OPERATIONAL RISK IN BANKS: A REVIEW

Mr. Sartaj Hussain  
Assistant Professor, Department of Business & Financial Studies,  
University of Kashmir Srinagar Kashmir, India  
Email: sartaj.hussain@gmail.com

Dr. Mohammad Shafi,  
Associate Professor, Department of Business & Financial Studies,  
University of Kashmir Srinagar Kashmir, India  
Email: meem_shafi@yahoo.com

ABSTRACT

Operational risk, in general, is inherent in every human activity and as such is akin to banking as well. It arises from a wide range of activities like acts of frauds, errors, negligence, violations, events of technological failures, process deficiencies, systems flaws, acts of terrorists and vandalism, natural disasters, like floods, earthquakes etc. Increased potential of operational risk during the last three decades witnessed in the form of some mega bank failures like Barings, LTCM and Daiwa has brought it under the capital adequacy ambit imposed by banking regulatory bodies across the world. In the times to come, Operational risk regulation is believed to be the next frontier of efficiency enhancement and value creation in the banks. Unlike other risks covered under regulatory capital regime (like credit and market risk), operational risk has attracted huge controversy surrounding its diverse nature which comprises of its definition, causes, management approaches, measurement models and imposition of regulatory capital charge. The current paper attempts to review various such issues concerning and confronting the operational risk management thought in banking industry.

Keywords: Operational Risk (OR), Basel Committee for Banking Supervision, LDCE, BIA, TSA, AMA, EVT, LDA.

Introduction:

The aftermath of the bank failures in the matured economies particularly during the early eighties marked by the failure of some prominent financial institutions like, Barings of UK, LTCM of US and Daiwa of Japan has led to increased concerns among bank regulatory bodies across the world about the disastrous consequences of Operational risk. Operational risk is in general inherent in every human activity, as such arises in banking as well. Operational risk is commonly defined as the risk of some adverse outcome resulting from acts undertaken or not (Jobst 2007). Operational risk is involuntary in nature, as it exists much before any loan is being made by a bank or any amount is invested in financial securities. As such, banks right from their inception, have been familiar about the consequences of operational risk, Operational risk, therefore, is not a new risk, however, the idea that operational risk management is a discipline with its own management structure, tools and processes, is new (Power 2005). Operational risk exposure in banks which primarily arises due to the failure of people, processes and systems, and from external events is believed to have been fuelled during the last two decades particularly by their increased thrust on IT enabled banking, massive shift from manual to computer based electronic operations, introduction of e-banking and internet banking facilities. All these developments have increased the pace at which banks process or manufacture transactions, so their exposure to this particular risk has equally multiplied leading to wider recognition of the operational risk across the banking industry. Though Operational risk is as old as banking, yet during the second half of the 1990’s and the early 2000’s, Operational risk has become more and more significant for the financial industry. Human beings are considered a major source of this risk. As reported by the Federal Reserve Bank of Boston, financial institutions have experienced more than 100 operational loss events exceeding $ 100 million over the past decade. (Resti & Sironi 2007) The majority of these loss events have been reportedly represented by human frauds. In response to this, Operational risk exposure of banks was brought under the explicit capital charge by the introduction of Basel II Accord during 2004, which has been by now adopted by majority of the banking regulators worldwide. Such a capital regulation in general is believed to create more
efficiency in banks and give them a competitive edge and ensure their long term sustenance, survival, better reputation and credibility in financial markets in particular.

**Review of Research on Operational Risk:** Until recently many researchers have shown interest in the field of management of operational risk in banks. Numerous empirical studies have been carried to cover various aspects of operational risk like its definitional issues, causes and effects of operational risk, management approaches, measurement models, evaluation of regulatory capital charge methods etc. Researches on the subject have also been conducted in India, although on a limited count. The main findings and suggestions of many of such studies are reviewed below taking the above dimensions as major premises. At the end, an attempt is made to identify the potential research areas in the field of Operational Risk.

**Definitional issues:** Unlike credit and market risk, Operational risk (OR) falls under a unique risk category which has until now witnessed a huge controversy in its understanding and scope among financial institutions, academia, and regulators across the world. Though introduction of regulatory definition of operational risk under Basel Accord II has to some extent helped financial industry worldwide to make a beginning towards development of operational risk management framework, however, controversies again seem to have erupted as the financial institutions have been stressed by regulators to progress and advance in operational risk management by adopting advanced operational risk measurement methods based on sophisticated statistical and mathematical models. Power (2005) argues that operational risk has been fiercely contested by the international banks and three key domains of policy controversy have been, and remain, particularly visible: definitional issues, data collection and limits of quantification. Until recently, operational risk was treated as a residual risk category, Rao and Dev (2006) argue that “it was not uncommon, five years ago, to consider OR as a residual”, and that “everything other than credit risk and market risk was, by default, OR”.

