures are only taken in case of business units having large foot fall (inflow of clients). The other respondent affirmed that not all but only main business units/facilities are covered under such surveillance. However, all ATMs and currency chests are fully covered under such CCTV surveillance programme. One of the respondents was of this opinion that all business units of the bank will be covered under CCTV surveillance during the current year. One more respondent asserted that as per the policy, all facilities have to be provided with CCTV surveillance, but currently only 20-30% facilities roughly have been covered and progress to acquire such equipments were on in rest of business units. Another respondent favored that CCTV surveillance was based on the size of a business unit.

All branches of the bank are not equipped with the ‘counterfeit currency detection machines’. Such measures are only taken at business units having large volume of transactions. As per policy, business units with a cash retention limit of rupees five lakh have to keep counterfeit currency detection machines for tracking of counterfeit currency notes.

As per respondents, robbery alarm is fitted in every branch and access to such safety measure has been kept at one or two locations, particularly, branch head and hall incharge or cash counters of the business unit. Similarly, ‘smoke detectors’ are also not everywhere but have been installed at all vital locations. Ones of the respondents agreed that all business units were protected by way of smoke detectors. All the respondents were of this view that bank has ‘fire extinguishers’ installed in every business unit and offices and such equipments are regularly checked for their effectiveness and also refilled properly without missing the expiry dates.

In response to whether any precautions were taken by the bank to minimise employee/customer physical accidents/injuries, there was a mixed response. Some respondents stressed that there was no need to have such measures as no such incidents had been reported in past. One response was that bank takes proper care of old and aged clients (who are more vulnerable to such hazards) by sensitising them adequately. Bank through its business support division also tries to ensure that business units are acquired in ground floors to avoid much inconvenience to the clients. One of the respondents expressed that safety measures were being taken by the bank to have multiple fire exits at all vital locations so as to avoid physical injuries in the times
of emergent situations leading to quick and unprecedented human evacuations. One more opinion argued that
bank had issued a code of conduct for its employees as to how to deal with the customers so as to avoid
physical assaults. All respondents unanimously agreed that bank had no financial litigations in past due to
clients/employees facing physical injuries or accidents while they were availing/providing banking services.
Under disaster recovery plan, bank has set two objectives named as **Recovery Time Objective (RTO)** and
**Recovery Point Objective (RPO)**. In the aftermath of a major disaster, in terms of these two objectives, a
business unit or overall bank is expected to be up and running within the shortest time i.e. half an hour and
without incurring any data loss. All data from the point when a disaster occurred is assumed to restore back
to ensure uninterrupted operations. One of the respondents expressed that the recovery time set ranged from a
day to two depending on severity of the disaster happened. One more opinion suggested that recovery time
was as short as two to three hours only, as bank can’t afford disruptions in operations for longer durations.

A respondent said that recovery time set was maximum one day. In response to a question, whether there was
any possibility that a failure event would lead to loss of key customers, response obtained were mixed. One
respondent expressed that business continuity plans covered all issues related to any possibility that a failure
event would lead to loss of key customers. Other respondents suggested that customers were pursued to stay
committed in the event of any such eventualities. Some respondents were of this opinion that the bank as a
whole had not such vulnerability of losing any key customer in the event of failures. Risk management
function is not assessing the impact of any possible exit/absence of key employees as per the respondents’
views. Such things were taken care of by the bank’s human resource wing by way of succession planning.
Under such succession planning, positions upto the level of assistant vice president were covered. The
perceptions of the respondents about how the banks’ business continuity plans have worked in past and how
they would rate them for future is analysed below:

*Diagram: 6 Business Continuity Plans*
As per the above data, respondents rate the working of bank’s business continuity plans in past and for future as, ‘excellent’.

5.6 Progress Of ORM Framework In The Organisation Under Study

The present study attempted to assess the current state of progress of the organisation using an assessment methodology based upon five prominent dimensions of operational risk management as given under Moody’s risk assessment tool.

**Evolved Framework**

A well developed organisation is ideally expected to have achieved progress in all the dimensions of operational risk management function as shown in the diagram - all rounded balls touching the inside boundary of the ORM wheel. Each shaded ball’s movement from the centre towards the inside boundary wall represent the dimension’s progress. Any retreat or fall back would be reckoned as a decline or stagnation in the progress. Banking institutions of advanced countries particularly those in Western Europe or Northern America have their ORM framework at an evolved stage – all dimensions well progressed. All dimensions are perfectly aligned and synchronised. Their organisational advancement is ideally the one indicated in the wagon wheel diagram 7.

