Dr. Srinivasan
Palamalai
Pramoda Hegde

A FUNDAMENTAL STUDY OF RISK MANAGEMENT OF COMMERCIAL BANK

ALEXIS PRESS
JERSEY CITY, USA

A FUNDAMENTAL STUDY OF RISK MANAGEMENT OF COMMERCIAL BANK

A FUNDAMENTAL STUDY OF RISK MANAGEMENT OF COMMERCIAL BANK

Dr. Srinivasan Palamalai

Pramoda Hegde

ALEXIS PRESS

Published by: Alexis Press, LLC, Jersey City, USA
www.alexispress.us

First Published 2022

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication Data

Includes bibliographical references and index.

A Fundamental Study of Risk Management of Commercial Bank
by *Dr. Srinivasan Palamalai, Pramoda Hegde*
ISBN 978-1-64532-970-1

CONTENTS

CHAPTER 1

FOREIGN CURRENCY EXPOSURE MEASUREMENT

Dr. Srinivasan Palamalai
Associate Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id:srinivasanp@presidencyuniversity.in

ABSTRACT:

Foreign currency exposure measurement is a vital aspect of risk management for businesses and investors operating in an increasingly globalized economy. This practice involves quantifying the potential impact of fluctuations in exchange rates on the financial performance of an entity. Accurate measurement of foreign currency exposure is crucial for making informed decisions and developing appropriate hedging strategies to mitigate currency risks. This study provides an overview of foreign currency exposure measurement, highlighting its significance and the key methods employed in assessing exposure levels. It also discusses the challenges faced in accurately measuring foreign currency exposure and the potential implications of misjudging these risks. The measurement of foreign currency exposure entails identifying and analyzing various types of exposures, including transaction exposure, translation exposure, and economic exposure. Transaction exposure refers to the impact of exchange rate fluctuations on specific foreign currency transactions, while translation exposure relates to the translation of financial statements of foreign subsidiaries into the reporting currency. Economic exposure represents the broader impact of exchange rate fluctuations on a company's overall competitive position and future cash flows.To quantify foreign currency exposure, several quantitative techniques are commonly utilized, such as sensitivity analysis, value-at-risk (VaR) models, and cash flow mapping. Sensitivity analysis examines the potential impact of exchange rate movements on financial variables, while VaR models estimate the potential loss in the value of a portfolio due to adverse exchange rate movements. Cash flow mapping involves projecting future cash flows and analyzing their sensitivity to exchange rate fluctuations.

KEYWORDS:

Banks,Cash Flows, Economic, Foreign Currencies, Financial Markets, Value-At-Risk (Var).

INTRODUCTION

Banks trade in a variety of foreign currencies, but they also have stakes in a few key ones. Therefore, a system must be established to calculate the total amount of foreign exchange exposures, which includes all on- and off-balance-sheet foreign exchange assets and liabilities. The first stage in managing exchange risk is measuring foreign currency exposure since banks need to know how much exposure they have and what will happen if the value of their foreign currency assets changes when the exchange rate changes. There are three ways to be exposed to foreign currencies: via transactions, translations, and economic activity. The exposure starts when a foreign currency transaction is made, such as when money is sold or bought, when securities or shares are bought and sold in foreign currencies, when foreign trade bills are discounted, when a foreign currency loan is made, or when a deferred payment guarantee is issued in a foreign currency. From the time the transaction is booked until the time the obligation

under the transaction is actually completed, the exposure is active. Banks are vulnerable to asset value degradation due to unfavorable changes in exchange rates during the transaction[1]–[3].

By holding stock, assets, and obligations in foreign currencies and receiving revenue from these goods from overseas, banks are exposed in a second manner. The vulnerability occurs when local cash is changed into foreign currency and sent abroad to satisfy the capital and commercial needs of overseas affiliates and branch offices. The assets and liabilities of the bank's overseas branches and related companies are converted into local currency at the prevailing rate for inclusion in the consolidated balance sheet, which introduces the exchange risk. Translation exposure is the name given to this kind of exposure. If the governing exchange rate was unfavorable in comparison to the rates in effect on the dates when the relevant transactions were recorded, the bank will have to record a loss from the conversion of foreign assets and liabilities into local currency. The third sort of exposure is referred to as economic exposure, and it affects a bank's potential earnings and cash flows as a consequence of changing the exchange rate parity. A bank's competitive position in the financial markets, the amount of business it does, and its profitability might all be impacted by the exchange rate adjustment.

Banks must come up with a mechanism that takes into account both the value of the exposure in a single currency and the value of the entire exposure to long and short positions across all foreign currencies in order to calculate the total exposure that is exposed to exchange risk. A minimum capital requirement has been established by the New Basel Capital Accord to address the risk associated with owning or taking positions in foreign currencies, including gold. The Accord suggests two methods for determining the capital cover for currency risk. "The first is to calculate the exposure in a position using only one currency. Measurement of the risk associated with a bank's mix of long and short positions in various currencies is the second step. Banks compute the net position in each currency to determine exposure in a single currency. The guarantees that are certain to be called and likely to be irrecoverable, together with a few other factors, make up the net position in a single currency. It also includes the net spot position and the net forward position.

Banks have an option between two different methodologies for calculating foreign exchange risk in a portfolio of foreign currency assets and gold, depending on the preferences of the national regulator or supervisor. The first is a quick strategy that doesn't distinguish between various currencies, and the second is the use of internal models that take into account the real level of risk present in the foreign currency portfolio. It is convenient for banks to use the shorthand method for measuring their foreign exchange exposure. For measurement of exposure under the shorthand method, the nominal amount of the net position in each currency and in gold is converted into the reporting currency at spot rates, and the overall net position. The latter must be assessed on a consolidated basis and should take into account both bank affiliates' and branch offices' international exposures. Numerous banks have significant domestic operations, but just a few international branch offices, or maybe only one or two minor linked businesses abroad. A bank may use a streamlined approach if it has a limited number of operations in foreign countries and it becomes technically challenging to identify and quantify all foreign currency risks. The bank may add the restrictions, regardless of the sign, to the net open position in each currency of the New Basel Capital Accord by using the internal limits on each currency as a proxy.

DISCUSSION

Quantification of Exchange Risk

The loss on foreign currency exposures that may result from unfavorable changes in exchange rates may be measured by banks using the VaR approach. Under typical market circumstances, over a predetermined holding time, and with a predetermined degree of confidence, the potential loss may be assessed. The greatest loss that might happen on foreign currency exposures or portfolios under typical market circumstances, taking into account the historical history of exchange rate movements, is what VaR assesses, not the worst potential loss. The total of the following is the foreign exchange portfolio's VaR:

1. VaR on available spots for the night.
2. VaR on foreign exchange disparities for future time periods. The following inputs are necessary to calculate VaR:

1. Volatility or standard deviation of the exchange rate during the previous one to two years.
2. Holding time period description.
3. Level of confidence specifications.

Banks may use past data on exchange rate fluctuations to compute VaR. They might gather information on the changes in exchange rates between two currencies over the course of the previous trade year, or around 250 trading days, and use the results they derive to determine the standard deviation. Banks may make the simple assumption that the value distribution is normally distributed. Let's calculate VaR on an open position of $100 million in US dollars for a 10-day holding period at a 95% confidence level, assuming that the yearly volatility of the USD/SGD exchange rate is 5% and that the USD/SGD exchange rate is stable. the value of a dollar is:

Understanding how key financial markets work globally, evaluating the likelihood that interest rates will move in those markets, and monitoring the daily movement of major currency exchange rates are the main tasks involved in managing foreign exchange risk. Banks should examine previous foreign exchange flow patterns and determine the causes of any deviations. Additionally, they should track and evaluate the intraday fluctuations in exchange rates between major currencies and the currencies in which they hold overnight holdings, displaying the day's high and low positions as well as the moves in key currency rates going ahead. A bank should determine the causes and the expected trajectory for the near future if the foreign currencies it maintains open positions in have gained or depreciated in reference to the domestic currency. Banks should identify the causes and determine how long the instability is likely to last if the supply and demand of significant currencies have changed beyond what is typically anticipated and the demand supply equation has affected the exchange rate. Important variables that direct treasury officials to profit from foreign currency operations include the findings drawn from economic analysis, exchange rate movement analysis, and an evaluation of the trend that is expected to prevail in the foreign exchange market[4]–[6].

Setting suitable exchange risk-related limitations and hedging risks for risk reduction are two complimentary tasks that must be implemented simultaneously as part of foreign currency management. The open position in spot and forward transactions, a maturity mismatch of foreign currency assets and liabilities, or a principal amount mismatch within the same maturity bucket are the three main causes of exchange risk. Spot position risk and forward position risk are the

main dangers. Due to the fluctuation in exchange rates throughout the day, open positions in spot foreign exchange transactions expose a bank to spot position risk, and open positions in forward foreign exchange transactions expose it to forward position risk due to potential adverse changes in interest rates and exchange rates during that time. By establishing suitable limitations, banks are able to manage these risks. The following sentences go above these restrictions.

Limits on Position

Both intraday and overnight position limitations should be established by banks. To ensure that the entire exposure stays under the predetermined limit, they should establish currency-specific intraday open position limitations, also known as daylight limits, as well as an overall daylight limit on intraday exposures in all foreign currencies combined. They should also establish overnight open position restrictions for each currency separately and for all currencies together. Maintaining an overnight position is a speculative activity, and aggressive bank treasury dealers often hold large overnight positions with the intention of generating significant profits quickly. The bank will suffer a sizable loss if the exchange rate is unfavorable the next day. Bank regulators and supervisors often set spot open position and overnight open position restrictions in terms of a percentage of Tier I regulatory capital in an effort to prevent speculatively accumulating foreign currency exposures. The difference between the daylight and nighttime limits is not defined, although generally speaking, the daytime limit is maintained higher than the nightly limit. Two factors serve as the basis for setting a greater daylight restriction. First, if unanticipated swings in the currency rate are recognized, corrective action may be performed right away as long as the market is open. As an opposing transaction may be scheduled to close out the open position before the market closes, a bigger daylight limit allows the bank to satisfy customer demands for large transactions throughout the day, sometimes even above the permitted limit. A position that is open overnight has a higher risk since it is impossible to accurately predict potential changes in the various financial markets that might cause overnight volatility in exchange rates.

Limit on Deal Size

To ensure that foreign currency transaction sizes remain within reasonable bounds, banks should set individual deal size restrictions. The deal size limit will be applied to all exposure types, including placements of foreign currency funds with local or international counterparties on an overnight or term basis as well as transactions in derivative instruments such currency swaps, currency options, and currency futures.

Gap Maximum

Banks should establish distinct gap limitations for each foreign currency and each maturity bucket, including spot and forward, as well as for all maturity buckets combined. Additionally, they should provide the aggregate gap limit for all currencies and maturity buckets combined, which is the total of the aggregate gap limitations for each currency separately. The discrepancy highlights any cash flow inconsistencies between the assets and liabilities at certain junctures. The gap analysis aids in identifying particular cash flow inconsistencies that must be fixed to lessen susceptibility to changes in exchange rates and interest rates. Banks should take into account the severity of recent interest rate and exchange rate swings when determining maturity-based limitations. Higher restrictions may be set for longer maturities if the market environment is generally favorable. Banks should routinely switch assets and liabilities across maturities in

response to the shifting market outlook for improved exchange risk management. Three different types of risk are present due to the maturity differences between foreign currency assets and liabilities:

Liquidity danger. Exchange-related risk. Rate-Risk Exposure

The bank is exposed to liquidity risk because open positions must be filled at the current market rate, which may be unfavorable, on the date that assets and liabilities are redeemed if the amount of maturing liabilities exceeds the amount of maturing assets in a given time bucket. Similar to gaps, interest rate risk is caused by them when assets and liabilities have different repricing dates. The maturing assets may need to be reinvested at a lower interest rate, while the maturing obligations may need to be renewed or newly acquired at a greater cost. Therefore, to minimize unnecessary risks, banks should maintain the gaps within normal bounds.

When managing foreign currency, it's important to regularly examine maturity gaps and consider how potential changes in spot and forward exchange rates can affect a bank's capital and earnings. This is comparable to doing an examination of the sensitivity to exchange rates. Banks should create a consolidated statement of maturity gaps for all time buckets with open positions, taking into account off-balance-sheet items, in order to detect gaps in foreign currency assets and liabilities. The bank is in a liability-sensitive position in the relevant time buckets if residual gaps, or the differences between the total of on-balance-sheet and off-balance-sheet foreign currency assets and liabilities, are negative. This implies that the amount of liabilities coming due for redemption or repricing in the relevant time buckets is greater than the amount of assets. The bank is in an asset-sensitive position in the relevant time buckets if the residual gaps are positive. The bank's earnings will be impacted by a negative change in exchange rates and interest rates on obligations and assets held in foreign currencies. Therefore, banks should analyze open position gaps under various exchange rate scenarios and determine how they may affect revenues. They may do the gap analysis based on the abridged assumptions listed below:

1. All assets and liabilities that are being repriced experience the same exchange rate changes.
2. The repricing period is determined by taking the midpoint of each bucket.
3. Liabilities and assets that have been repriced are still present on the balance sheet.
4. Impact analysis includes income from repriced assets and costs from repriced liabilities at revised rates for the relevant remainder periods.

Stop-Loss Capacity

Banks are required to set a stop-loss limit for their foreign currency trading positions. When a trading position is marked to market for value, the loss that results is referred to as a stop-loss limit. It aims to limit any loss that could result from a currency trading position at a certain moment due to a negative change in the exchange rate. The bank's dealer must cancel or square up the trading position whenever the specified stop-loss limit is reached in order to keep the loss to a predetermined sum. The stop-loss limits are often determined based on the mark lot of the position and are specified in terms of the maximum loss stated in local currency or the length of time for which a designated asset may be kept while its value is dropping[7]–[9].

VaR Ceiling

For controlling risks connected to foreign exchange, banks set a VaR limit that is applicable to the foreign exchange portfolio. The greatest loss that might result from the foreign exchange portfolio owing to unfavorable changes in exchange rates under prevailing market circumstances is measured by VaR. VaR is estimated for exposures involving foreign currency based on both overnight open positions and forward gaps. The limit for the prescription of the VaR limit is determined by the amount of capital put aside to address risk from exposures connected to foreign currency. The holding time and confidence level for the computation of VaR on foreign exchange-related risks should be specified by the banks as well. In order to reduce risk, banks must reevaluate their position, identify any gaps, and scan their whole portfolio when VaR is getting close to the permitted level.

Max. Tolerance

Treasury staff must record foreign currency transactions at current market rates to maintain internal control rigor. Dealers often cannot complete transactions for the appropriate amount or the desired duration at market-related prices because of market flaws, market shallowness, or a unidirectional trend among market participants. Giving the dealers some latitude to conclude foreign currency agreements at rates that may be somewhat lower or higher than the prevailing market rate is required for the business of the bank to run smoothly. Banks could let dealers to register transactions involving foreign currency at tiny margins different from market rates. To avoid the abuse of discretionary authority, they should establish clear and open norms and set tolerance limits for dealers making exceptions.There are several techniques available for hedging various types of foreign currency risk. There are several different derivative products available for hedging, including forward contracts, currency swaps, currency options, and currency futures. The forward contract, which is often used by banks to manage exchange risk, carries the risk of counterparty failure, which might result in a high replacement cost. When there are few participants in the forward exchange contract market, it might be challenging for banks to enter the market and book the transaction with solid counterparties at the targeted rate. Currency futures may be used as a substitute to forward contracts when they are not offered. Exchange-traded futures reduce or completely remove default risk. However, futures are offered in conventional formats, which could not fully satisfy the bank's criteria in terms of quantity or duration. Nevertheless, since they may cancel their commitments before the contract's settlement date, banks have more flexibility with currency futures.

Another tool for reducing foreign exchange risk is a currency option. A contract for the future delivery of a currency in exchange for another currency at the agreed-upon price is known as a currency option. Option purchasers compensate option sellers with a premium in exchange for the right to purchase the specified quantity of currency at the strike price at a later date. Although the seller is obligated to supply the currency at the agreed-upon price if the buyer exercises its option to buy, the buyer is not automatically required to purchase the currency. Options may be useful in certain situations since future exchange rate changes cannot be forecast with complete confidence. But options are very intricate devices that are hard to value. Contrarily, futures and forwards are more simpler products that are used by banks the most for risk hedging. Borrowing domestic currency in the money market and depositing the borrowed amount in a foreign currency deposit or investing in foreign currency assets or instruments that pay interest, taking advantage of the difference in interest rates between the two currencies, are two additional ways

to reduce the risk associated with future foreign currency commitments. This method, which serves as a replacement for forward contracts, is advantageous only if the interest earned on the foreign currency asset exceeds the interest paid on domestic currency borrowing after taking into account any potential value loss brought on by fluctuations in the exchange rate during the interim period. Banks should be aware that forward contracts entail replacement risk and investing in foreign currency instruments has default risk. They should consider the advantages and disadvantages of each kind of hedging mechanism before choosing the right combination of hedging instruments to reduce costs and other risks.

Even though these assessment methods are readily available, it might be difficult to determine your exposure to foreign currencies. The complexity and volatility of currency markets, as well as the built-in constraints of measurement methods, are the causes of these difficulties. Exchange rates may be considerably impacted by factors including geopolitical events, macroeconomic circumstances, and market emotion, making it challenging to precisely estimate and assess risk. For companies and investors, estimating foreign currency exposure incorrectly may have serious repercussions. It may result in unforeseen financial losses, decreased global market competitiveness, and greater susceptibility to economic shocks. The development of suitable hedging strategies and successful risk management thus depend on the precise assessment of foreign currency exposure[10]–[12].

CONCLUSION

To sum up, in the current global economy, measuring foreign currency exposure is essential for managing currency risks. For companies and investors to make wise choices and successfully reduce currency risks, it is crucial that they have a thorough understanding of the different kinds of exposures and use the right measuring methodologies. However, the difficulties in quantifying foreign currency exposure precisely underline the need of constant monitoring, flexibility, and effective risk management procedures in the face of volatile currency markets.

Foreign exchange risk is the possibility of probable loss brought on by a change in the exchange rate that is unfavorable for exposures held in foreign currencies. The risk of possible loss from foreign exchange business increases with the amount of exposure to foreign currencies and with exchange rate volatility. Position risk, gap risk, default risk, country risk, and control risk from activities in foreign countries are risks that banks are subject to. Due to the intricacy of the laws and regulations regulating foreign currency transactions, they are also vulnerable to legal danger. Transaction exposure, translation exposure, and economic exposure are all ways that you might get exposed to foreign currencies. The proper procedures for measuring exposure in a single currency as well as the total exposure from long and short positions across all foreign currencies should be established by banks. Using the value-at-risk technique, exchange risk on the foreign exchange portfolio may be calculated based on the historical volatility of currency rates and for certain confidence levels. Value-at-Risk is the largest possible loss that might result from a negative change in the exchange rate under normal market circumstances on the foreign exchange portfolio. Establishing suitable exchange risk-related limitations and implementing hedging methods are also part of exchange risk management. Daylight limitations, overnight open position restrictions, individual deal size limits, gap limits, stop-loss limits, and value-at-risk limits make up the framework of limits. For hedging exchange risk, banks may pick from a variety of derivative products, including forward contracts, currency swaps, currency options,

and currency futures. They should provide clear rules to allow dealing representatives to choose the proper set of hedging products in light of various circumstances.

REFERENCES

[1] A. A. Wahab, R. Abdul-Rahim, and H. Janor, "Impact of foreign exchange exposure and shariah-compliant status on Malaysian firms' hedging practice," *J. Pengur.*, 2020, doi: 10.17576/pengurusan-2020-58-05.

[2] S. S. Kim, J. Chung, J. H. Hwang, and J. H. Pyun, "The effectiveness of foreign debt in hedging exchange rate exposure: Multinational enterprises vs. exporting firms," *Pacific Basin Financ. J.*, 2020, doi: 10.1016/j.pacfin.2020.101455.

[3] A. A. Wahab, R. A. Rahim, and H. Janor, "Role of foreign exchange exposure in determining hedging practises in Malaysia," *Int. J. Econ. Manag.*, 2019.

[4] A. A. Wahab, R. Abdul-Rahim, and H. Janor, "Impact of foreign exchange exposure and shariah-compliant status on Malaysian firms' hedging practice [Kesan pendedahan matawang asing dan status patuh shariah terhadap amalan lindung nilai syarikat Malaysia]," *J. Pengur.*, 2020.

[5] A. Soelehan, A. M. Marpaung, and S. Dewi K., "Antisipasi Rencana Pembayaran Hutang Dagang Melalui Pengukuran Translation Exposure dengan Metode Current Rate dan Penggunaan Forward Contract Hedging," *J. Ilm. Manaj. Kesatuan*, 2013, doi: 10.37641/jimkes.v1i2.261.

[6] L. Isaac, "Assessing the Impact of Exchange Rate Risk on Banks Performance in Nigeria," *ISSN*, 2015.

[7] R. G. Rambo, D. Main, and L. Beaubien, "Reducing reporting risk: Designating foreign currency forward contracts as cash flow hedges," *J. Account. Educ.*, 2011, doi: 10.1016/j.jaccedu.2012.03.003.

[8] M. Díaz, J. Delgado Vaquero, M. Diaz, and D. Vaquero, "Foreign currency risk management practices in Spanish companies: An empirical analysis, AESTIMATIO," *IEB Int. J. Financ.*, 2017.

[9] N. F. F. M. Azhar and H. A. Wahab, "Assessing multiscale exchange rate exposure of electronic and electrical firms in malaysia: An application of wavelet analysis," *Journal of Critical Reviews*. 2020. doi: 10.31838/jcr.07.16.57.

[10] N. Apergis, P. Artikis, and J. Sorros, "Asset pricing and foreign exchange risk," *Res. Int. Bus. Financ.*, 2011, doi: 10.1016/j.ribaf.2011.02.005.

[11] R. Rupeika-Apoga, "Nowadays Approach to Foreign Exchange Risk Management," *Organ. Vadyb. Sist. Tyrim.*, 2005.

[12] T. S. Harris and S. Rajgopal, "Foreign Currency: Accounting, Communication and Management of Risks," *SSRN Electron. J.*, 2017, doi: 10.2139/ssrn.3031831.

CHAPTER 2

EQUITY EXPOSURE RISK MANAGEMENT

Dr. Ranganathan Kumar
Associate Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id:drsenthilkumar@presidencyuniversity.in

ABSTRACT:

Equity exposure risk management is a crucial aspect of financial planning and investment strategy in the realm of equity markets. It involves assessing and mitigating the potential risks associated with owning equity securities, such as stocks, shares, and equity derivatives. Effectively managing equity exposure risk is essential for investors, fund managers, and financial institutions to protect capital, optimize returns, and achieve long-term investment objectives. This study provides an overview of equity exposure risk management, emphasizing its significance and the key strategies employed to measure, monitor, and mitigate equity-related risks. It also discusses the challenges faced in managing equity exposure risk and the potential implications of inadequate risk management practices. Equity exposure risk management encompasses the identification, measurement, and monitoring of various sources of risk inherent in equity investments. These risks include market risk, which arises from fluctuations in stock prices and overall market conditions, as well as systematic and unsystematic risks associated with specific industries, sectors, or individual companies.

KEYWORDS:

Banks,Capital Markets, Exposure Risk, Equity Exposure, Risk Management.

INTRODUCTION

To manage equity exposure risk, several strategies and techniques are commonly employed. These include diversification, asset allocation, hedging, and active portfolio management. Diversification involves spreading investments across different asset classes, regions, and sectors to reduce the impact of adverse events on a portfolio's overall performance. Asset allocation determines the optimal mix of equity and other asset classes based on risk tolerance, investment objectives, and market conditions. Hedging strategies, such as options, futures, and derivatives, can be used to mitigate downside risk and protect against adverse price movements. Active portfolio management involves ongoing analysis, research, and decision-making to optimize risk-adjusted returns and respond to market dynamics.

Exposure to Equity Identification

Due to the daily fluctuations in stock values, which have the potential to cause substantial losses in a short amount of time, a bank's exposure to equities is a portfolio with a high risk. Banks often invest big sums in shares to generate rapid profits due to the high return nature of equity exposure, disregarding the substantial risk inherent with it. Bank authorities sometimes regulate the overall equity exposure of commercial banks and prohibit them from shorting stocks in order to avoid excessive speculation or the loss of considerable capital under unstable conditions. Since their duty is not to disrupt the market by excessively speculative trading in shares with the

aid of public money, they anticipate banks to exercise caution while taking exposure in the capital market.

For assessing any kind of direct or indirect risk, equity exposure must be defined properly. Equity exposure often refers to direct investment in company stocks, but it should also include all equity-related products to stop banks from using public funds for speculative trading via indirect channels. In addition, falling equity prices raise the likelihood that customers who trade in stocks or who have borrowed money to buy stocks may default, increasing the credit risk for the banks from such clients. Due to the high risk of suffering significant losses, equity exposure should include all lending and financial obligations made by banks to all kinds of customers in which the money dispensed eventually ends up on the capital market, either directly or indirectly. But unless the money is used to buy shares or securities on the capital market, it shouldn't include loans and overdrafts made to customers as security for company equity[1]–[3].

Both money provided to customers for investments in equity-related securities and the bank's own investments made in a proprietary capacity should be included when calculating equity exposure. The second class of investments is often not taken into account when determining how sensitively the bank is exposed to capital markets, but it is important to understand the potentially unstable effects of a significant amount of bank money being channeled via customers to capital markets. It is the duty of bank regulators and supervisors to stop commercial banks from using aggressive speculative trading to jeopardize the stability of the capital market. To help the authorities advance the stability of the financial system, banks should defend the interests of medium- and long-term investors, in particular small investors. As a result, the following components should at the very least be included in banks' exposure to equity:

1. Investments made by banks themselves in equity-oriented mutual funds, convertible debentures, and individual stock.
2. Loans to the general public to participate in corporate equity first public offerings.
3. Loans to clients for stock buying.
4. Loans to businesses to cover the promoters' equity issuance contributions.
5. Loans to market makers and stock brokers.
6. Making assurances on stock brokers' behalf.

Framework for Equity Exposure Management

When taking on equity exposures, banks should adhere to a number of core principles and put in place a robust structure to manage the risk. The framework ought to contain:

1. A suitable explanation of equity exposure.
2. Strategies and policies for handling high-risk equities exposures.
3. A clear investing strategy for stocks.
4. Delegation of responsibility for equity investment choices.
5. The voluntary imposition of a limit on overall capital market exposure.
6. Setting restrictions to prevent stock investment concentration in a single company or business group, including exposures in other forms.
7. The imposition of financial limits on exposures to certain people, stock brokers, and market makers.
8. A system for preventing conflicts of interest while managing the investment portfolio.
9. Insider trading scrutiny.

10. Providing the investment management team with analytical help via stock research.
11. Development of techniques for calculating the risk of equity exposure.
12. Monitoring by the administration to stop abuses and exceptions.
13. A system of independent oversight and management.

Measurement of Equity Exposure Risk

Banks should put up the proper procedures for monitoring stock exposure risk while taking the exposure's magnitude and the equity portfolio's makeup into consideration. In order to gauge the portfolio's value degradation, they should take into account changes in daily share prices and perform mark-to-market valuation on the holdings. If the bank's equity exposure is comparatively large, it should conduct sector- and industry-specific risk analyses. Industry research will provide early warning signs of industry slowdowns, stagnation, or sluggish growth. The findings of the research may be used to help investors leave stocks whose prices are anticipated to fall at the right moment. By using the VaR approach, like in the example shown below, one may estimate the amount of potential loss that might result from a stock portfolio. Let's say a bank has 1 million shares of a company that it bought for $10 each. Let's say that the annualized standard deviation of the movement in share price is 20%. What will the VaR on the stock exposure be at a 95% confidence level during a one-month holding period? VaR is determined as follows: Since possible loss, not prospective gain, is what we are concerned with in risk management, we disregard the circumstance when the share price rises. Based on the volatility rate at the specified confidence level, we are worried about the expected decline in share price.

Another method of calculation is possible

Equities from several firms make up the stock portfolios of banks; as a result, information on each equity's volatility is necessary in order to calculate VaR for the whole equity portfolio. Therefore, they should continue to maintain a suitable management information system that records daily stock price data as well as changes in share prices quoted on local and international capital markets. To get the overall VaR of the equity portfolio, they should compute VaR for each equity exposure and then add the results. Banks may evaluate the risk in terms of the movement in representative share price indices if there are many stocks and price volatilities of many shares are not accessible. If share prices are not listed on the stock market, they should examine the issuing firms' financial standing and determine their realizable values. To keep risks within acceptable bounds, they should set the VaR limit on the overall exposure, evaluate the possible loss from equity and equity-related instruments via the application of the VaR approach on a regular basis, and respond appropriately when the limit is exceeded.

DISCUSSION

Although risk management solutions for stock exposure provide useful tools for reducing risks, managing equity exposure effectively still presents difficulties. These difficulties are caused by things like market volatility, shifting investor mood, changing regulations, and unanticipated occurrences that may affect stock markets. Furthermore, it may be difficult and prone to inherent uncertainty to identify and quantify risks related to specific stocks or industries. Investors and financial institutions may suffer major repercussions from inadequate management of stock exposure risk. It may lead to significant financial losses, a decline in investor confidence, and the inability to achieve investment goals. Therefore, to traverse the volatile nature of stock markets

and achieve desired investment results, a thorough and proactive strategy to equity exposure risk management is crucial[4]–[6].

Management of stock exposure risk is a crucial discipline in the world of equity investing. For investors and financial institutions looking to successfully manage stock exposure risk, having a thorough understanding of the many sources of risk, putting suitable strategies into practice, and regularly monitoring and responding to market circumstances are essential. While obstacles still exist, proactive risk management techniques may aid in maximizing returns, safeguarding money, and coordinating investment portfolios with long-term objectives. The assessment, monitoring, and mitigation of possible risks related to equity investments are done via the use of a comprehensive framework and a set of procedures called "equity exposure risk management." It entails comprehending the numerous risk factors that affect stock markets, putting controls in place to restrict exposure, and optimizing investment portfolios to meet desired risk-return goals.