This was the most common view among the practitioners as Medov and Kyriacou (2001) are convinced that thinking of operational risk as “everything not covered by exposure to credit and market risk” remains prevalent among the practitioners. Jameson (1998) also held the same view when he found that the definition given most frequently during a telephonic survey was “every risk source that lies outside the areas covered by market and credit risk”. Till early 1990’s viewing operational risk as a residual and unquantifiable risk was merely because of lack of its understanding and its diversity due to innumerable causes. Following the Barings Bank fiasco, and other similar publicly disclosed bank losses due to fraud and control failures, the financial industry started to recognise rogue trading and the like as a separate risk category, comprising such a nature of risk that could not be classified as either credit or market risk. King (2001) supports this thought by defining operational risk as the risk, “not related to the way a firm finances its business, but rather to the way a firm operates its business”. Crouchy et al. (1998) define operational risk as, “the risk that external events, or deficiencies in internal controls or information systems, will result in a loss - whether the loss is anticipated to some extent or entirely unexpected. Moosa (2007) argues operational risk is the risk of losses arising from the materialization of a wide variety of events including fraud, theft, computer hacking, loss of key staff members, lawsuits, loss of information, terrorism, vandalism and natural disasters.

Chaudhury (2010) argues Operational risk is highly company and operations specific, and unlike market, credit, interest rate and foreign exchange risks, a higher level of operational risk exposure is not generally rewarded with a higher expected return. Cristina et al. (2008) define the operational risk as the risk of the direct income loss, which results from internal events connected to inadequate personal, important errors or illegal behavior because of the errors or the systems and processes inadequation, or from external events where the risks are not covered by the credit, market or interest rate risk. The Group of Thirty* (1993) defined operational risk as, “uncertainty related to losses resulting from inadequate systems or controls, human error or management”. The most widely used definition of operational risk, and also the definition adopted by Basel committee for banking supervision (BCBS) in their capital accord (2001a) which resulted from an industry study conducted by the British Bankers’ Association, the International Swaps and Derivatives Association, RMA and PricewaterhouseCoopers (BBA, ISDA, PwC, RMA, 1999) puts operational risk as, “the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events”. This definition which is based on the underlying causes (sources) of operational risk (or rather operational losses), includes legal risk but excludes business and reputational risk. Due to this reason, BCBS’s definition of operational risk has faced lot of criticism for lack of industry consensus and for being flawed.
Kuritzkes (2002) suggests that operational risk is a non-financial risk that has three sources. The first is internal risk such as risk of rogue traders. The second is external risk, which is uncontrollable external event such as a terrorist attack or weather destruction. The third is business event risk, which captures many things such as price wars or stock market downturn. Kuritzkes argues that business risk is the most important but is ignored in the proposed Basel accord. Thirlwell (2002) argues that the BCBS’s definition represents a “measurable view of operational risk if you are trying to come up with something which is quantifiable, but not good if you think about what causes banks to fail.” Similar view are put forth by Cagan (2001) while arguing that Basel committee’s definition of operational risk is designed solely for the purposes of quantifying the operational risk loss data for the sake of capital measurement, while the definition lacks coverage of operational risk that encompasses qualitative concerns (softer and less quantifiable losses for the sake of qualitative analysis).

