GUIDANCE NOTE

ON MANAGEMENT OF OPERATIONAL RISK

RESERVE BANK OF INDIA

DEPARTMENT OF BANKING OPERATIONS
AND DEVELOPMENT
CENTRAL OFFICE
MUMBAI

INDEX

GUIDANCE NOTE ON OPERATIONAL RISK MANAGEMENT

PREFACE

As a step towards enhancing and fine-tuning the risk management practices as also to serve as a benchmark to banks, the Reserve Bank had issued Guidance Notes on management of credit risk and market risk in October 2002. The guidance notes are placed on our web-site for wider dissemination.

The New Capital Adequacy Framework requires banks to hold capital explicitly towards operational risk. In view of this as also the felt need for a similar guidance note on management of operational risk, this Guidance Note has been prepared. This guidance note is an outline of a set of sound principles for effective management and supervision of operational risk by banks.

Banks may use the Guidance Note for upgrading their operational risk management system. The design and architecture for management of operational risk should be oriented towards banks' own requirements dictated by the size and complexity of business, risk philosophy, market perception and the expected level of capital. The exact approach may, therefore, differ from bank to bank. Hence the systems, procedures and tools prescribed in this Guidance Note are indicative.

Executive Summary

Growing number of high-profile operational loss events worldwide have led banks and supervisors to increasingly view operational risk management as an integral part of the risk management activity. Management of specific operational risks is not a new practice; it has always been important for banks to try to prevent fraud, maintain the integrity of internal controls, reduce errors in transaction processing, and so on. However, what is relatively new is the view of operational risk management as a comprehensive practice comparable to the management of credit and market risk. 'Management' of operational risk is taken to mean the '**identification, assessment, and / or measurement, monitoring and control / mitigation**' of this risk.

2. The Guidance Note is structured into 8 chapters. This Guidance Note defines Operational Risk and its likely manifestation in Chapter 1. In order to create an enabling organisational culture and placing high priority on effective operational risk management and implementation of risk management processes, Chapter 2 gives a typical outline of the organisational set-up in the bank, together with the responsibilities of the Board and Senior Management. Chapter 3 deals with the policy requirements and strategic approach to Operational Risk Management. The policies and procedures should outline all aspects of the bank's Operational Risk Management Framework. Chapter 4 deals with issues of identification and assessment of Operational Risk. Chapter 5 deals with monitoring of Operational Risk. This chapter has put in one place the business lines that a bank needs to identify and the principles underlying mapping of these business lines. Details of effective control / mitigation of Operational Risk are dealt in Chapter 6. Internal audit and its scope for an independent evaluation of the Operational Risk Management function are dealt under Chapter 7. Although the Guidance Note is an outline of sound principles for effective management and supervision of operational risk by banks, capital allocation for Operational Risk based on Basic Indicator Approach is outlined in Chapter 8.

3. The exact approach for operational risk management chosen by banks will depend on a range of factors. Despite these differences, clear strategies and oversight by the Board of Directors and senior management, a strong operational

risk management culture, effective internal control and reporting, contingency planning are crucial elements for an effective operational risk management framework. Initiatives required to be taken by banks in this regard will include the following:

- The Board of Directors is primarily responsible for ensuring effective management of the operational risks in banks. The bank's Board of Directors has the ultimate responsibility for ensuring that the senior management establishes and maintains an adequate and effective system of internal controls.
- Operational risk management should be identified and introduced as an independent risk management function across the entire bank/ banking group.
- The senior management should have clear responsibilities for implementing operational risk management as approved by the Board of Directors.
- The board of directors and senior management are responsible for creating an awareness of Operational Risks and establishing a culture within the bank that emphasises and demonstrates to all the levels of personnel the importance of Operational Risk.
- The direction for effective operational risk management should be embedded in the policies and procedures that clearly describe the key elements for identifying, assessing, monitoring and controlling / mitigating operational risk.
- The internal audit function assists the senior management and the Board by independently reviewing application and effectiveness of operational risk management procedures and practices approved by the Board/ senior management.
- The New Capital Adequacy Framework has put forward various options for calculating operational risk capital charge in a "continuum" of increasing sophistication and risk sensitivity and increasing complexity. Despite the fact that banks may adopt any one of these options for computing capital charge, it is intended that they will benchmark their operational risk management systems with the guidance provided in this Note and aim to move towards more sophisticated approaches.

Chapter 1

Background

1.1 Financial institutions are in the business of risk management and hence are incentivised to develop sophisticated risk management systems. The basic components of a risk management system are identifying the risks the entity is exposed to, assessing their magnitude, monitoring them, controlling or mitigating them using a variety of procedures, and setting aside capital for potential losses (including expected losses and unexpected losses)*

1.2. Deregulation and globalisation of financial services, together with the growing sophistication of financial technology, are making the activities of banks and thus their profiles more complex. Evolving banking practices suggest that risks other than credit risks and market risks can be substantial. Examples of these new and growing risks faced by banks include:

- Highly Automated Technology - If not properly controlled, the greater use of more highly automated technology has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on integrated systems.

- Emergence of E- Commerce – Growth of e-commerce brings with it potential risks (e.g. internal and external fraud and system securities issues)

- Emergence of banks acting as very large volume service providers creates the need for continual maintenance of high-grade internal controls and back-up systems.

- Outsourcing – growing use of outsourcing arrangements and the participation in clearing and settlement systems can mitigate some risks but can also present significant other risks to banks.

- Large-scale acquisitions, mergers, de-mergers and consolidations test the viability of new or newly integrated systems.

- Banks may engage in risk mitigation techniques (e.g. collateral, derivatives, netting arrangements and asset securitisations) to optimise their exposure to market risk and credit risk, but which in turn may produce other forms of risk (eg. legal risk).

---

* Para 669 (b) of the International Convergence of Capital Measurement & Capital Standards – A Revised Framework, June 2004.

Definition

1.3. Definition of operational risk has evolved rapidly over the past few years. At first, it was commonly defined as every type of unquantifiable risk faced by a bank. However, further analysis has refined the definition considerably. ***Operational risk has been defined by the Basel Committee on Banking Supervision[1] as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.*** This definition is based on the underlying causes of operational risk. It seeks to identify why a loss happened and at the broadest level includes the breakdown by four causes: people, processes, systems and external factors.

Likely forms of manifestation of operational risk

1.4. A clear appreciation and understanding by banks of what is meant by operational risk is critical to the effective management and control of this risk category. It is also important to consider the full range of material operational risks facing the bank and capture all significant causes of severe operational losses. Operational risk is pervasive, complex and dynamic. Unlike market and credit risk, which tend to be in specific areas of business, operational risk is inherent in all business processes. Operational risk may manifest in a variety of ways in the banking industry. The examples of operational risks listed at paragraph 1.2 above can be considered as illustrative.

1.5. The Basel Committee has identified[2] the following types of operational risk events as having the potential to result in substantial losses:

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

---

[1] *ibid, June 2004*
[2] *ibid, June 2004- Annex 6*

- ***Clients, products and business practices***. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorised products.

- ***Damage to physical assets***. For example, terrorism, vandalism, earthquakes, fires and floods.

- ***Business disruption and system failures***. For example, hardware and software failures, telecommunication problems, and utility outages.

- ***Execution, delivery and process management***. For example: data entry errors, collateral management failures, incomplete legal documentation, and unauthorized access given to client accounts, non-client counterparty misperformance, and vendor disputes.

Chapter 2

Organisational Set-up and Key Responsibilities for Operational Risk Management

Relevance of Operational risk function

2.1 Growing number of high-profile operational loss events worldwide have led banks and supervisors to increasingly view operational risk management as an integral part of risk management activity. Management of specific operational risks is not a new practice; it has always been important for banks to try to prevent fraud, maintain the integrity of internal controls, reduce errors in transaction processing, and so on. However, what is relatively new is the view that operational risk management is a comprehensive practice comparable to the management of credit and market risks.

2.2 Operational Risk differs from other banking risks in that it is typically not directly taken in return for an expected reward but is implicit in the ordinary course of corporate activity and has the potential to affect the risk management process. However, it is recognised that in some business lines with minimal credit or market risks, the decision to incur operational risk, or compete based on the perceived ability to manage and effectively price this risk, is an integral part of a bank's risk / reward calculus. At the same time, failure to properly manage operational risk can result in a misstatement of an institution's risk profile and expose the institution to significant losses. 'Management' of operational risk is taken to mean the '**identification, assessment and / or measurement, monitoring and control / mitigation**' of this risk.

Organizational set up and culture

2.3 Operational risk is intrinsic to a bank and should hence be an important component of its enterprise wide risk management systems. The Board and senior management should create an enabling organizational culture placing high priority on effective operational risk management and adherence to sound operating procedures. Successful implementation of risk management process has to emanate from the top management with the demonstration of strong

