

Chapter-6 Basics of Operational Risk

Certificate in Risk Management



Confidentiality Statement

This document should not be carried outside the physical and virtual boundaries of TCS and its client work locations. The sharing of this document with any person other than TCSer would tantamount to violation of confidentiality agreement signed by you while joining TCS.



Notice

The information given in this course material is merely for reference. Certain third party terminologies or matter that may be appearing in the course are used only for contextual identification and explanation, without an intention to infringe.

Contents

6.1 Operational Risk	5
6.2 Operational Risk measurement methodologies	12
6.3 Regulatory approach to BASEL II Implementation.....	19
6.4 Operational Risk Treatment	22
Summary.....	25



Chapter – 6 Basics of Operational Risk

Introduction

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This is another area where the Committee has developed a new regulatory capital approach. In Basel II there are flexible provisions for banks to develop an approach to calculate operational risk capital that is consistent with their mix of activities and underlying risks. This Chapter deals with such basics approaches of calculating operations risk capital.

Learning Objective

After reading this chapter you will:

- Understand the guidelines in Basel II in the context Operations Risk.
- Get an insight of various approaches for calculating Operational risk capital.
- Understand different qualifying criteria for this approaches

TATA CONSULTANCY SERVICES

6.1 Operational Risk

"The risk of direct or indirect losses resulting from inadequate or failed internal processes, people and systems or from external events"

The Basel committee wants to enhance operational risk assessment efforts by encouraging the industry to develop methodologies and collect data related to managing operational risk. The Basel committee has adopted a common industry definition of operational risk, namely:

Strategic and reputation risk is not included in this definition for the purpose of a minimum regulatory operational risk capital charge. This definition focuses on causes of operational risk and the Basel Committee believes that this is appropriate for both risk management and ultimately for measurement.

Types of Operational risk

Operational risks are not consciously taken. But they invariably arise in the course of conducting business activities. The key challenge is often to identify and anticipate the various kinds of operational risk that may arise. The Basle committee has provided a useful framework in this regard.

- **Internal fraud:** Examples include intentional misreporting of trading positions, employee theft, and insider trading on an employee's own account. This risk is considered low frequency, high severity.
- **External fraud:** Examples include computer hacking, robbery and forgery. This risk is considered high/medium frequency, low/medium severity.
- **Employment practices and workplace safety:** Examples include worker compensation claims and sexual discrimination claims. This risk is considered low frequency, low severity.
- **Clients, products, and business practices:** Examples include fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account and money laundering. This risk is considered low/medium frequency and high/medium severity.

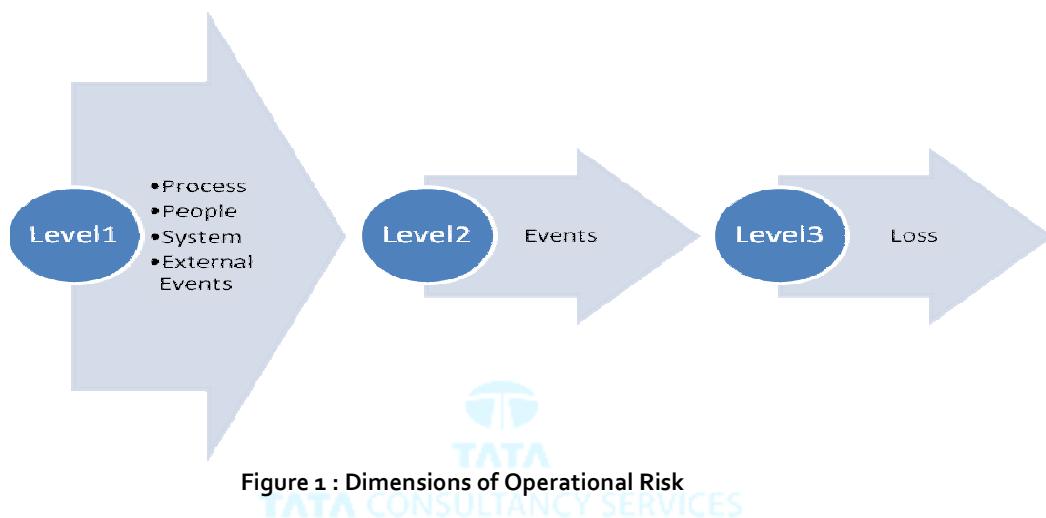
- **Damage to physical assets:** Examples include earthquakes, fires and floods. This risk is considered low frequency/low severity.
- **Business disruption and system failures:** Examples include hardware and software failures, telecommunication problems, and utility outages. This risk is considered low frequency/low severity.
- **Execution, delivery and process management:** Examples include data entry errors, collateral management failures, incomplete legal documentation, and unapproved access given to clients' accounts. This risk is considered high frequency, low severity.