Hadjiemmanuil (2003) describes the definition of operational risk given by BCBS as, “opaque and “open ended”, because it fails to specify the component factors of operational risk or its relation to other forms of risk. According to Hadjiemmanuil, the definition leaves unanswered many questions concerning the exact range of loss events that can be attributed to operational failures. Culp (2001) notes that operational risk is so broad a concept, that it can be found anywhere. Therefore, an appropriate strategy is not in identifying all operational risks, but rather in identifying important operational risks that can affect the value of a firm. Cagan (2001) argues that the definition of BCBS does not encompass the qualitative concerns of operational risk. Marliana et al. (2011) observe that the basic Basel definition of operational risk suits ideally to Islamic Banking institutions (IBI) also, however it needs adaptation to take care of their specific operational risk characteristics of such IBIs, (like sharia compliance risk, legal risks). Moosa (2007) examines and analyses various controversies surrounding the concept of operational risk, particularly its definition and nature. Due to this reason, Operational risk continues to be the only risk category having regulatory definition, and this definition also has confronted criticism of being too narrow or too wide. The author also discusses the disagreements in various characteristics of operational risk, like whether its one-sided, having loss potential only, whether it is idiosyncratic, limited to on organisation only without systemic implications and whether it is transferable like other risks. All these controversies raise an important question of whether operational risk should be regulated or left to be managed by the banks themselves through effective control only. Muermann and Oktem (2002) argue that operational risk being much of idiosyncratic in nature should have an organisation specific definition based on cause and consequences rather than a common definition. An appropriate operational risk definition which could serve both the management and measurement requirements of the financial industry remains a quest with the scholars, practitioners, regulators worldwide at large. As of yet, financial industry and the regulators are focusing on development of a prudent framework to address the issue of operational risk exposure, while laying less emphasis on finding a suitable organisation-specific definition of operational risk due to lack of understanding and ambiguity in the nature in which operational risk manifests and also due to their reliance on the BCBS’s definition. Developing perfect definition of operational risk seems difficult and the choice lies in finding one between idealism and pragmatism, with the later seeming to be a better choice. A pragmatic Operational risk definition marks the basic foundation of both an effective operational risk measurement and management programme, ultimately intended to ensure bank soundness and a source of enhancing competitive advantage.

**Causes and Effects of Operational Risk:** A number of studies have been done to find out the major causes and effects of operational risk. Among these studies, Operational Risk Loss Data Collection Exercise (LDCE) conducted by the Risk Management Group (RMG) of the Basel Committee on Banking Supervision from time to time since 2000 provides important insights about the major causes of operational risk in the financial industry. The first LDCE collected internal loss data for the three-year period 1998-2000 from 30 banks in 11 countries. The second LDCE (the 2002 LDCE) collected internal loss data for the year 2001 from 89 participating banks in 19 countries. As per the 2008 LDCE conducted by BCBS’s sub-group on operational risk, known as Operational Risk Subgroup of the Standards Implementation Group (SIGOR) by event type, the highest frequencies were related to Execution, Delivery, and Process Management (EDPM) (30.6%) and External Fraud (26.3%) events. Losses related to Damage to Physical Assets (DPA) and Business Disruption and System Failures (BDSF) each had 2% or less of annual frequency. These results differ slightly from the 2002 LDCE where the majority of losses (44%) were attributed to External Fraud followed by EDPM.
This apparent shift may reflect increased efforts by banks to capture losses relating to event types other than External Fraud as many banks had existing processes to collect External Fraud losses prior to implementing an operational loss data collection program. Thus in early years of data collection, collection of External Fraud losses may have been more complete. The study used a gross operational loss threshold of €20,000. Similarly, by event type, the highest annualized sum of losses (€5.1 billion) was for CPBP events. CPBP events contributed 52% of the annualized loss amount and only 18% of the annualized frequency, which suggests that CPBP losses tend to be larger than those related to other event types. The lowest loss amounts were related to DPA and BDSF, both of which accounted for less than 2% of the total annual loss amount. These results appear to differ from the 2002 LDCE where the majority of the total loss amount was attributed to EDPM (30%) followed by DPA (29%). The results for DPA were significantly lower in the 2008 LDCE as DPA was 29% of the total loss amount in the 2002 LDCE compared to 1% in the current LDCE. This change likely reflects the difference in the time periods of the underlying data in each exercise and particularly the large influence of losses related to the 2001 terrorist attacks in the United States. Moosa and Silvapulle (2010) argue that announcement of operational losses has an adverse effect on the stock price and market value of the announcing bank. Based upon analysis of 54 operational loss events experienced by eight Australian banks during the period 1990–2007 they found out that decline in the market value of a bank announcing an operational loss event is predominantly greater than the announced loss amount. Shib, Khan and Medapa (2000) argue size of the firm is weakly related to size of loss, and the authors suspect that majority of the variability is caused by factors, such as inherent differences, in risk (based on types of business conducted), the competence of management and quality of internal control environment. Moosa (2011) examines the frequency and severity of the operational losses incurred by U.S. firms during the period 1990–2007, as reported by Fitch Risk. The losses are examined in relation to the state of the U.S. economy as represented by the unemployment rate, which is the macroeconomic variable that is most intuitively appealing in terms of association with the incidence of operational losses. The results of structural time series modeling reveal that while total severity and average severity are positively related to the unemployment rate, the frequency of losses is not. Gillet, Hubner and Plunus (2010) analysed 154 events of operational risk occurring between 1990 and 2004 in companies belonging to the financial sector and that are listed on the major European and US Stock Exchanges and found that significant, negative effects on the stock market returns at the announcement date of the loss, along with an increase in the volumes of trade. Further, in cases of internal fraud, the loss in market value is greater than the operational loss amount announced, which is interpreted as a sign of reputational damage. Further, breaking down losses to frequency and severity, it is found that correlation with institution size and frequency parameter is stronger and is much more so than the correlation with size of individual loss events. The findings support the application of gross income for simple operational risk capital allocation methods.

