Operational Risk Modeling - Approaches and Responses

*Shibyanshu Sharma**

Risk is a situation involving the exposure of something valued to potential or actual loss. In the case of the financial industry, there are numerous types of risks that an organisation needs to be aware of in order to make sure it does not get into an unexpected crisis. Market risk, credit risk, liquidity risk and the newly recognized, operational risk are some of the types of risks that an organization has to face in the financial industry. Due to rapid technological advancements, companies are also facing the threat of cyber security risk, and, many organizations across the world have already started preparing for this risk using various approaches and responses with the help of operational risk modeling. This paper strictly focuses on Operational Risk (OR) Modeling and the various approaches and responses to operational risk.

Keywords: Operational Risk Modeling, ERM, Basel II, Cyber Risk, Risk Response

Risk

Risk is an event of exposure to loss. As an individual, every person is constantly facing various health, financial or reputational risks, although on a very small scale when compared to business organizations. It is important to understand the kind of risk a person or an organization might face, and make decisions accordingly. The idea of risk assessment has been in play for over 100 years. For example, farmers in the early age assessed the risk relating to their crops, and hedge them against the price fluctuations in their respective commodity (Cummins, 1998).They did this by trying to sell a part of or the entirety of their expected crop before harvest to a third party, which is called future markets in order to ensure their price, irrespective of the demand and supply, effects on the market for that commodity. This process transfers the risk of price fluctuations from the farmer to the buyer, ensuring business continuity for the farmer. This simple process the has led to what is now called, risk management, at its simplest level, is the process of decision making an individual or an organization takes to mitigate or transfer the risk.

Similar to an individual, a business organisation is defined as an artificial person that is created by law, legally has a distinct identity, performs various duties and holds certain rights. With new type

* *Vice President, Risk Management, SBI Life Insurance Co. Ltd.*
Email: shibyanshu.sharma@sbilife.co.in

of risks coming into light everyday by exposing its business to the ever-updating market, an organization needs to consciously follow proper risk management strategies, and take well-calculated decisions accordingly. Large-scale businesses are usually more exposed to various risks than small-scale businesses, and require a wide and highly enhanced team of professionals that work on analysing and mitigating those risks. This is known as the Enterprise Risk Management (ERM) which includes the methods and processes used by a business to manage risks and seize opportunities related to the achievement of their objectives or goals (Wikipedia, n.d.). It is a plan-based business strategy that aims to identify, assess, and prepare for any dangers, hazards, and other potentials for disaster, both physical and figurative, that may interfere with an organization's operations and objectives (Investopedia, 2019). ERM focuses on assessing, controlling, exploiting, financing and monitoring risks from all areas in order to increase the value of the organization in the short-term and long-term (Wikipedia, n.d.).

Risk is a very important factor that needs to be well evaluated before making, important, or any decisions in business or in life. Although we do not have models and methods to identify, evaluate, protect against or prevent all sorts of risks in life, the Basel Committee of Banking Supervision has fortunately defined and provided frameworks to manage risks for financial institutions in order to guide them to be prepared for any loss that may occur. In the next part, we define and understand the process of risk management, and discuss its the various components.

Risk Management

Risk management is the process that involves establishing the context with identifying, quantifying, integrating, assessing or prioritizing, treating or exploiting risks followed by monitoring and reviewing the risk management strategies. All of these processes combined, if functioning efficiently, are supposed to help the company stay aware of numerous potential threats and vulnerabilities it is facing, and deal with them in the most feasible way. And insurance itself is a very good example of a risk management strategy that a business or an individual can use in order to ensure protection against the risk of loss. Training and safety awareness programs are also examples of a risk management strategy that a company can take to avoid the expense of insurance while protecting itself against a given risk, i.e., by informing and training its employees against the risks. Whether a company wants to take insurance or engage in programs that prepares it to deal with the risk, these decisions can be made efficiently only by understanding the nature, size and potential of the risk, and, that has been made possible due to risk management.

Risk management and risk management strategies are newly introduced as subjects, but the concept has existed and used for at least a couple of centuries. The insurance industry itself is a business based on a risk management strategy. The Hamburg Fire Office (Hamburger Feuerkasse) is officially the oldest and the first ever insurance company set up in 1676 that offered the insured protection against the risk of loss of property in the event of a fire. The concept of protecting against property risk using property insurance came into existence way back in1666, after the Great Fire of London that destroyed more than 13,000 houses. This massive destruction has caused people to

worry about the risk of fire to their houses (property), so property insurance was introduced to pool the risks of house owners for a small premium that can help them support themselves by claiming for a fixed amount based on the loss incurred. In the following subsets of this paper, we will look at various risk management approaches, responses and methods, mainly focused on by enterprises in the current world of business.