For eleven years up to 1995, a bond trader of Daiwa Bank in New York had caused and hidden losses of USD 1.1 billion through non-compliant transactions and scam deals. Daiwa did not have any appreciable management controls nor even the simplest internal controls that could have immediately exposed the fraudulent transactions. The bank became insolvent, eleven senior executives were ordered to pay damages as they failed to supervise staff.

British Banker's Association defines the operational risk as "The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events". This definition includes all the various possibilities that can arise and are combined together to fall under the category Operational Risk. The important characteristics of this definition are:

- 1) The focus on internal aspects which the bank should keep under its regular monitoring system. These are often actions or failures to take action by the bank and its staff. These risks are clearly separate from market and credit risks.
- 2) The importance of process orientation in the operational risk concept. The operational risks in the banking sector resemble similar risks in industry more closely than they do market or credit risks in a bank.

- 3) The important role played by the internal control system, the elements and rules of which have been known and accepted for decades but which are often forgotten or neglected during periods of restructuring or product and process innovation.
- 4) The external incidents are natural disasters, political events, losses and deficiencies in the technical infrastructure, as well as changes in and problems with the legal, tax and regulatory environment.



Risk is not merely considered as the “uncertainty about the future” or “probability of sustaining a loss” but is defined as “an expression of the danger that the effective outcome will deviate from expected output in a negative way”. This definition implies that banks do not take risk for granted but deal with them actively. The risk is calculated in terms of probability and the impact of its deviation. It comes from the concept that every risk is associated with some opportunity.

Direct and Indirect Losses

As stated in its definition of operational risk, the Basel committee intends for the capital framework to shield the institutions from both direct and certain indirect losses. It is intended that the cost to fix an operational risk problem, payments to third parties and write downs generally would be included in calculating the loss incurred from operational risk event.

Furthermore there may be other types of losses or events which should be reflected in the charge, such as near misses, latent losses or contingent losses. The costs of improvements in controls, preventative action and quality assurance, and investment in new systems would not be included.

In practice, such distinctions are difficult as there is often a high degree of ambiguity inherent in the process of categorizing losses and costs, which may result in omission or double counting problems. The committee is cognizant of the difficulties in determining the scope of the charge and is seeking comment on how to better specify the loss types for inclusion in a more refined definition of operational risk. Further it is likely that detailed guidance on loss categorization and allocation of losses by risk type need to be produced, to allow the development of more advanced approaches to operational risk, and the Committee is also seeking detailed comment in this respect.

From 1986 to 1996, the chief trader of Sumitomo Corporation (Yasuo Hamanaka nicknamed "Mr Five Percent" due to the share of the global copper market that he controlled) built up losses of USD 1.8 billion through fraudulent copper transactions. His actions that affected the entire world copper market simply were not supervised by the bank.

Expected and unexpected losses

In line with the other banking risks, conceptually a capital charge for operational risk should cover unexpected losses due to operational risk. Provisions should cover expected losses. However, accounting rules in many countries do not appear to allow a robust, comprehensive and clear approach to setting provisions, especially for operational risk. Rather these rules appear to allow for provisions only for future obligations related to events that have already occurred. In particular, accounting standards generally require measurable estimation tests be met and losses be probable before provisions or contingencies are actually booked.