Management approaches: Operational Risk management attracts considerable attention from financial industry as well as academicians towards development of a distinct process for ORM. 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. 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. Nettet and Poulsen (2003) emphasize that either due to new regulations or the increasing level of operational risk in financial services 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. Basel Committee (2003) suggests ten principles of sound operational risk management which cover four important dimensions of operational risk management framework. The principles include,

**Principle 1. OR as a distinct risk category:** The board of directors should be aware of the major aspects of the bank’s operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank’s operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

**Principle 2. OR framework should be subject to internal audit:** The board of directors should ensure that the bank’s operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

**Principle 3. OR should be consistently implemented by senior management:** Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organization, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank’s material products, activities, processes and systems, material products, activities, processes and systems.

**Principle 4. Necessary OR assessment of new products, activities, processes and systems, etc:** Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

**Principle 5. Proactive management of OR by ensuring regular reporting to top management:** Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

**Principle 6. Periodic review of OR exposures:** Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

**Principle 7. Existence of Contingency and Business Continuity planning:** Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

**Principle 8. Presence of an effective framework for OR mitigation:** Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.

**Principle 9. Supervisory evaluation of OR framework:** Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank’s policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

**Principle 10. Sufficient disclosure to market participants:** Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

These principles provide banks with guidance regarding development of various segments of the operational risk management framework, like principle 1 to 3 concerns development of an appropriate risk management environment, principle 4 to 7 relate to various stages of risk management process,(identification, assessment, monitoring, and mitigation/control), principle 8 and 9 describe role of supervisors and principle 10 suggests role of disclosure. 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 and developing
monitoring systems. Moosa (2007) discusses the disagreements in various characteristics of operational risk, like whether its one-sided, having loss potential only, whether it is idiosyncratic, limited to on organisation only without systemic implications and whether it is transferable like other risks. All controversies raise a significant question of whether operational risk should be regulated or left to be managed by the banks themselves through effective control only. Ford and Sundmacher (2004) argue that 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. 

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. 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 “prioritizing 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.

Measurement models: There are numerous measurement models for measurement of operational risk. Hiwatashi (2002, p 2) discusses several ways in which operational risk is could be measured. These methods are broadly classified as “top down” or “bottom up” methods. In top-down methods, risk is estimated based on macro data without identifying the individual events or the causes of losses. One top-down method uses indicator approach, where some variable, perhaps gross income or cost is a proxy for firm performance and a certain percentage of the variation in that variable is considered as risk. Another approach relies on the CAPM, where total risk is estimated using CAPM model. Then, market risk and credit risk are subtracted and what is left is considered as operational risk. In the volatility approach, the volatility of some variable, say non-interest income is treated as the operational risk. Hiwatashi (2002) also provides illustrations of the bottom-up methods of measuring operational risk, which uses individual events to determine the source and amount of operational risk. These methods include the statistical measurement approach, where operational risk is measured using data from individual events with frequency based on a Monte Carlo simulation or an analytical solution. Another approach is scenario analysis, where losses are estimated based on scenarios derived from other banks and events. A third approach is factor analysis, where factors related to losses are identified and used to calculate risk. King (2001, p 73) discusses Delta methodology, which is based on error propagation. Under delta methodology, the uncertainty of risk factors is used to calculate the uncertainty in earnings based on sensitivities. The sensitivities represent the correlations of the changes in earnings with
change in risk factors. The delta methodology allows losses to be predicted when there is no comprehensive loss data. In addition, it is linked to business activities through the sensitivities. A final method of operational risk measurement considered by King uses Bayesian Network Models to model causes and effects of operational risk. Culp (2001, p. 435) also discusses methods of measuring operational risk based on four regimes suggested by the ISDA (International Swaps and Derivatives Association). The first is the “basic indicator” regime. Measurement is based on a few roughly defined risk indicators. The firm usually uses an adhoc control process that depends on existing controls (such as audits) for operational risk management. Often firms use industry or regulatory measures of operational risk. The second is the “standard lines of business” regime. Here the risk management process is less adhoc and operational risk is measured at the business unit level, often using survey data. The “internal ratings” regime uses subjectively determined quantitative ratings for specific operational risk factors in individual business units. Fourth, the “internal models” regime uses institution-specific loss data and then uses structural econometric models (like credit scoring models) or analytical-and simulation-based VaR-like constructs to determine operational risk.