In 2003, the Casualty Actuarial Society (CAS) divided risks into 4 types, namely, hazard risk, financial risk, operational risk and strategic risk. Strategic risk, briefly, requires a speculative analysis whereas financial, hazard and operational risk require complex quantified analysis. The reason it is this way is because strategic risk has the ability to think of future expectations only, as the strategies are introduced as updated or new strategies and are never in the same business environment. So, Modeling such risk is beyond quantifying, using the current methods and approaches, at least. Financial, operational and hazard risks can be quantified using internal and external data, judgements and past experiences using mathematical models, that have proven to be efficient when tested by numerous companies in developed countries, and also approved by the Basel Committee of Banking Supervision.

Importance of Risk Management

The Basel Committee of Banking Supervision was established in 1974 with an objective to enhance the understanding of key supervisory issues and improve the quality of banking supervision worldwide. The committee also frames guidelines and standards in different areas of banking, out of which the most known framework is the international standards on capital adequacy. The BCBS set the Basel Accords, which are three series of banking regulations, namely Basel I, Basel II and Basel III. These provide recommendations on banking regulations in regards to operational, capital and market risk. The purpose of these accords is to ensure that the financial institutions have set aside enough capital to meet and absorb the obligated and unexpected losses. Basel II, published initially in 2004, was intended to amend international banking standards that controlled the minimum capital requirements to be held to protect against financial and operational risks. Basel II uses a three-pillar concept, namely, (i) minimum capital requirements, (ii) supervisory review, and (iii) market discipline. The first pillar provides a regulatory minimum capital requirement calculation against three major components of risks banks face, called, credit, operational and market risk. This Basel Accord also provides three different approaches for operational risk, called Basic Indicator Approach (BIA), Standardized Approach (TSA) and the Internal Measurement Approach (IMA). The Advanced Measurement Approach (AMA) is the advanced version of IMA. The second pillar provides a framework for dealing with residual risk. The accord combines systematic risk, pension risk, concentration risk, strategic risk, reputational risk and legal risk under this single term, residual risk. The third pillar aims at market discipline by requiring institutions to disclose details on capital, risk exposures, risk assessment processes, and the capital adequacy of the institution (Investopedia, 2018). These disclosures also need to be similar to the actions of how the senior management assesses and manages the risks of the institution.

The European Union (EU) also put similar efforts to increase the efficiency of a type of financial institutions. A Directive of EU Law, Solvency I Directive 73/239/EEC, is a risk management directive that codifies and harmonises the EU insurance regulation. It was initially introduced in 1973, giving a pathway to the newly accepted Solvency II directive (2016), with more elaborate, developed and sophisticated risk management systems. The primary concern behind the introduction of these directives is to fix a required amount of capital that needs to be held by EU insurance companies to reduce the risk of insolvency. With close resemblance to the Basel II, this framework also consists of three main components or pillars. The first pillar consists of the quantitative requirements that define the amount of capital an insurance company should hold; the second pillar sets the requirements for the corporate governance, risk management and effective supervision of insurance companies; while the third pillar concentrates on the disclosure and transparency requirements. Due to its close similarity to the banking regulations of Basel II, Solvency II is often called as the "Basel for Insurers". Under the first pillar of the Solvency II, the Solvency Capital Requirement (SCR) is the amount of funds that insurance and reinsurance companies are required to hold in order to have a 99.5% confidence that they can survive the most extreme expected losses over the course of one year.

Enterprise Risk Management

Companies have foreseen and prepared for risks for a long time, even before enterprise risk, as a whole, was thought of. For example, historically, companies have contracted property insurance in order to protect its property from various risks such as natural disasters, fires, unintentional damage, etc. Another example is liability and malpractice insurance, where the insured, or companies, are insured to be protected against lawsuits and other legal claims and liabilities. Considering an insurance policy to protect against risk is one of the oldest and most common risk management strategies, and all actions a company takes in order to protect its operations against risk fall within the boundaries of Enterprise Risk Management (ERM). If a business decides to consider an insurance policy against some kind of risk, it can end up spending a lot of money on a policy that many provide over coverage that may not be used, or under coverage that may not be sufficient for the company when claimed for a particular loss. Hence, it needs to accurately estimate or predict the likeliness of a loss occurring and also estimate the potential impact – financial, physical or reputational - in order to understand what value, it needs to be insured for. This way the business can accurately spend and use the remaining funds, if any, on other business operations. This also improves the trust and confidence of the stakeholders, business owners and other people directly or indirectly interacting with the business. ERM, by the Basel Committee, provides a well-defined framework that allows companies to identify, assess, prioritize, estimate potential loss and protect against the risks it faces, so it can be prepared and make well informed and calculated decisions.

The four types of risks defined in the previous section – strategic, financial, operational and hazard-fall under the category of Enterprise Risk (ER), meaning, all risks faced by an enterprise are

collectively known as ER, and, the management framework of these risks lead to the development of ERM. ERM is a plan-based strategy that aims to identify, assess and prepare for any dangers, hazards and other potential disasters – both physical and figurative –that may interfere with and organizations' operations and objectives (Investopedia, 2019). Risk managers, project managers and other professionals who work with ERM critically focus on assessing the risks relevant to their company, prioritizing them, and making informed decisions on how to handle them. These risk management plans estimate the potential impact of the various disasters, and, also outline the responses in the event of these disasters taking place. ERM is categorically divided into 4 parts, namely, strategic risk management, operational risk management, hazard risk management and financial risk management. In this paper, we will strictly focus on Operational Risk Management (ORM), operational risk modeling, its approaches and responses. Hazard risk, although, has its own modeling, we consider hazard risk to be assessed as a subset of operational risk management.