In general, provisions set up under such accounting standards bear only a very small relation to the concept of expected operational losses. Regulators are interested in more forward looking concepts of provisions.

Committee proposed to calibrate the capital charge for operational risk based on expected and unexpected losses, but to allow some recognition for provisioning and loss deduction. A portion of end of period balances for a specific list of identified provisions or contingencies could be deducted from the minimum capital requirement (or recognized as part of an available capital cushion to meet requirements) provided the bank discloses them as such.

The capital charge for a limited list of banking activities where the annual deduction of actual operational losses is prevalent (e.g. credit card fraud) could be based on unexpected losses only, plus a cushion for imprecision.

Scaling

Losses due to operational risk can be scaled up if we know the exponent for scaling. In general the exponent will lie between zero and 1. Thus if a division with revenue R_1 has incurred losses of 100, a division with revenue = R_2 will have losses of ; where k is the exponent.



Ex-A bank with annual revenues of \$2 billion has incurred a loss of \$100 million on account of operational risk. What would be the losses for a bank with a similar business profile but with revenues of \$6 billion? Assume the exponent for scaling losses is 0.23.

$$\begin{aligned}
 \text{Loss for Bank B} &= \left(\frac{\text{Revenue of Bank B}}{\text{Revenue of Bank A}} \right)^{0.23} \times \text{loss for Bank A} \\
 &= \left(\frac{6}{2} \right)^{0.23} \times 100 \\
 &= 3.23 \times 100 \\
 &= \$128.75 \text{ million}
 \end{aligned}$$

Partial use

A bank will be permitted to use an AMA for some parts of its operations and the Basic Indicator Approach or Standardized 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.
- On the date of implementation of an AMA, a significant part of the bank's operational risks are captured by the AMA.
- 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.
- 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.

Sound Practices for the management and supervision of operational risk

Developing an Appropriate Risk Management Environment

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

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

Principle 3: Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organization. Senior management should develop policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems.

Risk Management: Identification, Assessment, Monitoring, and Mitigation/Control

Principle 4: 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 assessed.

Principle 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.

Principle 6: 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, in light of their overall risk appetite and profile.



Principle 7: 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.

Role of Supervisors

Principle 8: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks.

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

Role of Disclosure

Principle 10: Banks should make sufficient public disclosure with regard to operational risk management.

6.2 Operational Risk measurement methodologies

Three methods for calculating operational risk capital charges are presented in the framework outlined below in a continuum of increasing sophistication and risk sensitivity:

- The Basic Indicator Approach;
- The Standardized Approach; and
- Advanced Measurement Approaches (AMA).

As banks develop more sophisticated operational risk measurement systems and practices, they are encouraged to move along the spectrum of available approaches. Qualifying criteria for the Standardized Approach and AMA are presented below.

Internationally active banks and banks with significant operational risk exposures (for example, specialized processing banks) are expected to use an approach that is more sophisticated than the Basic Indicator Approach and that is appropriate for the risk profile of the institution. A bank will be permitted to use the Basic Indicator or Standardized Approach for some parts of its operations and an AMA for others provided certain minimum criteria are met.



Without supervisory approval, bank will not be allowed to revert to a simpler approach once it has been approved for a more advanced approach. However, if a supervisor determines that a bank using a more advanced approach no longer meets the qualifying criteria for this approach, it may require the bank to revert to a simpler approach for some or all of its operations, until it meets the conditions specified by the supervisor for returning to a more advanced approach.

i. The Basic Indicator Approach (BIA)

The basic indicator approach is a technique proposed under Basel II capital adequacy rules for banking institutions.

The capital that a bank must hold in BIA for operational risk is equal to the average of a fixed percentage (denoted alpha) of positive annual gross income over the previous three years. Figures for any year in which annual gross income is negative or zero should be excluded from both the numerator and denominator when calculating the average. The charge may be expressed as follows:

$$K_{BIA} = [\sum (GI_{1-n} * \alpha)] / n$$

Where:

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

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

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

$\alpha = 15\%$, which is set by the Committee, relating the industry wide level of required capital to the industry wide level of the indicator.