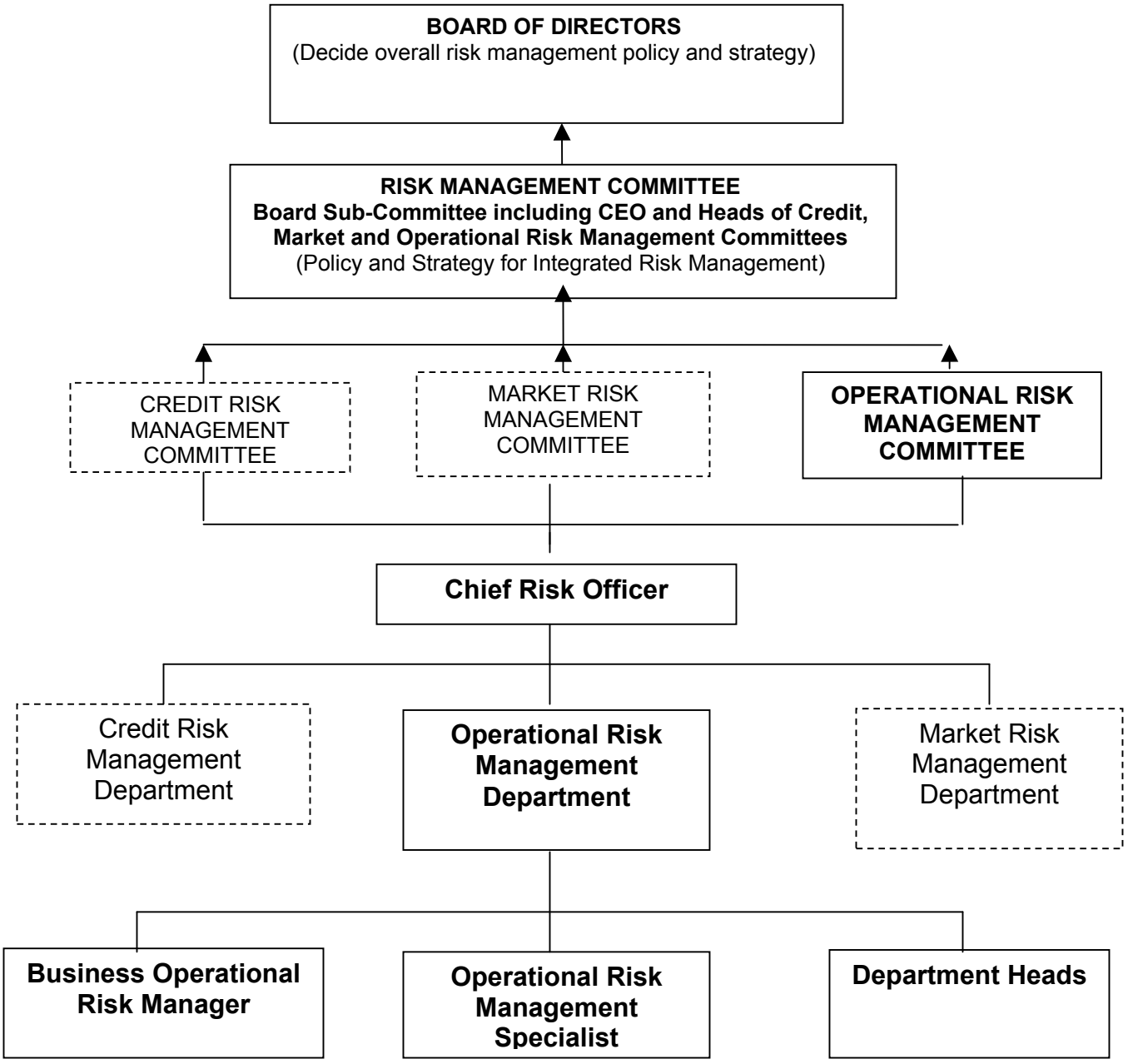
commitment to integrate the same into the basic operations and strategic decision making processes. Therefore, Board and senior management should promote an organizational culture for management of operational risk.

2.4 It is recognised that the approach for operational risk management that may be chosen by an individual bank will depend on a range of factors, including size and sophistication, nature and complexity of its activities. However, despite these differences, clear strategies and oversight by the Board of Directors and senior management; a strong operational risk culture, i.e., the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a bank's commitment to and style of operational risk management; internal control culture (including clear lines of responsibility and segregation of duties); effective internal reporting; and contingency planning are all crucial elements of an effective operational risk management framework.

2.5 Ideally, the organizational set-up for operational risk management should include the following:

- Board of Directors
- Risk Management Committee of the Board
- Operational Risk Management Committee
- Operational Risk Management Department
- Operational Risk Managers
- Support Group for operational risk management

2.6 A typical organisation chart for supporting operational risk management function could be as under:



It has to be ensured that each type of major risk viz. Credit Risk, Market Risk and Operational Risk, is managed as an independent function. Hence, banks should have corresponding risk management committees, which are assigned the specific responsibilities. Banks may structure the risk management department(s) as appropriate without compromising on the above principles.

Board Responsibilities:

2.7 Board of Directors of a bank is primarily responsible for ensuring effective management of operational risks. The Board would include Committee of the Board to which the Board may delegate specific operational risk management responsibilities:

- 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 an appropriate operational risk management framework for the bank and review it periodically.

- The Board of Directors should provide senior management with clear guidance and direction.

- The Framework should be based on appropriate definition of operational risk which clearly articulates what constitutes operational risk in the bank and covers the bank's appetite and tolerance for operational risk. The framework should also articulate the key processes the bank needs to have in place to manage operational risk.

- The Board of Directors should be responsible for establishing a management structure capable of implementing the bank's operational risk management framework. Since a significant aspect of managing operational risk relates to the establishment of strong internal controls, it is particularly important that the Board establishes clear lines of management responsibility, accountability and reporting. In addition, there should be separation of responsibilities and reporting lines between operational risk control functions, business lines and support functions in order to avoid conflicts of interest.

- Board shall review the framework regularly to ensure that the bank is managing the operational risks arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities or systems. This review process should also aim to assess industry best practice in operational risk management appropriate for the bank's activities, systems and processes. If necessary, the Board should ensure that the operational risk management framework is revised in light of this analysis, so that material operational risks are captured within.

- Board should ensure that the bank has in place adequate internal audit coverage to satisfy itself that policies and procedures have been implemented effectively. The operational risk management framework should be subjected to an effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not directly involved in the operational risk management process. Though, in smaller banks, the internal audit function may be responsible for developing the operational risk management

programme, responsibility for day-to-day operational risk management should be transferred elsewhere.

Senior Management Responsibilities

2.8 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 organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. The additional responsibilities that devolve on the senior management include the following:

- To translate operational risk management framework established by the Board of Directors into specific policies, processes and procedures that can be implemented and verified within the different business units.

- To clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability, and ensure that the necessary resources are available to manage operational risk effectively.

- To assess the appropriateness of the management oversight process in light of the risks inherent in a business unit's policy.

- To ensure bank's activities are conducted by qualified staff with the necessary experience, technical capabilities and access to resources, and that staff responsible for monitoring and enforcing compliance with the institution's risk policy have authority independent from the units they oversee.

- To ensure that the bank's operational risk management policy has been clearly communicated to staff at all levels in the units that incur material operational risk.

- To ensure that staff responsible for managing operational risk communicate effectively with staff responsible for managing credit, market, and other risks as well as with those in the bank who are responsible for the procurement of external services such as insurance purchasing and outsourcing agreements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

- To give particular attention to the quality of documentation controls and transaction-handling practices. Policies, processes and procedures related to advanced technologies supporting high transaction volumes, in particular, should be well documented and disseminated to all relevant personnel.

- To ensure that the bank's HR policies are consistent with its appetite for risk and are not aligned to rewarding staff who deviate from policies.

2.9 The broad indicative role of each organisational arm of the risk management structure both at the corporate level and at the functional level is indicated in brief in Annex 1. These can be customised to the actual requirements of each bank depending upon the size, risk profile, risk appetite and level of sophistication.

Chapter 3

Policy Requirements and Strategic Approach

3.1 The operational risk management framework provides the strategic direction and ensures that an effective operational risk management and measurement process is adopted throughout the institution. Each institution's operational risk profile is unique and requires a tailored risk management approach appropriate for the scale and materiality of the risk present, and the size of the institution. There is no single framework that would suit every institution; different approaches will be needed for different institutions. In fact, many operational risk management techniques continue to evolve rapidly to keep pace with new technologies, business models and applications. Operation risk is more a risk management than measurement issue. The key elements in the Operational Risk Management process include –

- Appropriate policies and procedures;
- Efforts to identify and measure operational risk
- Effective monitoring and reporting
- A sound system of internal controls; and
- Appropriate testing and verification of the Operational Risk Framework.

Policy Requirement

3.2 Each bank must have policies and procedures that clearly describe the major elements of the Operational Risk Management framework including identifying, assessing, monitoring and controlling / mitigating operational risk.

3.3 Operational Risk Management policies, processes, and procedures should be documented and communicated to appropriate staff i.e., the personnel at all levels in units that incur material operational risks. The policies and procedures should outline all aspects of the institution's Operational Risk Management framework, including: -

- The roles and responsibilities of the independent bank-wide Operational Risk Management function and line of business management.

- A definition for operational risk, including the loss event types that will be monitored.

- The capture and use of internal and external operational risk loss data including data potential events (including the use of Scenario analysis).

- The development and incorporation of business environment and internal control factor assessments into the operational risk framework.

- A description of the internally derived analytical framework that quantifies the operational risk exposure of the institution.

- A discussion of qualitative factors and risk mitigants and how they are incorporated into the operational risk framework.

- A discussion of the testing and verification processes and procedures.

- A discussion of other factors that affect the measurement of operational risk.

- Provisions for the review and approval of significant policy and procedural exceptions.

- Regular reporting of critical risk issues facing the banks and its control/mitigations to senior management and Board.

- Top-level reviews of the bank's progress towards the stated objectives.

- Checking for compliance with management controls.

- Provisions for review, treatment and resolution of non-compliance issues.

- A system of documented approvals and authorisations to ensure accountability at an appropriate level of management.

- Define the risk tolerance level for the bank, break it down to appropriate sub-limits and *prescribe reporting levels and breach of limits.*

- Indicate the process to be adopted for immediate corrective action.

3.4 Given the vast advantages associated with effective Operational Risk Management, it is imperative that the strategic approach of the risk management function should be oriented towards:

- An emphasis on minimising and eventually eliminating losses and customer dissatisfaction due to failures in processes.

- Focus on flaws in products and their design that can expose the institution to losses due to fraud etc.

- Align business structures and incentive systems to minimize conflicts between employees and the institution.

- Analyze the impact of failures in technology / systems and develop mitigants to minimize the impact.

- Develop plans for external shocks that can adversely impact the continuity in the institution's operations.

3.5 The institution can decide upon the mitigants for minimizing operational risks rationally, by looking at the costs of putting in mitigants as against the benefit of reducing the operational losses.