Studying how corporations manage the incredibly wide number of risks they face, can play an extremely important role in investment-decision making. Knowledge of individual corporate risk-profiles can lead investors to confidently understand and invest, believing that the company is prepared for its risks and is successfully working towards achieving its investor objectives and meeting the expectations of the investors. Investors, shareholders or the public can now decide if they want to allow a company to be part of its community as a new office or plant, trusting that it would do everything necessary to avoid different sorts of damages based on its "risk profile".

Operational Risk Modeling

Canadian Institutes of Actuaries states that Section V.A.644 of Basel II defines Operational Risk (OR) as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk. The Australian Prudential Regulation Authority also expressed a similar definition to life insurers in Section LPG 230. OR potentially exists in all business activities and encompasses a wide range of events, actions and inactions such as fraud, human errors, accounting errors legal actions and system failures. Many of these problems arise during the course of conducting the daily business operations and are typically managed with little or no incident.

As per Institute of Risk Management, UK, firms use operational risk models to quantify and better understand the risks they are facing. These models should be used to inform senior management decisions and firms that have successfully implemented such an approach can ultimately use the model for the purposes of regulatory and economic capital calculation. Most firms are utilizing some form of hybrid modeling approach, with the use of scenarios and loss data in varying combinations and to varying extents in order to calculate their capital figure for operational risk. Firms modeling by frequency and severity separately also appear more willing to use multiple types of distribution depending on the operational risk being modelled and the availability of meaningful loss data.

Operational losses are categorically divided into seven areas in order to gradually identify the source of risks faced by the company. This data can be used to fit into a model that will predict the minimum capital requirement for a company to hold in order to protect itself against potential operational losses. In the next part, we will look at the categorization and collection of operational loss data.

Operational Risk Modeling: Data

Data collection is the most important part of modeling operational loss in order to understand the frequency, influence and impact of operational losses. Efficient data collection helps the model become more efficient and allows the senior management take risk-based decisions. Operational losses are categorized into 7 parts:

I. Internal Fraud:

Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one party.

Examples: Theft of assets, unauthorized use of systems to defraud customer or company.

II. External Fraud:

Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, by a third party.

Examples: Hacking, fraudulent claims, forgery.

III. Employment Practices and Work-space Safety:

Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims or from diversity/ discrimination events.

Examples: Harassment, employee liability, industry activity.

IV. Damage to physical assets:

Losses arising from loss or damage to physical assets from natural disasters or other events.

Examples: Physical asset failure (not systems), losses from terrorism, natural disasters.

V. Business Disruptions and System Failures:

Losses arising from disruption of business or system failures.

Examples: Losses due to hardware, software, IT network, power outage.

VI. Clients, Products and Business Practices:

Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients, or from the nature or design of a product.

Examples: Money laundering, insider dealing, unintentional guarantees to customers.

VII. Execution, Delivery and Process Management:

Losses from failed transaction processing or process management, from relations with trade counter parties and vendors.

Examples: Customer service failure, data entry error, management failure.

Operational Risk Modeling: Approaches

Basel II, and other similar supervisory bodies have recommended various sound standards for Operational Risk Management for financial institutions. In order to complement these standards, Basel II has given guidance to 3 broad methods/approaches of capital calculation for operational risk. The Solvency II, a Directive of EU law for (re)insurance companies, has recommended an approach called, Solvency Capital Requirement (SCR). In the following sections of this part, we aim to expand these recommended methods by referring to the Basel Committee and Solvency frameworks, to gain an understanding of which approach is the best for a given company.

a) Basel II - Basic Indicator Approach (BIA)

BIA is a set of operational risk measurement techniques proposed under Basel II capital adequacy rules specifically for banks but can be used by other financial institutions as well. It is much simpler than the other Basel recommended approaches and has been recommended to financial institutions with insignificant international operations. Based on this approach, financial institutions using the BIA must hold capital reserve for operational risk equal to the average over the previous three years of a fixed percentage of positive annual gross income. If the figures for any year in which annual gross income is negative or zero, they should be excluded from both the numerator and the denominator when calculating the average. The fixed percentage 'alpha' is typically 15% of annual gross income.

Example: Let us assume that a financial institution, X Corp. has an annual gross income of $500, $600 and $650 million respectively in year 1, year 2 and year 3. What is the required capital supposed to be held by X Corp.?