The most basic approach allocates operational risk capital using a single indicator as a proxy for an institution's overall operational risk exposure. In this approach, operational risk capital is set equal to 15% of annual gross income over the previous three years. Gross income is defined as net interest income plus non interest income

The basic indicator approach is easy to implement and universally applicable across banks to arrive at a charge for operational risk. While basic indicator approach might be suitable for smaller banks with a simple range of business activities, the Basel Committee expects that the internationally active banks and banks with significant operational risk to use a more sophisticated approach.



Gross income is defined as net interest income plus net non-interest income. It is intended that this measure should:

- be gross of any provisions (e.g. for unpaid interest);
- Be gross of operating expenses, including fees paid to outsourcing service providers;
- Exclude realized profits/losses from the sale of securities in the banking book; and
- Exclude extraordinary or irregular items as well as income derived from insurance.

ii. The Standardized Approach

The Standardized Approach represents a further refinement along the evolutionary spectrum of approaches for operational risk capital. This approach differs from the Basic Indicator Approach, in that banks activities are divided into a number of standardized business units and business lines. Thus the Standardized approach is better able to reflect the differing risk profiles across banks as reflected by their broad business activities.

With each business lines, regulators have specified a broad indicator that is intended to reflect the size or volume of a banks activity in this area. The indicator is intended to serve as a rough proxy for the amount of operational risk proxy within each of this business lines.

In the Standardized 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 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.

The total capital charge is calculated as the three-year average of the simple summation of the regulatory capital charges across each of the business lines in each year. In any given year, negative capital charges (resulting from negative gross income) in any business line may offset positive capital charges in other business lines without limit.

However, where the aggregate capital charge across all business lines within a given year is negative, then the input to the numerator for that year will be zero. I.e. any negative gross income will be excluded both from numerator and denominator. The total capital charge may be expressed as:

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

where:

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

GI_{1-8} = annual gross income in a given year, as defined above in the Basic Indicator Approach, for each of the eight 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 eight business lines. The values of the betas are detailed below.

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

Qualifying Criteria:



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

- The bank must have an operational risk management system with clear responsibilities assigned to an operational risk management function.
- 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.
- 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's operational risk management system must be well documented.

- The bank's operational risk management processes and assessment system must be subject to validation and regular independent review.

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

iii. Advanced Measurement Approaches (AMA)

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.

If the allocation mechanism for the subsidiaries is appropriate and can be supported empirically, only then supervisory approval would be applicable to bank. 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 that the subsidiary is adequately capitalized in respect of those risks.

Subject to supervisory approval, 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 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).

Qualifying Criteria:

General standards

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 supervision of the operational risk management framework.

- The bank should have in place robust operational risk management system that is conceptually sound and is implemented with integrity.
- It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.

Qualitative standards

- 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 bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank.
- 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's operational risk management system must be well documented.
- Internal and/or external auditors must perform regular reviews of the operational risk management processes and measurement systems.
- The validation of the operational risk measurement system by external auditors and/or supervisory authorities.

Quantitative standards

- 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.
- 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.
- Risk measures for different operational risk estimates must be added for purposes of calculating the regulatory minimum capital requirement

- 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.

- 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.

Internal data

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.

- A bank must be able to map its historical internal loss data into the relevant level 1 supervisory categories

- 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 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

External data

- 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

- 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,
- The conditions and practices for external data use must be regularly reviewed, documented, and subject to periodic independent review.

6.3 Regulatory approach to BASEL II Implementation

The Basle framework

The Basle Committee has recommended some best practices in the area of operational risk.

- **Board approval** – The board of directors should approve and periodically review the Operational Risk Management framework.
- **Independent internal audit** – The board should subject the operational risk management framework to comprehensive and independent internal audit.
- **Management implementation** – Senior management should develop policies, processes and procedures for managing operational risk in the bank's important products, activities, processes and systems.
- **Risk identification and assessment** – Banks should identify and assess the operational risk inherent in all materials, products, activities, processes and systems.
- **Risk monitoring and reporting** – Operational risk profiles and material exposures to losses must be regularly monitored and reported to the senior management and the board of directors.
- **Risk control and mitigation** – Policies, processes and procedures must be put in place to control/mitigate material operational risks.

