ambitious baba .com
INDIA'S LARGEST TEST PREP PLATFORM

Module-B Unit-6

CAIIB PAPER-2

BANK Financial Management(BFM)

CAIIB BFM Module B Unit 6: Operational Risk and Integrated Risk Management

Operational Risk

Operational risk is one area of risk that is faced by all organisations. The more complex an organisation is, the more would be its exposure to operational risk. Operational risk would arise due to deviations from normal and planned functioning of systems, procedures, technology and human failures of omission and commission.

Operational Risk - Classification

Before we classify operational risk into various categories, we must understand the nature of the operational risk. Operational risk arises literally from all the activities undertaken and consequently it is present everywhere in an organisation. Impact of various forms of operational risk on the organisation may vary in degree i.e.,

The nature of operational risk may be listed as:

- Operational risk exists almost everywhere in the organisation.
- Operational risks vary in their components. Some are high occurrence low value risks, while some are low occurrence high value risks.
- Operational risks in the organisation continuously change especially when an organisation is undergoing changes.

The Second Consultative Paper of Basel II suggested classification of operational risks based on the **'Causes' and 'Effects'**. That is, classifications based on causes that are responsible for operational risks or classifications based on effects of risks were suggested. Classifications based on 'Causes' and 'Effects' are listed below.

Cause-based

- ***People oriented causes*** - negligence, incompetence, insufficient training, integrity, key man.
- ***Process oriented (Transaction based) causes*** - business volume fluctuation, organizational complexity, product complexity, and major changes.

- ***Process oriented (Operational control based) causes*** - inadequate segregation of duties, lack of management supervision, inadequate procedures.
- ***Technology oriented causes*** - poor technology and telecom, obsolete applications, lack of automation, information system complexity, poor design, development and testing.
- ***External causes*** - natural disasters, operational failures of a third party, deteriorated social or political context.

Effect Based

- Legal liability
- Regulatory, compliance and taxation penalties
- Loss or damage to assets
- Restitution
- Loss of recourse
- Write-downs

Event Based

- Internal Fraud
- External Fraud
- Employment practices and workplace safety
- Clients, products and business practices
- Damage to physical assets
- Business disruption and system failures
- Execution, delivery and process management

Operational Risk Classification By Event Type

- ***Internal Fraud:*** Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involve at least one internal party.
- ***External Fraud:*** Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party

- ***Employment Practices and Work Place Safety:*** Losses arising from acts inconsistent with employment, health or safety laws or agreements from payment of personal injury claims, or from diversity/ discrimination events.
- ***Clients, Products and Business Practices:*** Losses 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.
- ***Damage to Physical Assets:*** Losses arising from loss or damage to physical assets from natural disasters or other events.
- ***Business Disruption and System Failures:*** Losses arising from disruption of business or system failures.
- ***Execution, Delivery and Process Management:*** Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.

Operational Risk Management Practices

Fundamental principles of operational risk management

Principle 1

The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.

Principle 2

Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

Governance

The Board of Directors

Principle 3

The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

Principle 4

The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

Senior Management

Principle 5

Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

Risk Management Environment

Identification and Assessment

Principle 6

Senior management should ensure the identification and assessment of the operational risk inherent in all material products/activities, processes and systems to make sure the inherent risks and incentives are well understood.

Principle 7

Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

Monitoring Reporting

Principles 8

Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

Control and Mitigation

Principle 9

Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

Business Resiliency and Continuity

Principle 10

Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Principle 11

A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

Operational Risk Management Practices should be based on a well laid out policy duly approved at the board level that describes the processes involved in controlling operational risks. It should meet the standards set in terms of the principles mentioned above. In addition, well laid down procedures in dealing with various products and activities should be in place. The policies and procedures should also be communicated across the organisation.

The policy should cover

- Operational risk management structure
- Role and responsibilities
- Operational risk management processes

- Operational risk assessment/measurement methodologies

Management Overview and Organisational Structure

- **Role of Board:** The board of directors takes overall responsibility to manage and implement the operational risk framework. It should approve bank's ORM framework and review it periodically. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.
- **Role of Operational Risk Management Committee:** The operational risk management committee should identify the operational risks to which the bank is exposed to, formulate policies and procedures for operational risk management, set clear guidelines on risk assessment/measurement and ensure adequacy of risk mitigating controls.
- **Role of Operational Risk Management Department:** The operational risk management department is the nodal department for identifying, managing and quantifying operational risks. ORMD, in conjunction with groups, lays down procedures for management of operational risks.
- **Role of Internal Audit/Business Functions:** Roles and responsibilities relating to internal audit business functions in the operational risk processes should be clearly defined. These should include comprehensive audit of the ORM framework so as to assess its effectiveness. The internal audit function should be operationally independent and should not be directly responsible for operational risk management.

Processes and Framework

The processes and framework include the following:

- Mapping of Processes and Identification of Risks/Control.
- The key business processes in the bank must be mapped into sub-processes. This should be a joint exercise between the operational risk group and the business groups.

- Implementation of a Qualitative Approach to Aggregating and Assessing Operational Risks.
- A system to qualitatively analyse the operational risk profile using a scorecard approach should be implemented. This would involve self-assessment by the business group and normalization/collation by the operational risk management department.
- Implementation of a Quantitative Approach to Assessing Operational Risks New Product Processes.