The BCBS (2004a) suggests that if banks move from the BIA along a continuum towards the Advanced Measurement Approaches (AMA), they will be rewarded with a lower capital charge. The regulatory capital requirement is calculated by using the bank’s internal operational risk model. One of the objectives of the Basel II Accord is to align regulatory capital with the economic capital determined by the banks’ internal models, which can be achieved by using the AMA. Under this approach, banks must quantify operational risk capital requirements for seven types of risk and eight business lines, a total of 56 separate cells, where a cell is a combination of business line and event type. These estimates are aggregated to obtain a total operational risk capital requirement for the bank as a whole, thus ignoring correlation. The problem is that it is not quite clear what the AMA comprises. For example, Chapelle et al. (2004) define the AMA as encompassing “all measurement techniques that lead to a precise measurement of the exposure of each business line of a financial institution to each category of operational loss event”. It is sometimes described as encompassing three versions: the Loss Distribution Approach (LDA), the Scenario-Based Approach (SBA) and the Score Card approach (SCA). The basis of classification here is the nature of the data required to implement the procedure: while the LDA depends on historical data (hence, it is backward-looking), the other two approaches are forward-looking because hypothetical futuristic data is collected from “expert opinion” via scenario analysis and scorecards. The author argues that given the firm-specific nature of operational risk and the lack of high-severity experience for most units of measure, banks would normally be inclined towards relying on internal loss data for the estimation of their operational risk capital requirements. The author also highlights the crucial issues like presence of a shallow loss data history, reporting delays and measurement errors in the data, protracted loss events possibly spanning multiple units of measure and changing business dynamics including acquisitions and corporate restructurings which banks may face in LDA operational risk modelling. Shevchenko (2010), emphasizes that Bayesian methods can be well suited for modeling Operational Risk. Bayesian framework, in particular is convenient to combine different data sources (internal data, external data and expert opinions) and to account for the relevant uncertainties. Montia, Brunner, Piacenza and Bazzarello (2010), using internal risk model (loss distribution approach) based on monthly internal loss data of UniCredit Group (UCG) the authors have shown how operational risk dependencies can be modeled to produce correlation effect and thereby provide institution capital relief in terms of reduced capital requirements for operational risk. Chernobai et al. (2008), using 24 years of U.S. public operational loss data from 1980 to 2003, the authors demonstrate that the firm-specific environment is a key determinant of operational risk; firm-specific characteristics such as size, leverage, volatility, book-to-market, profitability, and the number of employees are observed as all highly significant in the models used for the study.

**Regulatory capital charge methods:** Banking is a unique business mainly involved into financial intermediation function and as such wide open to exposure to a wide variety of risks. Unlike other conventional businesses, banks are not allowed to operate on self-governance basis, but are duly regulated by the government authorities by monitoring, supervising and subscribing capital adequacy requirements on them. Such a regulation is necessitated to control and minimise the inherent Moral hazard’s problem arising due to their financial intermediation activity. Moral hazard problem can cause individual bank failures and this problem, if not controlled well, has a capacity to spill over to other financial institutions and thereby lead to a chain of such failures generally known as ‘system crisis’. These mutual sensitivities exist among financial
institution as unlike other forms of businesses they lend and borrow money to and from each other. Governments are generally keen to minimise such crises as the consequence may be passed on to them in the shape of bank bailouts. During late 1980’s, a global movement of bank capital adequacy started which culminated in recommending risk sensitive capital adequacy requirements for banks initially covering credit risk, later on market risk and finally operational risk as well. These three risks are believed to have systemic implications meaning to say that they have a capacity of disrupting the banking system as a whole which could create wider disturbances in a financial system. The capital regulations have been issued by the Basel Committee of Banking Supervision, (BCBS)