Chapter 4

Identification and Assessment of Operational Risk

4.1 In the past, banks relied almost exclusively upon internal control mechanisms within business lines, supplemented by the audit function, to manage operational risk. While these remain important, there is need to adopt specific structures and processes aimed at managing operational risk. Several recent cases demonstrate that inadequate internal controls can lead to significant losses for banks. The types of control break-downs may be grouped into five categories:

- **Lack of Control Culture** - Management's inattention and laxity in control culture, insufficient guidance and lack of clear management accountability.
- **Inadequate recognition and assessment of the risk of certain banking activities**, whether on-or-off-balance sheet. Failure to recognise and assess the risks of new products and activities or update the risk assessment when significant changes occur in business conditions or environment. Many recent cases highlight the fact that control systems that function well for traditional or simple products are unable to handle more sophisticated or complex products.
- **Absence/failure of key control structures** and activities, such as segregation of duties, approvals, verifications, reconciliations and reviews of operating performance.
- **Inadequate communication** of information between levels of management within the bank – upward, downward or cross-functional.
- **Inadequate / ineffective audit/monitoring** programs.

4.2 Managing Operational Risk is emerging as an important feature of sound risk management practice in modern financial markets in the wake of phenomenal increase in volume of transactions, high degree of structural changes and complex technological support systems. Some of the guiding principles for banks to mange operational risks are identification, assessment, monitoring and control of these risks. These principles are dealt in detail below:

Identification of operational risk

4.3 Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure

that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is identified clearly and subjected to adequate assessment procedures.

4.4 Risk identification is paramount for the subsequent development of a viable operational risk monitoring and control system. Effective risk identification should consider both internal factors (such as the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organisational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

4.5 The first step towards identifying risk events is to list out all the activities that are susceptible to operational risk. Usually this is carried out at several stages. To begin with, we can list:

- The main business groups viz. corporate finance, trading and sales, retail banking, commercial banking, payment and settlement, agency services, asset management, and retail brokerage.
- The analysis can be further carried out at the level of the product teams in these business groups, e.g. transaction banking, trade finance, general banking, cash management and securities markets.
- Thereafter the product offered within these business groups by each product team can be analysed, e.g. import bills, letter of credit, bank guarantee under trade finance.

4.6 After the products are listed, the various operational risk events associated with these products are recorded. An operational risk event is an incident/ experience that has caused or has the potential to cause material loss to the bank either directly or indirectly with other incidents. Risk events are associated with the people, process and technology involved with the product. They can be recognized by:

(i) Experience - The event has occurred in the past;
(ii) Judgment - Business logic suggests that the bank is exposed to a risk event;

(iii) Intuition - Events where appropriate measures saved the institution in the nick of time;

(iv) Linked Events - This event resulted in a loss resulting from other risk type (credit, market etc.);

(v) Regulatory requirement – regulator requires recognition of specified events.

4.7 These risk events can be catalogued under the last tier for each of the products.

Assessment of Operational Risk

4.8 In addition to identifying the risk events, banks should assess their vulnerability to these risk events. Effective risk assessment allows a bank to better understand its risk profile and most effectively target risk management resources. Amongst the possible tools that may be used by banks for assessing operational risk are:

- **Self Risk Assessment**: A bank assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment. Scorecards, for example, provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures. Some scores may relate to risks unique to a specific business line while others may rank risks that cut across business lines. Scores may address inherent risks, as well as the controls to mitigate them.

- **Risk Mapping:** In this process, various business units, organisational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management action.

- **Key Risk Indicators**: Key risk indicators are statistics and/or metrics, often financial, which can provide insight into a bank's risk position. These indicators should be reviewed on a periodic basis (such as monthly or quarterly) to alert banks to changes that may be indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.

Measurement:

4.9 A key component of risk management is measuring the size and scope of the bank's risk exposures. As yet, however, there is no clearly established, single way to measure operational risk on a bank-wide basis. Banks may develop risk assessment techniques that are appropriate to the size and complexities of their portfolio, their resources and data availability. A good assessment model must cover certain standard features. An example is the "matrix" approach in which losses are categorized according to the type of event and the business line in which the event occurred. Banks may quantify their exposure to operational risk using a variety of approaches. For example, data on a bank's historical loss experience could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systematically tracking and recording the frequency and severity of each loss event along with other relevant information on individual loss events. In this way, a bank can hope to identify events which have the most impact across the entire bank and business practices which are most susceptible to operational risk. Once loss events and actual losses are defined, a bank can analyze and perhaps even model their occurrence. Doing so requires constructing databases for monitoring such losses and creating risk indicators that summarize these data. Examples of such indicators are the number of failed transactions over a period of time and the frequency of staff turnover within a division.

4.10 Every risk event in the risk matrix is then classified according to its frequency and severity. By frequency, the reference is to the number/ potential number (proportion) of error events that the product type / risk type point is exposed to. By severity, the reference is to the loss amount/ potential loss amount that the operational risk event is exposed to when the risk event materializes. The classification can be on any predefined scale (say 1-10, Low, Medium, High etc.). All risk events will thus be under one of the four categories, namely high frequency-high severity, high frequency-low severity, low frequency-high severity, low frequency-low severity in the decreasing order of the risk exposure.

4.11 Potential losses can be categorized broadly as arising from “high frequency, low severity” (HFLS) events, such as minor accounting errors or bank teller mistakes, and “low frequency, high severity” (LFHS) events, such as terrorist attacks or major fraud. Data on losses arising from HFLS events are generally available from a bank’s internal auditing systems. Hence, modeling and budgeting these expected future losses due to operational risk potentially could be done very accurately. However, LFHS events are uncommon and thus limit a single bank from having sufficient data for modeling purposes. Scenario analysis can be used for filling up scarce data. Scenarios can be treated as potential future events which need to be captured in terms of their potential frequency and potential loss severity. Scenarios should be generated for all material operational risks faced by all the organizational units of the bank. An assessment of the generated scenarios is carried out by the business experts based on the information such as historical losses, key risk indicators, insurance coverage, risk factors and the control environment, etc. The above assessments are subjected to data quality check which may be based on a peer review of the estimates made by the business expert, internal audit, etc. The data can be fed into an internal model for generating economic capital requirements for operational risk.

4.12 Risk assessment should also identify and evaluate the internal and external factors that could adversely affect the bank’s performance, information and compliance by covering all risks faced by the bank that operate at all levels within the bank. Assessment should take account of both historical and potential risk events.

4.13 Historical risk events are assessed based on:

(i) Total number of risk events
(ii) Total financial reversals
(iii) Net financial impact
(iv) Exposure: Based on expected increase in volumes
(v) Total number of customer claims paid out
(vi) IT indices: Uptime etc.
(vii) Office Accounts Status.

4.14 The factors for assessing potential risks include:

(i) Staff related factors such as productivity, expertise, turnover

(ii) Extent of activity outsourced

(iii) Process clarity, complexity, changes

(iv) IT Indices

(v) Audit Scores

(vi) Expected changes or spurts in volumes

CHAPTER 5

Monitoring of Operational Risk

5.1 An effective monitoring process is essential for adequately managing operational risk. Regular monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss event.

5.2 In addition to monitoring operational loss events, banks should identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators (often referred to as early warning indicators) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, and so on. When thresholds are directly linked to these indicators, an effective monitoring process can help identify key material risks in a transparent manner and enable the bank to act upon these risks appropriately.

5.3 The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Monitoring should be an integrated part of a bank's activities. The results of these monitoring activities should be included in regular management and Board reports, as should compliance reviews performed by the internal audit and/or risk management functions. Reports generated by (and/or for) intermediary supervisory authorities may also inform the corporate monitoring unit which should likewise be reported internally to senior management and the Board, where appropriate.

5.4 Senior management should receive regular reports from appropriate areas such as business units, group functions, the operational risk management unit and internal audit. The operational risk reports should contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should be distributed to appropriate levels of management and to areas of the bank on which areas of concern may have an impact. Reports should fully reflect any

identified problem areas and should motivate timely corrective action on outstanding issues. To ensure the usefulness and reliability of these risk reports and audit reports, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general. Management may also use reports prepared by external sources (auditors, supervisors) to assess the usefulness and reliability of internal reports. Reports should be analysed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

Management information systems

5.5 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. In general, the Board of Directors should receive sufficient higher-level information to enable them to understand the bank's overall operational risk profile and focus on the material and strategic implications for the business. Towards this end it would be relevant to identify all activities and all loss events in a bank under well defined business lines.

Business Line Identification

5.6 Banks have different business mixes and risk profiles. Hence the most intractable problem banks face in assessing operational risk capital is due to this diversity. The best way to get around this intractable problem in computation is by specifying a range of operational risk multipliers for specified distinct business lines. The following benefits are expected to accrue by specifying business lines:

- banks will be able to crystallise the assessment processes to the underlying operational risk and the regulatory framework;
- the line managers will be aware of operational risk in their line of business;
- confusion and territorial overlap which may be linked to subsets of the overall risk profile of a bank can be avoided.

5.7 For the purpose of operational risk management, the activities of a bank may be mapped into eight business lines identified in the New Capital Adequacy Framework. The various products launched by the banks are also to be mapped to the relevant business line. Banks must develop specific policies for mapping a product or an activity to a business line and have the same documented to indicate the criteria. The following are the eight recommended business lines. Details and methodologies for mapping of these business lines are furnished in Annex 2.

1. Corporate finance
2. Trading and sales
3. Retail banking
4. Commercial banking
5. Payment and settlement
6. Agency services
7. Asset management
8. Retail brokerage

5.8 The following are the principles to be followed for business line mapping:

(i) All activities must be mapped into the eight level - 1 business lines in a mutually exclusive and jointly exhaustive manner.

(ii) Any banking or non banking activity which cannot be readily mapped into the business line framework, but which represents an ancillary function to an activity included in the framework, must be allocated to the business line it supports. If more than one business line is supported through the ancillary activity, an objective mapping criteria must be used.

(iii) The mapping of activities into business lines for operational risk management must be consistent with the definitions of business lines used for management of other risk categories, i.e. credit and market risk. Any deviations from this principle must be clearly motivated and documented.

(iv) The mapping process used must be clearly documented. In particular, written business line definitions must be clear and detailed enough to allow third parties to replicate the business line mapping. Documentation must, among other things, clearly motivate any exceptions or overrides and be kept on record.

(v) Processes must be in place to define the mapping of any new activities or products.

(vi) Senior management is responsible for the mapping policy (which is subject to approval by the Board of Directors).

(vii) The mapping process to business lines must be subject to independent review.