The amount of money invested in equities assets, such as stocks, shares, and equity derivatives, is referred to as equity exposure. Equities have the potential to provide high profits, but they also come with a number of inherent risks related to market volatility, the state of the economy, business-specific issues, and company-specific occurrences. To protect capital, reduce losses, and increase returns on equity investments, effective risk management methods are essential. The first step in managing stock exposure risk is to identify and analyze the various risks that might affect equity investments. Market risk and particular risk are two major categories that apply to these dangers. Market risk develops as a result of general market circumstances as well as elements that have an impact on stock prices, such as macroeconomic trends, interest rates, geopolitical developments, and investor attitude. Operational risks, financial risks, regulatory risks, and competitive risks are examples of specific hazards that are specific to certain businesses, markets, or industries.

After the risks have been identified, approaches for measuring risk are used to calculate the possible effect on investment portfolios. These methods include of value-at-risk (VaR) models, scenario analysis, stress testing, and statistical models. To calculate the likelihood of certain occurrences and their effects on stock portfolios, statistical models examine historical data. Construction of fictitious scenarios and evaluation of their influence on portfolio performance include scenario analysis. Through stress testing, the portfolio's resistance to volatile market circumstances is evaluated. VaR models calculate the highest possible loss over a certain time horizon with a particular degree of confidence.

A variety of risk management techniques and technologies may be used to reduce the risks associated with equity exposure. To lessen concentration risk, one important method is diversification, which entails distributing assets across several asset classes, geographical areas, industry sectors, and market capitalizations. Investors might possibly offset losses from underperforming equities with profits from other assets by diversifying their portfolios. Another crucial approach is asset allocation, which chooses the best combination of stocks and other asset classes depending on risk tolerance, investing goals, and market circumstances[7]–[9].

The risk of stock exposure is often managed through hedging measures. They include employing derivative instruments, such as options and futures contracts, to protect against unfavorable price fluctuations, or adopting opposing positions. Hedging may be used to safeguard portfolio profits, reduce downside risk, and hedge against certain market or sector hazards. Another important component of managing stock exposure risk is active portfolio management. Continuous market

circumstances, economic developments, and company-specific elements are monitored under this strategy. Investment managers may react to changes in risk profiles, make timely adjustments, and take advantage of market opportunities by actively managing the portfolio. The dynamic nature of equities markets and the associated uncertainties provide difficulties in managing equity exposure risk. Rapid changes in market circumstances make it difficult to foresee and evaluate risks with accuracy. In addition, unanticipated occurrences like natural catastrophes, political unrest, or unexpected financial shocks may have a big effect on stock markets and investment portfolios[10], [11].

CONCLUSION

Due to daily swings in share prices, which have a great potential to cause significant financial loss, banks' exposure to equities is extremely risk-sensitive. Equity price volatility increases credit risk by causing defaults from customers who trade in shares or who have taken out loans to buy equities. Assessing direct and indirect risks from stock-related products requires a thorough characterization of equity exposure. Since it is undesirable for banks to participate in speculative trading with public funds, either directly or indirectly, the definition of equity exposure should be wide. The bank's own investment made in its official role should be considered an element of its equity exposure, as should money provided to customers for investments in equities and equity-related securities. To calculate the potential loss on their equity portfolio, banks should use the value-at-risk method. They should also set a value-at-risk limit and implement adequate checks and controls to prevent speculative trading in equities and the loss of significant capital in the face of volatile capital market conditions.

REFERENCES

[1] S. S. Mohanty, O. Mohanty, and M. Ivanof, “Alpha enhancement in global equity markets with ESG overlay on factor-based investment strategies,” *Risk Manag.*, 2021, doi: 10.1057/s41283-021-00075-6.

[2] A. Andermann *et al.*, “Evidence-informed interventions and best practices for supporting women experiencing or at risk of homelessness: A scoping review with gender and equity analysis,” *Heal. Promot. Chronic Dis. Prev. Canada*, 2021, doi: 10.24095/hpcdp.41.1.01.

[3] D. Bongaerts, X. Kang, and M. van Dijk, “Conditional Volatility Targeting,” *Financ. Anal. J.*, 2020, doi: 10.1080/0015198X.2020.1790853.

[4] M. Fang, K. S. Tan, and T. S. Wirjanto, “Sustainable portfolio management under climate change,” *J. Sustain. Financ. Invest.*, 2019, doi: 10.1080/20430795.2018.1522583.

[5] J. Boudoukh, M. Richardson, A. Thapar, and F. Wang, “Optimal Currency Hedging for International Equity Portfolios,” *Financ. Anal. J.*, 2019, doi: 10.1080/0015198X.2019.1628556.

[6] S. Mobini, P. Becker, R. Larsson, and R. Berndtsson, “Systemic inequity in urban flood exposure and damage compensation,” *Water (Switzerland)*, 2020, doi: 10.3390/w12113152.

[7] A. Pichler, S. Poledna, and S. Thurner, “Systemic risk-efficient asset allocations: Minimization of systemic risk as a network optimization problem,” *J. Financ. Stab.*, 2021, doi: 10.1016/j.jfs.2020.100809.

[8] F. Li, J. Liu, Z. Chen, J. Huang, C. Liu, and Z. Qu, "Navigating to urban environmental health: Professionalized and personalized healthy living assistant based on intelligent health risk management," *Urban Clim.*, 2021, doi: 10.1016/j.uclim.2021.101020.

[9] A. Abdullah, R. Hassan, and S. Kassim, "A real asset management approach for Islamic investment in containerships," *J. Islam. Account. Bus. Res.*, 2020, doi: 10.1108/JIABR-07-2017-0105.

[10] K. L. Benson and R. W. Faff, "The relationship between exchange rate exposure, currency risk management and performance of international equity funds," *Pacific Basin Financ. J.*, 2004, doi: 10.1016/j.pacfin.2003.10.001.

[11] W. Solecki, R. Leichenko, and K. O'Brien, "Climate change adaptation strategies and disaster risk reduction in cities: Connections, contentions, and synergies," *Current Opinion in Environmental Sustainability*. 2011. doi: 10.1016/j.cosust.2011.03.001.

CHAPTER 3

ASSET LIABILITY MANAGEMENT REVIEW PROCESS

Dr. Muralidhar Sunil
Assistant Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id:sunilrashinkar@presidencyuniversity.in

ABSTRACT:

The asset liability management (ALM) review process is a crucial component of financial institutions' risk management framework, aimed at effectively managing the risks associated with asset and liability mismatches. ALM encompasses the strategies, policies, and procedures employed to ensure the alignment of a company's assets and liabilities in terms of their maturity, interest rate sensitivity, and liquidity characteristics. The ALM review process involves evaluating and assessing the institution's balance sheet, identifying potential gaps and vulnerabilities, and implementing appropriate measures to mitigate risks and optimize financial performance. This study provides an overview of the asset liability management review process, highlighting its significance and the key steps involved in conducting a comprehensive review. It also discusses the challenges faced in managing asset and liability risks and the potential implications of inadequate ALM practices.The asset liability management review process begins with a thorough assessment of the institution's balance sheet, including the composition and characteristics of its assets and liabilities. This involves analyzing the maturity profile, interest rate sensitivity, liquidity position, and cash flow dynamics of each component. By examining these factors, financial institutions can identify potential gaps, vulnerabilities, and potential mismatches that could expose the institution to risks such as interest rate risk, liquidity risk, and funding risk. Once the balance sheet analysis is complete, the ALM review process involves stress testing and scenario analysis to assess the impact of adverse events on the institution's financial position. Stress testing involves subjecting the balance sheet to hypothetical scenarios that simulate extreme market conditions, economic downturns, or liquidity shocks. This analysis helps identify potential weaknesses and vulnerabilities in the institution's asset-liability structure, enabling proactive risk management and contingency planning.

KEYWORDS:

Asset Liability Management (ALM), Bank, Management,Mitigation, Vulnerabilities.

INTRODUCTION

Review of Asset-Liability

Banks are exposed to numerous types of market risk due to the mismatch in the maturities and durations of their assets and liabilities. To effectively monitor and manage the rising risks, they should conduct routine evaluations of asset-liability items using an asset liability management system. The authority that examines the altering makeup of market risk-related asset-liability items, judges the severity of newly emerging risk factors, and takes remedial action is the Asset Liability Management Committee. The examination and risk analysis of the asset-liability maturity gaps under the various maturity buckets that emerge throughout a bank's business

operations serve as the first steps in the ALM review process. The weekly structural liquidity statements and monthly monthly dynamic short-term liquidity statements are used to determine maturity gaps. The bank's present gaps between its assets and liabilities in the designated maturity buckets are shown in the structural liquidity statements, and a study of those gaps indicates how sensitive the bank is to liquidity risk, interest rate risk, and foreign currency risk. The bank is guided by the findings to recognize the threats that may result from shifting market risk variables and develop plans to properly respond to new situations[1]–[3].

Two things determine how well the ALM review process works. First, all elements of on-balance-sheet and off-balance-sheet asset-liability items must be included in maturity gap statements, and they must be correct. Second, in order to accurately identify new issues that pose a danger to a bank's operations, maturity gap statements must be thoroughly and meaningfully examined. In addition to gap analysis, the ALM review process should highlight the current positions of major assets and liabilities and their ratios in comparison to the established standards. If the ALM support group submits analytical findings in a structured style after carefully examining the asset-liability statements, the ALM review process will be efficient and useful. Here, a model for delivering the ALM review report is proposed. The review report should highlight the situation with regard to compliance with the established standards and restrictions on market risks, identify the worries arising from changes in market risk variables, and explore the choices accessible to react to changing market risk scenarios.

Review of Liquidity Risk

The report on the liquidity risk should be divided into two sections: the first section should deal with the quantitative parameters that disclose the liquidity position as of the review date, and the second section should deal with the situation arising from asset-liability maturity mismatches and duration mismatches. Descriptions of the numerous alternatives for corrective action should be included in the report.

The second section of the report format

The report should describe the liquidity pressure that the bank could experience in various scenarios, go through the current state of liquidity in the financial market, and provide accessible solutions and tactics for dealing with any challenging circumstances. The report's analytical section should provide observations and advice on the following topics:

1. Is there a need for special action and how much liquidity mismatch exists between the first three time buckets and the permitted limits? Are gaps likely to result in liquidity issues if they are negative and unsustainable? What steps should be made to close the gaps, and what choices are there for dealing with emergencies?
2. How do liquidity managers assess cash flow mismatches within critical time buckets, and what are some potential solutions to urgent shortfalls? What is the history of the fund providers?
3. Does the maturity profile of assets and liabilities exhibit any structural imbalances? Is it necessary to lessen the maturity mismatch inside a certain time bucket or between several time buckets? What methods exist for risk reduction if maturity mismatches are irrational and vulnerable? What potential funding sources are there to make up the liquidity shortage in the case of a liquidity stress event?

4. Should the bank's liabilities be reorganized to lessen maturity mismatches, and if so, what are the options and associated costs (e.g., issuing certificates of deposit at rates above card rates, raising wholesale deposits at higher rates, floating incentive schemes for deposit mobilization, issuing bonds at rates above current market rates, and borrowing long-term funds from other financial institutions)? Is it possible to change an asset's tenure to lessen mismatches?
5. What effects did the sudden withdrawal of significant amounts of money prior to maturity, the non-renewal by customers of a number of matured term deposits on their maturity dates, which was not consistent with the historical trend, and the counterparties' default on their contractual obligations as a result of unforeseen events have on liquidity over the past two weeks?
6. Has the customer behavior pattern changed over the last three months with regard to substantial cash withdrawals before maturity, the rollover of time deposits that have reached maturity, the use of unused overdraft credit limits, the seasonality of cash withdrawals, and the prepayment of term loans? How does the current pattern of behavior compare to the trend that was discovered via the examination of historical data over the previous two to three years?
7. How much of the unutilized credit limits are expected to be drawn down over the course of the next three months, how much in maturing term deposits are there, and how much in potential contingent item claims are there? What additional obligations does the bank have, and how will the liquidity needs be met?
8. What kind of liquidity situation is most likely to develop over the course of the following three months, given realistic scenarios? How might a bad scenario effect the bank, and what approaches may be taken to handle unforeseen circumstances?
9. What obligations exist with respect to expiring foreign currency contracts? What percentage of switched foreign currency deposits are due to be paid when they reach their shorter time frames? What additional foreign currency short-term obligations are there? How will money be set up to pay off foreign currency commitments that are coming due?
10. In the next three to six months, is there any chance that money may be transferred to the bank's linked businesses operating both within and outside the nation? What is the anticipated sum, and how will the funding need be satisfied?

DISCUSSION

The creation and use of risk management solutions to address the identified vulnerabilities and gaps is the next phase in the ALM review process. This might include changing the ratio of assets to liabilities, refinancing operations, hedging tactics, and liquidity management procedures. In order to reduce risks and improve financial performance, it is important to make sure that the institution's assets and liabilities are correctly balanced. Key risk indicators and performance metrics are also continuously monitored and reported as part of the ALM review process. This makes it possible to identify new hazards quickly and determine how well risk mitigation strategies are working. The ALM framework and strategies need to be reviewed and updated often in order to keep up with evolving market circumstances, legal requirements, and risk tolerance of the organization[4]–[6].

The complexity of financial markets, the movement of interest rates, and the changing regulatory environment all provide difficulties in the asset liability management review process. It may be challenging to foresee and manage efficiently interest rate risk, liquidity risk, and financing risk,

particularly in unsteady economic circumstances. To provide accurate analysis and decision-making, the ALM review process also needs strong data management systems, advanced modeling methodologies, and qualified employees. Financial institutions may be more vulnerable to interest rate changes, liquidity problems, and financial instability as a result of poor asset liability management procedures. Asset and liability risks that are not properly managed may have an effect on a company's profitability, solvency, and reputation, resulting in losses and breaking the law[7]–[9].

Review of Interest Rate Risk

1. How does the market see the interest rate environment, and which way are future interest rate moves most likely to go?
2. Does the bank's present interest rate structure align with the anticipated interest rate environment and its objective to attain the desired credit spreads? What adjustments to prime lending rates, term deposit interest rates, and industry-specific lending rates are necessary? To lessen the negative effects of interest rate risk, what should the future growth ratio of fixed-rate and floating-rate assets and liabilities be?
3. Given the current interest rate environment, is it necessary to change the asset mix in the trading book and the banking book? Will the change comply with legal requirements and accepted accounting principles? What rules will apply when the necessary amount of investments is transferred from the "held for trading category" to the "available for sale" and "held to maturity" categories?
4. How do the differences between each time bucket's interest rate-sensitive assets and liabilities relate to the established limits? Under various interest rate situations, how sensitive are assets and liabilities to interest rates?
5. How much of your profits are at risk from potential changes in interest rates? What will happen if interest rates increase or decrease by.5% and 1%? How do the earnings that are potentially at risk stack up against the intended cap on income variation? What reorganization of the maturity profile of assets and liabilities is necessary to minimize the negative effect if the profits at risk are reasonably high? What guidelines and tactics should be used to help incremental assets and liabilities mature at the necessary rates?
6. Including off-balance-sheet entities, what is the weighted average adjusted duration of assets and liabilities? What actions are necessary to reduce the time gap? What effect will any changes in interest rates have on the bank's net worth?

Review of Foreign Exchange Risk

1. How have the main currencies' foreign exchange rates changed during the last week? Was there a substantial shift in the value of any key currency, and if yes, how did it affect the bank's exposure to foreign exchange?
2. What was the overnight open position pattern, and how does it relate to the bank-imposed limits?
3. How large is the discrepancy between the maturities of foreign currency assets and obligations, as well as the possible loss that might result from it? Is there ever a clear mismatch between foreign currency assets and obligations, and if so, how will that situation be fixed?
4. Do the daylight limit, nighttime limit, and gap limit meet the business needs of the bank? If not, what adjustments are necessary?

5. To what degree are bank clients exposed to foreign currencies? How would a negative change in exchange rates effect consumers who have not purchased insurance against exchange risk? Are the loans and advances made to the relevant consumers likely to develop into troubled accounts?
6. What are the bank's individual country exposures and overall global exposure? What proportion of total exposures are in low-risk, medium-risk, and high-risk nations? Exist any countries with large exchange rate changes that could have an impact on the exposure's quality?
7. Do outstanding transactions in any major currency show a clear mismatch? What tactics is the Treasury using to deal with currency mismatches?
8. Is the bank's exposure to foreign exchange concentrated in any one specific currency? How does the Treasury manage currency concentrations to reduce exchange risk, country risk, and settlement risk?
9. What was the range of values-at-risk for all currency exposures during the last two weeks? In what ways does it differ from the permitted limits?

Review of Equity Price Risk

1. How have stock prices changed during the last week? Was there any price fluctuation in any industrial sector or business group's shares?
2. How much equity does the bank have that is important from a business perspective? Are equity holdings concentrated in any way? What is the bank's overall exposure to business groupings when stock, bond, and credit exposure are taken into account? What effect would a stress scenario have on the bank?
3. What is the market worth of the bank's stock portfolio in comparison to the purchase prices? What is the entire equity exposure of the bank's value-at-risk?
4. What percentage of the bank's overall investments are made in equity? Is it consistent with the risk management strategy of the bank?
5. Is it necessary to restructure the bank's equity holdings as a result of price volatility in certain of the stocks it owns?

Value-At-Risk Analysis

What percentage of the bank's overall worth is vulnerable to risk? The following elements need be added together to figure this out:

1. The risk-based value of sovereign securities.
2. The bonds' and debentures' value-at-risk.
3. Value-at-risk for mutual funds and stocks.
4. Value-at-risk for exposure to foreign currency.
5. Gold and other commodity value-at-risk.

The asset liability management review process is a critical aspect of risk management for financial institutions. By conducting comprehensive reviews, identifying potential gaps and vulnerabilities, and implementing appropriate risk mitigation measures, institutions can effectively manage asset and liability risks, optimize financial performance, and ensure long-term stability. While challenges exist, a robust and proactive ALM framework is essential for navigating the complexities of financial markets and meeting regulatory requirements[10], [11].

CONCLUSION

Banks should compile structural liquidity statements at weekly intervals and dynamic liquidity statements at monthly intervals to identify structural mismatches in asset-liability maturity patterns and the intensity of different types of market risks to initiate corrective action.Banks should put in place an effective asset-liability management review process to effectively monitor market risks on a continuous basis and identify emerging risks from maturity mismatches and duration mismatches of assets and liabilities, including foreign currency assets and liabilities, and initiate action for risk mitigation. They should adopt structured formats for meaningful review of the asset-liability position.

REFERENCES

[1] A. Swishchuk, R. Zagst, and G. Zeller, "Hawkes processes in insurance: Risk model, application to empirical data and optimal investment," *Insur. Math. Econ.*, 2021, doi: 10.1016/j.insmatheco.2020.12.005.

[2] Y. Zhou, W. Xia, and S. Peng, "Analysis of an Optimal Model for Liquidity Management of Financial Assets Using an Intelligent Scheduling Approach," *J. Math.*, 2021, doi: 10.1155/2021/7267667.

[3] S. Iyengar *et al.*, "Critical NIH Resources to Advance Therapies for Pain: Preclinical Screening Program and Phase II Human Clinical Trial Network," *Neurotherapeutics*. 2020. doi: 10.1007/s13311-020-00918-2.

[4] S. Patwardhan, D. Yadav, and S. Parlikar, "A review of role of data mining techniques in portfolio management," *Journal of Advanced Research in Dynamical and Control Systems*. 2019.

[5] R. J. Ryan, "The Evolution of Asset / Liability Management (a Summary)," *Res. Found. CFA Inst. Summ.*, 2013.

[6] N. Lagodiienko, L. Ivanchenkova, L. Skliar, and V. Ivanchenkov, "Format And Content Of The Accounting Balance Sheet In The Modern Accounting And Economic Model," *Her. Khmelnytskyi Natl. Univ.*, 2021, doi: 10.31891/2307-5740-2021-294-3-3.

[7] B. Beauvais and R. Wells, "Does money really matter? A review of the literature on the relationships between healthcare organization finances and quality.," *Hospital topics*. 2006. doi: 10.3200/HTPS.84.2.20-29.

[8] S. P. Joshi and R. V Sontakay, "Review Paper on Asset Liability Management in Banking System," *Imp. J. Interdiscip. Res.*, 2017.

[9] H. S. Shin, *Risk and Liquidity*. 2019. doi: 10.1093/oso/9780198847069.001.0001.

[10] J. Hallden, "The original intent of workers' compensation: A team approach," *Work*, 2014, doi: 10.3233/WOR-141909.

[11] J. K. Bakari, "A Holistic Approach for Managing ICT Security in Non-Commercial Organisations - A Case Study in a Developing Country," *Dep. Comput. Syst. Sci.*, 2007.

CHAPTER 4

OPERATIONAL RISK MANAGEMENT FRAMEWORK

Mr. Ashok Bhat
Assistant Professor, Masters in Business Administration,
Presidency University, Bangalore, India.
Email Id:ashokbhat@presidencyuniversity.in

ABSTRACT:

Operational risk management is a crucial discipline within the broader field of risk management, focusing on identifying, assessing, and mitigating risks associated with an organization's operational processes and activities. An operational risk management framework provides a structured approach to systematically identify, measure, monitor, and control operational risks. This paper provides an overview of the operational risk management framework, highlighting its significance and the key components involved in establishing an effective framework. It also discusses the challenges faced in operational risk management and the potential implications of inadequate practices. The operational risk management framework begins with the identification and classification of operational risks specific to an organization. These risks can include a wide range of factors such as internal fraud, external events, process failures, technology disruptions, regulatory compliance issues, and human error. Through comprehensive risk assessment techniques such as risk mapping, scenario analysis, and historical data analysis, organizations can prioritize and quantify operational risks based on their potential impact and likelihood of occurrence.Once the risks are identified, the operational risk management framework incorporates risk measurement and evaluation processes. This involves developing risk metrics, key risk indicators (KRIs), and risk appetite statements to measure and monitor operational risks over time. Quantitative techniques such as loss data analysis, statistical modeling, and stress testing can be employed to estimate potential losses associated with different risk scenarios. These measures provide valuable insights into the organization's risk profile, allowing for informed decision-making and resource allocation.

KEYWORDS:

Bank, Business Ethics, Management, Mitigation,Operational Risk, Vulnerabilities.

INTRODUCTION

Operational risk is difficult to exactly quantify since it is less visible and often goes unnoticed in transactions and operations. Credit and market risks, on the other hand, have more visibility and are simpler to recognize and predict. Operational risk results from potential breakdowns in a bank's control system and business operation process. Operational risk is described as "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events" by the Basel Committee on Banking Supervision. Strategic and reputational risk are not included in this formulation but legal risk is. The Basel Committee's definition is based on specific occurrences that result in losses for banks but are difficult to categorically classify as default risk or value degradation risk. Operational risk may arise from instances like the embezzlement of cash by dealing personnel, unlawful transactions by front office workers, falsifying bank officials' signatures for fraudulent claims against the bank, accounting mistakes

that result in lost income, and similar situations. If we consider the variety of sources from which risks come, the quantity of events that result in loss, and the size of loss that develops if risks materialize, we find significant variations between credit risk, market risk, and operational risk on the one hand, and these risks on the other[1]–[3].

Operational risk, as defined by the Basel Committee, is the potential for loss to a bank that may be attributed to failures in systems, processes, or people. It can also be caused by the occurrence of an external event. This is a general term, but banks may establish a more specific definition using examples drawn from their own experiences to help staff members of all ranks comprehend it. To consistently detect operational risk throughout the whole bank, raise employee risk awareness, and improve control culture, banks should define operational risk in a clear and unambiguous manner. To establish consistency in the categorization of operational risk events, they should use a definition that is similar to that of other banks. The collection and transmission of risk events and loss data across banks will be made easier by the consistency and universality in the concept of operational risk. Since failing to recognize operational risk or mitigate it in a timely manner may result in significant losses, the number and severity of operational risk losses have increased over time, affecting how bank management views risk. Due to a delay in identifying operational risk, the Barings Bank of the United Kingdom failed. Operational risk may have disastrous effects, in contrast to credit and market risks. Due to the variety of operational risk events and the difficulty of managing it, bank management must acknowledge operational risk as a key risk management function. The management should allocate enough funds to control operational risk and provide enough capital for the economy to cover unforeseen losses. The process of corporate governance should take operational risk management seriously as a key component.

Sources of Operational Risk

Operational risk is pervasive, while credit risk and market risk are company-specific. The latter might take place in any sector of company and spread to the business process. System security, system failure, system viability and validity, utility services, and service outsourcing all have high amounts of operational risk occurrences. The next paragraphs provide an explanation of the various sources of operational risk with illustrative examples while keeping in mind the definition provided by the Basel Committee on Banking Supervision.

Risk to Operations from People

The danger posed by employees stationed in crucial sections of the bank's operations is growing more and more significant. People-related risk develops as a result of inadequate information, a lack of familiarity with procedures, the placement of questionable personnel in sensitive operational areas, a lack of business ethics and intellectual honesty, inadequate compensation for intellectual honesty, the management's lenient attitude toward corruption, lax oversight by higher authorities, and loose administration. Banks often fall behind in training staff members who deal with complicated financial products. Fraud is an example of a people-related operational risk incident.

Booking Illegal Transactions

Trading unlicensed in derivatives, foreign exchange, and securities. Trading and dealing with inside information. Financing loans without doing due diligence. Beyond the financial authority

granted. Compromising the requirements for hiring and training. Claiming unfair perks and recompense[4]–[6].

Risk to Operations from Processes

Due to the increasing pressure on profit margins, banks have developed new financial products to attract more customers. They have also used automated technologies to boost business volume, lower transaction costs, and expedite service delivery. To handle the volume of expanding domestic and international business and satisfy client expectations on time, they have established several processing facilities. Banks are required to provide data online to the supervisors in accordance with the latter's off-site supervision program in addition to completing their own business and risk management standards. As a result, they need the support of a reliable management information system that continuously gathers and analyses all operational data. As a result, they must analyze a large amount of data and information on their own operations and those of associated units simultaneously. Banks are putting in computer systems that handle business transactions while simultaneously capturing and storing all transaction-related data in order to save costs. The likelihood of errors occurring during the processing stage and producing inaccurate information and messages that may result in significant loss to banks has increased due to the clubbing of the transaction processing function for customer service delivery and the data classification and storage function for updating the management information system. Examples of operational risk incidents linked to processes include:

1. Incorrect pricing for goods and services.
2. Incorrect client asset appraisal.
3. Accountancy mistakes.
4. Errors throughout the execution, processing, and settlement of transactions.
5. Lending of stock mistakes.
6. Violation of protocol.

Systems Operational Risk

Banks' fixation with system development for company management derives from their desire to not only acquire the newest technology to compete in the market, but also to satisfy the convenience of their customers. Banks must often update their computer systems, adjust software programs, and deal with a number of challenges related to the acquisition and upkeep of operating systems since the information technology system is evolving quickly. Their computer systems are under a lot of strain and are very susceptible to operational problems. Failure of hardware and software systems are examples of operational risk occurrences connected to systems.

Operational Risk from Outside Sources

In addition to creating a protracted interruption of corporate operations, external catastrophes may result in significant financial losses. Since they cannot foresee the timing of the occurrences or gauge the severity of the effect beforehand, banks have little influence over external events. Although protective measures that might be set up to reduce the risk from external occurrences are likely to require extensive planning and costly design, they might not be very effective when events actually occur. However, external events do happen, and banks must understand the risk.

Natural catastrophes including floods, fires, and earthquakes are a few examples of operational risk occurrences linked to external factors.

1. Terrorist and criminal acts.
2. Burglary, robbery, and theft.
3. Failure of contracted out tasks.

DISCUSSION

Causes of Operational Risk

Due to bank mergers and acquisitions, financial activity diversification, business process automation, and outsourcing of financial services, significant changes have taken place in the structure and operation of the financial systems in many nations. First, fast financial institution expansion has enhanced the vulnerability of the banking system since strong economic growth, especially in emerging nations, has boosted the demand for financial services and chances for cross-border banking operations. The new financial institutions are more vulnerable to risk inside the financial system because they are more concerned with business expansion and take longer to set up reliable risk management and control systems. In addition, there have been a number of bank mergers and bank acquisitions of other financial institutions during the last 20 years. The integration of the two financial institutions' disparate operational systems and the creation of a friendly workplace for those with distinct work cultures and value systems become challenging after a merger or acquisition. The potential for additional operational risk events to occur has greatly grown as a result of financial institutions' rapid development and mergers and acquisitions that generate new operating settings[7]–[9].

Second, the potential for the formation of operational risk has been greatly increased by the growth and diversity of the banking industry. In addition to their basic banking operations, banks now engage in specialized lending, structured lending, insurance business, securities business, and insurance business, either directly or via subsidiary organizations. They have also taken on a number of other responsibilities, including offering utility services to clients and managing payment and collection processes on their behalf. Operational risk now has a new facet because to the financial services industry's dramatic growth in both volume and variety.

Third, banks have significantly enhanced the degree of automation for the provision of banking services, as well as the capability and area of application of computer systems. Financial services that operate automatically include automated teller machines that disburse cash, electronic money transfers, e-commerce, and Internet banking services. Numerous concerns concerning system failure, system security, hacking, entry of fraudulent transactions, and other issues have been brought up by the wave of automation. Operational risk in banks is mostly caused by the high degree of automation.

Fourth, banks are using outsourcing for both financial and nonfinancial services more and more. They have resorted to outsourcing services on a wider scale due to cost-benefit considerations, and the outsourcing market has grown dramatically over time. Banks use seasoned companies to provide protection for the location and assets, operate automated teller machines, transfer money and valuables from one location to another, maintain computer systems, and other services. Some banks even hire qualified companies to act as their agents while raising money and handling loan applications. Some risks related to outsourcing include service providers' inability

to fulfill commitments on time, their unavailability in stressful and emergency situations, their inability to deliver services, and their potential access to the bank's secret and confidential information. These kinds of situations provide banks with a significant level of operational risk.