Using the BIA,

$15\% (\$500 + \$600 + \$650) / 3 = \$262.5 / 3 = \$87.5$

(Figures are assumptions for one scenario)

This means, X Corp. is required to hold a capital of $87.5 million for operational risk.

b) Basel II – Standardized Approach

The standardized approach is a set of techniques to measure operational risk proposed under Basel II capital adequacy rules for banking institutions. In terms of degree of complexity, the standardized approach lies between the basic-indicator approach and the advanced-measurement approach. Under this approach, bank activities are categorized into 8 business lines namely:

1. Corporate Finance
2. Trading and Sales
3. Retail Banking
4. Commercial Banking
5. Payment and Settlement
6. Agency Services
7. Asset Management
8. Retail Brokerage

Within each of the business lines mentioned above, gross annual income is a broad indicator that serves as a proxy for the scale of business operations, and hence, also the likely scale of operational risk exposure within each of these business lines. In order to calculate the capital charge for each of the business lines, we multiply the gross income by a factor (beta) or multiplier assigned to that business line. Beta serves as a proxy for the industry-wide relationship between operational risk loss experiences for a given business line and the aggregate level of gross income for that business (Wikipedia, 2017). This version was released in 2014.

Beginning March 4, 2016, the Basel Committee updated its proposal on operational risk capital modeling by introducing a similar and much more robust approach. This approach is called the Standardized Measurement Approach (SMA), under which regulatory capital levels will be determined using a simple formula which also allows us to compare across the industry. This approach is to replace all other approaches, including the complex Advanced Measurement Approach (AMA). The formula for the SMA is given as follows (Source: Bank for International Settlements, www.bis.org):

Operational Risk Capital= Business Indicator Component * Internal Loss Multiplier

According to the Basel Committee, the Business Indicator Component (BIC) corresponds to a progressive measure of income that increases with an institution's size. It also states that it serves as the baseline capital requirement and is calculated by multiplying the Business Indicator (BI) by marginal coefficients. As per the framework, the business indicator is a financial statement-based proxy for operational risk consisting of three elements, each calculated as the average over three years. Marginal coefficients are regulatory determined constants based on the size of the business indicator. The three elements are as follows:

1. The interest, leases and dividend components
2. The services component; and
3. The financial component

The internal loss multiplier (ILM) is a risk sensitive component capturing a bank's internal operational losses. It is meant to serve as a scaling factor that adjusts the baseline capital

requirement depending on the operational loss experience of the institution. As per the Basel framework, it is proportional to the ratio of loss component and the BIC, where the loss component corresponds to 15 times the average annual operational risk losses incurred over the previous 10 years. In order to calculate the loss component, institutions need to meet the loss data identification, collection and treatment requirements.

c) Basel II - Advanced Measurement Approach (AMA)

The last and most complex approach recommended by the Basel committee is the Advanced Measurement Approach, with increased sophistication and risk sensitivity. Institutions using this approach are allowed to develop their own empirical model to quantify the capital required for operational risk. According to Section 664 of the Basel Accord, institutions must satisfy the following conditions, at a minimum, in order to be qualified to use the AMA:

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

An AMA framework must include the use of the following four elements, as per the supervisory guidelines of the BCBS:

1. Internal Loss Data (ILD)
2. External Data(ED)
3. Scenario Analysis (SA)
4. Business Environment and Internal Control Factors (BEICFs)

c i) Loss Distribution Approach

In this section, we examine the modeling of operational loss data, both ILD and ED, using the Loss Distribution Approach (LDA). The use of ILD in the model permits us to incorporate relevant information on the specific characteristics of the risk profile of an institution, as reflected in its loss experience dominated by high frequency events. The use of ED permits us to complement the modeling with the experience of other institutions within the same industry, accompanying ILD with low frequency/high severity events. LDA is the most popular approach for modeling operational risk. It seeks to answer, for a given operational loss event type, what the total aggregate loss an institution might expect over a given period, typically in a year. In this approach we combine two different distributions where one shows the frequency and the other shows the severity of operational losses based on the operational loss data.