5.9 The following principles might be relevant for determining mapping of activities into appropriate business lines:

i) activities that constitute compound activities may be broken up into their components which might be related to the level 2 activities under the eight business lines and these components of the complex activity may be assigned to the most suitable business lines, in accordance with their nature and characteristics.

ii) activities that refer to more than a business line may be assigned to the most predominant business line and if no predominant business line exist, then it may be mapped to the most suitable business lines, in accordance with their nature and characteristics.

Operational Risk Loss events

5.10 Banks must meet the following data requirement for internally generating operational risk measures.

- The tracking of individual internal event data is an essential prerequisite to the development and functioning of operational risk measurement system. Internal loss data is crucial for tying a bank's risk estimates to its actual loss experience.

- Internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological process and risk management procedures. Therefore, bank must have documented procedures for assessing on-going relevance of historical loss data, including those situations in which judgement overrides, scaling, or other adjustments may be used, to what extent it may used and who is authorised to make such decisions.

- Bank's internal loss data must be comprehensive in that it captures all material activities and exposures from all appropriate sub-systems and geographic locations. A bank must be able to justify that any activities and exposures excluded would not have a significant impact on the overall risk estimates. Bank may have appropriate de minimis gross loss threshold for internal loss data collection, say Rs.10, 000. The appropriate threshold may vary somewhat between banks and within a bank across business lines and / or event types. However, particular thresholds may be broadly consistent with those used by the peer banks. Measuring Operational Risk

requires both estimating the probability of an operational loss event and the severity of the loss.

- Banks must track actual loss data (i.e., where losses have actually materialised) and map the same into the relevant level 1 category defined in Annex 3. Banks must endeavour to map the actual loss events to level 3. Operational risk loss would be the financial impact associated with the operational event that is recorded in the financial statement and would include for example, (a) loss incurred, and (b) expenditure incurred to resume normal functioning, but would not include opportunity costs and foregone revenue etc. However, the banks must also track the potential loss (i.e. extent to which further loss may be incurred due to the same operational risk event), near misses, attempted frauds, etc where no loss has actually been incurred by the bank, from the point of view of strengthening the internal systems and controls and avoiding the possibility of such events turning into actual operational risk losses in future.

- Aside from information on gross loss amounts, bank should collect information about the data of the event, any recoveries, as well as some descriptive information about the cause/drivers of the loss event. The level of descriptive information should be commensurate with the size of the gross loss amount.

- Bank must develop specific criteria for assigning loss data arising from an event in a centralised function (e.g. information technology, administration department etc.) or any activity that spans more than one business line.

- External loss data – bank may also collect external loss data to the extent possible. External loss data should include data on actual loss amounts, information on scale of business operations where the event occurred, information on causes and circumstances of the loss events or any other relevant information. Bank must develop systematic process for determining the situations for which external data should be used and the methodologies used to incorporate the data.

- The loss data collected must be analysed loss event category and business line wise. Banks to look into the process and plug any deficiencies in the process and take remedial steps to reduce such events.

CHAPTER 6

Controls / Mitigation of Operational Risk

6.1 Risk management is the process of mitigating the risks faced by a bank. With regard to operational risk, several methods may be adopted for mitigating the risk. For example, losses that might arise on account of natural disasters can be insured against. Losses that might arise from business disruptions due to telecommunication or electrical failures can be mitigated by establishing redundant backup facilities. Loss due to internal factors, like employee fraud or product flaws, which may be difficult to identify and insure against, can be mitigated through strong internal auditing procedures.

6.2 Although a framework of formal, written policies and procedures is critical, it needs to be reinforced through a strong control culture that promotes sound risk management practices. Both the Board of Directors and senior management are responsible for establishing a strong internal control culture in which control activities are an integral part of the regular activities of a bank, since such integration enables quick responses to changing conditions and avoids unnecessary costs.

6.3 A system of effective internal controls is a critical component of bank management and a foundation for the safe and sound operation of banking organisations. Such a system can also help to ensure that the bank will comply with laws and regulations as well as policies, plans, internal rules and procedures, and decrease the risk of unexpected losses or damage to the bank's reputation. Internal control is a *process* effected by the Board of Directors, senior management and all levels of personnel. It is not solely a procedure or policy that is performed at a certain point in time, but rather it is continually operating at all levels within the bank.

6.4 The internal control process, which historically has been a mechanism for reducing instances of fraud, misappropriation and errors, has become more extensive, addressing all the various risks faced by banking organisations. It is

now recognised that a sound internal control process is critical to a bank's ability to meet its established goals, and to maintain its financial viability.

6.5 In varying degrees, internal control is the responsibility of everyone in a bank. Almost all employees produce information used in the internal control system or take other actions needed to effect control. An essential element of a strong internal control system is the recognition by all employees of the need to carry out their responsibilities effectively and to communicate to the appropriate level of management any problems in operations, instances of non-compliance with the code of conduct, or other policy violations or illegal actions that are noticed. It is essential that all personnel within the bank understand the importance of internal control and are actively engaged in the process. While having a strong internal control culture does not guarantee that an organisation will reach its goals, the lack of such a culture provides greater opportunities for errors to go undetected or for improprieties to occur.

6.6 An effective internal control system requires that

- an appropriate control structure is set up, with control activities defined at every business level. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorisations; and, a system of verification and reconciliation.
- there is appropriate segregation of duties and personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimised, and subject to careful, independent monitoring.
- there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.
- there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use

data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.

- effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.

6.7 Adequate internal controls within banking organisations must be supplemented by an effective internal audit function that independently evaluates the control systems within the organisation. Internal audit is part of the ongoing monitoring of the bank's system of internal controls and of its internal capital assessment procedure, because internal audit provides an independent assessment of the adequacy of, and compliance with, the bank’s established policies and procedures.

6.8 Operational risk can be more pronounced where banks engage in new activities or develop new products (particularly where these activities or products are not consistent with the bank’s core business strategies), enter unfamiliar markets, and/or engage in businesses that are geographically distant from the head office. It is incumbent upon banks to ensure that special attention is paid to internal control activities where such conditions exist.

6.9 In some instances, banks may decide to either retain a certain level of operational risk or self-insure against that risk. Where this is the case and the risk is material, the decision to retain or self-insure the risk should be transparent within the organisation and should be consistent with the bank’s overall business strategy and appetite for risk. The bank’s appetite as specified through the policies for managing this risk and the bank’s prioritisation of operational risk management activities, including the extent of, and manner in which, operational risk is transferred outside the bank. The degree of formality and sophistication of the bank’s operational risk management framework should be commensurate with the bank’s risk profile.

6.10 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.

- For all material operational risks that have been identified, the bank should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled, the bank should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely. Control processes and procedures should be established and banks should have a system in place for ensuring compliance with a documented set of internal policies.

- Some significant operational risks have low probabilities but potentially very large financial impact. Classification of operational loss event into various risk categories based on frequency and severity matrix prioritise the events to be controlled and tracked. Audit benchmarks can be set for high loss events. Moreover, not all risk events can be controlled (e.g., natural disasters). Risk mitigation tools or programmes can be used to reduce the exposure to, or frequency and/or severity of, such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalise the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

- However, banks should view risk mitigation tools as complementary to, rather than a replacement for, internal operational risk control. Having mechanisms in place to quickly recognise and rectify legitimate operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, or transfer the risk to another business sector or area, or even create a new risk (e.g. legal or counterparty risk).

- Investment in appropriate processing technology and information technology security are also important for risk mitigation. However, banks should be aware that increased automation could transform high frequency-low severity losses into low frequency-high severity losses. The latter may be associated with loss or extended disruption of services caused by internal factors or by factors beyond the bank's immediate control (e.g., external events). Such problems may cause serious difficulties for banks and could jeopardise an institution's ability to conduct key business activities. Banks should establish disaster recovery and business continuity plans that address this risk.

- Banks should also establish policies for managing risks associated with outsourcing activities. Outsourcing of activities can reduce the institution's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialised business activities. However, a bank's use of third parties does not diminish the responsibility of management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcing bank. Furthermore, banks need to manage residual risks associated with outsourcing arrangements, including disruption of services

- Depending on the scale and nature of the activity, banks should understand the potential impact on their operations and their customers of any potential deficiencies in services provided by vendors and other third-party or intra-group service providers, including both operational breakdowns and the potential business failure or default of the external parties. Banks should ensure that the expectations and obligations of each party are clearly defined, understood and enforceable. The extent of the external party's liability and financial ability to compensate the bank for errors, negligence, and other operational failures should be explicitly considered as part of the risk assessment. Banks should carry out an initial due diligence test and monitor the activities of third party providers, especially those lacking experience of the banking industry's regulated environment, and review this process (including re-evaluations of due diligence) on a regular basis. For critical activities, the bank may need to consider contingency plans, including the availability of alternative external parties and the costs and resources required to switch external parties, potentially on very short notice.

- 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. These plans needs to be stress-tested annually and the plans may be revised to appropriately address any new or previously unaddressed parameters for these plans. For reasons that may be beyond a bank's control, a severe event may result in the inability of the bank to fulfil some or all of its business obligations, particularly where the bank's physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses to the bank, as well as broader disruptions to the financial system through channels such as the payments system. This potential requires that banks establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the bank may be vulnerable, commensurate with the size and complexity of the bank's operations.

- Banks should periodically review their disaster recovery and business continuity plans so that they are consistent with the bank's current operations and business strategies. Moreover, these plans should be

tested periodically to ensure that the bank would be able to execute the plans in the unlikely event of a severe business disruption.

Chapter 7

Independent Evaluation of Operational Risk Management Function

7.1 The bank's Board of Directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate and effective system of internal controls, a measurement system for assessing the various risks of the bank's activities, a system for relating risks to the bank's capital level, and appropriate methods for monitoring compliance with laws, regulations, and supervisory and internal policies.

7.2 Internal audit is part of the ongoing monitoring of the bank's system of internal controls because internal audit provides an independent assessment of the adequacy of, and compliance with, the bank's established policies and procedures. As such, the internal audit function assists senior management and the Board of Directors in the efficient and effective discharge of their responsibilities as described above. Banks should have in place adequate internal audit coverage to verify that operating policies and procedures have been implemented effectively. The Board (either directly or indirectly through its Audit Committee) should ensure that the scope and frequency of the audit programme is appropriate to the risk exposures.