Operational risk is a result of how transactions are carried out, the systems used to conduct them, and the controls in place to monitor and mitigate the risk involved. Operational risk starts before to transaction execution, continues during transaction delivery, and even persists after transaction completion. At the transaction negotiation stage, it is possible to choose the incorrect customer or make a mistake since the client's requirement cannot be understood and the wrong product package cannot be chosen. The facilities could be designed by bank officials in a manner that doesn't necessarily meet the demands of the customer. There might be a programming mistake, a systems error, or a systems breakdown during the transaction processing phase. The risk of fraud, the danger of money laundering via the abuse of funds, the risk of documentation and collateral assessment, and the model risk to calculate the potential loss amount are all present at the product delivery stage. Operational risk so starts at the start of a transaction and continues until it is completed and the client connection is ended. Banks often ignore or pass over a few potential drivers of operational risk. Here, a few instances are shown.

Risk of Insufficient Communication

Staff members' trust in running the company is undermined by poor and insufficient communication. Staff members' productivity is impacted by poor communication, which causes them to make mistakes. There are several elements that effective internal communication entails. The effectiveness of the techniques and tools used to successfully transmit the message is just as important as the clarity of the circulars and directives sent to the employees to explain the processes. The goal is for every employee to be equipped with the knowledge necessary to comprehend and implement instructions and procedures in day-to-day tasks. Uncompleted communication may be seen, for instance, in the lack of job description cards or operating procedure manuals. Similar to this, a list of "do's and don'ts" is crucial to efficient communication. More instances of operational risk occur as a result of communication system flaws.

Risk from a Culture of Absence of Control

The practice of always acting morally and following the rules is known as control culture. It is a person's work ethic that directs them to be vigilant and refrain from misconduct. The depth of the control culture is used to evaluate the effectiveness of the corporate governance system. Employees at a company with a strong control culture are aware of the dangers involved in the work they are performing, they take safeguards to protect the company's interests, and they take control responsibilities seriously. Control culture does not develop naturally over time or by itself. It will emerge if there is a clear framework for recognizing intellectual integrity and application of thought while punishing negligence and duty-related indifference. If the workers are aware that there is a fair mechanism in place for assigning blame for misconduct, they will be control-conscious. Operational risk occurrences are more likely to occur when control cultures are poor.

Failure of the Control System Risk

Financial institutions need to have an effective control mechanism in place to survive over the long run. Large financial losses might result from the loss of control, especially in areas that are crucial to operations. One crucial component of the control system is the division of labor between operational employees and risk monitoring staff, for instance. The control system will become diluted if the firewall between the two groups of workers is not impenetrable, and control erosion might cause significant losses. The breakdown of the primary control system may result in a financial institution suffering a disaster, as shown by the collapse of the Barings Bank. One the one hand, the operational responsibilities and risk control function were concentrated in the hands of a single person, violating the concept of segregation of duties between the trading and arbitrage operations and the risk monitoring and control functions. However, the parent company of the bank in London disregarded the exercise of control. A control system failure occurred as a result of the massive, astounding losses that accumulated unobserved until the Barings Bank neared the point of insolvency.

Banks build a strict control system to keep enterprise-wide risks within the limits while also prescribing reasonable risk limits for lending, investment, trading, and off-balance-sheet operations. The risk level will exceed the defined threshold if there is dilution or a breakdown of control. The extra risk brought on by insufficient control is a control risk, which belongs under operational risk rather than business risk.

Risk associated with novel processes and products

Banks examine a new venture's viability when a new product or activity is launched, accounting for possible losses that can result from the venture's credit and market risks, but they do not adequately assess the operational risk component of the new venture. For instance, qualified staff with actuarial and other necessary knowledge are needed if a bank wishes to start a new business venture like the insurance industry. Alternatively, it needs the support of knowledgeable and experienced staff if it wishes to offer new products, such as the buying and selling of options and futures. Banks often are unaware that the introduction of new goods and operations may result in certain circumstances that have the potential to produce operational risk. First, the bank may not be entirely prepared to launch a new initiative or operation.Product because it uses cutting-edge technology and calls for skilled labor. Second, the kind of risk that will arise from the new activity or product may not be captured by the current risk monitoring and management system. Third, dealing with the new activity or product may not be possible using the present framework for reporting on the qualitative and quantitative components of risks. As a result, the control architecture will need to be changed to address risks brought on by the new activity and product. Before launching a new service or product, banks conduct a SWOT analysis. The study must evaluate potential new operational risk occurrences as well as how the risks will be monitored and controlled.

Unrevised Profile Risk

A bank's risk management efforts are in line with its risk profile, a self-compiled document that examines the kinds, quantities, and levels of hazards to which it is exposed. A bank's credit, market, and operational risks are specifically covered in the risk profile document's qualitative and quantitative parts. The risk profiles are affected by changes in the economy, politics, and environment, and they are also changed by efforts in regulatory or supervisory policy. As a

result, banks must periodically examine and revise the risk profile and determine if the current risk management architecture is adequate. In order to handle the novel circumstance resulting from the updated risk profile, they must adapt the procedures and systems. If the risk profile isn't updated, a bank can find itself unprepared for certain situations that might lead to new kinds of operational risk occurrences.

The danger of inefficient auditing

An internal audit independently assesses a bank's risk management system's performance. The audit team must evaluate whether the business heads are identifying operational risk in their individual business areas, owning and managing it, and highlighting in the audit reports deviations from procedures, excesses permitted and exceptions made by the operating staff, laxity in supervision and control, and other irregularities. A crucial component of the system of checks and balances is the audit function. The personnel may grow complacent or slack and adopt a casual attitude about the job if the audit is ineffective, fails to uncover frauds and irregularities, or compromises with the violation of regulations by the field staff. The frequency and severity of operational risk incidents will both rise as a result of this sort of development.

Objectives of the operational risk policy

Operational risk management's primary goals are to:

1. Recognize the potential for operational risk occurrences to cause losses.
2. Create a culture of awareness and control across the company.
3. Create methods for evaluating the effects of operational risk occurrences.
4. Create strategies for allocating resources to pay for possible operational risk losses.

Because operational risk has distinct characteristics from credit and market risk, banks must develop a unique operational risk management strategy. Recognizing the significant importance of operational risk in the total risk profile and incorporating it into the whole risk management process are the goals of a distinct policy. Banks should set up a procedure to help all employees comprehend operational risk's definition and scope, cultivate a culture of control, and work ethically and within set parameters. To maintain long-term solvency, they should establish a thorough framework for identifying operational risk, create tools and technologies to quantify risks under various scenarios, and effectively monitor and manage them. They should establish an atmosphere at work where tasks are completed with care and attention, a high standard of behavior is maintained, conflicts of interest are avoided or kept to a minimum, and openness and disclosure are integrated into corporate management. Limits for operational risk tolerance should be set, and the justification should be given.

Contents of the operational risk policy

Banks' operational risk policies may differ somewhat in substance, but only little. The organizational structure, size of the bank, range and complexity of products, business ethics, and human resource skill sets, and work and control cultures, among other things, all have an impact on the policy's substance. The policy paper should include the approaches and plans for managing operational risk throughout the whole bank, as well as the bank's views on operational risk tolerance and the parameters that staff members should work within. It should have a thorough description of operational risk, the methods for identifying and measuring risks, and plans for observing, managing, and reducing the risks. It should describe how the bank is

exposed to different operational risks in connection to its ongoing operations, provide a quantitative and qualitative analysis of that exposure, and describe the steps being taken to manage those risks. The policy should outline the typical loss occurrences and the effects such occurrences may have on the bank. It should draw attention to important problems with the way the bank runs, lingering problems that might be dangerous, and how these problems are being resolved. The document should make clear what the management expects from the workforce in terms of fostering a control culture and maintaining a productive reporting and review system. It should underline management's desire to fix responsibility for irregular activities and explain the management's promises to uphold transparency in all situations. It should outline the administrative process for handling violations of policies, unlawful overreach and exceptions in deals, and officials' ignorance and recklessness in carrying out their mandated duties.

Framework for Operational Risk Management

Operational risk may manifest itself in a number of ways and is a component of all corporate operations, in contrast to credit and market risks, which are industry-specific. Operational risk occurrences have become more frequent over time, and they are becoming more complicated in nature. It has gained popularity in a number of sectors, including system failure, security, validity and viability, utility service, and outsourcing. As a result, operational risk management places more emphasis on risk management than risk measurement. Operational risk management should be seen by banks as a separate risk management task that includes risk identification, assessment, monitoring, control, and mitigation. The operational risk management framework should be created with the needs of the bank in mind, taking into account factors like company size and complexity, risk tolerance, work environment, and desired level of capital. The following actions should be taken by banks as a bare minimum to mitigate operational risk:

1. Banks should draft a document outlining their operational risk management policies, practices, and guidelines and distribute it to the staff members that deal with operational risks on a daily basis. The document should identify risk tolerance limits, split them down into useful sublimits, and provide reporting thresholds for limits violations. These tactics for successfully implementing operational risk rules should also be included.
2. Banks should establish a procedure for identifying and evaluating operational risk that takes into consideration both past and anticipated risk occurrences. They should monitor actual and prospective operational risk loss data, categorize operational risk loss occurrences into various risk groups depending on the frequency and severity of those events, and map those groups for the purpose of prioritizing corrective action.
3. Banks should set up an efficient monitoring approach to enable quick identification of flaws in operational risk management systems and practices and the start of corrective action. Along with keeping an eye on operational risk loss incidents, they should also look for early warning signs of potential increases in future loss risk.
4. For the purpose of controlling operational risk, banks should create particular regulations for classifying goods and activities into the proper business units.
5. Banks should implement the necessary policies, procedures, and processes to manage and reduce significant operational risks. They should update the operational risk profile and assess the success of risk mitigation and control techniques on a regular basis.
6. Banks should set up procedures for controlling risks related to outsourcing activity. They should also have business continuity plans and contingency plans in place for operating

in the event of a significant company interruption. They need to assess the business continuity and catastrophe recovery strategies on a regular basis.

Based on the policy paper, banks should create a suitable operational risk management framework that would outline the operational risk management approach. The framework should not only include a clear description of operational risk but also the construction of an efficient communication system that will encourage staff comprehension of operational risk and improve risk awareness and the control culture across the business. The framework should outline important operational risk management procedures, define the roles of various functionaries, and provide rules for responsibility distribution and accountability fixing. It should have a process that clarifies and assesses risks associated with novel goods, novel activities, and novel systems and is aware of risks brought on by environmental elements and outside conditions.

For successful management of operational risk, banks should design a suitable organizational structure within the framework for enterprise-wide risk management and adhere to the concept of segregation of tasks when allocating responsibilities. They need to support human resource policies that reward truthfulness and integrity in business transactions and chasten inclinations to depart from the established protocols. They have to maintain the value of the monitoring and control function and submit the operational risk management function to a thorough internal audit for unbiased assessment and evaluation.

Mitigating operational risks is a crucial aspect of the framework. This includes designing and implementing robust internal controls, policies, and procedures to prevent or detect risks. Control measures may involve segregation of duties, regular reconciliations, risk-based audit programs, and incident reporting systems. Additionally, training and awareness programs are essential to educate employees about risk management practices and foster a risk-aware culture within the organization. The framework also emphasizes ongoing monitoring and reporting of operational risks. Regular risk assessments, internal audits, and independent reviews contribute to the continuous evaluation of risk controls and the identification of emerging risks. Reporting mechanisms, such as risk dashboards and risk heat maps, provide management with clear visibility into the organization's risk profile and aid in decision-making.

Challenges in operational risk management arise from the dynamic nature of business operations, technological advancements, regulatory changes, and emerging threats. Operational risks can be complex, interconnected, and difficult to predict. Furthermore, organizations must adapt their risk management practices to keep pace with evolving risks and the changing business landscape. Inadequate operational risk management practices can lead to financial losses, reputational damage, regulatory penalties, and business disruptions. It can also hinder the organization's ability to achieve strategic objectives and maintain stakeholder confidence. Therefore, establishing a comprehensive operational risk management framework is essential for organizations to proactively identify, assess, and mitigate operational risks[10]–[12].

CONCLUSION

In conclusion, the operational risk management framework provides organizations with a structured approach to identify, measure, monitor, and control operational risks. By implementing this framework, organizations can effectively manage operational risks, improve decision-making, and enhance overall resilience. However, the dynamic nature of operational risks necessitates ongoing evaluation, adaptation, and continuous improvement of risk

management practices.Operational risk is caused by flaws in systems, processes, and people, as well as by unforeseen external occurrences. It stays buried in transactions and operations and has less visibility and predictability than credit and market risks. Because operational risk is not business-specific, arises from various sources, manifests via a variety of events, and causes large loss when it materializes, it is more important than credit and market risk. It starts from the start of a transaction and continues until it is completed and the client connection is ended. The likelihood that operational risk will manifest itself in some way has significantly increased as a result of the financial industry's rapid expansion, bank mergers and acquisitions, financial activity diversification, business process automation, and outsourcing of financial services. Operational risk incidents are increased by ineffective and inadequate communication, a lack of a fair mechanism for enforcing responsibility, and the absence of clear criteria for rewarding and punishing behavior. The quantity and severity of operational risk events are also increased by the audit function's slowness and a lack of seriousness in assessing the operational risk component of new activities and products. Recognizing how much damage an operational risk event might do and taking appropriate action are the main goals of operational risk management. Because the importance and features of operational risk events varies from those relating to credit and market risk events, banks should have a distinct operational risk management strategy.

Banks should have a business continuity planning and outsourcing strategy as part of their operational risk management plan. Due to the failure or inadequateness of services provided by vendors and third parties, outsourcing of services has a significant risk of causing operational loss. Business continuity is disrupted by internal events like system failure and external events like terrorism and natural disasters that result in financial loss. In accordance with their size, company operations, risk appetite, operating environment, and desired level of capital, banks should set up an operational risk management framework that is suitable for them. The operational risk management process' design and accommodating human resource development laws that support the program's goals should be included in the framework.

REFERENCES

[1] M. J. Naude and N. Chiweshe, “A proposed operational risk management framework for small and medium enterprises,” *South African J. Econ. Manag. Sci.*, 2017, doi: 10.4102/sajems.v20i1.1621.

[2] J. Young, “Determinants for a risk-based audit of an operational risk management framework: A South African perspective,” *Acad. Account. Financ. Stud. J.*, 2020.

[3] A. van Niekerk, D. J. Geldenhuys, M. M. Levin, M. May, and K. P. Moalusi, “Implementing an Operational Risk Management Framework: Psycho-Social Factors in Tanzania,” *J. Psychol. Africa*, 2012, doi: 10.1080/14330237.2012.10874524.

[4] A. A. Rahman and Z. Yazid, “Developing a framework of islamic bank operational risk management: ‘People Risk,’” *J. Pengur.*, 2015, doi: 10.17576/pengurusan-2015-44-12.

[5] Y. Xu, L. Zhu, and M. Pinedo, “Operational risk management: A stochastic control framework with preventive and corrective controls,” *Oper. Res.*, 2020, doi: 10.1287/OPRE.2019.1960.

[6] J. Young, “Guiding criteria for an operational risk management framework for South African municipalities,” *Adm. Publica*, 2018.

[7] M. Roe *et al.*, "A six stage operational framework for individualising injury risk management in sport," *Injury Epidemiology*. 2017. doi: 10.1186/s40621-017-0123-x.

[8] Aisyah Abd Rahman and Zaleha Zaid, "Developing a Framework of Islamic Bank Operational Risk Management: 'People Risk,'" *J. Pengur.*, 2015.

[9] L. C. Osken and C. Onay, "An operational risk management framework for financial services industry," 2016.

[10] Z. Z. Aung, "Operational Risk Management Framework For Service Outsourcing: Consideration Of Risk Dimensions And Their Application Into The Framework," *Int. J. Electron. Bus. Manag.*, 2008.

[11] H. Akpolat and T. Pitinanondha, "A Framework for Systematic Management of Operational Risks," *Asian J. Qual.*, 2009, doi: 10.1108/15982680980001441.

[12] M. H. Muazu, R. Tasmin, and M. Javaid, "Operational excellence, regulatory framework and firm characteristics in the oil sector: The role of enterprise risk management implementation," *Int. J. Serv. Oper. Manag.*, 2021, doi: 10.1504/IJSOM.2021.114299.

CHAPTER 5

OPERATIONAL RISK IDENTIFICATION, MEASUREMENT AND CONTROL

Ms. Anandasrinivasan Deviprabha
Assistant Professor, Masters in Business Administration,
Presidency University, Bangalore, India.
Email Id:deviprabha@presidencyuniversity.in

ABSTRACT:

Operational risk identification, measurement, and control are integral components of an organization's risk management framework, aimed at proactively managing and mitigating the potential risks associated with its operational processes and activities. This paper provides an overview of the operational risk identification, measurement, and control processes, highlighting their significance and the key steps involved in effectively managing operational risks. It also discusses the challenges faced in these areas and the potential implications of inadequate practices.The process of operational risk identification begins with a comprehensive assessment of an organization's operational activities, including its people, processes, systems, and external factors. This involves conducting risk assessments, reviewing historical data, and engaging key stakeholders to identify potential sources of operational risk. Risks may include process failures, human error, technology disruptions, regulatory compliance issues, fraud, and external events. The identification process helps prioritize risks based on their potential impact and likelihood, allowing organizations to allocate appropriate resources for risk management efforts.

KEYWORDS:

Bank, Business Ethics, Key Risk Indicators (KRIs), Management, Mitigation,Operational Risk.

INTRODUCTION

After identifying operational risks, the measurement process involves quantifying and evaluating the potential impact of these risks on the organization. This can be achieved through various methods, such as scenario analysis, key risk indicators (KRIs), and loss data analysis. Scenario analysis involves constructing hypothetical risk scenarios and assessing their potential consequences on the organization's operations. KRIs provide quantitative metrics to track and monitor risk exposure, while loss data analysis utilizes historical data to estimate potential losses associated with specific risk events. These measurements provide valuable insights into the organization's risk profile, enabling informed decision-making and the development of appropriate risk mitigation strategies.

Approach to Operational Risk Identification

Operational risk should be included in the identification process for all business operations, goods, and services provided by banks. Operational risk used to be handled by banks, often using a control system backed by an internal audit function. To comprehensively identify operational risk, no systematic technique was used. The Basel Committee on Banking Supervision has highlighted the need for comprehensive treatment of operational risk in two documents: "Sound Practices for Management and Supervision of Operational Risk, December 2001" and

"International Convergence of Capital Measurement and Capital Standards: A Revised Framework—Comprehensive Version, June 2006". The identification process has to be thorough and take into account operational risk that arises from all company operations, products, and other sources, as shown above[1]–[3].

Business Operations

Granting credit, taking deposits, borrowing money, buying stocks, issuing credit cards, moving money, offering custodial services, and offering agency services are all examples of business activity.

Products

goods, which come in many varieties such as deposit and credit goods, bill purchase and discount products, financial guarantee and commitment products, credit card and derivative products, are tools used to supply services.

Processes

Transaction processing, client instruction processing, money transfer processing, data and message transmission, processing involving payment and settlement systems, and books of accounts reconciliation are all examples of processes.

Systems

Systems include computers, software, core banking solutions, automated teller systems that govern cash payments, networking systems, Internet banking systems, and systems for maintaining records and accounting.

External Factors

Service interruptions, natural disasters, break-ins, and terrorist operations are examples of external occurrences.

Services Outsourcing

Contracts for the operation and maintenance of automated teller machines, service agreements for the physical transfer of cash and valuables, and contracts for surveillance and security to protect buildings and other assets are all examples of services that may be outsourced.Establishing an efficient monitoring and control system requires thorough identification of operational risk. Therefore, banks should create checklists to categorically identify operational risk from each of the categories d above, as well as from new activities, products, systems, and procedures.

Process for Identifying Operational Risks

Banks may use a bottom-up strategy for risk mapping, classification, and aggregation while using a top-down technique to identify operational risk occurrences. The operations of the bank are divided into business lines under the top-down method, and activity groups related to each business line are identified. Following that, each business line's goods are divided, and risk events related to each product are listed. The bottom-up technique involves gathering data on individual risk occurrences, categorizing them into broad event-type categories within each

business line, and then aggregating the risks within those event-type categories to gain a full picture of the operational risk the bank is exposed to[4]–[6].

Organizational Line Identification

Banks have main and minor business lines, and certain activities are not part of their normal operations. The use of eight business lines for the Standardized Approach's computation of operational risk capital charges is advised by the Basel Committee on Banking Supervision.

Business lines include:

1. Business Finance
2. Selling and Trading
3. Consumer banking
4. Business Banking
5. Settlement and Payment
6. Agency Solutions
7. Asset Control
8. Wholesale Brokerage

These business lines may be adopted by banks for operational ease and capital adequacy testing to cover operational risk. Each business line consists of one or more broad activities, and each broad activity is grouped into a few distinct activity groups that provide various goods and services. In the New Basel Capital Accord, business lines have been assigned Level 1 category and broad activities Level 2 category. For instance, under the business line "Retail Banking," the broad activities are "retail banking, private banking, and card services" and the activity groups are "private lending and deposits, banking services, trust and estates, investment advice, merchant/commercial/corporate cards, private labels, and retail."

The process of identifying operational risks starts with grouping all of the bank's operations into the proper business divisions. Some business lines may not be applicable to some banks since they don't engage in all types of operations. For instance, certain banks may not engage in asset management, retail brokerage, or agency services.

The heart of the identification procedure is the identification of risk events from each product utilized by activity groups connected to each business line. Therefore, banks should create activity-group lists of historical operational risk incidents and distribute them to the business executives. The method will prevent the chance of omission by acquainting the business line managers with risk events that could occur in a certain business line.

DISCUSSION

Guidelines for Determining Business Lines

For the purpose of assigning a product or activity to the proper business line, banks should create precise rules. In Annex 8 of the New Basel Capital Accord, the Basel Committee on Banking Supervision lays out the guidelines for business line mapping. The New Accord's guiding principles make it easier to map items and activities to business lines. The definition of business lines used for calculating regulatory capital for credit and market risks should be utilized in conjunction with the mapping of activities to business lines for the calculation of operational risk capital needs. Banks should attribute the auxiliary function of an activity to the business line it

supports and map the activities to the business lines in a way that is mutually exclusive and jointly exhaustive. They may divide complex activities into their component parts and assign each part to the most salient or salient business line, for example, or they could allocate activities that fall under more than one business line to the most salient or salient business line. Banks should compile a record of all operations and categorize them according to one of the established business divisions while keeping these criteria in mind. A bank may disregard an activity if it does not engage in it and it does not fit within one of its business lines.

Identification of Product Groups and Activity Groups

Banks may define product teams, activity groups, and products that they employ for the delivery of services falling under those business lines after identifying the business lines. The product teams may do general banking, transaction banking, merchant banking, sale-purchase of securities and currencies, services related to debit and credit cards, cash management, wealth management, and other related tasks. For service delivery, each product team makes use of a range of goods. For instance, the general banking activity group may use various deposit products for people, businesses, and institutions as well as various credit and credit-related products for people of different types, such as term loans, overdrafts, letters of credit, the purchase and discount of trade bills, and the issuance of guarantees. However, there could be common product categories that fit under more than one business sector. For instance, both retail banking and commercial banking may apply to individual and corporate retail and wholesale deposits, overdrafts, and term loans. The primary goal of aligning goods with business lines and activity groups is to determine the gross revenue for each business line in order to use the Standardized Approach to determine operational risk capital charges. "Within each business line, gross income is a broad indicator that serves as proxy for the scale of business operations and, consequently, the likely scale of operational risk exposure within each of these business lines," according to the Basel Committee on Banking Supervision[7]–[9].

Understanding Risk Events

Finding the risk events linked to the goods is the next stage in identifying operational risk. An occurrence or experience that has directly or indirectly, via previous events, caused or has the potential to cause substantial loss to a bank is referred to as an operational risk event. Money laundering, check fraud, robbery, computer hacking, computer malfunction, and other risk events are a few examples of risk occurrences. Risk events may be categorized based on negative or unfavorable happenings that have happened in the past at a bank's branch offices, controlling offices, or head office. These events are linked to the people, procedures, and technology employed in the delivery of goods. We may even consider an occurrence that could happen and result in a bank losing money, assets, or reputation as a potential risk event. Regulatory requirements, personal experiences, and occurrences that have happened in other banks and financial institutions may all be used by banks to create lists of risk events.

Methods for Operational Risk Assessment

Banks should create their own operational risk assessment methods, taking into account the whole spectrum of operations, the nature of the company, and the accessibility of the data. Unlike credit risk, where the emphasis is on numerically quantifying potential credit loss, and market risk, where the emphasis is on numerically quantifying likely investment value erosion, the emphasis shifts under operational risk to quantifying loss in terms of relative magnitude, such

as small, moderate, large, and substantial. Operational risk is more of a management problem than a measurement one, thus banks should examine their overall operational risk exposure, pinpoint areas where there is a significant danger of loss, and move quickly to reduce that risk.

Banks may use one of three techniques to evaluate operational risk:

1. Risk and control self-assessment technique.
2. Method using key risk indicators.
3. Method of risk mapping.

Risk and Control Self-Assessment Technique

The self-assessment approach allows banks to evaluate potential risk associated with their goods and operations in terms of business processes and constraints, skill requirements, prospective threats, and slippages. The bank has an internal mechanism for assessing the advantages and disadvantages of the operational risk environment. Reviewing the main business risks the bank confronts, the effectiveness of the controls in place to manage and mitigate those risks, and determining whether the current environment can support corporate goals and corporate business perspectives all need the collaboration of specialists inside the company.

Assume for a moment that the company's goal is to dominate the retail banking market. To complete the "Control and Risk Self-Assessment" exercise, a team of experienced employees from several bank divisions who have exposure to many parts of retail banking is assembled. The team compiles a list of the bank-specific vulnerabilities found in the retail banking portfolio, conducts a formal evaluation of current business procedures and control systems, and pinpoints any shortcomings, difficulties, or management problems that the bank may encounter in achieving its corporate objective of becoming a leading retail banker. The team evaluates the threats in light of potential operational risk events that could arise, the controls already in place, and the severity of the consequences in the case an event does take place. It analyzes the control system from the user's perspective and offers suggestions for changing the control process to lessen the risks to the achievement of the corporate objective. After evaluating the inherent risk, the risk controls in place, the severity of the eventual effect, and the ranking of various operational risk scenario types, banks may issue ratings. To simplify control and risk self-assessment, banks should create uniform risk assessment templates, establish risk assessment criteria, and create standardized scorecards. They may use this approach to assess the efficacy of current controls that provide suggestions for improving the control system and identify the weaknesses in their systems and processes.

Method for Key Risk Indicators

Key risk indicators are data or measurements that are used to pinpoint key locations where operational risk may manifest as well as actions and risk factors that may result in losses. KRIs provide early warning signs for individuals, groups, and systems. KRIs are created by combining three different parameters:

1. Amount of business.
2. Environment supporting logistics.
3. Schedules for discretionary authority.

KRIs are often located in those operational areas where bank auditors discover the majority of irregularities or where bank management recognizes operational limitations and control weaknesses. The symptoms that lead a bank to look for KRIs include a sudden increase in business volume or transaction levels, out-of-proportion errors, losses in unexpected areas, arrears in books of account reconciliation, significant interbranch communications on payment and settlements, or a sudden rise in the number of irregularities in branch operations.

KRIs occur across all business lines, despite perhaps having originated from the same source across various activities, goods, and business lines. For instance, the treasury, credit, or finances departments may all have people-related KRIs. The business line leaders are in charge of finding KRIs in their specific business lines since they are better knowledgeable about the operational problems and vulnerabilities in their particular business sectors. To monitor negative developments, each KRI should be connected to the underlying cause and routinely reviewed for correctness and relevance. The authorized authorities should check for KRIs exceeding any thresholds or limitations of risk tolerance that the banks have established. The restrictions are designed to notify risk managers of any possible issues that could arise in certain operational areas. The process of choosing KRIs is ongoing, and the list of crucial KRIs evolves over time. Some KRIs are derived from historical loss event data statistics. Examples include the quantity of check encashment scams, the number of times staff abused their own accounts at the branch office, the quantity of incorrect outputs sent as a result of system issues, and so forth. Changes in company volume, business profile, and the introduction of complicated goods all lead to the creation of certain new KRIs. It is essential to build KRIs that are forward-looking by taking cues from these changes.

In order for risk managers to check for KRIs when the actual data exceeds the benchmarks, banks should establish benchmarks in each pertinent area to assess if the ratios and quantities of events, incidents, and transactions are disproportionate or substantial. They should regularly collect data on KRIs, grade them using a scale, determine their significance in terms of frequency and severity, and create a list of crucial KRIs so that they can pay closer attention to them. In order to evaluate the potential loss that might result from operational regions to which KRIs belong, actual operational risk loss data for the previous five to seven years with regard to identified KRIs must be gathered. Based on the frequency, severity, and past loss data of KRI-related occurrences, one may predict the probable loss. The identification of key and sensitive regions and concentrating efforts on those areas for risk mitigation are made easier with the help of the KRI-based evaluation of possible loss from each operating area.

Method for Mapping Risk

The main goal of risk mapping is to identify weak points so that corrective action may be prioritized. Using the loss event type categorization system in Annex 9 of the New Basel Capital Accord, banks should choose their own parameters for risk mapping, gather the operational risk loss data related to different business units, and categorize these events according to event types. To identify the most susceptible locations for suitable corrective action, they should map loss data independently with regard to each business line and rank the event-type and business line operational risk scenarios. The Basic Indicator Approach, the Standardized Approach, and the Advanced Measurement Approach are the three techniques for determining operational risk capital charges that the Basel Committee on Banking Supervision has advocated in the paper on the New Basel Capital Accord. The first two methods attempt to compute capital charges from

the side of revenue estimate; the third method does so from the side of loss estimation. The only approach that specifies a technique for estimating possible operational risk loss is the Advanced Measurement Approach. In order to calculate operational risk regulatory capital, it is advantageous to set up an operational risk measurement methodology that complies with the Advanced Measurement Approach requirements and can produce both the expected loss and the unexpected loss from operational risk exposures. "A bank's internal measuring system must adequately anticipate unexpected losses based on the combined use of:

a. Internal and external loss data that is pertinent.
b. Analysis of scenarios.
c. Internal control considerations and the business environment unique to banks.