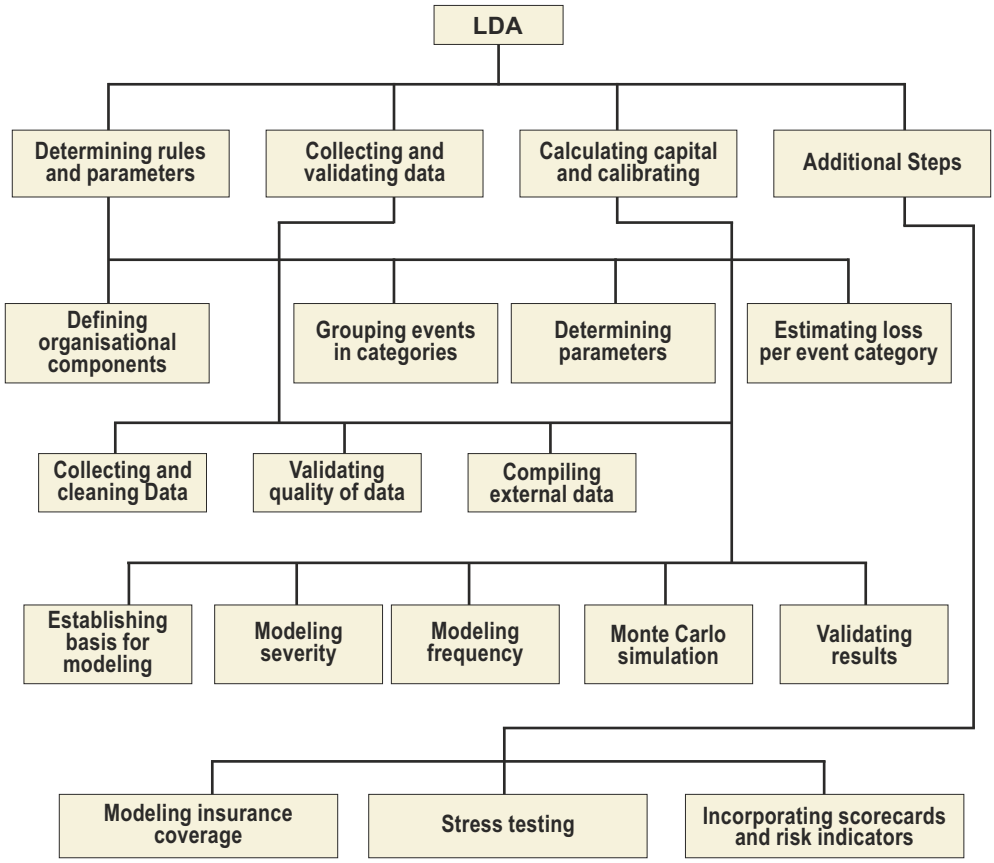
Operational risk is categorised according to a matrix of business lines and operational risk types, which would be standardized by supervisors. Under the LDA, financial institutions quantify

distributions for frequency and severity of operational risk losses for each risk cell (business line/event type) over a 1-year time horizon. The institutions can use their own risk cell structure but, specifically banks, must be able to map the losses to the Basel II risk cells. The standard LDA model expresses the aggregate loss as the sum of individual losses, which gives -

$$L=\Sigma nj=1Lj$$

where L is the aggregate loss, n is the number of losses per year (the frequency of events) and Lj is the loss amount (the severity of events). Hence, losses arise from two sources of randomness, frequency and severity, both of which have to be modelled. It is assumed that frequency and severity are independent, and that L1, … , Ln are independent random variables following the same distribution.

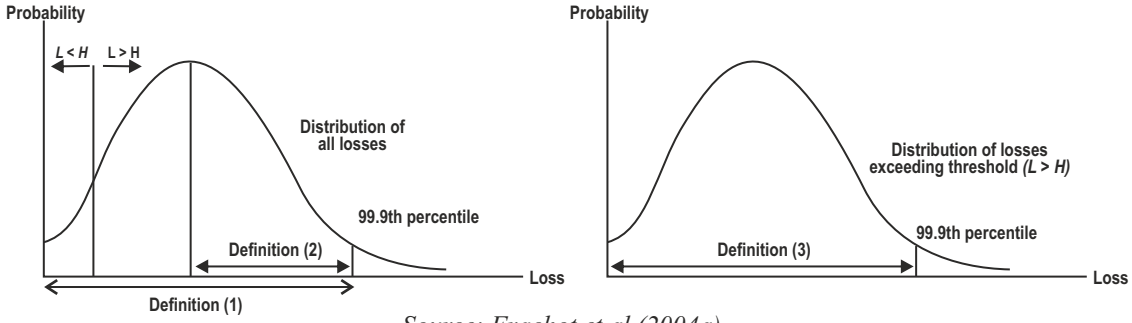
Haubenstock and Hardin (2003) put forward a schematic representation of the LDA, using a step-by-step procedure. This presentation involves three primary steps and additional steps with their components, which are shown in the figure below.



Source: Haubenstock and Hardin (2003)

From the figure above, we can see that the additional steps boil down to the incorporation of scorecards and risk indicators, which means crossing the boundaries of the LDA to the Score Card Approach (SCA). This means that the allocated capital charge is adjusted to reflect the quality of internal controls and the assessment of risk drivers, which is allowed under Basel II. In general, the capital charge is calculated from the total loss distribution (obtained from Monte Carlo simulation) by using the concept of VAR, which is a measure of the maximum limit on potential losses that are unlikely to be exceeded over a given holding period at a certain probability. Frachot et al (2004a) point to the ambiguity about the definition of the capital charge, hence suggesting three alternative definitions. The first definition is that it is the 99.9th percentile of the total loss distribution, which means that the probability of incurring a loss bigger than the operational VAR is 0.1 per cent. The 99.9th percentile implies a 99.9 confidence level that losses would not exceed the percentile (operational VAR). This means that, on average, only one out of 1000 similar banks experience losses that are greater than the percentile. Otherwise, it means that a particular bank would experience such a loss once in a thousand years. The second definition pertains to the unexpected loss only, which means that the capital charge is equal to the difference between the 99.9th percentile and the mean of the distribution. The third definition considers only losses above a threshold, which means that the capital charge is the 99.9th percentile of the distribution of losses in excess of the threshold. The three definitions are represented diagrammatically in the figure below.