7.3 The scope of internal audit will broadly cover:

- the examination and evaluation of the adequacy and effectiveness of the internal control systems and the functioning of specific internal control procedures;
- the review of the application and effectiveness of operational risk management procedures and risk assessment methodologies;
- the review of the management and financial information systems, including the electronic information system and electronic banking services;
- the review of the means of safeguarding assets;
- the review of the bank's system of assessing its capital in relation to its estimate of operational risk;

- the review of the systems established to ensure compliance with legal and regulatory requirements, codes of conduct and the implementation of policies and procedures;

- the testing of the reliability and timeliness of the regulatory reporting;

- mitigating risks through risk based audit

7.4 All functional departments should ensure that the operational risk management department is kept fully informed of new developments, initiatives, products and operational changes to ensure that all associated risks are identified at an early stage.

- Operational risk groups are likely to focus on regulatory liaison, operational risk measures, best practice in areas involving risk quantification such as model risk, new products approval and optimising operations and processes. Audit should periodically validate that the bank's operational risk management framework is being implemented effectively across the bank. To the extent that the audit function is involved in oversight of the operational risk management framework, the Board should ensure that the independence of the audit function is maintained. This independence may be compromised if the audit function is directly involved in the operational risk management process. The audit function may provide valuable input to those responsible for operational risk management, but should not itself have direct operational risk management responsibilities.

- Examples of what an independent evaluation of operational risk should review include the following:

  - The effectiveness of the bank's risk management process and overall control environment with respect to operational risk;

  - The bank's methods for monitoring and reporting its operational risk profile, including data on operational losses and other indicators of potential operational risk;

  - The bank's procedures for the timely and effective resolution of operational risk events and vulnerabilities;

  - The effectiveness of the bank's operational risk mitigation efforts, such as the use of insurance;

  - The quality and comprehensiveness of the bank's disaster recovery and business continuity plans

  - To ensure that, where banks are part of a financial group, there are procedures in place to ensure that operational risk is managed in an appropriate and integrated manner across the group. In performing

this assessment, cooperation and exchange of information with other supervisors, in accordance with established procedures, may be necessary.

Chapter 8

Capital Allocation for Operational Risk

8.1 This Guidance Note is an outline of a set of sound principles for effective management and supervision of operational risk by banks. As mentioned earlier, the exact approach may differ among banks and the operational risk management chosen by a bank would depend on a broad range of factors.

8.2 The Basel Committee has put forward a framework consisting of three options for calculating operational risk capital charges in a 'continuum' of increasing sophistication and risk sensitivity. These are, in the order of their increasing complexity, viz., (i) the Basic Indicator Approach (ii) the Standardised Approach and (iii) Advanced Measurement Approaches. Though the Reserve Bank proposes to initially allow banks to use the Basic Indicator Approach for computing regulatory capital for operational risk, some banks are expected to move along the range toward more sophisticated approaches as they develop more sophisticated operational risk management systems and practices which meet the prescribed qualifying criteria. Qualifying criteria for standardised Approach and Advanced Measurement Approaches are given in the Attachment. In order to have a better understanding of these approaches, it is suggested that the Attachment should be read together with the revised Framework.

The Basic Indicator Approach

8.3 Reserve Bank has proposed that, at the minimum, all banks in India should adopt this approach while computing capital for operational risk while implementing Basel II. Under the Basic Indicator Approach, banks have to hold capital for operational risk equal to a fixed percentage (alpha) of a single indicator which has currently been proposed to be "gross income". This approach is available for all banks irrespective of their level of sophistication. The charge may be expressed as follows:

$$K_{BIA} = [\sum (GI * \alpha)]/n,$$

Where

K_{BIA} = the capital charge under the Basic Indicator Approach.

GI = annual gross income, where positive, over the previous three years

α = 15% set by the Committee, relating the industry-wide level of required capital to the industry-wide level of the indicator.

n = number of the previous three years for which gross income is positive.

8.4 The Basel Committee has defined gross income as net interest income and has allowed each relevant national supervisor to define gross income in accordance with the prevailing accounting practices. Accordingly, gross income will be computed for this purpose as defined by the Reserve Bank of India for implementation of the new capital adequacy framework.

Annex 1
(paragraph 2.9)

Broad indicative role of each organisational arm of the risk management structure

A. Key functions of Risk Management Committee of Board (RMCB)

- Approve operational risk policies and issues delegated to it by the Board.
- Review profiles of operational risk throughout the organization
- Approve operational risk capital methodology and resulting attribution
- Set and approve expressions of risk appetite, within overall parameters set by the Board.
- Re-enforce the culture and awareness of operational risk management throughout the organization.

B. Key functions of Operational Risk Management Committee

The Operational Risk Management Committee is an executive committee. It shall have as its principal objective the mitigation of operational risk within the institution by the creation and maintenance of an explicit operational risk management process. The committee will be presented with detailed reviews of operational risk exposures across the bank. Its goals are to take a cross-business view and assure that a proper understanding is reached and actions are being taken to meet the stated goals and objectives of operational risk management in the bank. The Committee may meet quarterly, or more often as it determines is necessary. The meetings will focus on all operational risk issues that the bank faces. Key roles of the Committee are:

- Review the risk profile, understand future changes and threats, and concur on areas of highest priority and related mitigation strategy.
- Assure adequate resources are being assigned to mitigate risks as needed
- Communicate to business areas and staff components the importance of operational risk management, and assure adequate participation and cooperation

- Review and approve the development and implementation of operational risk methodologies and tools, including assessments, reporting, capital and loss event databases.

- Receive and review reports/presentations from the business lines and other areas about their risk profile and mitigation programs.

- To monitor and ensure that appropriate operational risk management frameworks are in place.

- To proactively review and mange potential risks which may arise from regulatory changes/or changes in economic /political environment in order to keep ahead.

- To discuss and recommend suitable controls/mitigations for managing operational risk.

- To analyse frauds, potential losses, non compliance, breaches etc. and recommend corrective measures to prevent recurrences.

- To discuss any issues arising / directions in any one business unit/product which may impact the risks of other business/products.

- To continually promote risk awareness across all business units so that complacency does not set in.

C. Key functions of Operational Risk Management Department (ORMD)

The ORMD is responsible for coordinating all the operational risk activities of the Bank, working towards achievement of the stated goals and objectives. Activities include building an understanding of the risk profile, implementing tools related to operational risk management, and working towards the goals of improved controls and lower risk. ORMD works with the operational liaisons within the business units, staff areas and with the corporate management staff. The group is organized within the Risk Management function. Specific activities of the ORMD include:

- **Risk Profile** – ORMD will work with all areas of the bank and assemble information to build an overall risk profile of the institution, understand and communicate these risks, and analyze changes/trends in the risk profile. ORMD will utilize the following four-pronged approach to develop these profiles:
    - Risk Indicators
    - Self-Assessment

    - Loss Database
    - Capital Model

- **Tools** – ORMD is responsible for the purchase or development and implementation of tools that the Bank will use in its operational risk management program.

- **Capital** – ORMD is jointly responsible with the department involved in capital management for development of a capital measurement methodology for operational risks. It will also coordinate the assembly of required inputs, documentation of assumptions, gaining consensus with the business areas, and coordination with other areas of the bank for the use of the results in the strategic planning, performance measurement, cost benefit analysis, and pricing processes.

- **Consolidation and Reporting of Data** – ORMD will collect relevant information from all areas of the bank, build a consolidated view of operational risk, assemble summary management reports and communicate the results to the risk committees or other interested parties. Key information will include risk indicators, event data and self-assessment results and related issues.

- **Analysis of Data** – ORMD is responsible to analyze the data on a consolidated basis, on an individual basis and on a comparative basis.

- **Best Practices** – ORMD will identify best practices from within the bank or from external sources and share these practices with management and risk specialists across the Bank as beneficial. As part of this role, they will participate in industry conferences surveys, keep up to date on rules and regulations, monitor trends and practices in the industry, and maintain a database/library of articles on the subject.

- **Advice/Consultation** – ORMD will be responsible for working with the Risk Specialists and the businesses as a team to provide advice on how to apply the operational risk management framework, identify operational risks and work on solving problems and improving the risk profile of the Bank.

- **Insurance** – ORMD will work with the Bank's insurance area to determine optimal insurance limits and coverage to assure that the insurance policies the bank purchases are cost beneficial and align with the operational risk profiles of the Bank.

- **Policies** – ORMD will be responsible for drafting, presenting, updating and interpreting, the Operational Risk Policy.

- **Self-Assessment** – ORMD will be responsible for facilitating periodic self-assessments for the purpose of identifying and monitoring operational risks.

- **Coordination with Internal Audit –**ORMD will work closely with Internal Audit to plan assessments and concerns about risks in the Bank. ORMD and

Internal Audit will share information and coordinate activities so as to minimize potential overlap of activities.

D. Key functions of Chief Risk Officer (CRO)

The CRO has supervisory responsibilities over the Operational Risk Management Department as well as responsibility over market risk and credit risk:

- **Review Recommendations** –The CRO will supervise the activities and review and approve the recommendations of the ORMD before submission to the Operational Risk Committee or Risk Management Committee.

- **Assess interrelationships between Operational, and other risk types** – The CRO will facilitate the analysis of risks and interrelationships of risks across market, credit and operational risks. The CRO will assure communication between risk functions and that risk measures and economic capital measures reflect any interrelationships.

- **Create Awareness** – The CRO will help assure that line and executive management maintains an ongoing understanding of operational risks and participates in related risk management activities.

E. Key function of Operational Risk Management Specialists

The bank-wide support departments (e.g., Legal, Human Resources, and Information Technology) shall assign a representative(s) to be designated as Operational Risk Specialists. Their main responsibility is to work with ORMD and the departments/businesses to identify, analyze, explain and mitigate operational issues within their respective areas of expertise. They will also act as verifiers for their related risks in the self assessment process. They will accomplish this responsibility by involving themselves in the following:

- **Committee Participation** – The Operational Risk Management Specialists shall be members of the committees and task forces related to operational risk management, as applicable. They must be ready to discuss operational issues and recommend mitigation strategies.

- **Risk-Indicators** – Assist in the development and review of appropriate risk indicators, both on a bank-wide and business specific basis for their area of specialty.