The Accord stipulates that "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." This capability includes supporting an allocation of economic capital for operational risk across business lines in a way that encourages better business line operational risk management. Banks should develop risk measurement methods that are compatible with their industry, product offering, and complexity. A combined application of four elements internal loss data, external loss data, scenario analysis and the unique business environment of the bank, and internal control factors must be used in the measurement process to assess the size of any prospective loss.

Measurement of Internal Losses Based on Data

Estimating the possible loss based on the bank's own internal loss experiences is a crucial step in the operational risk assessment process. In order to link their own risk assessments to the actual loss occurrences, banks should maintain internal loss event data. The internal loss data should be linked to the business lines and event categories listed in Annexes 8 and 9 of the New Basel Capital Accord, and it should be relevant to the present business operations. The information must be thorough, including all material exposures and activities from every region, as well as the full systems and processes. All significant losses that fall within the concept of operational risk, including those associated with operations involving credit risk and market risk, should be included in the statistics.

Banks should gather information about operational risk loss from their branch locations and combine it to get a comprehensive picture of operational risk loss across all business lines and the whole organization. To maintain consistency and uniformity in reporting by offices from various locations, they should establish distinct criteria for assigning loss data resulting from loss events into various business lines and design structured formats for reporting operational risk loss event and loss data by branch offices and regional offices. It is adequate to collect data over cutoff levels if the bank is big and has several branch offices in various locations. It is not desirable to gather operational risk loss data concerning extremely tiny amounts. The latter may differ across banks as well as between business lines and event kinds within a single bank. The following information should be included in the structured formats:

Period of the loss. Kind of occasion

Loss amount, recovered amount, and balance due. drivers or loss events' causes. The information should include both actual incidents and losses as well as prospective losses that may have happened and near-misses. The phrase "near-miss operational risk loss event" refers to a loss that

may have occurred but did not do so by accident or a loss that was prevented by the staff's attention and awareness. To generate a picture of the enterprise-wide operational risk loss that has actually happened and the probable loss that may have occurred but was prevented, banks should combine information on operational risk loss event information on actual losses and near-miss losses gathered from branch offices. They will be able to generate accurate projections of prospective operational risk losses that could occur this year and the next year thanks to the integrated picture. The quantity of operational risk loss should be used to calculate the risk-adjusted return on capital, which will be used to evaluate the performance of specific business lines. Banks should gather loss data by business line in order to rank the business lines in order of their sensitivity to operational risk.

Measurement of External Losses Based on Data

The measuring method is complemented with external data on operational risk loss occurrences, which can map scenarios that internal data often cannot. A variety of public papers, peer banks, and industry sources provide access to external data. For mapping of occasional but prospective high-severity losses, external data are more useful. Banks should gather external data on loss occurrences and assess the data's relevance to their own circumstances in light of their size, business operations, the geographic locations of the incidents, and the reasons and other factors that contributed to the loss events. The significance of external data is crucial from two perspectives: whether the loss event is a singular occurrence and whether the impact's severity is appreciably high despite the loss event being frequent and regular. Banks should have a methodical procedure in place to decide whether external data will be utilized and how it will be included into the measuring process.

Measurement Based on Scenarios

Another approach for assessing operational risk loss is scenario analysis, which is combined with external loss data to evaluate, in particular, a bank's susceptibility to high-severity events. Future occurrences called scenarios have the potential to result in significant losses, and analysis helps banks allocate financial resources to cover such prospective losses. Banks may create credible operational risk scenarios, evaluate the scenarios' applicability, and calculate possible losses that might result from various scenarios. Through the logical evaluation of conceivable catastrophic losses by knowledgeable company managers and risk management specialists, they may produce feasible operational risk scenarios in connection to each business line and develop the database of scenario-based events.

The New Basel Capital Accord's Basel Committee on Banking Supervision has advised that a bank utilizing the Advanced Measurement Approach for operational risk capital calculation must show that its approach catches potentially serious "tail" loss occurrences. The Committee believes that there may be circumstances in which estimations of the 99.9th percentile confidence interval, which are largely based on internal and external loss event data, are incorrect for business lines with heavily tailed loss distributions and few observed losses. Scenario analysis, the business environment, and control considerations may take on a more important role in such situations. On the other hand, for business lines where estimations of the 99.9th percentile confidence interval based largely on such data are judged trustworthy, operational loss event data may play a more dominating role in the risk assessment system.

Creating a database of scenario-based occurrences is the main obstacle to scenario analysis. Loss occurrences may arise if one or more mishaps take place that avoid being controlled. The efficacy of existing controls and the time of loss event detection determine the loss quantum, with earlier event detection resulting in less loss as event-specific monitoring and control may be reinforced. The first objective is to determine the potential cause of an event, and the second is to evaluate the proactive measures currently in place to stop it from happening, or the controls that are already in place. The third step is determining the event's prospective effects after the implementation of new, event-specific controls or the improvement of existing general controls. The fourth work entails estimating the potential loss that may ultimately materialize despite the augmentation of controls made shortly after the event was discovered. Banks may then utilize the database for scenario-based loss assessment and estimate the possible losses from various sorts of catastrophes[10]–[12].

CONCLUSION

Operational risk identification involves identification of risk events, which are incidents or experiences that have caused or have the potential to cause material loss to a bank either directly or indirectly with other incidents. Risk events arise from people, process, and technology failures in handling the business. Banks should formulate specific policies for mapping products and activities into appropriate business lines for identification of operational risk. They may first identify the business lines and then the activity groups and the products used by groups for delivery of services falling under that business line. Banks should classify individual risk events into broad event-type categories within each business line and arrive at the aggregate of risks under event-type categories to get a comprehensive picture of the operational risk they face. Banks should assess operational risk through the control and risk self- assessment method, key risk indicator method, and risk mapping method.

Operational risk control is concerned with putting procedures in place to manage, mitigate, and control risks that have been identified. To do this, strong internal controls, rules, and processes must be designed and put into place. Segregation of roles, routine reconciliations, risk-based audit programs, staff training, incident reporting systems, and business continuity planning are examples of control mechanisms. The objective is to create a robust control environment that efficiently manages operational risks and supports an organizational culture of risk awareness and responsibility. Due to the complexity of contemporary corporate operations, growing hazards, technology improvements, and regulatory changes, operational risk identification, measurement, and management provide unique challenges. Organizations must constantly update their risk management procedures and keep a close eye on emerging threats since operational hazards might be interrelated and hard to foresee.

Inadequate operational risk identification, measurement, and management procedures may cause monetary losses, harm to one's reputation, failure to comply with regulations, and interruptions in corporate operations. Additionally, it may make it more difficult for the company to meet its strategic goals, keep stakeholders satisfied, and ensure long-term success. In order for businesses to proactively identify, assess, and control operational risks, the development of a strong and thorough framework for operational risk management is crucial.For firms to effectively manage risk, operational risk identification, measurement, and control techniques are essential. Organizations may identify possible risks, evaluate their effect, and put the right controls in place to reduce operational risks by executing these procedures. To handle new risks and guarantee the

organization's resilience in a changing business environment, however, regular monitoring, adaptation, and continuous development of risk management techniques are required.

REFERENCES

[1] K. Rehman, H. H. Khan, B. Sarwar, N. Muhammad, W. Ahmed, and Z. U. Rehman, "A Multi-Group Analysis of Risk Management Practices of Public and Private Commercial Banks," *J. Asian Financ. Econ. Bus.*, 2020, doi: 10.13106/jafeb.2020.vol7.no11.893.

[2] D. L. Teker, "Implementing Operational Risk Management in Banks via Insurance Policies," *Elektron. Sos. Bilim. Derg.*, 2006.

[3] M. Urbaniak and D. Zimon, "Implementation Of Standardized Management Systems And The Requirements Of Production Companies Towards Suppliers," *Int. J. Qual. Res.*, 2021, doi: 10.24874/IJQR15.04-04.

[4] International Monetary Fund, "Islamic Financial Institutions and Products in the Global Financial System: Key Issues in Risk Management and Challenges Ahead," *IMF Work. Pap.*, 2002, doi: 10.5089/9781451859775.001.

[5] Yanuardin, "Studi Literatur Manajemen Risiko Hukum," *At-Tazakki*, 2020.

[6] R. E. Ako, D. Oghorodi, and A. E. Okpako, "A fuzzy logic risk control and self-assessment metrics for e-banking operational risk analysis," *J. Comput. Sci. Its Appl.*, 2021, doi: 10.4314/jcsia.v27i2.11.

[7] H. Maulana, Y. Firmansah, and N. Arkyananto, "Identifying Risks in Indonesian Zakat Institutions Using Enterprise Risk Management (ERM)," *Int. Islam. Econ. Syst. Conf.*, 2021.

[8] A. R. Nafchi and M. Dastgir, "Identification and ranking of the risk factors affecting the probability of occurrence of fraud in banks (a case study: An Iranian bank)," *Journal of Critical Reviews*. 2020. doi: 10.31838/jcr.07.02.36.

[9] "Strategy for Implementing Risk Management for Gold Pawn Products At PT. Bank Syariah Indonesia Regional Office II Medan," *Al-Sharf J. Ekon. Islam*, 2021, doi: 10.56114/al-sharf.v2i3.223.

[10] J. I. Chukwunulu, V. N. Ezeabasili, and M. N. Igbodika, "Risk Management and the Performance of Commercial Banks in Nigeria," 2019.

[11] Y. Chen, "Private Preschools ' Managerial Risk and Solutions to Risk Management Department of Early Childhood Education," *J. Educ. Soc. Policy*, 2016.

[12] C. Ciocea, "Operational Risk Management Approaches Within An Investment Fund. Sif Moldova Case Study," *Stud. Sci. Res. Econ. Ed.*, 2016, doi: 10.29358/sceco.v0i24.368.

CHAPTER 6

OPERATIONAL RISK MEASUREMENT PROCESS

Mr. Anil Gowda
Associate Professor, Masters in Business Administration,
Presidency University, Bangalore, India.
Email Id:anilbgowda@presidencyuniversity.in

ABSTRACT:

The operational risk measurement process is a vital component of an organization's risk management framework, aiming to quantitatively assess and quantify the potential losses arising from operational risks. Operational risk encompasses a wide range of risks associated with an organization's people, processes, systems, and external events. This paper provides an overview of the operational risk measurement process, highlighting its significance and the key steps involved in effectively measuring operational risks. It also discusses the challenges faced in operational risk measurement and the potential implications of inadequate practices. The operational risk measurement process begins with the identification and classification of potential operational risks specific to an organization. These risks may include process failures, human error, technology disruptions, fraud, regulatory compliance issues, and external events. By comprehensively identifying and categorizing these risks, organizations can establish a foundation for effectively measuring and managing operational risks.Quantitative techniques are employed in the operational risk measurement process to assess the potential impact and frequency of identified risks. One commonly used technique is the loss data analysis, which involves analyzing historical data to estimate potential losses associated with different risk events. This analysis provides valuable insights into the frequency and severity of operational risk events, enabling organizations to quantify the potential financial impact and prioritize risk mitigation efforts.

KEYWORDS:

Bank, Business Ethics, Management, Mitigation,Operational Risk.

INTRODUCTION

The estimate of prospective loss from operational risk is supported by historical loss experiences. The measuring method begins with the gathering of information on real operational risk losses from various sorts of prior incidents. In order to assess the possible loss that might happen during the current year, the next year, and so on, banks should gather internal loss data pertaining to all business activities and company locations, compute the average loss values referring to various occurrences, and then apply the obtained values. Based on the average loss numbers, they should estimate business-line and event-type losses before arriving at the aggregate to determine the possible loss for the whole company. According to the New Basel Capital Accord's paragraph 672, the data must be valid, reflect the actual frequency of risk occurrences and the severity of their effects, and initially pertain to at least five observation periods[1]–[3].

The internal loss statistics show the frequency with which each loss event happens during the year, the amount of loss that happened each time, and the reasons behind each loss event. The

data must be processed by banks in order to determine the frequency and severity of loss events. Through this method, they will be able to rate the loss events according to their frequency and severity, determine which loss events often have serious effects, and pinpoint the business lines that are most vulnerable to operational risk. According to the frequency of risk occurrences and the amount of loss connected with each incident, banks may divide loss events into three categories—low, medium, and high—in order to estimate the potential loss that might occur in the future. Due to variations in size, business activity, volume, risk appetite, and risk-bearing ability, banks may have different standards and scales for classifying loss occurrences in terms of frequency and severity. If their volume of business is high and the number of occurrences is great, banks may employ a finer measurement scale.

Observing operational risk

Operational risk monitoring's primary goals are to reduce the frequency and severity of loss incidents and to make sure that the authorized authorities are faithfully carrying out their assigned duties to minimize the risks. The monitoring team should monitor operational risk loss occurrences, KRIs, loss occurrences from outside sources, and potentially significant operational risk scenarios as they develop. The group should identify early warning signs that point to a higher likelihood of future losses and take precautions. The efficiency of the monitoring role should be periodically reviewed in retrospect by authorized personnel. The monitoring activity's foundation is comprised of reports from various departments and officials. Banks should examine these data to determine which regions need more regular and intensive monitoring. Only if the reports from the business units, activity groups, operational risk department, and internal audit department are useful and provide specifics on operational risk exposures will monitoring be successful. Therefore, banks should make sure that the reports are thorough and provide details on any recent occurrences and novel situations that have arisen in the banking sector. In light of the evolving operational risk profile that emerges from these reports, they should modernize the monitoring system.

Operational risk that could develop in a department's or business line's operations should be owned by the departmental and business line leaders. They should keep an eye out for operational risk occurrences in their specific domains and implement risk-reduction plans. To assess the sincerity and honesty of business/departmental heads in carrying out their monitoring duty, banks should periodically conduct independent evaluations of their performance.

Control and Mitigation of Operational Risks

To lessen the effects of operational risk, banks should set up an efficient internal control structure backed by risk mitigation instruments and methodologies. Since proactive and reactive controls affect both the frequency of operational risk occurrences and the severity of their effects, they should be assessed for appropriateness and effectiveness. The frequency and severity of loss occurrences will increase with the vulnerability of the control structure. Tools for risk mitigation should be used in addition to operational risk management rather than as a replacement. An operational risk mitigation plan against theft, robbery, or looting can include getting insurance for cash handled by the teller at the bank counter or insurance for cash in transit. The insurance provider may reject a claim owing to neglect in adhering to the established rules, thus the bank cannot take solace in the insurance and loosen its control over the observance of protocols by the employees handling cash at different locations. An additional risk-mitigation instrument to the

entire risk-control process is the provision of insurance. On a case-by-case basis, banks should use mitigating solutions to address identified operational risk exposures.

If a business has a strong control culture and banks implement pro-active human resource policies, monitoring and control will be simpler. Banks should penalise noncompliance and irregular behavior on the one hand and provide incentives for compliance and honest performance on the other. They need to address the problems that compromise the effectiveness of the control framework and make it challenging to implement the control processes. The causes of operational risk should be examined by banks, and appropriate corrective action should be taken, such as updating technological systems and enhancing system security, classifying sensitive data and information for computer system storage to prevent leakage and unauthorized use, and evaluating legal and vigilance issues for closing the loopholes that resulted in loss. They should also evaluate how well business line heads are doing at recognizing and keeping an eye on low-probability, high-severity operational risk events, managing the risk associated with outsourcing services in their specific fields, and coming up with management plans for such occurrences. Banks should make sure that the internal audit department is investigating the control environment and control culture at the branch office at the time of the on-site inspection and notifying management of any problems as part of the monitoring activity[4]–[6].

Business Continuity Planning for High Intensity Operational Risk Events

Concept of Business Continuity Planning

Banks must have a business continuity strategy to handle crises that may result from high intensity operational risk occurrences. A business continuity plan is a document that details how banking services will be restored to nearly normal levels in the event of a business interruption or failure brought on by the abrupt occurrence of large operational risk events. The strategy is designed to avoid total service interruption due to system failure or outside disruptions, which may sometimes be quite substantial. In a highly competitive industry, banks deploy advanced technology and make use of it to grow their client base. The likelihood of system corruption or system failure, which may cause business interruption, has considerably grown as a result of technology's rising complexity. Similar to how external catastrophes like fires, terrorist attacks, and natural disasters may seriously destroy a bank's property, communication system failures and power outages can abruptly halt banking operations. Banks often have backup plans in place to handle small catastrophes like a branch office running out of cash to pay clients, branch personnel suddenly disappearing, a sudden power outage or computer system failure, etc. However, the business continuity plan aims to handle crises that are far more serious and that result from circumstances that are not typical of daily life. Therefore, banks should have a thorough business continuity strategy to resume regular services in a timely manner.

Choice of Key Activities

The priority-based restoration of key operations is the goal of the business continuity strategy. Banks should compile a list of essential tasks, prioritize them, and outline the sequence of steps that may be necessary to resume operations. These steps are included in the business continuity plan. The primary functions of a bank include cash disbursement, cash management, payment and settlement, and the treasury function.

Settlement and Payment

A bank must fulfill obligations to clients, adhere to agreements, and participate in the clearinghouse every day since doing otherwise might disrupt the payment and settlement system. Its inability to make payments and settle accounts on time may cause financial market instability and threaten the stability of the financial system.

Financial Action

The treasury department is essential to daily operations since it manages the bank's liquidity and conducts trading and risk hedging activities. Treasury activities may halt in the case of system failure or interruption of the treasury function as a result of outside occurrences. Banks should have backup plans in place so that the treasury function may be restored immediately. They have to keep backup mirror accounts of all daily treasury transactions in secure locations for use in an emergency.

Liquidity Control

In the case of a company interruption, liquid money may be needed in substantially greater quantities than usual. Due to increased client demand for cash withdrawals during a crisis, the bank's liquidity will be under strain. During the crisis, banks should evaluate their possibilities for obtaining liquid capital and maintain them available.

Payment in Cash

The automated teller machine service must always be available at banks. The bank is required to immediately restore network connection and refill currency in the event that services are interrupted due to a mechanical fault. Alternative plans for handling the problem will need to be established if the kiosks are destroyed.

Customer Contact

Customer interaction is a crucial component of the financial services industry. Banks must establish call centers at designated locations to accommodate the increased volume of consumer enquiries that would follow a business interruption or company collapse caused by a natural or man-made catastrophe. Sometimes, the bank's reputation may be harmed by misleading publicity or propaganda. Customers should get assurances from the contact center about the security of their money and other assets, and the center should address their inquiries regarding the return of regular company activities.

DISCUSSION

Support Requirements for Business Continuity Plans

Banks should make the following steps to ensure that services are restored during the post-disruption phase.

Support for Computer Systems

The continuation of customer transactions depends on the ledger extraction of client accounts. Banks should back up their computer systems, save copies of their clients' accounts in a different, secure location, and update those copies every day.

Support for Outsourced Services

Banks should assess the importance of outsourced services and prepare contingency plans in case of crises brought on by the failure of service providers. Banks should demand that the service providers create their own business continuity plans and keep them prepared for use at short notice if the outsourced activities are critical, such as the upkeep of automated teller machines or the provision of armed guards at branch offices and other sensitive areas where cash and valuables are stored.

Administrative Assistance

After large unfavorable situations that have disrupted corporate operations, it is crucial to make quick, suitable choices in order to get things back to normal. During a crisis, it may become necessary to make administrative choices that are beyond the authorized authority of the affected bank executives. To take immediate action, mandated norms and regulations may need to be relaxed. Therefore, banks should establish clear policies about the easing of restrictions and the use of power to make hasty judgments during the crisis. The management of business continuity plans should be handled by a separate committee of executives for major banks with many branch locations both domestically and abroad.

Methodology for Business Continuity Planning

Impact Evaluation

The goal of the business continuity strategy is to lessen the negative effects of significant operational risk events on a bank's services. Before completing the strategy, banks should conduct impact analyses under various scenarios to see how they would affect various operational areas in the event that routine banking services are disrupted due to exceptional circumstances. When considering events that interrupt business, such as strikes and sabotage, equipment failure, damage to the backup facility, programming error, natural disasters, and terrorist actions, they should do an effect study. The impact study will determine the size of backup facilities needed to quickly return to regular operations after a catastrophe. Identification of recovery centers and assessment of recovery time are two essential elements for creating a business continuity strategy. Recovery time is the amount of time necessary to resume vital activities and fulfill ongoing obligations to customers and other counterparties. For various service types, recovery times might vary. Banks should consider the nature, severity, and logistics needed to restore the bare minimum of operations when determining the recovery time for a priority activity. The protection of the bank's reputation and the management of other risks are the main objectives[7]–[9].

Recovery centers are alternative locations where backup facilities are maintained and parallel data is saved in order to quickly retrieve lost data and resume bank operations. The backup locations need to be removed from the vulnerable and disaster-prone areas. When the current company premises are inaccessible, the business continuity plan should include a map of alternative locations where crucial business operations may be carried out. Banks should establish operational processes for catastrophe management and create specific response plans based on the business continuity strategy.

Business Continuity Plan Creation

The list of crucial business operations that the bank believes must be urgently restored should be included in the business continuity strategy. The timeline by which the bank plans to resume its prioritised operations should be included in the strategy, as well as the resources required to carry out the plan throughout the crisis. Business continuity plans for the head office, regional offices, and branch offices should be created separately by banks. Since retail banking services and essential business operations are conducted via branch offices, these strategies are crucial. Here is an example list of crucial tasks for creating the business continuity plan's blueprint:

1. Money distribution in a disaster-affected area. ATM cash withdrawal and distribution.
2. Involvement in the settlement and payment system. restoration of client ledger accounts.
3. The return of online banking. payment of bank-related claims.
4. Creation of a call and enquiry center for customers.

In order to create business restoration plans for each activity, banks should first determine the key and necessary financial services, taking into account the customer and company characteristics as well as the legal requirements. The following components should be included in the business continuity plan:

1. A description of the crucial action. prescription for rest period. prescription for a rehab facility.
2. Things that are necessary to provide the service. outlines of a plan. a list of the necessary steps.

Business Continuity Plan Testing

Banks must test the business continuity plan on a regular basis to make sure it will function in the event of a catastrophe. In particular, they must double-check the effectiveness of the measures planned and the availability of services for the restoration of normality. To maintain the plan sustainable and functional at all times, they should periodically perform mock disaster recovery exercises and implement the necessary corrective measures.

Organizational Structure for Operational Risk Management

To handle the operational risk management role, banks should establish a distinct administrative unit inside the risk management organizational structure. Due to the growing complexity of the function and rising operational risk losses, large banks that are involved in multiple business activities should have a separate operational risk management department, with its operations being overseen by an operational risk management committee. This is in contrast to small banks that only conduct traditional banking, which may have an operational risk management cell within the risk management department. When dividing up duties among operational tasks, risk monitoring and control functions, and other support services, banks should consider the problem of conflicts of interest. Due to the specialized nature of operational risk management, banks should staff at least four key areas with operational risk professionals or experts:

1. Evaluating one's own risk and control.
2. KRI identification.
3. Analyzing and identifying operational risk situations.
4. Gathering and analyzing loss event data

Operational risk must be addressed as soon as it arises, thus business line leaders should be responsible for managing it in their respective domains. They should be in charge of identifying loss occurrences and KRIs associated with their business lines, gathering, processing, and analyzing data, doing their own assessments of operational risk, and completing risk mitigation plans.

Another important tool used in the operational risk evaluation process is scenario analysis. It entails creating fictitious risk scenarios and evaluating the effects they could have on an organization's operations. Organizations may model different operational risk occurrences and assess their possible effects on financial performance, reputation, and regulatory compliance using scenario analysis. By prioritizing risk mitigation techniques, this approach aids in the identification of high-risk regions and improves the efficacy of risk management as a whole.

In the operational risk assessment process, key risk indicators (KRIs) are crucial. KRIs are quantitative measurements that are used to track and keep track of the exposures to operational risk over time. Organizations may identify early warning indications of possible operational risk events and take proactive steps to minimize risks by creating and monitoring relevant KRIs. Metrics relating to process effectiveness, mistake rates, compliance violations, and customer complaints are among the KRIs that are often employed. The complexity of contemporary company operations, the scarcity of data, and the dynamic nature of operational hazards all provide measurement challenges. Organizations must use strong modeling tools and adjust their risk measuring procedures to changing business contexts since operational hazards are often interrelated and hard to foresee. A lack of awareness of possible operational losses, poor resource allocation, and an inability to properly prioritize risk mitigation activities are all consequences of deficient operational risk measuring techniques. Organizations may be subject to monetary losses, reputational harm, regulatory non-compliance, and interruptions in company operations as a result[10], [11].

CONCLUSION

In conclusion, businesses must effectively identify and quantify possible operational losses via the operational risk assessment process. Organizations may improve their awareness of operational risks and make educated choices about risk mitigation methods by using quantitative methodologies, such as loss data analysis and scenario analysis, and monitoring KRIs. To handle new threats and keep an efficient operational risk management framework in place, it is essential to continually improve measurement methodology, data quality, and risk measuring processes.Using past internal loss event data, banks should estimate the possible operational risk loss and then contrast the predicted losses with the actual loss events. Additionally, they should identify scenario-based events to capture those instances that internal data cannot map and estimate possible losses using external data on operational risk loss occurrences that are relevant to them. They should set standards to gauge the likelihood of occurring and the severity of the relevant risk occurrences for this purpose.

The total of anticipated loss and unforeseen loss is the possible operational risk loss. The quantity of unexpected losses from low-frequency, high-severity events should be evaluated by banks. In order to reduce risks, operational risk monitoring's primary goal is to reduce the frequency and severity of loss incidents. The monitoring team should keep tabs on loss events related to operational risk, identify important risk indicators, gather data on loss events from outside sources, and pinpoint plausible operational risk scenarios. The departmental and business

line leaders should assume responsibility for any operational risks that may develop in their spheres of responsibility, identify risk events, and develop response plans.In the case of a business interruption brought on by very severe operational risk events, banks should establish a business continuity plan for the restoration of almost regular banking services. The business continuity plan aims to handle larger-scale crises that result from unanticipated, out-of-the-ordinary situations. Before giving the business continuity plan its practical form, banks should conduct impact evaluations of significant operational risk events that cause significant business interruption. The plan should outline alternate locations for carrying out crucial business operations, a list of crucial tasks that must be completed immediately, a timeline for the restoration of vital banking services, and the administrative and logistical support required to carry out the plan during a crisis. Establishing a distinct administrative structure with operational risk specialists and experts is a good idea for banks because it will help them see operational risk management as an independent risk management function.

References

[1] M. A. Cristea, "Operational Risk Management In Banking Activity," *Ibima Bus. Rev.*, 2021, Doi: 10.5171/2021.969612.

[2] Y. Yudiana, D. Hafidhuddin, And R. Ismal, "Pengukuran Risiko Operasional Pada Bank Syariah Indonesia (Studi Kasus Bank Syariah Xyz)," *J. Apl. Bisnis Dan Manaj.*, 2018, Doi: 10.17358/Jabm.4.2.179.

[3] E. Fahmy, "Analisa Pengukuran Beban Modal Risiko Operasional Metode Basic Indicator Approach (Bia) Dan Advance Measurement Approach (Ama) Di Bank Efg," *E-Mabis J. Ekon. Manaj. Dan Bisnis*, 2020, Doi: 10.29103/E-Mabis.V21i1.474.

[4] S. Pakhchanyan, "Operational Risk Management In Financial Institutions: A Literature Review," *International Journal Of Financial Studies*. 2016. Doi: 10.3390/Ijfs4040020.

[5] J. R. Ríos, D. F. M. Duque, And J. C. O. Gómez, "Operational Supply Chain Risk Identification And Prioritization Using The Scor Model," *Ing. Y Univ.*, 2019, Doi: 10.11144/Javeriana.Iyu23-1.Oscr.

[6] H. Handoko, C. Catherine, And R. Riche, "Pengukuran Kinerja Teknologi Informasi Perusahaan Abc Menggunakan It Balanced Scorecard Dan Btripplee Framework," *Komik (Konferensi Nas. Teknol. Inf. Dan Komputer)*, 2019, Doi: 10.30865/Komik.V3i1.1608.

[7] M. Y. Abjasiqo, W. Winarko, And E. Sari, "Pengaruh Kebisingan, Umur, Masa Kerja, Lama Paparan Dan Penggunaan Alat Pelindung Telinga Pada Tenaga Kerja Di Perusahaan Kabel Otomotif," *Ruwa Jurai J. Kesehat. Lingkung.*, 2021, Doi: 10.26630/Rj.V14i2.2165.

[8] H. Juliza And H. O. S. Anggiat, "Identify The Operational Risk Of The Port By The Risk Breakdown Structure (Rbs) Method," 2019. Doi: 10.1088/1757-899x/505/1/012012.

[9] A. Jobst, "Operational Risk: The Sting Is Still In The Tail But The Poison Dependson The Dose," *Imf Work. Pap.*, 2007, Doi: 10.5089/9781451868036.001.

[10] L. O. Prymostka And N. S. Sokolovska, "The Measurement (Assessment) And Modeling Of The Operational Risk Of Bank," *Bus. Inf.*, 2021, Doi: 10.32983/2222-4459-2021-11-144-153.

[11] N. Arifah And S. Haryono, “Analisis Determinan Pengungkapan Emisi Karbon (Studi Perbandingan Perusahaan Di Indonesia Dan Malaysia Periode 2013-2018),” *At-Taradhi J. Stud. Ekon.*, 2021, Doi: 10.18592/At-Taradhi.V12i1.4654.