2 through their various capital adequacy accords. The popular among these is Basel II Accord which is based on three pillars, viz, minimum capital requirements, supervisory review process and market discipline. The first pillar, i.e. minimum capital requirements describes the methodology for banks for measurement of their credit, market and operational risk exposures towards arriving at their risk sensitive capital requirements. Basel Committee (BCBS) suggests three different, operational risk capital charge measurement methods (Basic Indicator Approach, The Standardized Approach and Advanced Measurement Approach) with increasing degree of sophistication and capital incentives for banks. The first two methods, BIA and TSA rely on a bank’s gross income for measurement of operational risk capital charge, while the third one which has a family of statistical methods uses a variety of inputs, mainly historical operational loss data. Most of the researches conducted on the efficacy of these models suggest that institutions have capital advantage as they advance from simple methods like BIA and TSA to AMA.

Some researches argue that since BIA and TSA depend on gross income, they don’t produce reliable operational risk capital estimates as operational risk exposures generally rise in recessionary times with a corresponding fall in income due to business downturns, thereby leading to underestimation or overestimation issues. Couto and Bulhoes (2009), analyse the impact on capital requirements towards operational risk due to migration from a basic capital charge measurement method, Basic Indicator Approach (BIA) to The Standardised Approach (TSA) and Basic Indicator Approach (BIA) directly to Alternative Standardized Approach (ASA) in Portuguese banks. More specifically, they observe that when abdicating from the BIA and adopting TSA, the financial institutions will benefit from a capital charge reduction of, approximately, 3.2%. Jose, Rodriguez, Dominguez and Marin (2009) argue using internal operational loss data taken from a Spanish bank that an advanced operational risk measurement methodology like LDA produces capital relief for an entity in comparison to non-advanced methods like Basic Indicator Approach (BIA) and The Standardised Approach (TSA). Also, capital charges estimates of non-advanced approaches are proportional to an entity’s business volume, so that, in cycles of flourishing economic activity, the regulatory capital is expected to increase independently of the scale of risk controls established by the entity. Moreover, gross income (exposure indicator) used by such approaches also suffers from conceptual deficiency, as it depends on the accounting system of a country and thereby embodies a potential risk of regulatory arbitrage. Teker (2005), argue that basic indicator approach and standardised approach may be viewed as insufficient in measuring operational risk as the amount of gross income used by these approaches may not be a good indicator to be used in measuring operational risk since it does not take into account the transaction volume, which is considered to be closely related to the operational risk exposure of banks. Sundmacher (2007) assessed whether the Basel’s methodologies of measurement of operational risk capital like BIA would have captured the National Australia Bank’s build-up in the bank’s operational risk exposure between 2001 and 2004 during which bank faced some operational losses and found that using the BIA, the institution’s gross income would have been a poor indicator for operational risk as it showed a declining capital charge over time. Mongid and Tahir (2011) argue on the basis of historical data for 77 rural banks in Indonesia for a three-year period, 2006 to 2008, using various operational risk capital charge calculation methods like, Basic Indicator Approach, The Standardised Approach and Alternative Standardised Approach, the study found that capital charge requirements reduce as bank moves from a less sophisticated approach like BIA to an advanced approach like ASA.

Researchers conducted in India: Very few researches have been found on the subject of operational risk in banks in India. This subject has been of little interest of researchers probably due to the reasons of lack of awareness and inadequate operational risk disclosures on part of Indian banks. Banks in India are currently developing operational loss data and improvements in their operational risk disclosures
practices are expected to be witnessed in the ensuing years. Lack of secondary published data in the form of proprietary operational losses of banks in India is currently considered as one of the major impediments in developing research interest in the area of operational risk. Janakiraman (2008) argues that process of designing the framework for operational risk is at the nascent stage in Indian Banks. In a survey of 22 Indian Banks, it is observed that insufficient internal data, difficulties in collection of external loss data and modelling complexities, represent the significant impediments in the implementation of operational risk management framework. Bodla and Verma (2008) observed in a survey conducted on the private and public sector banks in India, that 60% of the banks have designed their operational risk management framework on the lines of new Basel Capital Accord. People and processes are considered to be the most important factors causing operational risk and no difference in such importance was visible across size and sector of the banks. Rao and Ghosh (2008) observe in a survey conducted on the preparedness of Indian Banks in managing operational risk, that operational risk is perceived to be important because it directly affect the bottom line. Most of the Indian banks are still in the preparatory stage of ORM and lack competitiveness, face vagueness and inadequacy of historical loss data, and also difficulties in mathematical modelling of OR.