Source: Imad A. Moosa, Quantification of Operational Risk under Basel II, Springer Nature, 2008.

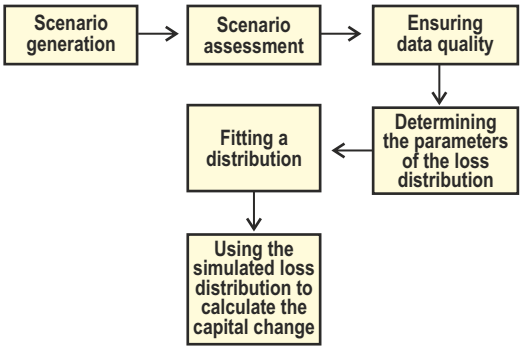


Source: Frachot et al (2004a)

c ii) Scenario Analysis

For events that occur in a very low-frequency, estimating the expected frequency of occurrence may require a long period of observation to collect historical data, at least more than 10 years in this case. This is apart from other parameters such as the mean and standard. deviation of the severity of the operational risk. Scenario Analysis (SA) is a method that allows us to fill this gap by creating synthetic data containing various scenarios. In operational risk modeling, scenario analysis is a means of assuming the amount of loss that will result from, and the frequency of, operational risk incidents that may be faced by a financial institution (Bank of Japan, 2007). If a number of staff members feel that, based on their experience, a loss amounting to several million dollars may occur once in 10 years, it is possible to use this information when formulating risk scenarios (Moosa, 2008). Bilby (2008) defines scenario analysis as a "systematic process of obtaining expert opinions

from business managers and risk management experts to derive reasoned assessment of the likelihood and impact of plausible operational losses." In the SA, the frequency and severity distributions are guesstimated using all available quantitative and qualitative information, including the subjective judgement of business line and senior management (Moosa,2008). Once the simulated loss distribution is obtained, expected and unexpected losses should be compared against similar businesses and evaluated for reasonableness by the risk management team and business line managers. The whole process must be repeated if the risk management team finds the necessity to make adjustments after the comparison. SA consists of the steps as shown in the figure below.



Source: Moosa, 2008

Typically, scenarios used in the analysis are updated on an annual basis and when material changes to the business occur, based on the judgement of experienced risk managers and chief officers in the business, and requires the evaluation of the validity of the scenarios compared to actual experience (Moosa,2008). It is also important to incorporate an appropriate number of low-frequency, high-severity scenarios to represent tail events. Attention is paid to the following points:

a) whether or not the scenario frequency projections match internal annualized loss experience;

b) whether or not the distribution of losses in the scenarios match the actual loss experience; and

c) whether or not the maximum loss data will influence scenario model inputs.

One of the perceived benefits of the SA is that it generates data that can be used to supplement historical data, particularly at the tail of the distribution. For example, it is possible to construct an optimistic scenario, a pessimistic scenario and a catastrophic scenario for operational losses. Once these scenarios have been constructed, these can be converted into three data points that are added to the set of historical data. Otherwise, the weighted average loss resulting from the three scenarios (where the weights are the corresponding probabilities of occurrence) can be added as one data point. Another procedure is to generate the loss-distribution parameters from the scenarios, and these can be combined with similar parameters derived from historical data. The advantage of supplementing historical internal data with scenario data, as opposed to external data, is that external data suffer from different kinds of biases. On the other hand, scenarios are thought to be relevant and most accurate in the absence of good-quality internal data.

Source: Imad A. Moosa, Quantification of Operational Risk under Basel II, Springer Nature, 2008.

c iii) Score Card Approach

Blunden (2003) describes a scorecard as "simply a list of a firm's own assessment of its risks and controls, containing the risk event, risk owner, risk likelihood, risk impact, controls that mitigate the risk event, control owner, control design and control impact". The scores are expressed in monetary terms for potential loss severities, in the number of times per year for potential-loss frequencies, and in the form of ratings for operational qualities, for example, excellent, good, and poor (Moose, 2008). The results derived from this risk evaluation process are reported on scorecards, or simply called questionnaires, and this process defines the "Score Card approach" (SCA). Typically, these results project the scores for operational risk. Although a scorecard may specify a range of expected frequency of occurrence, the exact point on the range would be fixed by scenario analysis, using comparison with actual loss data, or external data when actual internal loss data is unavailable. Frequency may be defined in relation to the frequency classes corresponding to certain probability ranges. For example, an event that is considered to be "almost impossible" has a probability range of 0–0.0001, whereas an event that is considered to be "very likely" falls in the probability range 0.90–1.0.