- **Self-Assessment** – Assist in the review of Self-Assessment results and opine on the departmental/business assessment of risk types, quantification and frequency.

- **Loss Database** – Assist in the timely identification and recording of operational loss data and explanations.

- **Gaps/Issues** – Ensure that all operational risk issues are brought to the attention of ORMD and the Department/business.

- **Mitigation** – Assist the department/business in the design and implementation of risk mitigation strategies.

F. Key functions of Business Operational Risk Managers

It is expected that each business/ functional area will appoint a person responsible to coordinate the management of operational risk. This responsibility may be assigned to an existing job, be a full time position, or even a team of people, as the size and complexity justify. Business/Functional areas should determine how this should be organized within their respective areas. Risk Managers will report to their respective departments/businesses, but work closely with ORMD and with consistent tools and risk management framework and policy. The Operational Risk Management Committee will assure that these liaisons are appointed and approve their selection. The key responsibilities of the liaisons are:

- **Self-Assessments** – Will help facilitate, partake and verify the results of the self-assessment process.

- **Risk Indicators** – Design, collection, reporting, and data capture of risk indicators and related reports. Liaisons will monitor results and help work with their respective departments on identified issues. Resulting information will be distributed to both the departments and ORMD on a timely and accurate basis.

- **Loss Events** – Coordinate collection, recording and data capture of loss events within the businesses and regular reporting of these events, the details, amounts.

- **Gaps/Issues** – Responsible for the timely follow-up, documentation and status of action plans, open issues (Internal Audit, External Audit, Regulator and Inspector) and other initiatives waiting to be completed.

- **Committee Participation** – Must prepare to be called upon to attend the Operational Risk Management Committee meetings, when necessary, to discuss operational risk issues.

- **Risk Mitigation** – Responsible for consulting/advising the business units on ways to mitigate risks. Work with business areas and respective departments on risk analysis and mitigation.

G. Key functions of Department Heads

Business/Functional area heads are responsible for risk taking, related controls and mitigation. They are ultimately responsible for implementation of sound risk management practices and any resulting impact for operational losses. To support this responsibility, they will have the following responsibilities related to operational risk management.

- **Risk Ownership** – The department heads shall take ownership of the operational risks faced in their departments/businesses.

- **Understanding** – Understanding the profile of operational risk facing the area and monitoring changes in the business and risk profile. Department Heads may be expected to present their risk profiles and action plans to the Operational Risk Management Committee.

- **Risk Indicators** – Collection and Preparation of various risk indicator reports.

- **Loss Events** - Identification of loss events within the businesses and regular reporting of these events, the details, amounts and circumstances to ORMD on a complete and timely basis.

- **Self-Assessment** – Responsible for the periodic completion of self-assessments.

- **Risk Mitigation** – The businesses are responsible for developing strategies for the mitigation of risk where required (or managing those risks deemed to be acceptable).

ANNEX 2
(Paragraph 5.7)

Mapping of Business Lines			
Buisness Unit	**Business line**		**Activity Groups**
	Level 1	**Level 2**	
Investment Banking	Corporate Finance	Corporate Finance	Mergers and Acquisitions, Underwriting, Privatisations, Securitisation, Research, Debt (Government, High Yield) Equity, Syndications, IPO, Secondary Private Placements.
		Municipal / government finance	
		Merchant Banking	
		Advisory Services	
	Trading and sales	Sales	Fixed Income, equity, foreign exchanges, commodities, credit, funding, own position securities lending and repos, brokerage, debt, prime brokerage.
		Market Making	
		Proprietary Positions	
		Treasury	
Banking	Retail Banking	Retail Banking	Retail lending and deposits, banking services, trust and estates
		Private Banking	Private lending and deposits, banking services, trust and estates, investment advice.
		Card Services	Merchant/Commercial/Corporate cards, private labels and retail.
	Commercial Banking	Commercial Banking	Project finance, real estate, export finance, trade finance, factoring, leasing, lends, guarantees, bills of exchange
	Payment and Settlement	External Clients	Payments and collections, funds transfer, clearing and settlement.
	Agency Services	Custody	Escrow, Depository Receipts, Securities lending (Customers) Corporate actions
		Corporate Agency	Issuer and paying agents
		Corporate Trust	
Others	Asset Management	Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open, private equity
		Non - Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open
	Retail Brokerage	Retail Brokerage	Execution and full service

ANNEX 3
(Paragraph 5.9)

Loss Event Type Classification			
Category (Level 1)	**Definition**	**Category (Level 2)**	**Category (Level 3)**
Internal Fraud	Lossess due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity / discrimination events, which involves at least one internal party.	Unauthorized activity	Transactions not reported (intentional)
			Trans type unauthorized (monetary loss)
			Mismarking of position (intentional)
		Theft and Fraud	Fraud/ credit fraud /worthless deposits
			Theft / extortion / embezzlement / robbery
			Misappropriation of assets
			Malicious destruction of assets
			Forgery
			Check kiting
			Smuggling
			Account take-over / impersonation /etc.
			Tax non-compliance /evasion (willful)
			Bribes/ kickbacks
			Insider trading (not on bank's account)
External Fraud	Lossess due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.	Theft and Fraud	Theft/ robbery
			Forgery
			Cheque Kiting
		Systems Security	Hacking damage
			Theft of information
Employment Practices and Workplace Safety	Lossess arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events.	Employee Relations	Compensation, benefit, termination issues
			Organized labor activity
		Environmental safety	General liability (Workplace accidents - slip & fall etc)
			Employee health & safety rules events

Loss Event Type Classification			
Category (Level 1)	**Definition**	**Category (Level 2)**	**Category (Level 3)**
			Workers compensation
		Diversity and discrimination	All discrimination types
Clients, Products & Business Practices	Lossess arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, Disclosure & Fiduciary	Fiduciary breaches / guideline violations
			Suitability / disclosure issues (KYC etc)
			Retail consumer disclosure violations
			Breach of privacy
			Aggressive sales
			Account churning
			Misuse of confidential information
			Lender Liability
		Improper Business or Market Practices	Antitrust
			Improper trade / market practices
			Market manipulation
			Insider trading
			Unlicensed activity
			Money laundering
		Product flaws	Product defects (unauthorized etc.)
			Model errors
		Selection, Sponsorship & Exposure	Failure to investigate client per guidelines
			Exceeding client exposure limits
		Advisory activities	Disputes over performance of advisory activities
Damage to physical assets	Losses arising from loss or damage to physical assets from natural disasters or other events	Disasters and other events	Natural disaster losses
			Human losses from external sources (terrorism, vandalism)

Loss Event Type Classification			
Category (Level 1)	**Definition**	**Category (Level 2)**	**Category (Level 3)**
Business disruption & system failures	Losses arising from disruption of business or system failures	Systems	Hardware
			Software
			Telecommunications
			Utility outrage / disruptions
Execution, Delivery & Process Management	Losses from failed transcations processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution Maintenance	Miscommunication
			Data entry, maintenance or loading error
			Missed deadline or responsibility
			Model / system misoperation
			Accounting error / entity attribution error
			Other task misperformance
			Delivery failure
			Collateral management failure
			Reference data maintenance
		Monitoring and Reporting	Failed mandatory reporting obligation
			Inaccurate external report (loss incurred)
		Customer intake and documentation	Client permissions /disclaimers missing
			Legal documents missing / incomplete
		Customer client account management	Unapproved access given to accounts
			Incorrect client records (loss incurred)
			Negligent loss damage of client assets
		Trade Counterparties	Non client counterparty misperformance
			Misc. non-client counterparty disputes
		Vendors & Suppliers	Outsourcing
			Vendor disputes

ATTACHMENT
(Paragraph 8.2)

Advanced Measurement Methodologies

It is suggested that for a better comprehension, this attachment should be read together with the "International Convergence of Capital Measurement and Capital Standards – A Revised Framework" released by the Basel Committee on Banking Supervision in June 2004.

The Standardised Approach

2. In the Standardised Approach, banks' activities are divided into eight business lines: corporate finance, trading & sales, retail banking, commercial banking, payment & settlement, agency services, asset management, and retail brokerage. The business lines are defined in detail in Annex 3 (Para 5.9).

3. Within each business line, gross income is a broad indicator that serves as a proxy for the scale of business operations and thus the likely scale of operational risk exposure within each of these business lines. The capital charge for each business line is calculated by multiplying gross income by a factor (denoted beta) assigned to that business line. Beta serves as a proxy for the industry-wide relationship between the operational risk loss experience for a given business line and the aggregate level of gross income for that business line. It should be noted that in the Standardised Approach gross income is measured for each business line, not the whole institution, i.e. in corporate finance, the indicator is the gross income generated in the corporate finance business line.

4. The total capital charge is calculated as the simple summation of the regulatory capital charges across each of the business lines. The total capital charge may be expressed as:

$$K_{TSA} = \{\Sigma_{1\text{-}3 \text{ years}} \ max\ [\sum (GI_{1\text{-}8} * \beta_{1\text{-}8}), 0]\}/3$$

Where:

K_{TSA} = the capital charge under the Standardised Approach

$GI_{1\text{-}8}$ = annual gross income in a given year, for each business lines

β_{1-8} = a fixed percentage, set by the Committee, relating the level of required capital to the level of the gross income for each of the 8 business lines. The values of the β are detailed below:

Business Lines	Indicator	Beta factors (%)	Beta values (%)
Corporate finance	Gross income	β_1	18
Trading and sales	Gross income	β_2	18
Retail banking	Gross income	β_3	12
Commercial banking	Gross income	β_4	15
Payment and settlement	Gross income	β_5	18
Agency services	Gross income	β_6	15
Asset management	Gross income	β_7	12
Retail brokerage	Gross income	β_8	12

Qualifying Criteria for Standardised Approach

5. In order to qualify for use of the Standardised Approach, a bank must satisfy its supervisor that, at a minimum:

- Its Board of Directors and senior management, as appropriate, are actively involved in the oversight of the operational risk management framework;
- It has an operational risk management system that is conceptually sound and is implemented with integrity; and
- It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.

6. Supervisors will have the right to insist on a period of initial monitoring of a bank's Standardised Approach before it is used for regulatory capital purposes.