- **Contingency and continuity planning** – Contingency and continuity plans must be in place to cope with severe business disruption.
- **Disclosure** – Banks should make adequate disclosures to allow the markets to assess the approach of the bank towards managing operational risk.

According to the Basel II definition, the behavior and actions of people in an organization is one of the sources of operational risk, thus employees' motivation and satisfaction with their work is essential for ensuring their identification with the corporate objectives.

The Reserve Bank of India is the regulator and supervisor of the banking system in India and is entrusted with the task of framing the capital adequacy guidelines for banks in India under Basel II. It would be essential here to understand the structure of the Indian banking system under the regulatory purview of Reserve Bank of India to put things in perspective.

Currently, India has 88 scheduled commercial banks (SCBs) - 27 public sector banks (that is with the Government of India holding a stake), 31 private banks (these do not have government stake; they may be publicly listed and traded on stock exchanges) and 38 foreign banks. They have a combined network of over 53,000 branches and 17,000 ATMs.

Public sector banks, where the Government of India is the major shareholder, dominate the Indian banking system, accounting for nearly three-fourths of total assets and income (RBI 2007b). These banks are large and very old banks, operating through thousands of branches spread all over the country.

Measuring Operational Risk in Banks

Greater dependence on technology and centralized operations mean that banks are becoming increasingly exposed to operational risk. Some recent trends are:

- Banks are expanding their use of the Internet to service customers and perform basic functions;
- Globalization is creating complex linkages between institutions and countries;
- Part of the risk has been outsourced to third parties and so cannot be directly controlled

- Rules and regulations are expanding in an increasingly litigious society.

Measuring operational risk requires identification of the underlying operational drivers or risk factors. As shown in Figure, PricewaterhouseCoopers provides a useful summary as part of its Generally Accepted Risk Principles (GARP). This approach decomposes operational risk into those risks that are closely related to internal processes, people and systems (referred to as 'operational risks') and those that are more related to the external environment (termed 'business or event risks').

A quick scan through the list reveals that the most worrying events are those that are very rare, yet could have a devastating impact on a business.

Operational Risk	Business/Event Risk
<ul style="list-style-type: none"> • Transaction risk ► <ul style="list-style-type: none"> • Execution error • Product complexity • Booking error • Settlement error • Commodity delivery risk • Documentation/contract risk 	<ul style="list-style-type: none"> • Regulation risk ► <ul style="list-style-type: none"> • Breaching capital requirements • Regulatory changes
<ul style="list-style-type: none"> • Operational control risk ► <ul style="list-style-type: none"> • Exceeding limits • Rogue trading • Fraud • Money laundering • Security risk • Key personnel risk • Processing risk 	<ul style="list-style-type: none"> • Disaster risk ► <ul style="list-style-type: none"> • Natural disasters • War • Collapse/suspension of markets
<ul style="list-style-type: none"> • Systems risk ► <ul style="list-style-type: none"> • Programming error • Model/methodology error • Mark-to-market error • Management information • IT systems failure • Telecommunications failure • Contingency planning 	<ul style="list-style-type: none"> • Currency convertibility risk • Shift in credit rating • Reputation risk • Taxation risk • Legal risk

Figure 2 : Sources of Operational Risk (Source: Risk Management in Banking, by Elmer Funke Kupper)

Allocating capital to these very large but very low-probability risks is not necessarily useful. Consider settlement risk for example. If an international systemic problem occurred during the Year 2000 date change, the amount of capital that is currently available to support ongoing operations is unlikely to prevent failure. In such cases, it is better to ensure that there are clear controls in place to minimize the probability of the event and the impact of an occurrence.