CHAPTER 7

RISK-BASED INTERNAL AUDIT SCOPE, RATIONALE AND FUNCTION

Ms. Pramoda Hegde
Assistant Professor, Masters in Business Administration,
Presidency University, Bangalore, India.
Email Id:pramodah@presidencyuniversity.in

ABSTRACT:

The risk-based internal audit scope, rationale, and function play a crucial role in ensuring the effectiveness of internal audit activities within an organization. A risk-based approach to internal audit focuses on aligning audit efforts with the organization's key risks, thereby enhancing the value and relevance of the audit function. This study provides an overview of the risk-based internal audit scope, rationale, and function, highlighting their significance and the key components involved in implementing a risk-based approach. It also discusses the challenges faced in adopting a risk-based internal audit approach and the potential benefits of effective implementation. The risk-based internal audit scope involves determining the areas and processes that are subject to internal audit review based on their level of risk to the organization. This scope is established through a comprehensive risk assessment, which identifies and evaluates the organization's key risks. The risk assessment considers various factors such as financial risks, operational risks, compliance risks, and strategic risks. By aligning the internal audit scope with the identified risks, organizations can ensure that audit resources are directed towards areas that pose the greatest potential impact and likelihood of risk.The rationale behind adopting a risk-based internal audit approach lies in its ability to provide assurance and insights on the management of significant risks within the organization. By focusing on key risk areas, internal auditors can provide a more targeted and relevant assessment of the organization's control environment, risk management practices, and governance processes. This enables management and stakeholders to gain a better understanding of the organization's risk profile and make informed decisions to enhance risk mitigation strategies.

KEYWORDS:

Bank, Business, Management, Mitigation,Operational Risk.

INTRODUCTION

Internal Audit's Purpose and Justification

A bank's internal control system is not complete without the internal audit function. The following definition of internal audit was accepted by the board of directors of the Institute of Internal Auditors in June 1999: Internal audit is an independent, objective assurance and consulting activity intended to add value and enhance an organization's operations. By applying a systematic, disciplined approach to review and enhance the efficacy of risk management, control, and governance processes, it aids a company in achieving its goals.

Internal auditing has a broad range of responsibilities, but the Institute of Internal Auditors defines it as having a primary emphasis on risk management and corporate governance processes and procedures. Internal audit is generally concerned with the study of corporate processes and

procedures, the inspection of transactions, the verification of conformity with laws and regulations, and the assessment of the internal control system[1]–[3].

The following characteristics of how a bank operates are often of interest to the internal auditor:

1. Whether or not company operations are carried out in line with established processes in various places.
2. If every transaction is properly carried out and documented.
3. Whether management and operational employees are acting within their stated authority and that official roles and responsibilities are properly defined.
4. Whether or whether operational authorities consistently adhere to the set risk limitations.
5. Whether the financial reports that dealing representatives send to the in charge authorities are correct and complete.
6. The accuracy of the balance sheet is supported by the books of accounts and if the accounting of transactions is performed in line with accepted accounting principles.

Because banks' business operations, business profiles, business practices, and business processes vary from one another, so does the internal audit's scope.

Relationship between Internal Audit and Internal Control

The results of the internal audit may be used to determine the effectiveness of the internal control system since an audit is supposed to draw attention to control weaknesses. An efficient internal audit function verifies that the operating systems are suitable, approves the soundness of the operating processes, and assures compliance with the established rules and regulations. A bank's internal audit division independently assesses the effectiveness and integrity of the internal control architecture, identifies any gaps, and makes recommendations for the addition of new controls or improvements to current controls. Internal auditing helps to identify overlapping tasks that weaken the control process and discrepancies in controls. Internal auditors aid bank management in strengthening the control system by giving them crucial information regarding the bank's functional flaws. Banks must thus uphold the internal audit function's independence.

Adapting Internal Audit's Role

Many banks now have internal audit programs that are mostly focused on transaction audits; these programs do not emphasize risk management functions or provide comments on the effectiveness and appropriateness of risk management systems and practices. To increase its usefulness, internal audit, which is a step in the internal control process, has to have its scope enhanced. Banks should transition from a transaction-based internal audit system to a risk-based one and provide the audit department autonomous authority to evaluate the efficiency of risk management tools and corporate governance procedures. The shortcomings in the risk management methods and procedures should get greater attention in the risk-based audit reports.

According to the New Basel Capital Accord, banks must implement stronger risk management procedures, better match capital coverage to underlying risks, and retain regulatory and financial capital to protect against residual risks such as those related to credit, markets, operations, and other factors. The Accord emphasizes the need for establishing a mechanism that independently evaluates the risk management systems and procedures and provides assurance about the accuracy of the bank's risk profile and the adequacy of internally assessed capital, and it encourages greater use of internal systems for risk assessment and capital calculation. The

auditing profession has evolved from scrutinizing individual transactions to checking policies and practices for risk identification, measurement, and management. If the audit reports are trustworthy and objective, bank supervisors and external auditors may utilize the results of a risk-based internal audit to evaluate the soundness of a bank's operations without conducting their own independent investigation. The internal audit or inspection department should be given the task of conducting an unbiased assessment of the risk management function by banks.

Differences Between Transaction-Based and Risk-Based Audits

Banks have their own internal audit rules, which typically encompass branch office audit coverage throughout the budget year, audit frequency (which is correlated with a rating system), and audit completion time. In accordance with the transaction-based audit system, the internal audit team evaluates the performance of the branch office in terms of a few qualitative and quantitative criteria and provides grades such as outstanding, good, mediocre, and unsatisfactory using five- or six-grade rating scales. The emphasis of the transaction-based audit is on the inspection of each item of assets and liabilities, the verification of transactions and accounting records, the investigation of conformity with laws and regulations, and the correctness and promptness of control reports issued to the controlling authorities. The audit reports draw attention to the procedural inconsistencies, the excesses that branch officials permitted that were beyond the scope of their financial authority, and the unapproved exceptions. An audit committee is often present in banks to monitor the operation of the transaction-based internal audit system. The risk-based internal audit, on the other hand, is a proactive and dynamic method of audit that focuses emphasis on the policies and procedures used by banks to identify, quantify, and manage risks related to the transactions. Although sparingly and selectively, the risk-based audit also looks closely at specific transactions to assess compliance with established policies and procedures. It places greater emphasis on the internal control system's sufficiency and appropriateness as well as the identification of control weaknesses to notify the bank management of elevated risks[4]–[6].

Risk-based audit reports provide suggestions for enhancing operational practices and implementing risk mitigation techniques, which add value and support the stability of the business. Instead of concentrating on listing the irregularities found during the audit, the risk-based audit identifies the causes of the irregularities through selective transaction testing and makes recommendations for changing the procedures to stop them from happening again. A risk-based audit identifies the operational weak points of the bank, and the audit reports warn the bank management of looming risks. The distinctive characteristic of a risk-based audit is that it detects risks that escape the awareness of business leaders and risk managers and alerts management to flaws and gaps in the control system that may result in loss for the bank. In the end, a successful risk-based internal audit system safeguards the bank's solvency and reassures the bank management about the soundness of the operations.

DISCUSSION

Internal Audit: Risk-Based Internal Audit: Transactional Internal Audit

a. examination of all transactions between the previous audit and the present audit to look for abnormalities.a. examination of a small number of transactions in order to assess risk-related systems and processes.

b. Examination of the sanction, oversight, and monitoring of loans and advances since the previous audit.b. Examining compliance with risk limitations, exposure restrictions, and other mandated limits as it relates to the loan sanction function.
c. examination of each asset and liability item, as well as the veracity of the trial balance.c. Analyzing specific assets and liabilities on a sample basis.
d. checking and balancing the records of finances.d. A sample examination of the books of accounts with a provision for a more thorough inspection in the event of a question.
e. Validity, enforceability, and currentness of all papers and agreements are examined.e. Sample document and agreement checks with a clause for more thorough reviews in case of uncertainty.
f. Verification of the bank's own assets, the collateral and valuables, the vouchers and posts in the ledger books, the control returns, and the management information reports.f. Physical assets, jewels, collateral, vouchers, books of accounts, control returns, and financial reports are all examples of verification.
g. routine inspection for rules and regulations compliance, including anti-money laundering and Know Your Customer guidelines. The application of Know Your Customer guidelines, anti-money laundering rules and regulations, and identification legislation procedures are all sample checked for compliance and critically examined.as well as the reporting of shady transactions.

Additional components

1. Detection of flaws in the control system and operational processes.
2. Identifying the sources of the problems.
3. Finding the root causes of anomalies that occur often in branch offices, especially irregularities that are common.
4. Creation of suggestions for credit improvement options and risk avoidance strategies.
5. Evaluation of how well management has responded to new hazards from different goods, activities, and locations.
6. Verification of the branch office's risk profile that is being audited. During a head office audit, risk management policies and practices are evaluated.
7. Suggestions for system and procedural improvement.

Change to an Internal Audit System Based on Risk

Over the years, the bank regulators have greatly loosened their supervision over commercial banks' activities and given them more autonomy. In order to stop banks from abusing their autonomy and engaging in risky and unsound banking activities, authorities must exert stronger oversight. Due to the diversification of their business operations and the usage of a broad variety of goods and services, banks are now more susceptible to more occurrences and dangers of a bigger scale. Commercial banks must transition from the transaction-based audit system to the risk-focused audit system while bank supervisors convert to the risk-based bank supervision system to implement stricter techniques of bank supervision. Since risk-based internal audit is a crucial component of the risk management architecture, it should be set up as a separate department inside the bank. The shift from transaction verification to systems verification for risk management and compliance checking via selective transaction testing is part of the move to

risk-based internal audit. The risk-based internal audit system prioritizes dangerous operational areas for preferred scrutiny and allots audit resources in line with the priority.

Since the internal audit department will be required to carry out the difficult and technical work of reviewing the risk management policies and procedures as well as the internal control system, the shift to risk-based audit implies major changes in the way the department operates. There should be at least three goals accomplished by the risk-based internal audit. First, the audit should attest that business operations are conducted in line with the bank's risk-bearing capability and philosophy of risk management. It should also provide the management a fair amount of comfort about the security and soundness of the bank's operations, and it should offer the management excellent advice for enhancing the corporate governance procedure[7]–[9].

Functions of Internal Audit Based on Risk

Risk-based internal audit's main purpose is to review a bank's risk management policies and practices and provide an unbiased evaluation of all risks the bank is exposed to. The internal control system's appropriateness and integrity are endorsed, and in the process, it is possible to identify the operational and control processes that are most vulnerable and so carry the most risk. Therefore, banks should set up processes to evaluate the various kinds of risks faced by the branch office, controlling office, and corporate office as well as the risk management system in place. Internal audit should perform this function and develop its own technique for risk assessment, taking into account the volume, complexity, and importance of each business activity.The internal audit department's risk evaluation involves many different aspects. The risk management department's risk assessment practices and procedures should be evaluated first. The audit department should also look at the methods used by the risk management department to determine capital requirements for all types of risk-taking activities and certify that the procedure adequately addresses the issues with regulatory and economic capital calculation. The credit, market, operational, and other residual risks should all be identified and measured using methods and methodologies that the audit department should review both individually and collectively. Second, in order to prioritize the audit and determine its scope and focus which may change across branch offices owing to variations in the business mix and risk profile the audit department should conduct an independent evaluation of the risks encountered by each branch office. Third, the internal audit division should examine each business line and each portfolio in addition to an audit of the field offices. The department should assess the risk of various portfolios with a focus on those that are considered to be relatively high-risk, such as the credit card portfolio, the capital market portfolio, the commercial real estate portfolio, and other credit portfolios that have higher default rates, in order to complete this task. All offices, all business operations, and portfolios, including outsourced operations and bank subsidiary units like the insurance subsidiary and securities trading subsidiary, should be subject to a risk-based audit by the department.

Internal Audit Policy Based on Risk

The long-term sustainability of banks is protected by risk-based internal audit since it greatly lowers the likelihood of severe losses from rapid shocks and unexpected causes. To emphasize its significance, banks should develop a unique risk-based auditing strategy, provide the internal audit department preferential treatment in comparison to other departments, emphasize the department's roles, duties, and authority, and support its independence. The technique for compiling risk profiles for portfolios, business lines, and branch offices, as well as for assigning

risk ratings before to the audit and performance ratings after the audit, should be included in the audit policy. The policy should include the standards for determining the frequency of audits, the distribution of audit resources among various audit activities, and general guidelines for the scope of transaction testing and the deadline for audit completion. It must address operational scope and depth of the audit, which will vary across branch offices owing to variations in risk profiles, as well as the methods for identifying priority areas for preference examinations.

The policy should specify the methods and deadlines for adhering to audit findings, as well as the steps to be taken in the event that serious irregularities or failure to adhere to audit findings are committed. If the provision of incentives to employees is based on audit ratings and the performance of company leaders is assessed after taking into account the audit results, the audit function will be more advantageous.

The risk-based internal audit policy should, at the very least, cover the following topics, in brief:

1. Methodology for evaluating the risk of portfolios, business lines, and branch offices.
2. Standards for grading the portfolio, business lines, controlling office, head office department, and branches.
3. a methodology for managing audits of controlling offices and head office divisions.
4. Standards for prioritizing auditing tasks, offices, portfolios, and commercial sites for priority auditing.
5. selection of locations for a required audit, regardless of risk level.
6. timing and audit cycle.
7. Maximum permissible interval between two audits for low-risk operations and activities.
8. the degree of transaction testing in many operational areas.
9. Procedure for handling significant frauds and anomalies exceeding a threshold.
10. Timeframe for implementing audit recommendations, as well as penalties for late and incomplete compliance.
11. Norms for rewards and penalties that are consistent with auditor evaluations and remarks.

Structure of the Internal Audit Department

Compared to transaction-based auditing, risk-based auditing has a considerably wider reach and a more complex role. As a result, the internal audit department's organizational design should adhere to the specific needs of a risk-based audit. The following administrative concerns should be taken into consideration by banks when they decide the internal audit department's organizational structure:

1. The style of management and the business culture.
2. The audit department's need for independence.
3. The audit team's expertise needs.
4. The nature of the connection between the subsidiary units and the main office.

Some change management challenges arise when moving from transaction-based auditing to risk-focused auditing. Because the audit department does not generate income, it is often assigned a secondary rank, and the audit team does not have the proper position within the hierarchy. It is often seen as an unnecessary component that interferes with the operational staff's ability to do their jobs. The fundamental objective of the audit is defeated if this mentality permeates the company. Internal audit personnel are required to conduct a management audit of

the bank's regional offices and head office departments. During this process, they are also expected to carefully examine the decisions made by the bank's full-time directors and other senior management to evaluate their performance and report their findings in the management audit reports. If the results of the management audit are needed to be routed via the higher authorities in line with the hierarchical sequence, the independence and impartiality of the audit team will be compromised. The formality of passing the audit results along to the management executives who participated in the decisions under audit may compel the audit team to take a conciliatory stance and make concessions to the bank's business standards. So that its results are acknowledged, it is crucial to provide the internal audit department a high status. The high prominence accorded to the audit department would foster a feeling of responsibility among the employees at all levels and discourage them from engaging in misconduct. It is more acceptable if the head of internal audit reports directly to the board's audit committee or the board chairman, who is not a full-time employee of the bank.

Because the main goal of a risk-based audit is to thoroughly analyze the bank's risk management practices and carefully investigate each asset and liability from a risk perspective, its work is qualitatively different from that of a standard audit. The expertise of the staff members assigned to the audit department must thus correspond to the difficulty of the position. Typically, banks do not place much emphasis on hiring the right people for this area. If the management intends to make the risk-based audit meaningful, they must adopt a different attitude. In several nations, banks have formed nonbanking and banking subsidiaries, each of which is in charge of its own internal audit and has a distinct legal position. But since the parent office has the ultimate obligation to save the subsidiaries in times of trouble, the internal audit department at the parent office should have unrestricted access to the operations of the totally owned or majority-owned subsidiaries. In the absence of host country bank regulations requiring a separate arrangement for auditing offices situated in their country, the parent office may have a centralized internal audit department with the duty of auditing over branch offices and subsidiary units located overseas.

A permanent internal audit division that is adequate for a bank's size, complexity, and volume of activities should exist. To prevent conflicts of interest, the head of the audit department should not be an official with additional duties or be associated with risk management activities, and the audit department should refrain from participating in risk management and risk control operations. The risk management department and the internal audit department should be separated by a wall, with the latter being free to disclose sensitive discoveries, outliers, and excesses. From the perspective of objectivity and impartiality in the execution of the audit and in the reporting of the results, they should evaluate the effectiveness of the internal audit function. Internal auditors are anticipated to serve as internal consultants to enhance systems and practices. The dedication and motivation of the audit employees in carrying out their assigned task is influenced by the senior management's attitude toward the audit. If the top management puts significant weight on audit results, their morale will be high. Value-added services are now included in the scope of risk-based internal audit, which goes beyond compliance monitoring. Internal auditors may find possibilities for process improvements, efficiency benefits, and cost reductions by examining and evaluating risks. With suggestions for boosting risk management procedures, bolstering internal controls, and enhancing overall organizational performance, this expanded role places internal audit as a strategic partner to management.

The complexity of risk identification and assessment, resource limitations, and the changing nature of hazards provide difficulties in adopting a risk-based internal audit strategy.

Organizations must make sure that their risk assessment procedures are reliable, current, and in line with their strategic goals. In order to successfully manage the identified risks and provide value-added insights, they must also allot enough resources to the internal audit function. Organizations may gain from the efficient use of a risk-based internal audit methodology in a number of ways. It helps them to concentrate on the riskiest areas, improve the efficiency and efficacy of internal audit efforts, and provide stakeholders timely and relevant assurance. Additionally, it encourages responsibility, supports the fulfillment of strategic goals, and builds a risk-aware culture inside the firm[10], [11].

CONCLUSION

In conclusion, the scope, justification, and purpose of risk-based internal audits are crucial elements of a successful internal audit system. Internal auditors may provide focused assurance and insights that bring value to the company by matching the internal audit scope with the organization's principal risks. To effectively deploy a risk-based internal audit methodology and reap its advantages, firms must solve issues with risk identification, resource allocation, and ongoing risk assessment. Since the audit must concentrate on risk management and corporate governance concerns, the internal audit role has become more sophisticated over time. As it focuses on protecting profits and asset values that support financial stability, banks should migrate from the transaction-based internal audit system to the risk-based one. The risk-based audit is concerned with the assessment of risk management systems and control procedures as well as the selective transaction testing for compliance. The transaction-based audit is concerned with the detailed verification of transactions and accounts, compliance with rules and procedures, and the detection of irregularities. The bank management is forewarned by the risk-based audit system when it detects warning signs of high risk and insufficient control in specific exposures and operations. The internal audit department will need to develop its own methodology for risk assessment and risk rating of field offices, business activities, and portfolios and establish procedures to conduct a risk-focused audit. This will result in significant changes to how the department operates. To emphasize the value of internal auditing and encourage long-term survival, banks should develop a risk-based internal audit policy. They should give the internal audit department unique treatment in comparison to other departments and develop a clear strategy to assess employee performance and provide rewards while keeping the audit results in mind.

REFERENCES

[1] Amalendu Ghosh, “Risk-Based Internal Audit-Scope, Rationale, And Function,” In *Managing Risks In Commercial And Retail Banking*, 2015. Doi: 10.1002/9781119199250.Ch24.

[2] C. Cilli, S. Aldal, S. Fleginsky, And C. Ledesma, “IS Auditing Procedure: P8 Security Assessment - Penetration Testing And Vulnerability Analysis,” 2004.

[3] O. Hazzan *Et Al.*, “Preface,” *J. Syst. Softw.*, 2009.

[4] N. Betti And G. Sarens, “Understanding The Internal Audit Function In A Digitalised Business Environment,” *J. Account. Organ. Chang.*, 2021, Doi: 10.1108/JAOC-11-2019-0114.

[5] O. C. Olatunji And D. R. Adekola, “The Roles Of Auditors In Fraud Detection And

Prevention In Nigeria Deposit Money Banks: Evidence From Southwest," *Eur. Sci. Journal, ESJ*, 2017, Doi: 10.19044/Esj.2017.V13n31p290.

[6] B. Oyewo, O. Ajibola, And M. Ajape, "Characteristics Of Consulting Firms Associated With The Diffusion Of Big Data Analytics," *J. Asian Bus. Econ. Stud.*, 2021, Doi: 10.1108/JABES-03-2020-0018.

[7] T. Skobeltsyna And E. Zamiralova, "Use Of Internal Audit Processes To Improve The Economy Of Preschool Institutions," *CITISE*, 2020, Doi: 10.15350/24097616.2020.1.12.

[8] M. F. Safonova And A. Y. Alekseenko, "Statistical Techniques For Planning Internal Audit Engagements And Analytical Procedures Selection," *Accounting. Anal. Audit.*, 2021, Doi: 10.26794/2408-9303-2021-8-4-51-68.

[9] B. J. Cooper, L. Leung, D. Dellaportas, P. Burnaby, And S. Hass, "A Summary Of The Global Common Body Of Knowledge 2006 (CBOK) Study In Internal Auditing," *Manag. Audit. J.*, 2009, Doi: 10.1108/02686900910994782.

[10] M. O. F. Education, "Internal Governance And Role Of Internal Audit In Financial Institutions. Case Study: Risk Based Planning," *Ann. Univ. Oradea Econ. Sci.*, 2015.

[11] E. Li, H. Xu, And G. Li, "Analysis On Improvement Of Internal Audit In China's Listed Companies Based On Artificial Intelligence," 2020. Doi: 10.2991/Aebmr.K.200402.004.

CHAPTER 8

RISK-BASED INTERNAL AUDIT METHODOLOGY AND PROCEDURE

Dr. Yagnamurthy Raja
Assistant Professor, Masters in Business Administration,
Presidency University, Bangalore, India.
Email Id:narasimharaja@presidencyuniversity.in

ABSTRACT:

The risk-based internal audit methodology and procedure form the foundation of an effective internal audit function, enabling organizations to identify, assess, and mitigate risks systematically. A risk-based approach ensures that internal audit activities are aligned with the organization's key risks, providing relevant and valuable insights to stakeholders. This paper provides an overview of the risk-based internal audit methodology and procedure, highlighting their significance and the key steps involved in implementing a risk-based approach. It also discusses the challenges faced in adopting a risk-based internal audit methodology and the potential benefits of effective implementation. The risk-based internal audit methodology begins with a comprehensive risk assessment, which identifies and evaluates the organization's key risks. This assessment involves a thorough analysis of various risk factors, including financial risks, operational risks, compliance risks, and strategic risks. By understanding the organizations risk landscape, internal auditors can prioritize their audit efforts and allocate resources effectively. Based on the risk assessment, the internal audit procedure involves planning and scoping the audit engagements. This includes defining the objectives and scope of the audit, identifying key processes and control areas to be assessed, and determining the audit approach. The audit plan is tailored to focus on areas of significant risk exposure, ensuring that internal audit resources are directed towards areas that are most critical to the organization's objectives.

KEYWORDS:

Bank, Business Ethics, Management, Mitigation,Operational Risk.

INTRODUCTION

Internal Audit Methodology Based on Risk

The risk-based internal audit methodology and risk-based bank supervision methods are comparable in many ways. In both instances, thorough on-site inspection has been drastically scaled down, and the emphasis has switched from evaluating all transactions to focusing on particularly dangerous operational areas and controlling and scrutinizing sample transactions. The use of risk-based internal audit and risk-based bank supervision has reduced examination time and optimized audit resources. The examination reports draw attention to flaws in risk management and control methods, and the examination results are assessed to make system and procedure modifications.

The risk profile of banks and risk analysis of their operations and control are the first steps in the risk-based bank supervision process. Similar to this, the risk-based internal audit process starts with risk profiling of a bank's field offices, operational divisions, portfolios, and other functional units. These profiles are then analyzed to determine priorities and where attention should be

focused. The audit resources are concentrated on the important operations and regions of the bank, and an audit plan is created by prioritizing the audit's locations and activities based on risk profiles. In order to determine the frequency, extent, and depth of audits, banks must evaluate the business and control risks of each branch office and map the amount of hazards in a risk matrix to categorize them into low, moderate, high, and extraordinarily high-risk categories. To move to the risk-based internal audit system, they must perform the following actions[1]–[3].

1. Designing a risk-based auditing policy.
2. Building risk profiles for departments, business lines, and portfolios at branch offices, controlling offices, and head offices.
3. Creating audit strategies and analyzing risk profiles.
4. Determining the audit's scope.
5. Internal auditors doing the audit.
6. Reporting on audits is prepared.
7. Starting the remedial action process.
8. Assessment of audit results to improve systems and processes.

Branch office risk profiles should be compiled and analyzed by the bank's internal audit department before the actual audit. The department should independently examine the risks associated with all functional units, portfolios, and business lines. The internal audit department's risk profile document should be verified by the audit team, and the risk profile should be approved or revised. The risk profiling exercise should be conducted by the department in a methodical and organized way, and the risk profile document should include all pertinent data and information on how the branch office operates, as well as critical remarks on the areas that should raise alarm. By creating templates for risk profile and standards for grading risk components, banks must preserve impartiality in rating and consistency in the execution of the technique for evaluating branch offices.

Banks have a variety of branch offices; some exclusively handle a certain sort of business, while others handle all business. As a result, they should divide the branch offices into several groups according to the services they provide, such as full function and limited function branch offices, industrial and agricultural financing branch offices, foreign branch offices, etc. Because these branch offices serve different purposes, the dangers they encounter will likewise vary in sort and severity. For instance, credit risk is the most significant risk in the industrial finance branch, but country, transfer, and foreign currency risk are more significant risks in the overseas banking branch. Because risk variables fluctuate across branch offices owing to functional variances, banks should develop unique templates for risk profiling of various kinds of branch offices. In order to achieve impartiality and precision in the evaluation of branch offices, they will next finish the chart for assigning weights to risk factors and risk components in accordance with their relative relevance.

Compared to controlling offices and operational divisions, branch offices face various business risks as well as control and compliance issues. A bank's branch office may be located in a challenging area where there are multiple branch offices of rival banks operating and where there is fierce competition for a bigger portion of the market. The business climate is not suitable to achieving company goals if the customers' attitudes and business ethics are poor in the branch office's command region. On the other hand, if a better business climate prevails and the customers uphold business ethics, it is considerably simpler for the branch offices to accomplish

commercial development. As a result, a branch office's operating environment is a significant risk element that banks should be aware of when risk profiling.

Branch offices are subject to varied levels of control and compliance risk, as well as credit risk, liquidity risk, profits risk, and operational risk. Therefore, when creating templates for risk profiling, banks should identify the various risks that various branch office types face, ascertain their relative importance, and subsequently assign weights to risk factors and risk elements. They should also calculate weighted scores and award ratings in a predetermined rating scale.

Here are the sequential processes for compiling branch office ratings:

1. Determine the risk elements that apply to a branch office and that make up the business risk, control risk, and compliance risk.
2. Determine the risk components that make up each control and compliance risk factor and business risk.
3. Create standards for allocating ratings to each risk factor.
4. Establish the weights that should be given to risk components and risk variables.
5. Adopt a suitable grading system.
6. Work up weighted scores for each business risk, control risk, and compliance risk component, then rate each risk factor using the scale.
7. Combining individual risk factor ratings will provide overall ratings for business risk, control risk, and compliance risk components.
8. Compile the scores for the business risk, control risk, and compliance risk.
9. Components of a matrix for a composite risk assessment.
10. Calculate the total score that applies to the branch office.

DISCUSSION

Identifying Risk Elements and Risk Factors

Business risk and control and compliance risk are the two main risk components included in the models for assessing the risk of branch offices. Operational risk can be included in business risk for the limited purposes of branch office rating because, in most branch offices, operational risk factors are limited to control and compliance risk, which is included in the rating model as a separate risk component and takes into account many operational risk events. Several risk variables, including business environment risk, business strategy risk, credit risk, liquidity risk, profits risk, and operational risk, make up the business risk component of a fully functional branch office. Foreign currency risk and nation risk will also be present in the event of a foreign branch office or an overseas branch office. The risk associated with control and compliance will also include a few risk variables. The branch offices' control and compliance risk will be present in the division of labor, use of loan sanction authority, control of credit, access to vaults and computers, handling of ledgers and other records, reporting of transactions, submission of periodic returns/business reports, surveillance of fraud hotspots, adherence to anti-money laundering laws, and other areas. Each business risk and control and compliance risk component will therefore be present. For instance, credit risk is a factor in business risk, and the risk factors that make up credit risk are the rate of credit growth, the caliber of credit appraisal and follow-up, the volume of large exposure, the volume of capital market exposure, the volume of exposure to commercial real estate, the degree of credit concentration, the trend of non-performing accounts, the occurrence of new non-performing loans in the current year, the success of non-

performing loan recovery, and so on. For the purpose of compiling ratings, banks must appropriately identify risk factors and risk aspects relevant to each kind of branch office[4]–[6].

Weights Are Assigned to Risk Factors

Due to changes in operations and roles, business risk factors may differ across branch offices, but risk factors for control and compliance will generally be the same. The risk variables that make up the business risk of various branch office types must be identified by banks, and their relative significance must be determined. Assume that a branch office's business risk is composed of the following five major risk factors: operational risk, profits risk, credit risk, liquidity risk, and risk related to the business environment and strategy. Since the business operations that are exposed to market risk are often centered in the head office or the corporate office, market risk is not included as a risk factor since it typically does not apply to a branch office. The relevance of each risk component that makes up business risk is not equal when determining the risk level. At the branch offices, for instance, credit risk and operational risk are given greater weight because they are more significant than liquidity risk and profitability risk. For the purpose of calculating the business risk and control and compliance risk component ratings, banks must assign risk weights to various risk elements that relate to the branch offices and make up the business risk and control and compliance risk components. The indicative weighting of the five risk components that make up the business risk component, totaling 100. In a similar way, banks must determine the risk variables that make up the control and compliance risk component and give each risk element a weighting. The risk factors for control and compliance will often be shared by all of the branch offices. Control and compliance risk component, like business risk component, has a total risk weight of 100, which is divided across various risk elements in line with their relative relevance.

Weights Are Assigned to Risk Factors

There are a number risk component that make up each business risk, control, and compliance risk factor, but not all of them are equally significant for determining the degree of risk connected to that risk factor. Some risk factors are crucial and more significant than others, and as a result, they are given greater weight. Examples of significant risk elements of the credit risk factor that should be given higher weights than the risk elements like credit growth, amount of off-balance-sheet exposure, and so on are quality of credit appraisal, intensity of credit supervision and follow-up, volume of large exposures, volume of sensitive-sector exposures, extent of credit concentration, and incidences of nonperforming loans. such that the branch office's estimated level of credit risk accurately reflects the circumstances. The distribution of weights among the many risk components that make up each business risk and control and compliance risk factor may then be standardized by banks. For instance, the many risk components that make up the credit risk factor are to be allocated according to risk weight 45.