Mehra (2009) surveyed the range of practices used by Indian Banks in management of operational risk essential for achievement of Advanced Measurement Approach (AMA) and found that size of a banking institution is a deterrent to collection of external loss data, deeper level of involvement of operational risk functionaries, data collection and analysis. The author further argues that practices of average and small sized public sector and old private sector banks were observed to be lagging behind that of new private sector banks in usage of BEICFs like RCSA, KRI, usage of scenarios, updating of these indicators and collection and usage of external loss data. Her research also observed a wide gap in the range of practices followed by Indian Banks and the AMA compliant banks worldwide. Correa and Raju (2010) observed that most of the banks in India are operating at capital adequacy ratios higher than the prescribed Basel II requirements. Their study present estimates of operational risk capital charges for Indian banks using two Basel II approaches, namely the basic indicator approach and the standardized approach, as well as two alternative approaches, the cost-to-asset ratio and the cost-to-income ratio and its impact on their tier one capital. The study reveals that substantial proportion of the additional capital requirements fall to public sector banks rather than private sector ones.

Potential Research Areas in Operational Risk: The review of the research on the subject of operational risk management in banks reveals that topics researched at international level extensively covers conceptual, measurement models and regulatory capital charge methods related issues to operational risk, while in India, a limited research has been conducted wherein progress of ORM in banks, constraint or challenges faced by the banks in implementing a ORM framework have been touched. In many countries, including India, development of operational risk measurement and management framework on principles of Basel accord is yet at a nascent stage due to many reasons, among which professional inadequacies, poor risk management culture and lack of sufficient operational loss data top the list. Also, research in the area of operational risk in banks in India has not progressed well due conservative attitude and poor disclosure practices of operational risk related information by the Indian banks. Otherwise, operational risk represents a huge potential for research particularly in conceptual aspects, problems faced by Indian banks in implementation of operational risk framework, impact of the Basel initiatives of operational risk management on the performance of banks, issues related to operational risk modelling, scope of improvement in operational risk disclosure practices and its potential to improve market discipline, operational risk management and value creation, etc.

Note
1. The Group of Thirty established in 1978, based in Washington DC, USA is a private, non-profit, international body composed of very senior representatives of the private and public sectors and academia. It aims to deepen understanding of international economic and financial issues, to explore the international repercussions of decisions taken in the public and private sectors, and to examine the choices available to market practitioners and policy makers.
2. The Basel Committee on Banking Supervision (BCBS) whose secretariat is located at the Bank for International Settlements in Basel, Switzerland was established by the central-bank Governors of the Group of Ten countries at the end of 1974. BCBS which meets regularly four times a year is a forum for regular cooperation on banking supervisory matters with the objective of enhancing understanding of key supervisory issues and improving the quality of banking supervision worldwide. The Committee's members come from Argentina, Australia, Belgium, Brazil, Canada, China, France, Germany, Hong Kong SAR, India, Indonesia, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. Countries are represented by their central bank and also by the authority with formal responsibility for the prudential supervision of banking business where this is not the central bank. The Committee does not possess any formal supranational supervisory authority, and its conclusions do not, and were never intended to, have legal force, rather act as a recommendatory entity to the global central banks. In 1988, the Committee decided to introduce a capital measurement system commonly referred to as the Basel Capital Accord. This system provided for the implementation of a credit risk measurement framework with a minimum capital standard of 8% by end-1992. Since 1988, this framework has been progressively introduced not only in member countries but also in virtually all other countries with internationally active banks. In June 1999, the Committee issued a proposal for a revised Capital Adequacy Framework. The proposed capital framework consists of three pillars: minimum capital requirements, which seek to refine the standardised rules set forth in the 1988 Accord; supervisory review of an institution's internal assessment process and capital adequacy; and effective use of disclosure to strengthen market discipline as a complement to supervisory efforts.

3. Moral hazard in banks is considered as a situation which arises when a bank makes the decision about how much risk to take and therefore reaps the rewards if everything goes well, while in case the things go bad, governments are always there to rescue them by paying for such losses with the tax payers money. Such a mechanism has been widely criticised for leading to lack of required care and due diligence on part of the banking institutions.

References