7. A bank must develop specific policies and have documented criteria for mapping gross income for current business lines and activities into the standardised framework. The criteria must be reviewed and adjusted for new or changing business activities as appropriate. The principles for business line mapping are set out in Annex 2 of the Guidance Note.

8. As some internationally active banks will wish to use the Standardised Approach, it is important that such banks have adequate operational risk management systems. Consequently, an internationally active bank using the Standardised Approach must meet the following additional criteria (for other

banks, these criteria are recommended, with national discretion to impose them as requirements):

(a) The bank must have an operational risk management system with clear responsibilities assigned to an operational risk management function. The operational risk management function is responsible for developing strategies to identify, assess, monitor and control/mitigate operational risk; for codifying firm-level policies and procedures concerning operational risk management and controls; for the design and implementation of the firm's operational risk assessment methodology; and for the design and implementation of a risk-reporting system for operational risk.

(b) As part of the bank's internal operational risk assessment system, the bank must systematically track relevant operational risk data including material losses by business line. Its operational risk assessment system must be closely integrated into the risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the banks operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting, and risk analysis. The bank must have techniques for creating incentives to improve the management of operational risk throughout the firm.

(c) There must be regular reporting of operational risk exposures, including material operational losses, to business unit management, senior management, and to the board of directors. The bank must have procedures for taking appropriate action according to the information within the management reports.

(d) The bank's operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which must include policies for the treatment of non-compliance issues.

(e) The bank's operational risk management processes and assessment system must be subject to validation and regular independent review. These reviews must include both the activities of the business units and of the operational risk management function.

(f) The bank's operational risk assessment system (including the internal validation processes) must be subject to regular review by external auditors and/or supervisors.

The Alternative Standardised Approach

9. At national supervisory discretion a supervisor can choose to allow a bank to use the Alternative Standardised Approach (ASA) provided the bank is able to satisfy its supervisor that this alternative approach provides an improved basis by, for example, avoiding double counting of risks. Once a bank has been allowed to use the ASA, it will not be allowed to revert to use of the Standardised Approach without the permission of its supervisor. It is not envisaged that large diversified banks in major markets would use the ASA. Under the ASA, the operational risk capital charge/methodology is the same as for the Standardised Approach except for two business lines – retail banking and commercial banking. For these business lines, loans and advances – multiplied by a fixed factor 'm' – replaces gross income as the exposure indicator. The betas for retail and commercial banking are unchanged from the Standardised Approach. The ASA operational risk capital charge for retail banking (with the same basic formula for commercial banking) can be expressed as:

KRB = β_{RB} **x m x LARB**

Where

- KRB is the capital charge for the retail banking business line
- β_{RB} is the beta for the retail banking business line
- LARB is total outstanding retail loans and advances (non-risk weighted and gross of provisions), averaged over the past three years
- m is 0.035

10. For the purposes of the ASA, total loans and advances in the retail banking business line consists of the total drawn amounts in the following credit portfolios:

retail, SMEs treated as retail, and purchased retail receivables. For commercial banking, total loans and advances consists of the drawn amounts in the following credit portfolios: corporate, sovereign, bank, specialised lending, SMEs treated as corporate and purchased corporate receivables. The book value of securities held in the banking book should also be included.

11. Under the ASA, banks may aggregate retail and commercial banking (if they wish to) using a beta of 15%. Similarly, those banks that are unable to disaggregate their gross income into the other six business lines can aggregate the total gross income for these six business lines using a beta of 18% with negative gross income treated at para 3 of the Standardised Approach for operational risk.

12. As under the Standardised Approach, the total capital charge for the ASA is calculated as the simple summation of the regulatory capital charges across each of the eight business lines.

Advanced Measurement Approaches (AMA)

13. Under the AMA, the regulatory capital requirement will equal the risk measure generated by the bank's internal operational risk measurement system using the quantitative and qualitative criteria for the AMA discussed below. Use of the AMA is subject to supervisory approval.

14. A bank adopting the AMA may, with the approval of its host supervisors and the support of its home supervisor, use an allocation mechanism for the purpose of determining the regulatory capital requirement for internationally active banking subsidiaries that are not deemed to be significant relative to the overall banking group but are themselves subject to this Framework in accordance with the scope of application. Supervisory approval would be conditional on the bank demonstrating to the satisfaction of the relevant supervisors that the allocation mechanism for these subsidiaries is appropriate and can be supported empirically. The board of directors and senior management of each subsidiary are responsible for conducting their own assessment of the subsidiary's operational risks and

controls and ensuring the subsidiary is adequately capitalised in respect of those risks.

15. Subject to supervisory approval as discussed in paragraph 23 (d) below, the incorporation of a well-reasoned estimate of diversification benefits may be factored in at the group-wide level or at the banking subsidiary level. However, any banking subsidiaries whose host supervisors determine that they must calculate stand-alone capital requirements (Scope of Application in the Revised Framework – Part 1) may not incorporate group-wide diversification benefits in their AMA calculations (e.g. where an internationally active banking subsidiary is deemed to be significant, the banking subsidiary may incorporate the diversification benefits of its own operations – those arising at the sub-consolidated level – but may not incorporate the diversification benefits of the parent).

16. The appropriateness of the allocation methodology will be reviewed with consideration given to the stage of development of risk-sensitive allocation techniques and the extent to which it reflects the level of operational risk in the legal entities and across the banking group. Supervisors expect that AMA banking groups will continue efforts to develop increasingly risk-sensitive operational risk allocation techniques, notwithstanding initial approval of techniques based on gross income or other proxies for operational risk.

17. Banks adopting the AMA will be required to calculate their capital requirement using this approach as well as the 1988 Accord as outlined in paragraph 46 of the Revised Framework.

(i) General standards

18. In order to qualify for use of the AMA a bank must satisfy its supervisor that, at a minimum:

- Its board of directors and senior management, as appropriate, are actively involved in the oversight of the operational risk management framework;

- It has an operational risk management system that is conceptually sound and is implemented with integrity; and

- It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.

19. A bank's AMA will be subject to a period of initial monitoring by its supervisor before it can be used for regulatory purposes. This period will allow the supervisor to determine whether the approach is credible and appropriate. As discussed below, a bank's internal measurement system must reasonably estimate unexpected losses based on the combined use of internal and relevant external loss data, scenario analysis and bank-specific business environment and internal control factors. The bank's measurement system must also be capable of supporting an allocation of economic capital for operational risk across business lines in a manner that creates incentives to improve business line operational risk management.

(ii) Qualitative standards

20. A bank must meet the following qualitative standards before it is permitted to use an AMA for operational risk capital:

(a) The bank must have an independent operational risk management function that is responsible for the design and implementation of the bank's operational risk management framework. The operational risk management function is responsible for codifying firm-level policies and procedures concerning operational risk management and controls; for the design and implementation of the firm's operational risk measurement methodology; for the design and implementation of a risk-reporting system for operational risk; and for developing strategies to identify, measure, monitor and control/mitigate operational risk.

(b) The bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the bank's operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting, internal capital allocation, and risk analysis. The bank must have techniques for allocating operational risk capital to major business lines and for creating incentives to improve the management of operational risk throughout the firm.

(c) There must be regular reporting of operational risk exposures and loss experience to business unit management, senior management, and to the board of directors. The bank must have procedures for taking appropriate action according to the information within the management reports.

(d) The bank's operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which must include policies for the treatment of non-compliance issues.

(e) Internal and/or external auditors must perform regular reviews of the operational risk management processes and measurement systems. This review must include both the activities of the business units and of the independent operational risk management function.

(f) The validation of the operational risk measurement system by external auditors and/or supervisory authorities must include the following:

- Verifying that the internal validation processes are operating in a satisfactory manner; and

- Making sure that data flows and processes associated with the risk measurement system are transparent and accessible. In particular, it is necessary that auditors and supervisory authorities are in a position to have easy access, whenever they judge it necessary and under appropriate procedures, to the system's specifications and parameters.

(iii) Quantitative standards

AMA soundness standard

21. Given the continuing evolution of analytical approaches for operational risk, the Committee is not specifying the approach or distributional assumptions used to generate the operational risk measure for regulatory capital purposes. However, a bank must be able to demonstrate that its approach captures potentially severe 'tail' loss events. Whatever approach is used, a bank must demonstrate that its operational risk measure meets a soundness standard comparable to that of the internal ratings-based approach for credit risk, (i.e. comparable to a one year holding period and a 99.9^{th} percentile confidence interval).

22. The Committee recognises that the AMA soundness standard provides significant flexibility to banks in the development of an operational risk measurement and management system. However, in the development of these systems, banks must have and maintain rigorous procedures for operational risk model development and independent model validation. Prior to implementation, the Committee will review evolving industry practices regarding credible and

consistent estimates of potential operational losses. It will also review accumulated data, and the level of capital requirements estimated by the AMA, and may refine its proposals if appropriate.

Detailed criteria

23. This section describes a series of quantitative standards that will apply to internally-generated operational risk measures for purposes of calculating the regulatory minimum capital charge.

(a) Any internal operational risk measurement system must be consistent with the scope of operational risk defined by the Committee in paragraph 644 of the Revised Framework and the loss event types defined in Annex 3.

(b) Supervisors will require the bank to calculate its regulatory capital requirement as the sum of expected loss (EL) and unexpected loss (UL), unless the bank can demonstrate that it is adequately capturing EL in its internal business practices. That is, to base the minimum regulatory capital requirement on UL alone, the bank must be able to demonstrate to the satisfaction of its national supervisor that it has measured and accounted for its EL exposure.

(c) A bank's risk measurement system must be sufficiently 'granular' to capture the major drivers of operational risk affecting the shape of the tail of the loss estimates.

(d) Risk measures for different operational risk estimates must be added for purposes of calculating the regulatory minimum capital requirement. However, the bank may be permitted to use internally determined correlations in operational risk losses across individual operational risk estimates, provided it can demonstrate to the satisfaction of the national supervisor that its systems for determining correlations are sound, implemented with integrity, and take into account the uncertainty surrounding any such correlation estimates (particularly in periods of stress). The bank must validate its correlation assumptions using appropriate quantitative and qualitative techniques.