Rating of Risk Factors

Banks may calculate the sum of the weighted scores assigned to the risk components that make up a risk factor, map that score against the rating scale, and then award a rating to that risk factor. The following actions may be taken by the bank if it wishes to rate the branch office's "credit risk" risk factor:

1. Each risk factor that contributes to credit risk should be given a score in line with the scoring norm table, based on a risk assessment.
2. Give risk factors weights in accordance with the authorized weight distribution pattern.
3. To get the risk-weighted scores each risk factor got, multiply the scores by the weights.
4. Obtain the total of the weighted scores.
5. Calculate the percentage using the highest weighted score possible.
6. Using the proportion of the risk-weighted score, rate the credit risk factor.

Additionally, based on the assigned weights and scores, banks may determine the proportion of scores obtained by each business risk and control and compliance risk component, and then give a rating to each risk factor in the four-scale rating framework in line with the percentage of score. After assigning ratings to each risk element, banks may use the method described in the following section to get the branch's overall risk rating. Branch offices will be classified as "moderate risk" if the business risk component for that branch office has a weighted score of greater than 60% and less than 75%. The rating of the control and compliance risk component is obtained in the same manner. The business risk is moderate and the control and compliance risk is high if the weighted score for the business risk component is 62% and the score for the control and compliance risk component is 55%. Banks may determine the branch office's composite risk rating by combining these two scores. In this instance, the branch office's overall risk rating is high because, despite the business risk being moderate, high control and compliance risk will lead the overall rating to go up a grade.

Given that lose control and a failure to comply with laws and regulations have the potential to result in considerable losses, it is logical to infer that control and compliance risk is more important than commercial risk when grading a branch office. If there are extremely strong controls and a high degree of compliance, that is, if the risk of control and compliance is very low, the severity of loss from high business risk may be decreased. The branch office's composite rating is very high if the control and compliance risk is also high, and it is extremely high if both are high. The business risk is very high. The composite grade is moderate if the business risk is high but the control and compliance risk is low.

One aspect of the risk assessment is the categorization of branch offices into low, moderate, high, very high, very high, and extremely high-risk categories. The second component deals with the risk classification of company operations and branch offices in line with the anticipated frequency and severity of risk occurrences. Banks must assess these two factors in order to pinpoint branch locations and business operations that are at high risk. Some risky situations happen often and have a significant effect. For instance, a bank's treasury branch would be classified as high-frequency, high-risk if its dealing authorities often go beyond transaction limitations or maintain large overnight open holdings in foreign currency. On the other hand, certain risk occurrences happen often yet have little significance. For instance, granting loans to borrowers in excess of their financial capabilities by branch office loan officers is a high-frequency, low-impact event because it occurs frequently at almost every branch office of a bank, but the risk is low overall as the loan amounts are moderate. Risk frequency and impact may occur in a variety of combinations, including low frequency, high impact, high frequency, low impact, and moderate frequency, moderate impact. Branch offices and other operating locations should be categorized by the internal audit department according to the frequency and severity of risk events. This kind of risk evaluation need to include company operations like treasury and foreign currency, derivatives, credit cards, merchant banking, commercial real estate financing,

capital market finance, and so forth. Banks should prioritize audits and establish audit cycles after classifying branches according to the frequency of risk occurrences and the severity of the effect[7]–[9].

Inputs for Risk Profiling

Prior to starting the actual audit, the internal audit department should gather the risk profiles of the operating departments and branch offices. Since the audit department is responsible for independent risk profiling, it should have access to all data pertaining to the operations of the bank and the branch offices.

Audit Planning and Scope Based on Risk

The internal audit department must create a proper audit plan that takes into account the resources at hand and determine the sequence in which the offices and activities will be audited. Prior to the audit year starting, the department should finish risk profiling branch offices, portfolios, and business lines based on the inputs available, rank the offices and activities based on risk categorization and the materiality of the business, and then analyze the profiles to determine the focus and coverage of the audit. Banks must create an audit plan that can be carried out throughout the audit year and standardize the audit's scope in accordance to a branch office's duties, risk category, and risk propensity. The topics pertaining to the planning and scope of risk-based audits are covered in this section.

Planning an Audit Based on Risk

The data and findings from the branch office risk profile analysis serve as the foundation for developing the internal audit strategy specific to the audit year. Risk profile analysis highlights the aspects of the branch offices' operation that need immediate and focused attention. In order to prioritize audit operations, banks should develop risk profiles for each of their branch offices, determine their risk category distribution, and identify high-risk transactions and risky business ventures. The risk profiles should include both quantitative and qualitative data on how the branch office is operating and how it has performed since the previous audit. The quantitative portion should include general information on business growth, asset-liability composition, cost-income trend, nonperforming loans, as well as details on risk-sensitive topics like significant credit exposures, credit concentration, risk-grade distribution of credit, fraud and asset and valuables misappropriation, etc. The qualitative portion should draw attention to procedural inconsistencies, a decline in asset quality, poor branch office management, a blurring of responsibility boundaries, and inadequate supervision and compliance. The data in the quantitative and qualitative sections of a branch office's risk profile will be used to determine the audit cycle, level of scrutiny, scope of transaction testing, and deadline for completion of the audit.

The division of branch offices into distinct risk categories and the materiality element in determining audit priority should be taken into consideration by banks when drafting the audit plan. According to the risk-based auditing concept, audit resources should be focused on high-risk operational areas and places where there is a considerable amount of business that has to be attended to right away. Along with high-risk operations and exposed sectors of business, banks should give emphasis to branch offices that are very dangerous and linked to frequent, large-scale risk occurrences. In order to organize them for audit by turn, they should categorize the

branch offices and the business operations according to the descending order of risk category, frequency of risk occurrences, and size of risk.

The audit plan should include, in addition to special audits and targeted scrutiny, when necessary, the timetable and sequence of branch office audits, the justification for allocating audit priority, and a time budget for audit completion. Branch offices should be inspected more often for those in the moderate and low-risk categories, and less frequently for those in the high, very high, very high, and extremely high risk categories. Banks should not adopt a complacent attitude toward low-risk branch locations and set a protracted audit cycle. They must be aware that low-risk branch offices or those with modest business volumes may have considerable dangers that are concealed or unnoticed. To ensure that every branch office is audited at least once every three years, the plan must call for the audit of a minimum number of low-risk, low-transaction branch offices each year. Banks should uphold the purity and integrity of the internal audit department's audit plan and staff it with qualified personnel to carry out the role as outlined in their risk management and risk-based internal audit policies.

Scope of a Risk-Based Audit

Based on risk profiles that may differ in emphasis and coverage across the branch offices, the internal audit department should choose the internal audit's scope. The risk profile won't provide an accurate picture, and the goal of the risk-based audit may not be met if the data used to compile it were inaccurate or some crucial information was missing. The risk profile created by the audit department based on data and information available at the branch office should be verified by the audit team during the audit and modified as necessary. Therefore, the audit team's reevaluation of the business risk as well as the control and compliance risk of at least major and large-size branch offices should be included in the scope of internal audit. The results of the reevaluation will show how much the risk profiles can be trusted to execute the program of risk-focused internal audit.

The audit department should concentrate on the current status of significant irregularities discovered during the most recent internal audit, negative aspects mentioned in the most recent external audit report and the supervisory authority's examination report, as well as branch office failures to follow the established systems and procedures, when summarizing the issues for special examination during the course of audit. It should draw attention to the issues surrounding accepting faulty and incomplete documentation, failing to monitor how borrowers use their money in the end, inadequate supervision and follow-up of loans and advances, delays in standard advances, lax control over areas that are vulnerable to fraud, breaking anti-money laundering laws, and failing to keep an eye on who has access to the bank's valuables and computer systems.

To lessen the disparities in audit coverage, banks should standardize the scope and coverage of internal audit in line with the risk classification of branch offices. The audit will be objective and transparent in addition to being thorough if the scope and coverage are standardized in accordance with the risk categories of branch offices. The bank should outline in the audit policy the criteria for special investigation and intense scrutiny, as well as the scope and coverage of audits pertaining to branch offices, business lines, and portfolios. The bank should also prepare standardized lists of issues and concerns that should be investigated during the audit, which will be fairly common.

In order to address the concerns pertaining to conflicts of interest among the operating staff, the reporting staff, and the controlling staff, the scope of the audit should include a critical examination of the application of internal control procedures at the branch office and its methods of operation. This internal audit job entails an unbiased assessment of the control and compliance risk inherent at branch offices. The evaluation of compliance with legal and regulatory requirements, policies and practices, strategies and limitations, anti-money laundering laws and regulations, and the results of the prior audit are all included in the scope[10].

CONCLUSION

The audit team should evaluate the quality and content of the branch office financial and performance reports sent to higher authorities, the process used to input data and other information into the computer network system for the creation of management information reports and borrower rating reports, and the security of the electronic information system in use at the branch office. The audit's scope will include an evaluation of the controlling offices' and head office departments' effectiveness in managing risks as well as a critical study of how they operate. The internal audit department should pinpoint weaknesses in handling business, control, and compliance risks as shown in the audit reports of various offices, recommend corrective actions that should be taken by the operational departments, and then assess the efficacy of those steps.Conducting the audit fieldwork is the next phase in the risk-based internal audit approach. Internal auditors thoroughly test and analyze controls, procedures, and transactions to determine how well they mitigate uncovered risks. In order to achieve this, it is necessary to examine the paperwork, conduct personnel interviews, data analytics, and sample testing. The auditing processes are intended to provide a fair level of confidence about the performance of internal controls and the control over important risks. Internal auditors also spot control flaws, inadequacies, or opportunities for improvement during audit fieldwork. They inform management of these conclusions and provide suggestions for increasing controls, reducing risks, and boosting operational effectiveness. The risk-based internal audit technique relies heavily on this communication because it makes it possible for management and auditors to work together to solve problems and effect positive change. Obtaining accurate and trustworthy risk information, managing resource restrictions, and responding to changing hazards and business settings are all difficulties in implementing a risk-based internal audit process. To keep the internal audit technique current, organizations need to set up reliable risk assessment procedures, provide access to high-quality data, and regularly update their risk profiles. Organizations may gain from the efficient use of a risk-based internal audit approach in a number of ways. By concentrating on the riskiest areas, it improves the value of the internal audit function by ensuring that audit efforts are focused where they are most required. Additionally, it gives stakeholders timely and pertinent information, encourages informed choice, and strengthens the organization's overall risk management and control environment. To sum up, a successful internal audit function relies heavily on the risk-based internal audit methodology and process. Internal auditors may provide focused assurance, insightful suggestions, and help for risk reduction by coordinating audit efforts with the organization's major risks. To effectively adopt a risk-based internal audit methodology and optimize its advantages for the business, it is crucial to overcome issues related to risk assessment and resource allocation.

References

[1] N. A. M. Puad, Z. Shafii, And N. I. Abdullah, "The Practices Of Risk-Based Internal Shariah Auditing Within Malaysian Takaful Operators: A Multiple Case Study," *Int. J. Acad. Res. Bus. Soc. Sci.*, 2020, Doi: 10.6007/Ijarbss/V10-I7/7396.

[2] A. Brown, M. Santilli, And B. Scott, "The Internal Audit Of Clinical Areas: A Pilot Of The Internal Audit Methodology In A Health Service Emergency Department," *Int. J. Qual. Heal. Care*, 2015, Doi: 10.1093/Intqhc/Mzv085.

[3] A. V. Petukh, M. F. Safonova, And V. A. Gribushenkova, "Planning Of The Internal Audit Of Supply Chain Management In Foreign Economic Activity: Theory And Practice (Internal Audit Planning)," *Int. J. Supply Chain Manag.*, 2020.

[4] G. D. Vasilescu *Et Al.*, "Methodology For Assessing The Degree Of Occupational Safety Specific To Hydrotechnical Construction Activities, In Order To Increase Their Sustainability," *Sustain.*, 2021, Doi: 10.3390/Su13031105.

[5] A. Karmudiandri, "Peranan Audit Internal Dalam Manajemen Risiko Bank," *Media Bisnis*, 2014.

[6] D. H. Akbulut, K. Ozoner, And I. Kaya, "Big Data Analytics In Internal Audit," *Pressacademia*, 2018, Doi: 10.17261/Pressacademia.2018.893.

[7] S. Mitrovic And V. P. Suits, "A Methodology For Applying Modern Information Technologies In The Economic Analysis Of Organization's Risks," *Econ. Anal. Theory Pract.*, 2020, Doi: 10.24891/Ea.19.2.268.

[8] V. Fedorcova, "Audit In The Conditions Of Digital Economy," *Vestn. Volgogr. Gos. Univ. Ekon.*, 2020, Doi: 10.15688/Ek.Jvolsu.2020.2.18.

[9] V. Nevidomyi, Y. Myronenko, K. Kanonishena-Kovalenko, And Y. Horobchuk, "Implementation Of International Standards Of Supreme Audit Institutions To The Financial Audits Of The Accounting Chamber Of Ukraine," *Bull. Taras Shevchenko Natl. Univ. Kyiv. Econ.*, 2020, Doi: 10.17721/1728-2667.2020/208-1/4.

[10] D. Schroeder And T. Singleton, "Implementing The It-Related Aspects Of Risk-Based Auditing Standards," *Cpa J.*, 2010.

CHAPTER 9

A SUMMARY OF CORPORATE GOVERNANCE: A FEW FUNDAMENTALS

Dr. Varsha Pratibha
Associate Professor,Masters in Business Administration,
Presidency University, Bangalore, India.
Email Id:varsha.ps@presidencyuniversity.in

ABSTRACT:

The policies, procedures, and practices used to oversee and manage businesses are collectively referred to as corporate governance, which is a crucial component of organizational management. In order to ensure transparency, accountability, and ethical conduct inside organizations, this paper summarizes the basic concepts, elements, and relevance of corporate governance. Corporate governance is fundamentally built on a set of values that regulate interactions between shareholders, management, the board of directors, and other stakeholders. These values protect the rights of shareholders and encourage justice, honesty, openness, and accountability in the decision-making process. Companies seek to develop sustainable value, increase stakeholder trust, and promote long-term success by adhering to these principles. One aspect of running a firm is corporate governance. Good Fairness, openness, and transparency are encouraged by corporate governance when it comes to its obligations to stakeholders. By concentrating on activities that provide value, good corporate governance processes promote economic efficiency and help in the effective distribution of limited resources. This is accomplished through businesses using their resources effectively, attracting low-cost capital, fulfilling society expectations, and enhancing overall performance. The critical challenges in corporate governance that contribute to achieving these goals are covered in this study.

KEYWORDS:

Bank, Business, Corporate Governance, Management, Mitigation,Operational Risk.

INTRODUCTION

The components of corporate governance include the roles and responsibilities of various entities within the organization. The board of directors plays a crucial role in providing oversight, strategic guidance, and accountability. Independent directors, who are free from conflicts of interest, bring objectivity and diverse perspectives to the decision-making process. Management, led by the CEO and senior executives, is responsible for implementing the board's directives, executing business strategies, and ensuring effective risk management and compliance.According to the Oxford Dictionary, "corporate" is an adjective that describes a company, while "governance" is an act that performs a governing role. Since the word "governance" comes from the Latin verb "gubernare," which means "to steer," it is implied that corporate governance comprises more of a directing role than a controlling one. As a result, corporate governance is a component of corporate management[1]–[3]. Corporate governance, which is concerned with the structures and practices connected to the course that a company chooses to pursue, includes the issues of accountability, ethics, and social responsibility to

society and stakeholders. Fairness, accessibility, and transparency are encouraged by corporate governance when it comes to stakeholder obligations.

The awareness that sound corporate governance necessitates consideration of the impact a business has on the larger community and the environment has been strongly related to the development in significance of a firm's environmental reporting. Regardless of how it is defined, corporate governance refers to the fundamental procedures by which ultimate corporate authority and responsibility are shared and exercised by shareholders, directors, and management in order to make sure that the assets provided by investors to the company are used in an efficient and effective manner. The notion of corporate governance has diverse meanings in various nations, despite the fact that it refers to actions on how to effectively control a firm in the benefit of its stakeholders. For instance, corporate governance in Anglo-Saxon nations like the United States (US) and United Kingdom (UK) is centered on shareholder interests. Corporate governance focuses on a larger view of stakeholders, including workers, consumers, and shareholders, in other nations like Japan, Germany, and France. business governance is now crucial for improving ethical, truthful, and open approaches to achieve business objectives and survival in the face of increased global competition. For a workplace to be organized, effective, accountable, and responsible, good governance is crucial. The significance of promoting good governance has been made clear by sociopolitical shifts during the previous 20 years.

Over the last several decades, 2 nations have developed their capital markets and participated in financial liberalization, setting an example for other emerging nations to follow. However, during the prosperous economic period, the 1997/1998 financial crisis exposed their shortcomings in enforcing effective corporate governance practices (such as poor transparency and disclosure, a lax regulatory framework, underdeveloped market infrastructures, cronyism, nepotism, and the moral hazard of politicians making economic decisions). In systems that largely depend on "crony capitalism," policymakers have learnt that persistent failures of investor protection measures, coupled with lax capital market regulation, may result in failures of trust that extend from specific companies to whole countries. Lending and investing practices based on relationships rather than a careful analysis of risk and reward were supported by inadequate financial disclosure and capital market regulation, a lack of minority shareholder protection, and a board and controlling shareholder accountability failure.

Many Asian nations have implemented formal corporate governance rules as a result of the lessons learnt from the crisis in an effort to restore trust in their business sector. The viewpoint of corporate governance systems in developed countries goes beyond these conventional elements and also takes good corporate citizenship into account. This includes environmental preservation, weighing the interests of all parties involved fairly, and committing to innovation that will result in better use of both natural and human resources. Businesses that uphold the highest standards of corporate governance by incorporating social, environmental, and economic principles into all of their decision-support systems are more likely to improve the value of their shareholders over the long term by managing risks and opportunities more effectively. After the financial crisis of 1997 and other business failures in industrialized nations, the government in Malaysia has given the topic of corporate governance its full attention. A testament to this dedication is the Malaysian Code on Corporate Governance's implementation in 2001. All facets of governance that may increase investor trust in our business sector were given the necessary consideration and enforcement. As markets become more competitive on a global scale, most nations are relying more on the private sector to spur economic development.

Corporate governance develops into a crucial manual for assisting economic companies to use resources effectively, draw in low cost capital, satisfy social expectations, and enhance overall performance. Through accountability and openness, good corporate governance should enable management to act in the corporation's best interests and promote economic growth. According to the company, the importance of good corporate governance seems to result in greater shareholder value due to improved stock selection (McKinsey, 2002). According to Ganesan (2003), there are five main benefits of good corporate governance for an organization: (i) establishing and enhancing a corporation's competitive advantage; (ii) protecting shareholders' interests; (iii) influencing the enterprise's valuation; (iv) enabling an organization to operate effectively and prevent fraud; and (v) ensuring compliance with laws and regulations. Regardless of the company's goal, good governance makes sure that management and boards are responsible for all choices that affect the goal. By encouraging the efficient use of limited resources for the creation of the products and services that are most in demand, effective corporate governance will maximize the wealth of stakeholders.

DISCUSSION

Corporate managers must create novel tactics on the spot to adapt to shifting customer expectations if they are to thrive in cutthroat marketplaces. To make judgments within the framework of current rules, regulations, and stakeholder expectations, managers must have some discretion. This calls for a formalized, impartial system to oversee managerial choices, openness on the ownership, control, and performance of the company, as well as shareholder involvement in certain key choices. As a result, corporate governance may be a useful tool for monitoring and holding managers and boards responsible for the management of company assets. Improved business performance should result from this monitoring and accountability, better resource use, more access to lower cost capital, and enhanced responsiveness to social demands and expectations. Because there are so many other elements that might affect performance, corporate governance may not always result in better corporate performance at the level of the individual firm. However, it should increase the likelihood that the firm will react quickly to changes in the marketplace, crises, and the inevitable times of decline. It should assist decrease management complacency and enable managers to concentrate on enhancing company performance while being aware that they will be fired if they fail to meet their commitments. Corporate governance that is effective would lessen corruption in company transactions. Corrupt activities in business and political circles are fostered by bad corporate governance. Effective corporate governance makes it easier to spot and stop these abuses early, creating a more favorable climate for both local and international investors[4]–[6].

Corporate Governance Essentials

Corporate governance is often discussed in industrialized nations in relation to the legal framework intended to support economic development. Governance is viewed in the context of laws that acknowledge shareholders as the rightful owners of the company and call for fair treatment of minority and foreign shareholders; enforcement mechanisms that can be used to uphold these shareholder rights; securities, corporate, and bankruptcy laws to prevent bribery that allow corporations to change; anticorruption laws to prevent bribery and protections against fraud on investors; sophisticated court Developed nations are also more likely to have well-established private sector institutions, including organizations for institutional investors, professional associations for directors, corporate secretaries, and managers, as well as rating

services, security analysts, and an advanced financial press to support best practices. The majority of developing and emerging market countries, like Malaysia, still need to build their market micro-infrastructure, which includes the institutions needed in the private sector and in the legal and regulatory systems, enforcement capabilities, and corporate governance systems. Therefore, initiatives to improve corporate governance in these countries often need to concentrate on the basic structure. The development of basic stock exchanges, systems for registering share ownership, laws enacting basic minority shareholder protection from potential self-dealing by corporate insiders and controlling shareholders, financial press education and empowerment, better audit and accounting standards, a shift in culture and laws prohibiting bribery and corruption as an accepted form of doing business are just a few examples of reforms that may be necessary[7]–[9].

Nations vary greatly in the cultural values that shape the development of their financial infrastructure and corporate governance, in addition to variances in the market micro-infrastructure needed to properly enforce good governance practices. Due to these cultural variations, governance techniques must be improvised in order to accommodate local needs. Corporate governance, as well as the framework that underpins it, must ultimately be relevant to each nation's particular legal system. While some market-driven convergence of systems may be necessary, it must be in accordance with each country's and the private sector's requirements. Common characteristics of efficient governance may be discovered to allow national systems to attract global capital and heighten investor trust. Transparency and disclosure are fundamental aspects of corporate governance. Companies are expected to provide accurate and timely information to shareholders and the public, allowing stakeholders to make informed decisions. Financial reporting, including audited financial statements, plays a vital role in promoting transparency and trust in financial markets.

Corporate governance practices vary across jurisdictions, and many countries have established codes, guidelines, and regulations to promote effective governance. These frameworks provide recommendations on issues such as board composition, executive compensation, risk management, and shareholder rights. Compliance with these standards is important for companies to build credibility, attract investment, and ensure regulatory compliance. The significance of corporate governance extends beyond the individual company. Good corporate governance practices contribute to the overall health and stability of financial markets, as they promote investor confidence, reduce the risk of fraud and misconduct, and enhance market integrity. Sound corporate governance practices also foster ethical behavior, social responsibility, and positive relationships with employees, customers, suppliers, and the broader society. While corporate governance frameworks provide a solid foundation, challenges persist in implementing effective governance practices. These challenges include ensuring independence and diversity within the board, aligning executive compensation with performance and long-term value creation, and striking a balance between short-term financial objectives and long-term sustainability goals.

CONCLUSION

In conclusion, corporate governance is an essential aspect of organizational management, emphasizing transparency, accountability, and ethical behavior. By adhering to its fundamental principles and components, companies can enhance their performance, build stakeholder confidence, and contribute to the overall health and stability of financial markets. Continuous

evaluation, improvement, and adaptation of corporate governance practices are essential to meet evolving business dynamics and societal expectations.

Corporate governance is a collection of procedures, laws, and rules that affect how businesses are managed and administered. Corporate governance, to put it simply, is the process through which managers operate their companies effectively and efficiently. This essay explores the significance of the key concerns with corporate governance. Additionally, it discusses the critical components of sound governance in both developed and developing nations as well as the contribution of governance to increased economic efficiency. Due to the recent wave of corporate scandals, there has been a resurgence in interest in corporate governance both worldwide and in Malaysia. How vulnerable Malaysian firms are to changes in the capital market and how their failures are ascribed to lax corporate governance standards were made clear by the Asian Financial Crisis of 1997–1998. Global governments are paying close attention to this problem and have taken a number of steps to maintain the public's trust and confidence in their national financial markets. The Malaysian government has taken a number of steps to address governance needs, including the introduction of the Malaysian Code on Corporate Governance and revisions to the Bursa Malaysia Listing needs. Good corporate governance will assist in ensuring that appropriate and effective systems are in place that facilitate efficient use of limited resources to increase long-term shareholder value, in line with the general public expectation of fairness in business dealings, transparency in financial reporting, management accountability, and socially responsible corporate.

REFERENCES

[1] R. Kulkani and B. Maniam, “Corporate Governance — Indian Perspective,” *Int. J. Trade, Econ. Financ.*, 2014, doi: 10.7763/ijtef.2014.v5.399.

[2] C. Flammer, B. Hong, and D. Minor, “Corporate governance and the rise of integrating corporate social responsibility criteria in executive compensation: Effectiveness and implications for firm outcomes,” *Strateg. Manag. J.*, 2019, doi: 10.1002/smj.3018.

[3] L. D. Brown and M. L. Caylor, “Corporate governance and firm valuation,” *J. Account. Public Policy*, 2006, doi: 10.1016/j.jaccpubpol.2006.05.005.

[4] F. D. Lipman, “Summary of major corporate governance principles and best practices,” *Int. J. Discl. Gov.*, 2007, doi: 10.1057/palgrave.jdg.2050064.

[5] G. J. Martin, “Summary: Ecologization Of Corporate Governance: Toward A Reviewal Of The Issue?,” *Rev. Int. Droit Econ.*, 2021, doi: 10.3917/ride.352.0257.

[6] Z. Ping and C. W. W. Andy, “Corporate governance: A summary review on different theory approaches,” *Int. Res. J. Financ. Econ.*, 2011.

[7] U. A. Mustapha, N. Rashid, A. B. Ado, and S. A. Lateef, “Development of corporate governance and the effect of corruption on the Nigerian financial institutions,” *J. Adv. Res. Dyn. Control Syst.*, 2020, doi: 10.5373/JARDCS/V12I1/20201003.

[8] Tencent Holdings Limited, “Tencent Annual Report 2016,” *2016 Annu. Rep.*, 2017.

[9] I. Parachkevova-Racine, “Summary: Why Is The Rise Of Sustainable Corporate Governance Inevitable?,” *Rev. Int. Droit Econ.*, 2021, doi: 10.3917/ride.352.0129.

CHAPTER 10

AN OVERVIEW ON CORPORATE GOVERNANCE

Dr. Vinay Muddu
Professor, Masters in Business Administration,
Presidency University, Bangalore, India.
Email Id:muddu.vinay@presidencyuniversity.in

ABSTRACT:

Corporate governance is a critical framework that guides the way organizations are managed, controlled, and operated to ensure transparency, accountability, and ethical behavior. This study provides an overview of corporate governance, highlighting its significance and key components. It discusses the principles, structures, and practices that contribute to effective corporate governance and its impact on organizational performance, stakeholder confidence, and long-term sustainability. Corporate governance encompasses a set of principles and guidelines that define the relationships between shareholders, management, the board of directors, and other stakeholders. It establishes a framework for decision-making, risk management, and the protection of stakeholders' interests. Key components of corporate governance include clear roles and responsibilities, independent oversight, transparent reporting, and mechanisms for accountability. The principles of corporate governance revolve around fairness, integrity, transparency, and responsibility. They promote ethical behavior, responsible business practices, and the protection of shareholders' rights. These principles guide organizations in maintaining a balance between the interests of various stakeholders, including shareholders, employees, customers, suppliers, and the broader society.

KEYWORDS:

Bank, Business, Corporate Governance, Mitigation,Operational Risk, Risk Management.

INTRODUCTION

Concept of Corporate Governance

Corporate governance refers to the laws, regulations, and rules that are put in place to ensure that a firm is conducted ethically and in the best interests of its shareholders and other stakeholders. It describes a form of government where the board of directors and top management are required to strictly adhere to set policies and procedures and operate the company effectively while abiding by legal and regulatory requirements. Senior executives are expected to take the initiative in leading the company. The management devised internal processes to assure adherence to the laws, while the rules and regulations are a component of the legal system. The focus of the corporate governance process is on the sincerity of the management in developing strong business processes and procedures and sticking to them in order to accomplish the company objectives since it is founded on good principles, ethics, and values. The key elements that are assessed to determine the caliber of corporate governance procedures are the transparency of company transactions and administration, the application of staff administration policies without prejudice, and compliance with good governance regulations. A basic level of governance is implied by corporate governance. Bad management practices, which are devoid of ethics and

values and endanger the organization's long-term viability, are basically what bad corporate governance refers to[1]–[3].

In order to foster good governance, banks should strongly prohibit greed, corruption, and nepotism and strongly support integrity, honesty, and transparency. They should also create a friendly work atmosphere. Senior bank executives often seek to follow impartial, merit-based business processes and administrative procedures, but influence from promoters and outside directors distorts the administration's impartiality and degrades the workplace atmosphere. A company's top management must contend with two competing forces every day, and when the bad forces prevail over the sound principles of governance, business tragedy results. Banks must operate in a suitable atmosphere if they are to adhere to ethical corporate governance principles. Three parties are accountable for building a framework that allows banks to act ethically when we speak about corporate governance in banks. The three partners that affect the environment in which the banks do their business are the federal or central government, the state government, and the bank regulator. The state government is in charge of upholding law and order and delivering utility services, the federal government is in charge of preserving macroeconomic stability, and the bank regulator is in charge of fostering the stability of the financial system.

Since corporate governance is a collaborative process, these authorities and the financial institutions must work in harmony. The efficacy of the legal system in resolving individual concerns as well as the media's and shareholders' vigilance in reviewing management decisions are all significant components that support the corporate governance system. If all four organizations the federal government, the state government, the bank regulator, and the banks themselves view their respective roles in the right light and foster a climate where the interests of depositors, bondholders, shareholders, employees, and the government are protected, governance will improve. The government seeks socially fair economic development, and banks are expected to actively participate in it. That duty must be shared by banks, but within acceptable bounds. Government budgetary resources that promote economic development cannot be replaced by resources from the financial sector. A strong legal environment with effective enforcement machinery that is aware of willful violation of contracts, agreements, and other laws and regulations and ensures prompt remedial and punitive action will prevail if there is an appropriate sharing of responsibilities between the government and the banks.