The SCA depends heavily on the concept of risk classes, Key Risk Drivers (KRDs) and Key Risk Indicators (KRIs). KRDs are defined by the BCBS (2002) as "statistics and/or metrics, often financial, which can provide insight into a bank's risk position." KRDs are obtained from performance measures and from intuition, based on deep knowledge of the business activity. KRIs are a broad category of measures used to monitor the activities and control environment. While drivers constitute an ex ante concept, indicators constitute an ex post concept. Examples of KRIs are profit and loss breaks, open confirmations, failed trades, and system reliability.

c iv) Business Environment and Internal Control Factors

Business environment and internal control factors (BEICFs) are defined as measures that track changes in operational risk in the business environment and changes in the effectiveness of a firm's controls (Basel,2006). The environment is defined by the Risk Management Association (RMA) to include both the internal and external circumstances of the firm's businesses, and, controls are defined as processes that the firm has in place to reduce or eliminate its operational risks. According to the Industry Position Paper published in December 2008 by the RMA, business environment is the internal and external circumstances of a firm's businesses that can materially affect its operational risk profile, which includes:

- the quality and availability of the firm's people, vendors, and other resources;
- the complexity and riskiness of the businesses, the products they deliver and the processes they use to deliver them;
- the degree of automation of the product process and the firm's capacity for automation;
- the legal and regulatory environment for the businesses; and

- the evolution of the firm's markets, including the diversity and sophistication of its customers and counterparties, the liquidity of capital markets it trades in and the reliability of the infrastructure that supports those markets.

Source: (rmaweb.rmahq.org)

Organizations need to have processes in place that can detect and prevent operational risk losses or eliminate operational risk events. These processes are meant to reduce the frequency or the severity of operational risks and their losses. These processes are called internal controls. Factors are leading measures or indicators of change in the environment or in control effectiveness (RMA, 2008). While capital estimation, loss data is excluded from factors in order to avoid double-counting, as this data is already included in the remaining three elements of the AMA approach. Otherwise many kinds of objective and subjective measures can be used as factors, including such things as:

- the number of audit points and other measures tracking regulatory and policy compliance and progress in closing any gaps in the existing practices;
- outputs from risk and control self-assessments, including indicators reflecting the emergence of new risks, the effectiveness of existing controls, control gaps, and progress in closing them; and
- other risk indicators, including general indicators like staff turnover and specific ones like peak capacity utilization in a trading system.

BEICFs are more useful for risk management than measurement. Firms need flexibility to tailor their choice of BEICFs, depending on availability, applicability, usefulness, purpose and integration. If it is ever possible to establish significant statistical relationships with future loss distributions, BEICFs may become more useful in capital estimation. Until then, their use should remain secondary to internal and external loss data and scenario analysis. For capital estimation, there should be an input into scenario analysis or into a global adjustment to a calculated capital estimate reflecting considerations not otherwise taken into account.

An Example of Operational Risk Modeling (Cyber Risk Modeling)

Need for Cyber Risk Modeling

Cyber risk is one of the prominent subsets of operational risks and since provision of Risk Based Capital, Own Risk & Solvency Assessment and Personal Data Protection Act are increasingly becoming essential, modeling of the cyber risks is one of the best suited tools to arrive at the cyber VaR (Value at Risk).

Initial Stage of the Model:

The cyber-risk model was initially developed using percentile method (due to absence of data) and information of cyber-attacks internationally. This was a critical source of information as it provided a world-wide as well as individual country-wise analysis of cyber data breaches of the past. The details provided include cost per data breach, probability of breach in the next two years, mean time

to identify and control the damage post breach, factors that influence the cost of data breach, etc. However, the percentile method was deemed inappropriate as the estimated parameters had high amount of errors while fitting them in the MS Excel model using R software. The main suggestion was to use actual empirical data in the model and make necessary arrangements for collection of the same.

External Data Compilation

There is no reported internal data related to any form of cyber-attack or losses arising due to it. In the absence of internal data, reliance for empirical data was on external data, which was not readily available without charges. Consequently, a rigorous internet search for relevant cyber loss data ensued and finally the loss data of some US organizations from 2004 till 2018 across industries was found. By and large, the data was reasonable, quantifiable and well supported with references, extensive description, media publishing details, etc. Thus, it was concluded to be apt as raw data input for cyber model and subsequently data cleaning and scaling processes were implemented.

Scaling External Data

Scaling of data based on country is required because loss data of US would be typically inflated (after currency conversion) as compared to what could have occurred due to such similar events domestically in India. To offset the inherent inflation in loss data, a country multiplier was used, which was based on 7 types of living costs comparing both countries. The data used for deriving multiplier is relevant, reliable, consistent and accurate. Next, financial scaling of data was done based on value of total assets, revenue and profits of those companies. This exercise was carried out on a selected sample comprising of the most related companies and then some randomly-selected companies, as deriving the financial data for every organization was a very tedious task. The average of these ratios was used for scaling of other data points, and, finally the refined dataset was used in the model.