Basel II has indicated three methodologies for measuring operational risk: Basic Indicator Approach; Standardized Approach; and Advanced Measurement Approach (AMA). The RBI has clarified that banks in India would follow the Basic Indicator Approach to begin with. Subsequently, only banks that are able to demonstrate better risk management systems would be asked to migrate to the Standardized Approach and AMA. Internationally, in the US, as various papers indicate, very few banks would eventually migrate to AMA, whereas in the EU, regulators have stated that they would make AMA mandatory for banks under their jurisdiction.



The Basic Indicator approach specifies that banks should hold capital charge for operational risk equal to the average of the 15% of annual positive gross income over the past three years, excluding any year when the gross income was negative.

6.4 Operational Risk Treatment

The basic management elements for coping with identified and valued operational risks are:

i. **Risk Avoidance**

In a cost-benefit analysis, a bank should opt for risk avoidance if the expected margin of activities is lower than the expected risk cost taking account of all the risks. Such activities should be abandoned or not be launched in the first place. Such a decision has to consider several aspects, such as time horizon, available specialized expertise, strategic objectives and reputational risks.

ii. **Risk mitigation**

Risk mitigation measures to address operational risk would be by way of

- a. using latest and relevant technology,
- b. having straight-through-processing interfaces,
- c. placing controls in the form of maker-checker practices and building proper audit trails, (d) encouraging vendor-neutral platforms and products,
- d. Addressing scalability issues by monitoring adequacy of infrastructure and performance, etc.

Under the AMA, a bank will be allowed to recognize 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 provided:

- The insurance provider has a minimum claims paying ability rating of A.
- The insurance policy must have an initial term of no less than one year.
- 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.
- The risk mitigation calculations must reflect the bank's insurance coverage in a manner that is transparent
- The insurance is provided by a third-party entity.
- The framework for recognizing insurance is well reasoned and documented.

iii. Risk Sharing and Transfer

Risk sharing or transfer is mainly of interest if a risk cannot or only inadequately be reduced by internal controls or if the cost of controls is higher than the expected loss. Another condition is that, in comparison with the company's risk appetite, the risk is so high that it cannot simply be accepted.

Important instruments of risk sharing and/or risk transfer are insurance and outsourcing of activities and functions. Very careful examinations are needed to see whether the desired effect can be fully or only partly achieved and whether undesirable effects are possible. Thus, there are cases where only risk sharing is possible instead of a full risk transfer or where circumstances change over time that also shift the relation between the risk borne by the company itself and by a third party. Owing to different deductibles, insurances allow for

a differentiation with a view to risk appetite and risk profiles of companies and their individual activities.

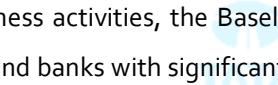
iv. Risk Acceptance

As a rule, risk acceptance depends on a cost-benefit analysis or weighting of expected income versus risk. A rational reason for accepting risks would be that the expected loss is lower than the cost of management activities to mitigate the risks.

It is recommendable that such decisions are systematically prepared and documented in a suitable form especially when the amounts involved are rather high. Systematization can be achieved by using a risk matrix criteria , such as thresholds, and decision-making processes, including escalation procedures, should exist for accepting risks.



Summary

- The Basel committee has adopted a common industry definition of operational risk, namely: "The risk of direct or indirect losses resulting from inadequate or failed internal processes, people and systems or from external events"
- Basel committee intends for the capital framework to shield the institutions from both direct and certain indirect losses.
- Conceptually a capital charge for operational risk should cover unexpected losses due to operational risk.
- The chapter details on different approaches for calculation of operational risk and also the qualifying criteria for these approaches.
 - The Basic Indicator Approach;
 - The Standardized Approach; and
 - Advanced Measurement Approaches (AMA).
- While basic indicator approach might be suitable for smaller banks with a simple range of business activities, the Basel Committee expects that the internationally active banks and banks with significant operational risk to use a more sophisticated approach.  **TATA CONSULTANCY SERVICES**
- Standardized Approach differs from the Basic Indicator Approach, in that banks' activities are divided into a number of standardized business units and business lines.



TATA CONSULTANCY SERVICES

www.tcs.com