Objectives for Corporate Governance

The main goal of corporate governance is to advance the interests of shareholders, grow the market value of equity, and continuously increase the company's net worth. Banks, however, act as financial intermediaries, and as such, their duties significantly diverge from those of other businesses. Banks are required by law to safeguard the interests of depositors, debt holders, and other money sources, therefore protecting shareholder interests cannot be the exclusive goal of corporate governance in these institutions. As the dominant participants in the financial system, banks are required to exercise all due caution in order to maintain the institution's solvency and advance the stability of the financial system. Therefore, protecting stakeholders other than shareholders will be one of the banks' corporate governance goals. One may argue that banks are solvent as long as the equity value is positive and the shareholders get a portion of the net profit as dividends on capital. In this case, the bank is in a position to pay its current depositors and other creditors since the market value of its assets exceeds the market value of its obligations. However, if risk management and accounting standards are subpar or the accounts are

manipulated, this positive difference between the market values of the bank's assets and liabilities on a given date is not a guarantee for the bank's long-term solvency. Unexpected effects of credit, market, and operational risks might significantly reduce the value of the bank's assets and revenue in a year or two and lead the bank to go into the red, which could undermine the bank's ability to fully remit payments to its current depositors and debt holders. Aside from this, a bank's long-term viability is assessed based on its ability to pay its current depositors in full as well as the soundness of its operating procedures and governing policies, which guarantee its ability to cover all potential future liabilities as they materialize.

Banks should set up a good risk management system in order to follow sound corporate governance standards and safeguard the value of equity. The risk-adjusted return on capital is more important to consider when assessing a bank's long-term survival than the return on assets, which does not gauge a bank's financial health. Sound risk management methods and processes will aid banks in preserving asset quality and avoiding unanticipated asset value declines. Banks must have a strong risk management system to handle credit, market, operational, and other residual risks if corporate governance goals are to be successfully accomplished.

Banks are required to set up suitable business practices, procedures, and a clear administration as part of their corporate governance policies. In order to address responsibility, guarantee that the administrative system is effective and equitable, and boost employee morale, banks should clearly define roles and responsibilities among the personnel. Corporate governance's primary goal is to reassure the bank's shareholders, depositors, and debt holders that their interests are protected and the institution is well-run. Another goal is to enhance brand recognition and establish long-term public trust in order to get simple access to the capital market and raise further stock[4]–[6].

DISCUSSION

Foundation for Corporate Governance

Banks must base their corporate governance practices on a set of moral and ethical standards that are particularly important for organizations that deal with public funds. Explain these values, ethics, and principles provide steps that banks should take to improve their corporate governance procedures.

Elements of Corporate Governance

To support an efficient corporate governance structure, banks should set up the proper rules and processes regarding the following factors:

1. Openness and responsibility.
2. Ownership accountability.
3. Efficiency of internal controls.
4. Independence of the auditing process.
5. Disclosure requirement.
6. System for checks and balances.

Objectivity and Accountability

Transparency should be present in financial organizations in at least two areas: decision-making and the powers of the board of directors and senior management. The obligations of the senior

management and board of directors of banks are outlined in banking regulations and statutes. In certain nations, the boards of banks serve as advisors and deal with organizational concerns including worldwide growth, mergers, and acquisitions as well as policies and strategies. However, they do not have operational responsibility for or participate in business decisions. In several other nations, the boards of banks have authority over operational decisions including loan approval, money investment, staff advancement, and hiring. In accordance with the laws and regulations governing banking, banks are required to clearly define the authority of board members and top executives. The corporate governance process will suffer if board members have excessive authority and become involved in operational issues that are typically handled by senior executives or line management. The effectiveness of the corporate governance system will increase with the degree of impartiality in the division of authority between the board of directors and senior management. Any choices made, whether by the board or senior management, must be supported by a thorough due diligence procedure. The governance process suffers when the due diligence step is forgone.

To comply with corporate governance criteria and make sure that the officials make choices in line with written policies and printed regulations, banks should preserve openness in decision-making. Even the exceptions to the rule, which are viewed as deviations from the norm, must be made within predetermined bounds. Decisions made by higher authorities that are not transparent may lead to employee rumors that might harm the institution's image and cast doubt on the legitimacy of transactions. The atmosphere at work in the company could also be negatively impacted. Therefore, bank executives should refrain from taking business judgments on informal guidance, since these decisions are more hazardous, sometimes not based on merit, and do not adhere to corporate governance norms.

In order to encourage accountability in corporate choices and administration, banks should maintain it. They should establish acceptable standards for determining culpability for decisions made without due deliberation or reason and implement sanctions. Many banks disregard accountability when unauthorized actions are taken even though they do not result in financial losses or other damages. Instead, they see accountability as an administrative option that should only be used in cases of bad decisions or motivated decisions that cause financial loss. However, the corporate governance system mandates that, regardless of the outcome of the activity, attention should be taken of acts that are not based on defined standards or norms for establishing responsibility. This should be the case because, although being temporally legitimate, dispositions to participate in illicit transactions are detrimental to the long-term health of the governing system.

Ownership Responsibilities

Individual and institutional shareholders of banks both play a critical role in advancing the corporate governance structure. Individual shareholders often have little interest in a bank's operations and don't want to voice concerns to the management that would make them nervous. Institutional shareholders with substantial holdings of shares are often uninterested in corporate issues, and even when they are, their involvement may not be in the bank's best interests in the long run. The opinions of the shareholders are crucial because they may function as checks on choices that are not merit-based, such as those regarding the compensation of directors, the employment of auditors, geographic growth, unprofitable company activity, or significant staff offenses. The goals of corporate governance, however, won't be met if the shareholders continue

to be inactive. Banks should establish a system for frequent communication between the board of directors and shareholders in order to broaden the scope of corporate governance and include the shareholders' wise recommendations into the development of policies and plans. If the depositors are uninterested in or unaware of the business of the bank, the individual and institutional owners are also accountable to them.

Efficacy of Internal Controls

An essential component of the banking industry's governance structure is the internal control system. The basic goal of corporate governance, the improvement of equity value, cannot be realized unless the control mechanism is effective in spotting and stopping adverse situations that might result in significant losses for a bank in time. The sensitivity of the monitoring and control people to preserve the integrity of the control system at all costs is more crucial than the diversity and widespreadness of controls. It goes without saying that having an effective framework for controls is crucial, but it is also important to be able to see how they are operating in order to assess how well they are supporting the corporate governance process. Visibility in this sense refers to the timely and effective application of controls to avoid financial calamities. This may be assessed by calculating the financial and non-financial harm that would have come from misbehavior that was not discovered in time and managed[7]–[9].

The bank should address the following concerns to demonstrate that its control system is thorough and efficient:

1. Separation of roles and tasks to prevent conflicts of interest. separation between reporting and operational responsibilities. doing your research before making a conclusion.
2. Monitoring carefully the correct implementation of controls. improvement of technology infrastructure with suitable security measures. Risk assessment and reduction for contracted out work.
3. Adoption of internal auditing with a risk emphasis. financial crime avoidance.

The board of directors, management, and several committees in charge of monitoring various facets of the organization's activities often make up the framework of corporate governance. When it comes to giving management direction, selecting and assessing managers, and ensuring efficient risk management and compliance, the board of directors is essential. Independent directors maintain the board's separation from management and provide a variety of opinions to the table. The implementation of strong internal controls, risk management programs, and ethical standards of behavior are all examples of effective corporate governance procedures. Compliance with legal standards, regular performance review and transparency, and financial reporting are also critical. Trust and transparency are promoted through effective stakeholder interaction, especially with shareholders and workers.

Strong corporate governance systems assist organizations by enhancing decision-making, boosting investor trust, and facilitating capital access. In addition to lowering the risk of fraud and misbehavior, effective governance also promotes long-term sustainability. Additionally, it encourages a better fit between the goals of the company and the interests of its stakeholders, improving both performance and value generation. Effective corporate governance measures may be hard to develop and keep up, however. These difficulties include opposition to change, competing interests, complicated regulatory issues, and balancing short-term demands with long-term sustainability objectives. To meet these issues, organizations must promote an ethical

culture, ensure diversity on their boards, and constantly examine and improve their governance procedures[10], [11].

CONCLUSION

To sum up, corporate governance is an essential framework that establishes the rules and frameworks for efficient organizational management, responsibility, and moral conduct. Organizations may increase stakeholder trust, enhance decision-making, and achieve sustainable development by adhering to good governance standards. Corporate governance processes must be continuously assessed, adjusted, and improved in order to navigate the changing business environment and responsibly and openly satisfy stakeholder expectations. Corporate governance in banks refers to the rules, morals, and values put in place to ensure that the organization is operated ethically and in the best interests of shareholders, customers, and other stakeholders. As a communal effort, corporate governance culture has to spread to the lowest echelons of the bank administration.

REFERENCES

[1] J. Bardy, "Summary: Sustainable Corporate Governance: What Are The Accounting Issues?," *Rev. Int. Droit Econ.*, 2021, Doi: 10.3917/Ride.352.0207.

[2] R. Kulkani And B. Maniam, "Corporate Governance — Indian Perspective," *Int. J. Trade, Econ. Financ.*, 2014, Doi: 10.7763/Ijtef.2014.V5.399.

[3] C. Flammer, B. Hong, And D. Minor, "Corporate Governance And The Rise Of Integrating Corporate Social Responsibility Criteria In Executive Compensation: Effectiveness And Implications For Firm Outcomes," *Strateg. Manag. J.*, 2019, Doi: 10.1002/Smj.3018.

[4] Z. Ping And C. W. W. Andy, "Corporate Governance: A Summary Review On Different Theory Approaches," *Int. Res. J. Financ. Econ.*, 2011.

[5] U. A. Mustapha, N. Rashid, A. B. Ado, And S. A. Lateef, "Development Of Corporate Governance And The Effect Of Corruption On The Nigerian Financial Institutions," *J. Adv. Res. Dyn. Control Syst.*, 2020, Doi: 10.5373/Jardcs/V12i1/20201003.

[6] D. D. Keum, "Innovation, Short-Termism, And The Cost Of Strong Corporate Governance," *Strateg. Manag. J.*, 2021, Doi: 10.1002/Smj.3216.

[7] T. Bekefi, B. Jenkins, And B. Kytle, "Social Risk As Strategic Risk," *Corp. Soc. Responsib.*, 2006.

[8] M. Goranova, R. Abouk, P. C. Nystrom, And E. S. Soofi, "Corporate Governance Antecedents To Shareholder Activism: A Zero-Inflated Process," *Strateg. Manag. J.*, 2017, Doi: 10.1002/Smj.2472.

[9] V. F. M. B. Dias, M. A. Cunha, F. M. Peixoto, And D. Jesuka, "Do Ownership Concentration And The Board Of Directors Affect Exports?," *Rev. Adm. Mackenzie*, 2021, Doi: 10.1590/1678-6971/Eramf210009.

[10] W. Jiang, P. Lee, And A. Anandarajan, "The Association Between Corporate Governance And Earnings Quality: Further Evidence Using The Gov-Score," *Adv. Account.*, 2008, Doi: 10.1016/J.Adiac.2008.08.011.

[11] A. A. Putri, "Analisis Leverage, Ukuran Perusahaan, Good Corporate Governance Pada Manajemen Laba Dengan Struktur Modal Sebagai Variable Moderasi," *J. Akunt. Trisakti*, 2020, Doi: 10.25105/Jat.V7i2.7216.

CHAPTER 11

A BRIEF STUDY ON INDEPENDENCE OF THE AUDIT SYSTEM

Mr. Mrinmoy Biswas
Assistant Professor,Masters in Business Administration,
Presidency University, Bangalore, India.
Email Id:biswas@presidencyuniversity.in

ABSTRACT:

The independence of the audit system is a fundamental pillar of the financial reporting process, ensuring the reliability and credibility of financial statements. This study provides an overview of the independence of the audit system, highlighting its significance, key principles, and potential challenges. It discusses the role of independent auditors, the importance of impartiality, and the benefits of maintaining a robust and unbiased audit system. The independence of the audit system refers to the impartiality and objectivity of auditors in conducting their assessments of an organization's financial statements. Independent auditors are external professionals who are free from any conflicts of interest or undue influence that could compromise their judgment and integrity. Their primary responsibility is to provide an unbiased and objective opinion on the accuracy and fairness of financial information. Key principles of audit independence include the independence in appearance and independence in fact. Independence in appearance refers to the perception of external stakeholders that auditors are free from any bias or influence that could compromise their objectivity. Independence in fact refers to the actual absence of conflicts of interest or undue influence that may impair an auditor's judgment. Both principles are essential to maintain the credibility and trustworthiness of the audit process.

KEYWORDS:

Audit System, Business, Corporate Governance, Mitigation,Operational Risk.

INTRODUCTION

Maintaining the integrity of corporate governance standards requires the availability of a setting where auditors may carry out their duties independently. The bank management should provide the internal auditors entire flexibility, keep a safe distance from the audit's targets, and stop dictating the audit's methodology and level of scrutiny. In banking firms, there are two levels of auditing; the first level involves internal audit teams auditing branch offices, portfolios, and business lines, and the second level involves external auditors who are trained chartered accountants auditing yearly accounts. While external audit certifies that the accounts represent the genuine financial situation of the bank and the management reports expose the true affairs, internal audit concentrates on compliance with internal norms and regulations. Despite the fact that banks have a separate audit committee of the board made up of independent members, which is responsible for supervising the internal audit function and preserving the integrity of the audit, the independence of internal auditors is often compromised for a variety of reasons. The quality of external audit is also compromised if there is a connection between management and the auditors. Corporate governance suffers when management interferes with the obligations and freedom of internal or external auditors or undermines the quality of external audit[1]–[3].

As representatives of shareholders, depositors, bank regulators, and supervisors, external auditors cannot limit their attention to the correctness of the accounts and adherence to accounting rules. Bank auditing is a holy profession, and bank auditors have a specific role in defending the interests of depositors. As a result, the external auditor must not only remark on the bank's current situation but also shed light on the effectiveness of management policies, plans, and corporate governance procedures. In order to guarantee the security of the depositors' money over the short and long periods, external auditors should assess the policies, processes, and practices as well as the methods of operation. The independence of auditors to uphold professional standards is necessary for the promotion of corporate governance in banks.

The potential formation of conflicts of interest between the auditing duty and consultant assignment is a cause for worry. Large audit companies employ specialists with a variety of skills and expertise, and they also provide consulting services in addition to auditing. In order to perform an audit for the assessment of systems and processes such the risk management system, internal control system, management information system, systems audit, and credit rating system, external audit companies often take consulting assignments from banks. In exchange for a consulting assignment in the post-audit phase, the bank management may persuade the external auditors to temper their criticism of the audit results. This kind of behavior is against company governance guidelines and has serious drawbacks.

Disclosure Requirement

Disclosure is a powerful tool used in banking institutions to safeguard the integrity of the nation's financial system and corporate governance framework. The inability of business management to adhere to corporate governance standards of behavior was one of the major factors that led to the systemic crisis in the US. Due to the institutions' poor corporate governance processes, the banks were exposed to significant risks from interbank transactions due to a lack of transparency and disclosure over the amount of their engagement in dangerous credit default swap derivatives and subprime mortgages. The Companies Act has made it mandatory for the board of directors in the majority of countries to disclose in the annual report and the statement of accounts the status of compliance with the corporate governance codes and to provide an explanation for any exceptions or deviations. The company laws also include provisions for the imposition of fines and penalties for failure to comply with the codes of good practices. These harsh penalties have, in large part, forced businesses to create corporate governance rules and adhere to minimal governance requirements. The less important information is protected from being withheld for reasons of materiality or secrecy, and the more disclosure is spread out, the harder it is for the directors to engage in unethical behavior.

A framework for disclosure has been established by the New Basel Capital Accord, which mandates that banks publish a minimum amount of data on risk exposure, risk management practices, and capital adequacy evaluation. The Third Pillar of the New Accord's disclosure criteria is thorough and has reduced banks' propensity to hide crucial information. Banks will now need to specify what constitutes a significant disclosure and what is not, as well as adhere to a set of minimum qualitative and quantitative disclosure requirements. The New Accord's prescription for basic transparency standards has made it more likely that corporate governance processes in banks would be improved. Banks must make significant disclosures, some of which are regulated and delicate in nature since they are the caretakers of public funds. The disclosures involve delicate topics such the amount and movement of nonperforming loans and advances as

well as provisions against identified loan losses. They also cover the status of related party lending, exposure to the capital market, and exposure to the real estate industry. The disclosures preserve the financial institutions' long-term solvency by limiting excessive exposure to high-risk and vulnerable regions. The disclosure standards aim to significantly boost the corporate governance process[4]–[6].

Suitable Business Environment

It is incorrect to assess the performance of banks' governance in isolation without taking into consideration the commercial restrictions they must contend with since banks function in a sociopolitical setting. They suffer as a result of the weak legal system and the lack of enforcement tools to help them prosecute criminal cases or collect on judgment debts. The corporate governance process is significantly influenced by the business environment in the case of banking organizations. The legal system, worldwide best practices, and rules and regulations all have a role in the business climate. First and foremost, the nation should have banking-specific rules and regulations that are effective at promoting corporate governance, comprehensive, and in line with international norms. The laws and the regulations made in accordance with the laws should have measures that, on the one hand, prohibit the abuse of power and, on the other, ensure openness and accountability. It has been discovered that the regulation in nations where self-regulation in the financial sector is the norm is insufficient and inefficient. Due to lax regulatory requirements, the directors and top management may participate in unethical and unfair banking activities, as was shown during the U.S. financial crisis of 2007. In order to safeguard the interests of depositors, shareholders, and other stakeholders, it is crucial for the bank regulator to lay out a uniform set of rules, controls, and disclosures for banks to adhere to.

The second issue is a lack of knowledge on the finest accounting and regulatory procedures used by banks worldwide. It is the duty of the nation's central bank or bank regulatory/supervision body to draft rules that are compliant with global best practices. Strong rules and accepted accounting procedures should be implemented, and banks should be made aware of any governance system flaws and risk management system weaknesses that have been found by examiners during bank inspections. However, supervisory authorities shouldn't become involved with operational matters; such should be handled by the bankers' association, auditors, expert committees, or boards of the banks.

Thirdly, many nations lack proper legislative frameworks to safeguard financial institutions' interests. If the legal system is weak and fails to instill instinctive respect for the law and fear of penalty for breaking the law, the corporate governance process will suffer. Both the legal system and the timing of court rulings must be effective. The tendency to break laws and regulations will continue, and the environment will taint the governance system, unless the court's decision for redress of complaints is swift. It is essential that the legal system functions well and that the enforcement agencies remain vigilant in order to quickly identify anomalies and take corrective action. Dereliction of duty and criminal activity are prevented by a vigilant enforcement apparatus. The government, the central bank, the supervisory authority, the securities regulator, the stock exchange, the insurance regulator, the court, and the enforcement apparatus must all play their respective supporting roles for the corporate governance system in banks to be successful.

DISCUSSION

Corporate Responsibility in Banks

In order to build an efficient corporate governance process in any organization, but especially in financial institutions, the board's suitable structure, its role's clarity, and the board members' activities' visibility are all essential. The board is heavily involved in the operations of the bank, hence working as a board demands much greater cohesion. Any decision made by board members that affects the security of public funds has a certain amount of risk. To maintain the integrity of the corporate governance process, the bank directors must carry out certain duties and adhere to specified rules of behavior. The duties and responsibilities of the board members and the senior management must also be clearly defined. These topics are covered in this section.

Bank Specific Requirements

Banks should have unique elements in their corporate governance model since, in contrast to other corporate entities, they deal with public funds. They have specific benefits because, although having a limited equity basis, they may generate significant sums of public funds via deposits and debt instruments. Except for the need to keep minimum regulatory capital against hazardous assets and economic capital to cover significant losses from risks, there is no predetermined debt-to-equity ratio for banks. The trust of depositors is negatively impacted by poorly managed banks, which also enhance systemic vulnerability and damage the payment and settlement systems. Bank failures are caused by bad corporate governance, thus restoring public trust in the financial system is very important for the government and the central bank. As it is a communal activity, corporate governance culture must spread to the lowest echelons of the bank administration. The development of solid risk management policies and strategies by the board of directors, as well as their execution and oversight by senior management, are key components of corporate governance in banks. However, bank management often falls into complacency and makes concessions to the risk management requirements. They assume that the Deposit Insurance Corporation and, ultimately, the government, which does not want a bank to collapse and disrupt the financial system, will defend the interests of depositors in considerable measure. Since they believe that the statutory supervisor is responsible for identifying weaknesses in managerial procedures and safeguarding the organization's solvency, the bank management finds some solace in the oversight provided by the supervisory body. However, there are a few significant concerns with the board of directors and senior management that are described below and have an impact on the level of corporate governance in banks.

The Board of Directors' structure

A diversified board of directors with members from various academic subjects and economic sectors is more suited to enhancing the standard of corporate governance. The Banking Regulation Act typically specifies how bank boards should be organized to achieve diversity of expertise and requires that board members possess the necessary academic qualifications as well as knowledge of the commercial, industrial, and trade policies and practices that are relevant to banks. A sound board is more effectively created by a cross section of individuals from various backgrounds, including economists, financial experts, engineers, chartered accountants, industrialists, farmers, and information technology specialists. It is advantageous if some of the board members are knowledgeable with global risk management and accounting standards as well as international banking laws.

Bank boards are made up of nonofficial directors who just attend board and committee meetings and official directors like the managing director and executive directors. To ensure objectivity in decision-making and prevent conflicts of interest, the board should have a balance between the number of full-time in-house directors and outside directors, as well as wide participation from a variety of expertise domains. Merit-based governance is more likely to occur in a setting where the majority of the board members are chosen or elected on the basis of their qualifications rather than their ties to the bank's owners. Promoting shareholders' interests and safeguarding depositors' money may be accomplished by striking the right balance between internal directors and independent professional directors. However, if the independent or outside board members keep silent throughout the debates in board and committee sessions, the quality of governance would deteriorate. To increase the knowledge of outside board members with banking practices and procedures, particularly risk management systems, banks could host training sessions. This kind of session is likely to increase their interest in how the bank operates, give them confidence, and encourage them to actively participate in board and committee meetings.

Board members' and senior management's relationship

One key factor that affects the corporate governance standards in banks is the dynamic between the board members and top management. Good governance requires a clear separation of duties between board members and top executives as well as the growth of mutual respect and trust between them. The corporate governance process is tainted by the board members' abuse of senior management's authority. In a perfect world, senior management would act as the implementing authority while board members would act as the policy-making and supervisory authority[7]–[9].

Multiple Directorships Problem

Bank board members often serve as members of internal directors' committees such the audit committee, pay committee, and recruiting committee in addition to holding directorships in other corporations. The quality of governance will worsen if bank directors are simultaneously responsible for several firms and internal committees because they cannot give the bank's issues the attention they need. To prevent overlap in responsibilities and conflicts of interest, banks should set reasonable restrictions on the total number of businesses a director may serve on as a director as well as the number of committees on which he or she may serve.

Board of Directors' accountability and responsibility

According to the Companies Act, directors of corporations must use due diligence to protect the interests of the shareholders and fulfill their fiduciary obligations, which include the duty of care and the duty of loyalty. Directors of nonbank companies typically take care to safeguard the interests of the shareholders, but directors of banks are expected to go above and beyond the call of duty to safeguard the interests of depositors, bondholders, and shareholders as well. Both official and unofficial bank directors are jointly responsible for making sure that business operations are secure and that solvency is not in danger. The board must create the proper checks and balances to protect against forces who want to take unjustified control of the bank.

The Basel Committee on Banking Supervision has provided detailed guidelines on "sound corporate governance principles" in the document titled "Enhancing Corporate Governance for Banking Organizations." The Committee has recommended certain principles to be followed by

banks in order to improve the quality of the governance process. Based on these principles, the board of directors' accountability and responsibilities are briefly described here:

1. For both themselves and the senior management throughout the business, the board should establish and enforce clear lines of duty and accountability. There shouldn't be any unclear, conflicting, or numerous lines of duty.
2. The board should establish clear corporate rules and strategies that can be used to assess both the performance of the organization as a whole and the individual contributions of each member.
3. The board should be aware of its role in supervision and make sure top management is being overseen properly.
4. The board should prevent conflicts of interest in their activities and commitments to other organizations, advocate sensible procedures, and provide objective counsel.
5. The board and senior management should meet often to discuss and adopt policies and track progress. However, it shouldn't take part in the bank's daily management.
6. The board should establish corporate standards, behavior codes, and other guidelines and make sure they are followed.

The advantages of keeping an independent audit system are many. By giving stakeholders like investors, creditors, and regulatory agencies certainty, it improves the validity and trustworthiness of financial statements. In order to protect the interests of shareholders and the general public, independent auditors may spot and report financial irregularities, fraud, or non-compliance with legislation. As a result of the audit system's independence, investors and economic development are made possible in the capital markets. There are several potential threats to the audit system's independence. Some of the elements that may jeopardize independence include pressure from management, conflicts of interest, financial ties, and the supply of non-audit services by audit firms to their audit customers. To lessen these difficulties and strengthen audit independence, regulatory agencies and professional accounting organizations set regulations and standards. These regulations call for the rotation of audit firms, a ban on non-audit services, and independent auditor reporting requirements [10].

CONCLUSION

It takes dedication from auditors, audit firms, regulators, and the larger business community to address issues with audit independence. Organizations need to place a high priority on independence and create a culture that encourages moral conduct, professionalism, and impartiality. Regulators must ensure audit firms maintain the highest standards of integrity and independence by enforcing and monitoring compliance with the criteria for independence. In conclusion, a key component in maintaining the accuracy and legitimacy of financial reporting is the audit system's independence. Independent auditors are essential for giving stakeholders certainty and preserving public confidence in the financial system. The integrity and efficacy of the audit system must be maintained by adhering to the principles of independence in fact and appearance. To preserve trust in the financial reporting process, ongoing efforts to rectify issues and increase audit independence are required.

REFERENCES

[1] S. Setiawan, Y. Carolina, And A. Kristiani, "The Effect Of Auditor's Competence And Independence On Information System Audit Quality," *Asia Pacific Fraud J.*, 2020, Doi: 10.21532/Apfjournal.V5i2.155.

[2] M. K. Wright And I. I. I. Capps Charles J., "Auditor Independence And Internal Information Systems Audit Quality.," *Bus. Stud. J.*, 2012.

[3] T. O. Asaolu, S. A. Adedokun, And J. U. Monday, "Promoting Good Governance Through Internal Audit Function (Iaf): The Nigerian Experience," *Int. Bus. Res.*, 2016, Doi: 10.5539/Ibr.V9n5p196.

[4] R. P. Sari, S. Hastuti, And O. Tannar, "Audit Quality Based On Internal Audit Capability Model (Iacm) And Gender As Mediating Variabel In The Public Sector," *J. Econ. Business, Gov. Challenges*, 2019, Doi: 10.33005/Ebgc.V2i1.61.

[5] A. Pairingan, P. K. Allo Layuk, And B. J. . Pangayow, "Pengaruh Kompetensi, Dan Independensi Terhadap Kualitas Audit Dengan Motivasi Sebagai Variabel Pemoderasi," *J. Akuntansi, Audit. Dan Aset*, 2018, Doi: 10.52062/Jurnal_Aaa.V1i1.2.

[6] A. A. Khalid, W. A. Ahmed, Y. A. Abdalla, A. M. Ibrahim, And A. Ahmi, "Challenges Of Independence Of Internal Audit Police Officers: Evidence From Sudan," *Journal Of Critical Reviews*. 2020. Doi: 10.31838/Jcr.07.06.106.

[7] Y. Yuniarto, "Pengaruh Kompetensi Dan Independensi Auditor Terhadap Kualitas Audit Pada Audit Mutu Internal Iso 9001:2008 Di Universitas Bunda Mulia, Jakarta," *Bus. Manag. J.*, 2017, Doi: 10.30813/Bmj.V12i1.603.

[8] S. M. O'connor, "The Inevitability Of Enron And The Impossibility Of 'Auditor Independence' Under The Current Audit System," *Ssrn Electron. J.*, 2005, Doi: 10.2139/Ssrn.303181.

[9] P. Maisaroh And M. Nurhidayati, "Pengaruh Komite Audit, Good Corporate Governance Dan Whistleblowing System Terhadap Fraud Bank Umum Syariah Di Indonesia Periode 2016-2019," *Etihad J. Islam. Bank. Financ.*, 2021, Doi: 10.21154/Etihad.V1i1.2752.

[10] K. S. D. Singh, S. Ravindran, Y. Ganesan, G. A. Abbasi, And H. Haron, "Antecedents And Internal Audit Quality Implications Of Internal Audit Effectiveness," *Int. J. Bus. Sci. Appl. Manag.*, 2021.

CHAPTER 12

ROLE OF BOARD OF DIRECTORS AND SENIOR EXECUTIVES IN RISK MANAGEMENT

Ms. Leena George
Assistant Professor,Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id:leenageorge@presidencyuniversity.in

ABSTRACT:

The role of the board of directors and senior executives in risk management is crucial for ensuring the long-term success and sustainability of organizations. This study provides an overview of the responsibilities and contributions of the board of directors and senior executives in effective risk management. It explores their key roles in setting the risk appetite, establishing a robust risk management framework, and promoting a risk-aware culture throughout the organization. The board of directors holds the ultimate responsibility for overseeing risk management within an organization. Its primary role is to provide strategic guidance and direction while ensuring that risks are identified, assessed, and appropriately managed. The board sets the risk appetite, which defines the level of risk the organization is willing to accept in pursuit of its objectives. It plays a critical role in defining the organization's risk tolerance and ensuring that risk-taking aligns with the organization's overall strategy and objectives. Senior executives, including the CEO and other members of top management, are responsible for implementing the board's risk management directives and ensuring their integration into the organization's operations. They establish a robust risk management framework that includes policies, procedures, and control mechanisms to identify, assess, monitor, and mitigate risks. Senior executives are accountable for embedding risk management practices into the day-to-day activities of the organization and fostering a culture that values risk awareness and accountability.