Model Structure

The internal controls are quantified on a scale between 0 and to estimate the net amount of risk exposure post the effect of controls. Estimates for inflation rates and other parameters are made using the prevailing economic conditions. The data is categorized in 3 types based on the type of attack, namely malicious or criminal attack, system glitch and human error. Macros are written for quantifying copulas in order to account for any existing correlations between the types of attacks. Then the entire data is fitted into a distribution using R, and the calculated parameters are used for running simulations of loss events. The 99th percentile of the simulated data determines the Value at Risk (VaR) in event of a cyber loss. All major factors are sensitivity tested and multiple simulations are run to have a range of values of VaR, which is then tested for consistency.

Need for Scenario Analysis

Scenario-analysis exercise is done in order to account for events which might not have occurred in the empirical data but do have a non-negligible probability of occurrence. It is essentially important

when the empirical data is relatively small. In order to consider 99th percentile, there should be 100 years of empirical cyber loss data, which clearly is not possible. Hence scenario analysis is all the more necessary for such cases.

Scenario Template

An MS Excel template is developed for organization-wide scenario analysis relating to cyber attack, and is filled in by all relevant process owners. To begin with, 3 types of scenarios were finalized for quantification of cyber risk, namely Malware Attack, Website Defacement and DDoS Attack. A sample of scenario analysis was done in order to guide the users in using the template and provide similar inputs for all 3 risk scenarios. The template asked for all the required data for consequent quantification of cyber risks, such as risk category, severity, probability, etc. It also asked for basis on which the inputs were provided, like stakeholders involved, attack category, confidentiality of data, etc. so that the respondents get into the zone to better imagine the whereabouts of that scenario.

Scenario Analysis Process

The filled in templates are tested for completeness, reliability, accuracy and consistency, and subsequently, queries are raised to the respondents when required. The cyber VaR is evaluated using the alternate approach. The process is repeated until a satisfactory value would be deduced which is appropriate for being considered. The alternate approach is used because the respondents are too few and the response data cannot be modeled using traditional methods (like interval approach) with any confidence. Under this approach, for frequency, the mid-points of probability range were used; while for severity, uniform distribution was assumed throughout the range. Each of the responses was individually evaluated for 99th percentile and then arithmetic mean of responses was used to arrive at the final VaR.

Risk Response Strategies

In our journey so far, we have understood how to identify and assess risks using various approaches approved by the Basel Committee. These approaches only help us get to a capital amount that will be required to meet the regulation standards, and protect the company against operational losses in the event of occurrence. These processes, though, do not ensure that the company has diverted itself from the risk by evaluating it. An organization still has the risk of some of the expected loss events coming true and hence, needs response strategies in place to implement them during an event of loss. There are four strategies one can use against risks, namely:

Avoid: Avoid is simply the strategy of wholly avoiding a risk. In order to implement this strategy, a decision is taken in such a way where an organization can avoid a particular risk entirely by doing things differently. For example, after assessing risk before making a decision, senior management can decide not to make an investment in land after realizing that the area is more prone to earthquakes than expected, hence diverting away from the risk.

Reduce: Reduce is a strategy where certain processes are implemented in order to reduce the risk exposure. For example, if a company finds out that the number of a type of employee errors are an exposure to loss, senior management can implement training programs or control processes to train and check the employee operations in order to reduce errors, hence reducing risk exposure.

Transfer: Transfer is a strategy of transferring risk partly or entirely to a third-party entity in order to avoid the potential loss that might impact the business. An insurance is a perfect example of this strategy. A company can choose to get an insurance policy and transfer risk to the insurance company by paying a small amount of premium periodically, and hence, in the event of loss the policy kicks in and helps the company indemnify after the loss.

Accept: Accept is a strategy where an organisation simply accepts the risk and implements a business decision that is thought of before assessing the risk. Sometimes, it can be efficient for an organization to just accept the risk and avoid the greater costs of practices such as transferring risk or implementing control processes that will reduce the risk.

References

- Kenton, W. (2019, July 02),"How Enterprise Risk Management (ERM) Works", Retrieved from https://www.investopedia.com/terms/e/enterprise-risk-management.asp
- Cummins, J.D. (1998, February),"The Rise of Risk Management". Retrieved from https://www.researchgate.net/publication/5025590_The_rise_of_risk_management
- Pearson, S. (2018, August 03), What is Operational Risk Management:Definition and Core Concepts. Retrieved from https://tallyfy.com/operational-risk-management/
- Moosa, I. (2008), Quantification of Operational Risk under Basel II: The Good, the Bad and the Ugly. Retrieved from https://researchbank.rmit.edu.au/view/rmit:21454
- Institute of Risk Management, (n.d.). Operational Risk Modeling: Common Practices and Future Development. Retrieved from https://www.theirm.org/media/1454276/IRM_Operational-Risks_Booklet_hi-res_web-2-.pdf
- https://en.wikipedia.org/wiki/Standardized_approach_(operational_risk)
- https://quizlet.com/15768703/operational-risk-management-flash-cards/
- https://www.slideshare.net/jigyasasoni1/summer-training-report-on-operational-risk-management-at-state-bank-of-bikaner
- http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/587400/IPOL_IDA(2017)587400_EN.pdf
- https://www.openriskmanual.org/wiki/Business_Execution

♦♦♦