**Primitive Framework**

A primitive ORM framework is the one whose all five dimensions have not progressed at all. All of them are at nascent stage as indicated in the Diagram 5, Primitive Framework. ORM framework in the primitive could be true more in theory, however, in practice, banks whatever regions they operate or how old they may be, somewhat progress is found everywhere as the operational risk is very old and its management has been with banks ever since their origin. As such, banks right from their
beginning have been somehow managing operational risk traditionally by safety measures, control mechanism, audit exercises and other checks and balances which puts them at a stage above the primitive stage.

**An unaligned, unsynchronised ORM framework for the Bank under study**

The ORM framework in all its dimensions as testified and researched in the organisation under study does not conform the standards of a highly evolved ORM framework. Pertinently, it does not even fall to primitive stage framework either, at least, not in all dimensions. Some of the dimensions are a nascent stage (primitive) like data quantification and modelling and OR knowledge and awareness. The dimensions of the ORM framework in the organisation under study do not synchronise with each other and the ORM framework, as a result, is not properly aligned.

6. Conclusions

The state of affairs in respect of development of these two stages of ORM, knowledge and awareness and data quantification and modelling is generally observed in the whole banking industry in India. Lack of operational risk awareness is due to the reasons that operational risk though being very old banking risk, but the evolution as its quantification and explicit capital requirement are recent and banks have not been able to emphasise its understanding at the operative level. Until now, focus has been on the development of a global level risk management function to support ORM framework creation activity. There has been lack of stress on understanding and creation of awareness among the business unit level people about the issue of operational risk. This state has led to the problems in identification of operational risk, its documentation and finally the reporting for loss data aggregation. The bank under study also lacks adequate emphasis on training and creating awareness of operational risk among the people at ground level in terms of the new demands. Bank need to create linkages between risk management function, training departments, human resources wing and the business units in order to create mass awareness about the operational risk. Traditional understanding of management of operational risk through controls, safety measures, checks and balances and audit mechanism are well known to the constituents working at all levels in the bank, but need actually exist for creation of awareness about how to address ORM for its quantification and modelling related issues.
Banks in India have in general started late in addressing the new challenges and as such continue under to be under preparatory stage. Similarly bank under the present study lacks sufficient operational loss data. Much of the rich data is present about fraud risk because fraud risk reporting has been followed in the bank even before operational risk reporting has come into being. Though data collection exercise has been started as early as since year 2007, but rich data about operational risk is flowing only since last two years. Operational risk modelling is grounded in a rich operational risk loss data of atleast five years. Data collection is facing huge problems presently also due to the lack of proper understanding of operational risk at the reporting entity levels. This is what is hampering the progress in the stage of data quantification and risk modelling.

**Explanatory notes**

1. ICAAP is a procedure ensuring that executive bodies appropriately identify, measure, aggregate and monitor the risks incurred by the institution, possess the capital coverage determined by internal regulations that is sufficient for the fundamental risks the institution is exposed to and have an adequate risk management system in place, which they continuously develop in accordance with the risk factors identified.

2. Whistle blowing is when a worker reports suspected wrongdoing at work. Officially this is called ‘making a disclosure in the public interest’. A worker can report things that aren’t right, are illegal or if anyone at work is neglecting their duties, including someone’s health and safety is in danger, damage to the environment, a criminal offence the company isn’t obeying the law (like not having the right insurance) covering up wrongdoing.

3. A near miss is an unplanned event that did not result in injury, illness, or damage but had the potential to do so.

4. Core Banking Solution (CBS) is the networking of bank branches which enables customers to operate their accounts and avail banking services from any branch of the bank on CBS network, regardless of where they maintain their account. The customer is no more the customer of a branch. He becomes the bank’s customer. Thus CBS is a step towards enhancing customer convenience through anywhere and anytime banking. With the introduction of CBS, the limitations of time and space have been done away with as customers can now operate their accounts from any location of the bank regardless of where they would have been maintaining their accounts.

5. A firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on a rule set. A network’s firewall builds a bridge between the internal network or computer it protects, upon securing that the other network is secure and trusted, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted.

6. The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit
a website where they are asked to update personal information, such as passwords and credit card, social security and bank account numbers that the legitimate organisation already has. The website, however, is bogus and set up only to steal the user information.

7. A loss data consortium is a group of financial institutions that has agreed to pool its loss data, according to defined reporting levels and category definitions.

7. References


Martin Philip H. 2009. “As risk management evolves, is operational risk management important?” The Journal of Operational Risk, Volume 4, Number 4, pp. 75-84.