KEYWORDS:

Business, Corporate Governance, Mitigation,Operational Risk.

INTRODUCTION

The most important activity in banking companies is risk management since an effective system reduces losses brought on by risks taken on by the bank, increasing equity value and safeguarding depositor interests. The board of directors is ultimately responsible for determining the company's risk appetite and risk tolerance levels, developing the best risk management policies and strategies, and approving the instruments and methods used to quantify, monitor, and manage risk. The New Basel Capital Accord has placed a strong emphasis on the board's responsibility for creating a suitable risk management structure. The latter must adopt a risk-return balancing strategy and concentrate on the capital return after accounting for risk. In order to safeguard the interests of shareholders and other stakeholders, the corporate governance process mandates that the boards of banks take into account a number of crucial balance sheet management problems. The board should be aware that risk management and balance sheet management are closely related, and that expanding the balance sheet would need more capital to

meet the risk profile of new assets. The board of directors and senior management must actively engage in the risk management process in order to face the demands of corporate governance. In the section that follows, their distinct roles are briefly discussed. The board of directors and top management work closely together to monitor risks and make decisions. Regular communication channels that enable the exchange of risk information, updates on risk mitigation activities, and discussion of developing issues include board meetings and management reports. Senior executives provide thorough and timely risk reports to the board, facilitating informed decision-making and guaranteeing that risk-related problems get the attention and resources they need[1]–[3].

Function of the Board

1. To describe the risk management philosophies and appetite of the bank. to accept guidelines and plans for handling and accepting risks.
2. To engage in activities that are consistent with the bank's strength.
3. To establish responsible upper limits on credit risk, market risk, and operational risk throughout the whole bank, as well as to assess compliance.
4. To obtain and examine papers outlining the scope and severity of the bank's risks.
5. To provide the method for determining capital adequacy approval.
6. To divide capital among credit, operational, market, and other residual risks.
7. To accept internal models for counterparty credit risk assessment. to approve techniques and methods for risk assessment.
8. To comprehend management reports on rating system functioning and the bank's counterparty rating system.
9. To periodically examine and adjust risk exposure levels.
10. To make sure that risk limitations are in line with the state of the market and company plans.
11. Should be aware of any extra dangers posed by novel goods or activities. to establish a thorough and exact reporting system.
12. To guarantee that the reporting system includes information on risk exposure for all locations and business models.

Senior Executives' Function

1. To establish business strategies that adhere to predetermined risk boundaries. to establish policies, frameworks, and processes for managing the bank's operations.
2. To keep an eye on how the operational environment is changing and to put risk-reduction measures in place.
3. Must make sure that the operational team is knowledgeable enough to comprehend risk boundaries and work within them.
4. To guarantee that methods for risk identification and risk management are in place when new endeavors and goods are presented.
5. To place qualified employees in a risk management role.
6. To ensure that staff members maintain intellectual integrity and honesty.
7. To keep an eye on the day-to-day operations of the business line leaders, risk managers, and risk control officers.
8. To verify that the rating system is working effectively by understanding the counterparty rating system's architecture and functioning.

9. To conduct a regular assessment of the rating process and address any issues that are discovered.
10. Must notify the board of significant modifications to the risk rating methodology.
11. To make sure that the functioning of the rating system is a crucial component of the board reporting system.
12. Should disclose to the board any significant components of operational, market, and credit concerns.
13. In order to set standards for responsibility inside the company.

Moving Banks Toward Better Corporate Governance

A robust corporate governance structure in banks cannot be pursued due to several outstanding difficulties. The corporate governance process will improve if these challenges, which were briefly described below, are resolved.

Creating Long-Term Corporate Objectives

Banks often don't consider about long-term company objectives and instead focus on the expansion of their yearly revenue and profit. Annual plans provide a summary of the company priorities and strategies to be used throughout the year. They often include goals for profit development, the use of cash, and the mobilization of resources, as well as suggestions for opening additional offices. Banks fail to define their medium- and long-term objectives clearly, envision the kind of commercial operations they wish to specialize in, and align their yearly plans with the accomplishment of their longer-term objectives. For instance, a bank's business emphasis and business strategies presented via the yearly plans must support its long-term aim of becoming a wholesale banking specialist. Therefore, banks should clearly define their long-term objectives and develop short, medium, and long-term plans that are in line with those objectives. In accordance with their long-term objectives, they should create a road map for company development, activity expansion, and geographic expansion and publish their intentions to the shareholders and the bank regulator/supervisor[4]–[6].

Choosing the Board of Directors for the Bank

Banks should use a suitable due diligence procedure when choosing the members of their boards. For banks to be required to nominate qualified individuals to the board, the Banking Regulation Act must include specific requirements. Political factors are taken into account during the selection process at government-owned banks, when the procedure is conventional and not merit-based. The government should develop an open and responsible procedure for the designation of qualified individuals in institutions that it completely owns. A proportional number of independent directors should be chosen by the private shareholders to the board in lieu of government-nominated directors in banks where institutions and the general public hold equity. If companies and institutions own a significant amount of private equity instead of people, effort must be taken to ensure that the individuals they designate for the board of directors meet the fit and appropriate standard. The bank supervisor's assistance may be necessary in banks that are wholly owned by private shareholders to guarantee that academic performance, social background, and professionalism are given fair consideration in the election or nomination of directors to their boards.

Enhancing the Judicial Process

The court system urgently needs to be improved in order to speed up the determination of cases involving the recovery of bank debts from failed loans and financial embezzlement. Typically, borrowers use dilatory strategies, taking advantage of gaps in the law that prolong court cases and postpone the court's delivery of decision. Additionally, even after receiving a court order, banks find it difficult to carry it out owing to the lack of an effective enforcement mechanism, which negatively impacts the likelihood of a recovery. Not all jurisdictions have special courts for swiftly resolving bankruptcy and insolvency issues.

DISCUSSION

Despite being legal specialists, judges may not be familiar with banking operations and processes or fraud modi operandi, which causes court proceedings to go longer than necessary. The government and banks might work together to provide seminars for judges to get acquainted with banking practices and processes that may be helpful for the swift settlement of bank matters. A platform for accelerating the court process will be established by workshops for judges that involve an exchange of experiences on the stalling strategies used by uncooperative borrowers and the methods used by criminals engaged in money laundering, fraud, and the theft of valuables and assets. The goals of corporate governance are to protect the interests of depositors and shareholders while also facilitating the prompt recovery of bank debts for use in the economy. For successful decree implementation, an effective court system supported by an equally effective enforcement apparatus is required.

Existence of Dispute Resolution Equipment

Examining the options shareholders and clients of the bank have for resolving legitimate complaints is important for evaluating the effectiveness of corporate governance. The most frequent complaints that shareholders have against banks are that they do not promptly send invitations to the annual general meeting, register names on market purchases of shares, send annual reports and other information regarding company resolutions, or pay declared dividends. Customers also have a variety of complaints, such as bad counter service, delays in issuing duplicate checks for lost drafts, money being taken from accounts, private information being revealed to other parties, etc. A crucial aspect of corporate governance is the level of customer service provided by banks. The government, the bank regulator, and the bank itself are all concerned with protecting individual shareholders who own modest quantities of shares and consumers who have small sums of deposits. Additionally, banks are required to defend the rights of customers who use their services. If the complaints of specific shareholders and consumers are not handled and resolved in a timely manner, corporate governance cannot be said to be successful. Banks must consequently have effective systems for resolving shareholder and consumer complaints.

Creating a System of Preventive Vigilance

Misuse of financial authority has the potential to cause banks to suffer substantial losses that might seriously harm their financial situation. They must put in place a system of oversight to stop employees from abusing their authority or collaborating with other parties to commit fraud. In order to monitor financial power abuse and deviations from established systems and procedures, banks should set up an administrative unit that will act as a vigilance body. This unit

will identify suspicious transactions from audit reports and other control returns and evaluate the seriousness of the offenses before launching disciplinary actions. Sometimes it is necessary for the vigilance unit to examine dubious transactions directly after they are brought to its attention via anonymous written complaints or phone calls. The governance process will become corrupted in the absence of vigilance equipment to quickly identify anomalies and implement disciplinary actions and punishments. To avoid creating unrest among the workers that lowers their morale and obstructs the expansion of the company, banks should set up a distinct vigilance cell or department and describe the way in which the vigilance machinery will operate. The vigilance unit should reassure the personnel that its mission is to maintain and advance honesty and integrity in all commercial dealings involving the bank.

Positive Attitude Towards Money Laundering

The movement of illicit funds used to fund terrorism and other criminal activity goes via banks. Every nation has strict anti-money laundering regulations that mandate banks form connections with new clients through the "Know Your Customer" process. Banks have a duty to diligently fulfill anti-money laundering laws and regulations in order to serve the interests of the country and their own businesses. The anti-money laundering rules place a strong emphasis on finding questionable transactions and reporting them to the appropriate authorities. However, banks often fail to take anti-money laundering regulations seriously, either because they are unfamiliar with the processes or because they lack the knowledge to identify suspicious transactions. To identify suspicious transactions, it is crucial to raise public awareness of the dangers of money laundering and to improve knowledge of anti-money laundering laws and dealing practices. A proactive corporate governance system is shown by suitable anti-money laundering behavior.

Avoiding Abuse of Autonomy

To ensure an impartial governance process, external authorities must refrain from interfering with corporate management. Banks abhor intervention in their internal issues and desire autonomy in their management and operations. However, it is anticipated that government and bank regulator noninterference won't result in a circumstance where the bank's activities become exposed and cronyism and inefficiency spread across the company. Where banks have the status of independent entities, merit- and value-based management and rigorous adherence to laws and regulations are important. The financial system may experience major issues if banks are given complete autonomy without having adequate procedures in place for monitoring, vigilance, and reporting. While excessive regulation and control by the government and the bank regulatory authority pose challenges for banks, doing so might harm such institutions. In order to support the housing mortgage finance market, regulatory requirements were loosened before the US financial crisis began. However, supervisory control and oversight were not tightened in order to keep track of the risk profiles of systemically large financial institutions, which ultimately caused the systemic crisis. A severe violation of the corporate governance regulations is the misuse of autonomous powers[7]–[9].

Organizations gain a lot from the board's and senior executives' effective risk management. It improves the organization's capacity to see opportunities, grab them, and successfully manage uncertainty while defending itself from possible dangers. By displaying a dedication to effective risk management methods, it increases stakeholder trust, including that of shareholders, workers, clients, and regulators. As it aids companies in developing resilience, adapting to changing circumstances, and making choices that are in line with their strategic goals, effective risk

management also promotes long-term sustainability. Striking the correct balance between risk-taking and risk avoidance, integrating risk management techniques into the organization's culture, and staying on top of changing hazards and regulatory requirements are all difficulties in carrying out the board's and senior executives' responsibilities in risk management. It calls for a proactive, adaptable strategy, ongoing learning, and a dedication to making risk management an integral part of corporate governance[10], [11].

CONCLUSION

To allow banks to adhere to good corporate governance norms, the government and bank regulator should provide the proper atmosphere. Corporate governance in financial institutions cannot be solely centered on safeguarding shareholder interests. The roles that banks play as financial intermediaries are significantly different from those of other businesses. In addition to the interests of the shareholders and the government, they are required by law to defend the interests of depositors, debt holders, and other fund providers. To show their commitment to upholding corporate governance codes, ethics, and values, banks should always be transparent in their decision-making, create accountability for wrongdoing, support an independent audit system and effective control framework, and set up a grievance redress mechanism to investigate customer and shareholder complaints. Since the shareholders' opinions serve as checks and balances in the governance structure, banks should set up frequent interactions between the board and them. In the annual report and the statement of accounts, banks should provide thorough disclosures about their financial situation and other affairs, the status of compliance with corporate governance regulations, and the causes of exceptions and deviations. It becomes harder for management to engage in unethical behavior and undermine the corporate governance process the more thorough the disclosure requirement is. Since banks deal with public funds, their corporate governance model should be unique in terms of the makeup of the board of directors, the specific responsibilities of each member, and the requirements for operational and administrative standards. In order to safeguard the interests of depositors and the value of the stock via minimizing risk-related losses, banks should have an effective risk management system. The board of directors and top executives, in particular, play crucial roles in risk management by providing leadership, supervision, and direction to guarantee efficient risk attribution, evaluation, and mitigation. The accomplishment of company goals and guaranteeing long-term success depend on their cooperation and dedication to creating a strong risk management framework and cultivating a risk-aware culture. Boards and senior executives support their firms' resilience, sustainability, and stakeholder trust by accepting their duties and adopting good risk management strategies.

REFERENCES

[1] L. Xing, T. Duan, and W. Hou, “Do Board Secretaries Influence Management Earnings Forecasts?,” *J. Bus. Ethics*, 2019, doi: 10.1007/s10551-017-3478-6.

[2] H. A. H. Al-Farsi, “The Influence Of Chief Risk Officer On The Effectiveness Of Enterprise Risk Management: Evidence From Oman,” *Int. J. Econ. Financ. Issues*, 2020, doi: 10.32479/ijefi.8932.

[3] S. A. Ojeka, A. Adeboye, and O. Dahunsi, “Does Audit Committee Characteristics Promote Risk Management Practices in Nigerian Listed Firms?,” *Account. Financ. Res.*, 2021, doi: 10.5430/afr.v10n2p70.

[4] T. R. Viscelli, D. R. Hermanson, and M. S. Beasley, "The integration of ERM and strategy: Implications for corporate governance," *Account. Horizons*, 2017, doi: 10.2308/acch-51692.

[5] H. Al-Farsi, "Factors influencing the effectiveness of enterprise risk management (ERM) in publicly listed companies in oman," *Int. J. Sci. Technol. Res.*, 2020.

[6] N. Smith, M. B. Watkins, J. J. Ladge, and P. Carlton, "Interviews with 59 black female executives explore intersectional invisibility and strategies to overcome it," *Harv. Bus. Rev.*, 2018.

[7] S. Vollmer, "The board's role in promoting an ethical culture," *J. Account.*, 2018.

[8] A. Rehman and F. Hashim, "Impact of Mature Corporate Governance on Detective Role of Forensic Accounting: Case of Public Listed Companies in Oman," *KnE Soc. Sci.*, 2019, doi: 10.18502/kss.v3i22.5080.

[9] D. Weekes-Marshall, "The role of internal audit in the risk management process: A developing economy perspective," *Journal of Corporate Accounting and Finance*. 2020. doi: 10.1002/jcaf.22471.

[10] P. Weill, T. Apel, S. L. Woerner, and J. S. Banner, "It Pays to Have a Digitally Savvy Board: Having board members with experience in digital business is the new financial performance differentiator," *MIT Sloan Manag. Rev.*, 2019.

[11] T. Petri and R. Soublin, "Turbulent times require a greater focus on board effectiveness," *Strateg. HR Rev.*, 2010, doi: 10.1108/14754391011050379.

CHAPTER 13

REASONS FOR AND EFFECTS OF THE FINANCIAL CRISES IN ASIA AND THE UNITED STATES

Dr. Kadambat Kumar
Professor,Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id:krishnakumark@presidencyuniversity.in

ABSTRACT:

Two notable occurrences that had a profound impact on the world economy were the Asian financial crisis of 1997 and the American financial crisis of 2008. The fundamental drivers, systemic vulnerabilities, and ensuing economic, social, and political repercussions of these financial crises are highlighted in this paper, which offers a general overview of their origins and effects. A number of reasons, including excessive borrowing, lax financial regulation, currency pegs, and speculative investments, led to the Asian financial crisis. Numerous currency devaluations, stock market crashes, and economic downturns were caused by unmanageable debt levels, weak banking institutions, and speculative currency assaults in various Asian nations. The financial crisis revealed systemic flaws, a lack of transparency, and insufficient risk management procedures. In contrast, a housing market bubble that was stoked by loose lending rules, the securitization of mortgage loans, and sophisticated financial derivatives was the root cause of the 2008 U.S. financial crisis. Subprime mortgage defaults contributed to a severe credit crunch, bank failures, and a severe recession, which were all brought on by excessive leverage and interconnections within the global financial system. The crisis revealed flaws in corporate governance, regulatory monitoring, and risk assessment procedures.

KEYWORDS:

Business, Corporate Governance, Financial Crisis, Mitigation,Operational Risk.

INTRODUCTION

The financial crises that happened in Southeast Asian nations in 1997 and the United States from 2006 to 2008 revealed that the risk assessment methods and rules that were in place to regulate financial operations were insufficient. The financial crisis showed that banks' standard risk assessment guidelines were insufficient because they failed to effectively account for systemic and contagion risks as well as risks from specific credible occurrences. The crises gave risk assessment processes and procedures a new dimension as it became clear that significant risk may occur because of the intimate ties that exist between global financial markets and economies. The bank's risk assessment procedure must thus take into account the contagion and domino impacts of risk events that may occur in both developed and developing nations. Due to a significant inflow of short-term foreign funds and the use of novel financial and derivative instruments to fuel the credit boom, banks were found to have improperly assessed and measured the risk that can result from an excessive acceleration of credit in order to increase economic growth. This failure was made clear by the financial crises. The crises made it clear that there are deficiencies in the supervision of financial institutions and the framework for regulating financial activity[1]–[3].

Causes and Effects of The Asian Financial Crisis

During the first part of the 1990s, Southeast Asian nations saw an investment boom that accelerated economic expansion in a few carefully chosen areas. The majority of its funding came from short-term foreign investments, mostly in U.S. dollars, which put the local financial institutions and private companies at considerable exchange risk. The money was mostly used to construct residential and commercial real estate in Thailand and Hong Kong as well as in a few particular sectors in Malaysia, Korea, and Indonesia. Because the asset price in the real estate sector is often unstable and the output price in companies that are export-oriented is heavily reliant on ongoing export demand, the loan boom exposed the financial institutions to increased risk. As private businesses and financial institutions had unfettered access to borrowing money directly from foreign banks to finance their investments, the systemic risk to the financial sector rose. The investment boom produced surplus capacity, which in turn caused a drop in the value of real estate and industrial production, which severely reduced borrowers' income and ability to pay back institutional loans.

The Asian financial crisis began in Thailand in the first quarter of 1997, initially as a result of the inability of real estate developers to repay loans to financial institutions as a result of falling real estate values, and then as a result of the ensuing devaluation of the Thai baht. The Thai baht's value versus the US dollar significantly decreased as a consequence of Thailand's switch to a floating exchange rate regime in July 1997, significantly raising the burden of local currency debt for borrowers. The decline in real estate values and the weakening of the baht made it difficult for Thai financial institutions and other corporate entities to pay back their loans to creditors, especially those with dollar values. The unexpected rise in demand for the U.S. dollar to pay off foreign currency debts combined with speculative trading in it in advance of the local currency's depreciation put enormous pressure on the exchange rate. Large-scale defaults resulted from the considerable decline in the value of native currency relative to the U.S. dollar, which correspondingly increased the repayment requirements of borrowers. The local currencies of the other nations in the area were adversely affected by the depreciation of the Thai baht. The Malaysian ringgit, Philippine peso, and Indonesian rupiah all witnessed significant depreciation in the first phase, while in the second phase, the South Korean won, Singaporean dollar, and Hong Kong dollar also saw pressure on their exchange rates. The financial and economic crisis was brought on by the foreign exchange issues in these nations. The nations saw a steep decline in the value of their currencies, a significant drop in the price of stocks and other assets, a slowdown in the economy, and a decline in gross domestic product.

DISCUSSION

The Risks Associated With The Asian Financial Crisis

Due to the interdependence of the regional and global financial markets, the Asian financial crisis made clear that financial institutions are exposed to increased risks when big inflows of foreign money are used to fuel economic development. The following extra risks applied to banks and other lending organizations.

Infection Risk

The financial crisis showed how a lack of foreign currency in one financial market has an impact on the exchange rates of foreign currencies in other financial markets in the region, forcing those

countries to devalue their currencies, which significantly reduces borrowers' ability to repay their debt and causes them to default on their debt obligations to foreign investors and institutional lenders. To determine the type of exposures in terms of direct lending, investment in financial instruments, and activities of financial subsidiaries, banks must also identify the important foreign lenders and investors in their nations and the area.

Other currencies in the area significantly depreciated as a consequence of the currency devaluation in Thailand in 1997, which had a cascading impact on their values. Local borrowers' repayment obligations were significantly increased as a result of the currency devaluation, which in turn caused widespread defaults and the buildup of nonperforming assets at the credit institutions that caused some of them to become insolvent and liquidate. In determining the risk, banks must consider the economic situation, the brittleness and vulnerability of the financial systems of the nations that are pertinent to their operating environment, as well as the potential for adverse developments to have a domino effect and a cascading effect on other risks. Banks must carefully consider the financial and trade ties with the United States, evaluate the impact of negative developments in the United States on the local financial sector, and be aware of any additional risk that may emerge if the country is dependent on the U.S. markets for exports, the exchange rate is aligned to the U.S. dollar or a basket of currencies dominated by the dollar, and the financial exposures are primarily in dollars[4]–[6].

Risk of Credit Concentration

The 1990s saw an increase in investment in Southeast Asian countries, although it was mostly focused on the commercial and residential real estate markets in Thailand and Hong Kong, as well as a few carefully chosen industries in Malaysia, South Korea, and Indonesia. The investments were funded by sizable bank and financial institution borrowings that included international capital. Evidently, banks did not make reasonable predictions of demand for the real estate and industrial production. As a result, there was soon an excess of capacity in the relevant industries, which significantly decreased the prices of real estate and industrial output, which in turn had an impact on stock prices. Credit risk for banks and other financial institutions rose due to credit concentration in certain sectors and industries and lax lending rules, which eventually led to more defaults and massive bad debts. Regardless of the circumstances that cause loans to become concentrated, banks should be aware of the potential for greater credit risk.

Credit Risk Driven by Market Risk

Due to a lack of foreign currency starting in early 1997 to repay foreign currency debts obtained by local banks, financial institutions, and private businesses, the Asian financial crisis developed. Since borrowing in foreign currencies was generally more affordable, private sector borrowers took out direct loans from foreign banks and financial institutions to fund their projects, but it appears that there were insufficient macroeconomic controls on the total inflow of foreign funds. Due to this, there is now an unbalance between the total amount of foreign currency loans that must be repaid and the amount of accessible foreign currency. Many borrowers defaulted as a consequence of the sharp rise in repayable amounts and the deterioration of the capital market, which led to an accumulation of bad debts with the financial institutions and the closure of many of them. It became clear that there is a direct connection between credit and market risks, and that if the exchange rate weakens and stock prices fall, banks' credit risk would rise. This phenomena must be taken into account by banks when assessing risk.

Risk of Maturity Mismatch

As they financed long-term projects with short-term borrowings, the banks and financial institutions in the afflicted nations exposed themselves significantly to interest rate risk and liquidity risk. Real estate development and industrial projects need the support of longer-term loans since they have gestation periods of over a year to provide advantages and generate cash flows that allow the borrowers to pay the debt. According to the information that is currently available, the six Asian nations mostly depended on loans and funds with a maturity of less than a year to cover their credit needs. "At the end of 1996, Indonesia had a 62 percent share of loans with a maturity of one year or less, South Korea had a 68 percent share, the Philippines had a 50 percent share, Thailand had a 65 percent share, and Taiwan had an 84 percent share. The prospect of raising more money at a higher interest rate puts further pressure on the exchange rate and borrowing costs when short-term foreign currency obligations are used to finance medium-term projects. If banks choose to finance medium-term projects using short-term foreign funds, they must account for increased liquidity and interest rate risks from asset-liability maturity mismatches in their framework for measuring risk.

Lesson

The consequences of the Asian financial crisis emphasize the need of a coordinated strategy between policy liberalization for promoting free trade and liberal capital inflows and outflows, and improvement of financial sector regulation and supervision. To avoid the occurrence of systemic crises in the financial sector, the authorities must evaluate the potential risks brought on by loosening restrictions on private sector direct access to foreign funds and a disproportionate inflow of short-term foreign funds.

Effects of the U.S. monetary crisis

Beginning in October 2006, there was a decline in the value of residential homes, which was financed by commercial and investment banks, insurance companies, securities businesses, and other mortgage lenders. The impact was first felt in the residential real estate industry, but it quickly expanded to other economic sectors. Numerous borrowers of home loans began missing payments, the unemployment rate rose, and the rate of economic growth slowed. As a result, institutional lenders and financial institutions experienced severe liquidity shortages and went bankrupt, merged with other, more robust institutions, or were bailed out by the government.

The financial crisis had two effects on the American economy: it reduced family and individual wealth as well as institutional wealth. The loss of home equity, household assets, savings, investments, and pension assets totaled more than $11 trillion in US dollars3, with a large portion of the loss coming from speculatively purchasing residential real estate and stocks using borrowed funds. Due to failures in loan repayment or the return of investments in financial instruments that were made possible by the securitization of mortgages, U.S. banking institutions suffered enormous losses. Lehman Brothers filed for bankruptcy, Bear Stearns and Merrill Lynch were acquired by other businesses, Goldman Sachs and Morgan Stanley were bailed out, and Morgan Stanley was transformed into a commercial bank. The five major U.S. investment banks had a total debt of $4 trillion.

A worldwide economic and financial crisis resulted from the financial crisis that started in the United States in 2006 spreading to other financial hubs and economies in Europe, Asia, and other

developing countries. A halt in economic expansion, a drop in exports, a record dip in commodity and stock prices, and a collapse in the value of home currencies were all seen in several nations. Because they had made substantial investments in the American real estate and stock markets using borrowed money, banks and financial institutions all across the world, but particularly in Europe, suffered. The decline in stock and real estate values significantly reduced family wealth, which had a detrimental impact on consumption. As a result, the financial sector crisis spread to the real economy. Due to their diminished confidence, investors began to pull their money out of the afflicted nations, which caused the global financial markets to contract and stifle the credit flows necessary to maintain production and consumption. A number of national governments unveiled assistance plans to boost the economy and support the financial institutions that are struggling under the weight of bad loans.

Causes of the U.S. Financial Crisis and Related Risks

The financial crisis in the United States, which extended to other nations and intensified into a worldwide catastrophe, was neither primarily brought on by the financial system's exposure to subprime mortgages, nor did it develop quickly as a result of the unexpected appearance of uncontrolled causes. The financial system's macro-level issues and the wrongdoing of certain financial institutions, as well as the lack of adequate regulation of some market sectors, combined to cause the crisis. It is not difficult to pinpoint the reasons of a crisis after it has occurred; instead, it is advantageous to draw lessons from the experience and utilize the causes to enhance the process for identifying risks and assessing their severity. In the section that follows, the crisis's root causes and related hazards are examined. Banks must analyse the risk environment and identify new hazards that result from it while analyzing the risk[7]–[9].

These crises had extensive and lingering effects. The financial crisis in Asia resulted in severe economic downturns, job losses, and societal unrest. Significant GDP reductions were seen by nations like Thailand, Indonesia, and South Korea, and those nations struggled to recover. The U.S. financial crisis had an impact on the whole globe, contributing to a global recession, stock market falls, and a drop in investor and consumer confidence. Government interventions, significant financial institution bailouts, and long-term effects on employment and economic development were all caused by the crisis. The significance of efficient regulation, risk management, and transparency in financial institutions was brought home by both crises. They resulted in changes to banking and financial legislation, such as the creation of global financial standards, higher capital requirements, and better methods for risk evaluation. Governments and central banks took action to stabilize the financial system, boost consumer confidence, and support economic growth[10], [11].

CONCLUSION

These financial crises' origins and effects show how intertwined and prone to failure the global financial system is. The world over, financial policies, risk management techniques, and regulatory frameworks have been impacted by the lessons learnt from these crises. However, there are still issues with preserving financial stability, dealing with systemic risks, and lessening the effects of upcoming crises. In conclusion, the 1997 Asian financial crisis and the 2008 U.S. financial crisis were important occurrences that had a huge impact on the world economy. Systemic weaknesses, excessive risk-taking, and regulatory shortcomings were the primary causes of these disasters. Economic recession, job losses, and long-lasting consequences on financial markets were among the effects. To reduce the likelihood of future crises, efforts have

been made to improve financial regulation, risk management, and transparency. However, continual vigilance is necessary to avoid and reduce the dangers connected with a fast changing global financial system.

REFERENCES

[1] G. J. Fraser-Moleketi, "Democratic governance at times of crisis: Rebuilding our communities and building on our citizens*," *Int. Rev. Adm. Sci.*, 2012, doi: 10.1177/0020852312438524.

[2] M. Fakheri, "The Effects of Regional Arrangements on China's Foreign Policy in Central Asia," *Cent. Eurasia Stud.*, 2021, doi: 10.22059/jcep.2021.310112.449952.

[3] W. Szymański, "Globalisation, money, taxes – past and present," *Kwart. Nauk o Przedsiębiorstwie*, 2017, doi: 10.5604/01.3001.0010.4691.

[4] Frans van Waarden and Robin van Dalen, "Hallmarking Halal Regulating Halal: a Case of - as yet - Private Regulation," 2010.

[5] J. K. Galbraith, "How the economists got it wrong," *Am. Prospect*, 2000.

[6] K. O. Villalba-Condori, "Formación Docente Para Desarrollar El Pensamiento Computacional," *World Dev.*, 2018.

[7] H. Tong, "An investigation of the insurance sector's contribution to economic growth," *Proquest LLC*, 2008.

[8] L. S. Johnson, *Winning Debates*. 2018.

[9] N. A. Achsani and H. G. Strohe, "Asymmetric stock market interdependencies: Us dominance and spillover effects into Asia and Europe," in *Integration in Asia and Europe: Historical Dynamics, Political Issues, and Economic Perspectives*, 2006. doi: 10.1007/3-540-28730-2_11.

[10] N. Raihanah, "Analisis Pengendalian Kualitas Produk Coklat Batang (BAR) Berdasarkan Kebutuhan Konsumen di Pusat Penelitian Kopi dan Kakao Indonesia (PPKKI)," 2018.

[11] A. Kinicki and M. Fugate, "Organizational behavior," *McGraw Hill Educ.*, 2020.