Risk Monitoring and Control Practices

Risk Monitoring and Control Practices encompasses the following:

- Collection of Operational Risk Data (incident reporting framework).
- Regular monitoring and feedback mechanism in place for monitoring any deterioration in the operational risk profile.
- Collation of incident reporting data to assess frequency and probability of occurrence of operational risk events.
- Monitoring and control of management of large exposures. The modalities to be prescribed in the Loan Policy document.

Information System Infrastructure: Information system infrastructure should be responsive to the ORM framework.

Operational Risk Quantification

This is by far the most difficult of all risk measurements. The behaviour pattern of operational risk does not follow the statistically normal distribution pattern and that makes it difficult to estimate the probability of an event resulting in losses. The historical loss distribution pattern, which may provide a method to estimate operating losses requires a data set that has statistically acceptable numbers of loss. Related data may be captured only over a period. Basel II has recognised the difficulties in measurement of operational losses. **Consequently, it has provided options in the measurement of operational risk for the purpose of capital allocation purposes. They are:**

- The Basic Indicator Approach (BIA)

- The Standardised Approach (TSA)
- Advanced Measurement Approaches (AMA)

Of these, the Basic Indicator and the Standardised Approaches are based on the income generated. The Advance Measurement Approach is based on operational loss measurement. A brief description of the Basel II prescriptions under these approaches is given below. For details, it is advised that Basel II document may be consulted.

The Basic Indicator Approach

- Banks using the Basic Indicator Approach must hold capital for operational risk equal to the average over the previous three years of a fixed percentage (15%) of positive annual gross income. 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. This 15% of average gross income is called as Alpha.

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 realised profits/losses from the sale of securities in the banking book; and
- Exclude extraordinary or irregular items as well as income derived from insurance.

To make it further simple, Gross Income of the bank can be arrived at using three formulae given below:

Formula No.1:

Gross Income = Net Profit + Provisions & Contingencies + Expenditure incurred under Schedule 16 – minus profit on HTM and irregular/ non-banking transactions income/ income non-banking transactions (such as insurance etc.).

Formula No. 2:

Gross Income = Operating Profit + Expenditure incurred under Schedule 16 – minus profit on HTM and irregular/ non-banking transactions income /income from non-banking transactions (such as insurance etc.)

Operating Profit = Net Profit + Provisions & Contingences.

Formula No.3:

Gross Income is defined as the net interest income plus non-interest income.

Non-Interest income excludes the profits/losses arising out of the following:

- HTM transactions.
- Income from Insurance business
- Any irregular/ non-banking transactions.

The Standardised Approach

In the Standardised Approach, banks' activities are divided into eight business lines:

- Corporate finance, trading and sales, retail banking, commercial banking, payment and settlement, agency services, asset management, and retail brokerage.
- 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 Factors).

Business Lines Beta Factors

- Corporate finance - 18%
- Trading and sales - 18%
- Retail banking - 12%
- Commercial banking - 15%
- Payment and settlement - 18%
- Agency services - 15%
- Asset management - 12%

- Retail brokerage - 12%

Advanced Measurement Approach (AMA)

- 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.

A Generic Measurement Approach

The first step in measurement approach is operation profiling. The steps involved OP Profiling are:

- Identification and quantification of operational risks in terms of its components.
- Prioritisation of operational risks and identification of risk concentrations - hot spots resulting in lower exposure.
- Formulation of bank's strategy for operational risk management and risk based audit.

Estimated level of operational risk depends on

- Estimated probability of occurrence
- Estimated potential financial impact
- Estimated impact of internal controls

Estimated Probability of Occurrence

This will be based on historical frequency of occurrence and estimated likelihood of future occurrence. Probability is mapped on a scale of 5 say where

- Implies negligible risk
- Implies low risk
- Implies medium risk
- Implies high risk
- Implies very high risk

Estimated Potential Financial Impact

- This will be based on severity of historical impact and estimated severity of impact from unforeseen events. Probability is mapped on a scale of 5 as mentioned above.

Estimated Impact of Internal Controls

- This will be based on historical effectiveness of internal controls and estimated impact of internal control on risks. This is estimated as fraction in relation to total control, which is valued at 100%.
- Estimated level of operational risk = Estimated probability of occurrence impact x Estimated potential financial x Estimated impact of internal controls

In case of a hypothetical example where

- Probability of occurrence = 2 (Medium)
- Potential financial impact = 4 (very high)
- Impact of internal controls = 50%
- Estimated level of operational risk = [(2 * 4* (1 - 0.50)] ^ 0.5 = 2.00 or 'Low'

Scenario Analysis

Basel II guidelines on scenario analysis are as follows.

- A bank must use scenario analysis based on 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.
- ***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.

The Necessity of Integrated Risk Management

Risk Management is a basic necessity for financial institutions of all sizes, and ultimately central to their success and survival. It integrates an organisation's internal and external business processes by applying standard risk terminology, metrics and reporting to facilitate optimal risk/return decisions. An integrated approach to risk management centralizes the process of supervising risk exposure so that the organisation can determine how best to absorb, limit or transfer risk.

When properly implemented, Integrated Risk Management:

- Aligns the strategic aspects of risk with day-to-day operational activities.
- Facilitates greater transparency for investors and regulators.
- Enhances revenue and earnings growth.
- Controls downside risk potential.

Integrated Risk Management: Approach

The Process of Integrated Risk Management Consists of

- Strategy
- Organisation
- Process
- System


CAIIB
NEW
SYLLABUS
Video Course
Mock Tests
Capsule PDFs
New Syllabus
JOIN NOW
Visit us for more information