(e) Any operational risk measurement system must have certain key features to meet the supervisory soundness standard set out in this section. These elements must include the use of internal data, relevant external data, scenario analysis and factors reflecting the business environment and internal control systems.

(f) A bank needs to have a credible, transparent, well-documented and verifiable approach for weighting these fundamental elements in its overall operational risk measurement system. For example, there may be cases where estimates of the 99.9^{th} percentile confidence interval based primarily on internal and external loss event data would be unreliable for business lines with a heavy-

tailed loss distribution and a small number of observed losses. In such cases, scenario analysis, and business environment and control factors, may play a more dominant role in the risk measurement system. Conversely, operational loss event data may play a more dominant role in the risk measurement system for business lines where estimates of the 99.9^{th} percentile confidence interval based primarily on such data are deemed reliable. In all cases, the bank's approach for weighting the four fundamental elements should be internally consistent and avoid the double counting of qualitative assessments or risk mitigants already recognised in other elements of the framework.

Internal data

24. Banks must track internal loss data according to the criteria set out in this section. The tracking of internal loss event data is an essential prerequisite to the development and functioning of a credible operational risk measurement system. Internal loss data is crucial for tying a bank's risk estimates to its actual loss experience. This can be achieved in a number of ways, including using internal loss data as the foundation of empirical risk estimates, as a means of validating the inputs and outputs of the bank's risk measurement system, or as the link between loss experience and risk management and control decisions.

25. Internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological processes and risk management procedures. Therefore, a bank must have documented procedures for assessing the on-going relevance of historical loss data, including those situations in which judgement overrides, scaling, or other adjustments may be used, to what extent they may be used and who is authorised to make such decisions.

26. Internally generated operational risk measures used for regulatory capital purposes must be based on a minimum five-year observation period of internal loss data, whether the internal loss data is used directly to build the loss measure or to validate it. When the bank first moves to the AMA, a three-year historical data window is acceptable (this includes the parallel calculations in paragraph 46 of the Revised Framework).

27. To qualify for regulatory capital purposes, a bank's internal loss collection processes must meet the following standards:

- To assist in supervisory validation, a bank must be able to map its historical internal loss data into the relevant level 1 supervisory categories defined in Annexes 2 and 3 and to provide these data to supervisors upon request. It must have documented, objective criteria for allocating losses to the specified business lines and event types. However, it is left to the bank to decide the extent to which it applies these categorisations in its internal operational risk measurement system.

- A bank's internal loss data must be comprehensive in that it captures all material activities and exposures from all appropriate sub-systems and geographic locations. A bank must be able to justify that any excluded activities or exposures, both individually and in combination, would not have a material impact on the overall risk estimates. A bank must have an appropriate *de minimis* gross loss threshold for internal loss data collection, for example Rs.10,000. The appropriate threshold may vary somewhat between banks, and within a bank across business lines and/or event types. However, particular thresholds should be broadly consistent with those used by peer banks.

- Aside from information on gross loss amounts, a bank should collect information about the date of the event, any recoveries of gross loss amounts, as well as some descriptive information about the drivers or causes of the loss event. The level of detail of any descriptive information should be commensurate with the size of the gross loss amount.

- A bank must develop specific criteria for assigning loss data arising from an event in a centralised function (e.g. an information technology department) or an activity that spans more than one business line, as well as from related events over time.

- Operational risk losses that are related to credit risk and have historically been included in banks' credit risk databases (e.g. collateral management failures) will continue to be treated as credit risk for the purposes of calculating minimum regulatory capital under this Framework. Therefore, such losses will not be subject to the operational risk capital charge (This applies to all banks, including those that may only now be designing their credit risk and operational risk databases). Nevertheless, for the purposes of internal operational risk management, banks must identify all material operational risk losses consistent with the scope of the definition of operational risk (as set out in the definition of operational risk and the loss event types outlined), including those related to credit risk. Such material operational risk-related credit risk losses should be flagged separately within a bank's internal operational risk database. The materiality of these losses may vary between banks, and within a bank across business lines and/or event types. Materiality thresholds should be broadly consistent with those used by peer banks.

- Operational risk losses that are related to market risk are treated as operational risk for the purposes of calculating minimum regulatory capital under this Framework and will therefore be subject to the operational risk capital charge.

External data

28. A bank's operational risk measurement system must use relevant external data (either public data and/or pooled industry data), especially when there is reason to believe that the bank is exposed to infrequent, yet potentially severe, losses. These external data should include data on actual loss amounts, information on the scale of business operations where the event occurred, information on the causes and circumstances of the loss events, or other information that would help in assessing the relevance of the loss event for other banks. A bank must have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate the data (e.g. scaling, qualitative adjustments, or informing the development of improved scenario analysis). The conditions and practices for external data use must be regularly reviewed, documented, and subject to periodic independent review.

Scenario analysis

29. A bank must use scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high-severity events. This approach draws on the knowledge of experienced business managers and risk management experts to derive reasoned assessments of plausible severe losses. For instance, these expert assessments could be expressed as parameters of an assumed statistical loss distribution. In addition, scenario analysis should be used to assess the impact of deviations from the correlation assumptions embedded in the bank's operational risk measurement framework, in particular, to evaluate potential losses arising from multiple simultaneous operational risk loss events. Over time, such assessments need to be validated and re-assessed through comparison to actual loss experience to ensure their reasonableness.

Business environment and internal control factors

30. In addition to using loss data, whether actual or scenario-based, a bank's firm-wide risk assessment methodology must capture key business environment and internal control factors that can change its operational risk profile. These factors will make a bank's risk assessments more forward-looking, more directly reflect the quality of the bank's control and operating environments, help align capital assessments with risk management objectives, and recognise both improvements and deterioration in operational risk profiles in a more immediate fashion. To qualify for regulatory capital purposes, the use of these factors in a bank's risk measurement framework must meet the following standards:

- The choice of each factor needs to be justified as a meaningful driver of risk, based on experience and involving the expert judgment of the affected business areas. Whenever possible, the factors should be translatable into quantitative measures that lend themselves to verification.

- The sensitivity of a bank's risk estimates to changes in the factors and the relative weighting of the various factors need to be well reasoned. In addition to capturing changes in risk due to improvements in risk controls, the framework must also capture potential increases in risk due to greater complexity of activities or increased business volume.

- The framework and each instance of its application, including the supporting rationale for any adjustments to empirical estimates, must be documented and subject to independent review within the bank and by supervisors.

- Over time, the process and the outcomes need to be validated through comparison to actual internal loss experience, relevant external data, and appropriate adjustments made.

(iv) Risk mitigation

31. Under the AMA, a bank will be allowed to recognise the risk mitigating impact of insurance in the measures of operational risk used for regulatory minimum capital requirements. The recognition of insurance mitigation will be limited to 20% of the total operational risk capital charge calculated under the AMA.

32. A bank's ability to take advantage of such risk mitigation will depend on compliance with the following criteria:

- The insurance provider has a minimum claims paying ability rating of A (or equivalent).

- The insurance policy must have an initial term of no less than one year. For policies with a residual term of less than one year, the bank must make appropriate haircuts reflecting the declining residual term of the policy, up to a full 100% haircut for policies with a residual term of 90 days or less.

- The insurance policy has a minimum notice period for cancellation of 90 days.

- The insurance policy has no exclusions or limitations triggered by supervisory actions or, in the case of a failed bank, that preclude the bank, receiver or liquidator from recovering for damages suffered or expenses incurred by the bank, except in respect of events occurring after the initiation of receivership or liquidation proceedings in respect of the bank, provided that the insurance policy may exclude any fine, penalty, or punitive damages resulting from supervisory actions.

- The risk mitigation calculations must reflect the bank's insurance coverage in a manner that is transparent in its relationship to, and consistent with, the actual likelihood and impact of loss used in the bank's overall determination of its operational risk capital.

- The insurance is provided by a third-party entity. In the case of insurance through captives and affiliates, the exposure has to be laid off to an independent third-party entity, for example through re-insurance, that meets the eligibility criteria.

- The framework for recognising insurance is well reasoned and documented.

- The bank discloses a description of its use of insurance for the purpose of mitigating operational risk.

33. A bank's methodology for recognising insurance under the AMA also needs to capture the following elements through appropriate discounts or haircuts in the amount of insurance recognition:

- The residual term of a policy, where less than one year, as noted above;
- A policy's cancellation terms, where less than one year; and
- The uncertainty of payment as well as mismatches in coverage of insurance policies.

Partial use

34. A bank will be permitted to use an AMA for some parts of its operations and the Basic Indicator Approach or Standardised Approach for the balance (partial use), provided that the following conditions are met:

- All operational risks of the bank's global, consolidated operations are captured;

- All of the bank's operations that are covered by the AMA meet the qualitative criteria for using an AMA, while those parts of its operations that are using one of the simpler approaches meet the qualifying criteria for that approach;

- On the date of implementation of an AMA, a significant part of the bank's operational risks are captured by the AMA; and

- The bank provides its supervisor with a plan specifying the timetable to which it intends to roll out the AMA across all but an immaterial part of its operations. The plan should be driven by the practicality and feasibility of moving to the AMA over time, and not for other reasons.

35. Subject to the approval of its supervisor, a bank opting for partial use may determine which parts of its operations will use an AMA on the basis of business line, legal structure, geography, or other internally determined basis.

36. Subject to the approval of its supervisor, where a bank intends to implement an approach other than the AMA on a global, consolidated basis and it does not meet the third and/or fourth conditions in paragraph 34 above, the bank may, in limited circumstances:

- Implement an AMA on a permanent partial basis; and
- Include in its global, consolidated operational risk capital requirements the results of an AMA calculation at a subsidiary where the AMA has been approved by the relevant host supervisor and is acceptable to the bank's home supervisor.

37. Approvals of the nature described in paragraph 36 above should be granted only on an exceptional basis. Such exceptional approvals should generally be limited to circumstances where a bank is prevented from meeting these conditions due to implementation decisions of supervisors of the bank's subsidiary operations in foreign jurisdictions.

BIBILOGRAPHY

1. Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, February 2003.

2. Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards – A Revised Framework, June 2004.

3. Basel Committee on Banking Supervision, Framework for Internal Control Systems in Banking Organisations, September 1998