Muhammad SHAHBAZ

A FRAMEWORK FOR MEASUREMENT AND IMPLEMENTATION OF OPERATIONAL RISK MANAGEMENT IN SMALL AND MEDIUM ENTERPRISES (SMEs)

M.S.
2013

FATİH UNIVERSITY

The Graduate School of Sciences and Engineering

Master of Science in
Industrial Engineering

A FRAMEWORK FOR MEASUREMENT AND IMPLEMENTATION OF OPERATIONAL RISK MANAGEMENT IN SMALL AND MEDIUM ENTERPRISES (SMEs)

by

Muhammad SHAHBAZ

September 2013

A FRAMEWORK FOR MEASUREMENT AND IMPLEMENTATION OF OPERATIONAL RISK MANAGEMENT IN SMALL AND MEDIUM ENTERPRISES (SMEs)

by

Muhammad SHAHBAZ

A thesis submitted to

the Graduate School of Sciences and Engineering

of

Fatih University

in partial fulfillment of the requirements for the degree of

Master of Science

in

Industrial Engineering

September 2013
Istanbul, Turkey

APPROVAL PAGE

This is to certify that I have read this thesis written by Muhammad SHAHBAZ and that in my opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science in Industrial Engineering.

_____
Prof. Dr. Nader NADA
Thesis Supervisor

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science in Industrial Engineering.

_____
Assoc. Prof. Dr. Ali TÜRKYILMAZ
Head of Department

Examining Committee Members

Prof. Dr. Nader NADA _____

Assist. Prof. Dr. Özgür UYSAL _____

Prof. Dr. Cevdet MERIÇ _____

It is approved that this thesis has been written in compliance with the formatting rules laid down by the Graduate School of Sciences and Engineering.

_____
Assoc. Prof. Dr. Nurullah ARSLAN
Director

September 2013

A FRAMEWORK FOR MEASUREMENT AND IMPLEMENTATION OF OPERATIONAL RISK MANAGEMENT IN SMALL AND MEDIUM ENTERPRISES (SMEs)

Muhammad SHAHBAZ

M.S. Thesis – Industrial Engineering
September 2013

Thesis Supervisor: Prof. Dr. Nader NADA

ABSTRACT

Small and Medium Enterprises (SMEs) encounter many internal and external problems that distract SMEs from their main business goals. These problems create operational risks for market share, economic crisis, production and manufacturing. To deal with this disturbances SMEs need a systematic approach, tools and techniques to identify and treat these potential risks. The purpose of this research is to find a practical solution for measurement and implementation of operational risk management system in SMEs that co-relates the presented model and operational risk management different dimensions. The thesis demonstrates how quantitative modeling of risk can be undertaken for SMEs based on opinions provided by experts within the organization. This research offers an affordable and effective framework for SMEs operational risk management and minimization through operational risk modeling, and model validation through data collection, analysis and verification.

Keywords: Operational Risk, Market risk, Quantitative modeling, Framework.

KÜÇÜK VE ORTA ÖLÇEKLİ İŞLETMELERDE (KOBİ) OPERASYONEL RİSK YÖNETİMİ ÖLÇME VE UYGULANMA SİSTEMİ

Muhammad SHAHBAZ

Yüksek Lisans Tezi – Endüstri Mühendisliği
Eylül 2013

Tez Danışmanı: Prof. Dr. Nader NADA

ÖZ

Küçük ve orta ölçekli bir çok şirket iç ve dış problemle karşılaşır ki bu durum onları iş amaçlarından uzaklaştırır. Bu problemler pazar payı, ekonomik kriz, üretim ve imalat için operasyonel risk meydana getirir. KOBİ'lerin olası riskleriyle başadebilmeleri için sistemli bir yaklaşımla, araç gereçleri ve teknikleri tesbit etmek gerekir. Bu araştırmanın amacı sunulan model ve Operasyonel Risk Yönetiminin farklı boyutlarıyla ilgilenmek, KOBİ'lerde Operasyonel Risk Yönetimi Sistemi uygulama ve ölçümü için pratik bir çözüm bulmaktır. Tez, risk sayısal modelleme örgütü içinde bir organizasyon bünyesinde uzman kişilerin görüşlerine dayalı KOBİ'ler için yapılabilir hale getirilmiştir. Bu araştırmada düşük bütçeli ve etkili bir operasyonel risk modelleme yoluyla KOBİ'lerin Operasyonel Risk Yönetimi çerçevesinde veri toplama ve analiz doğrulama ile model doğrulama sunuluyor.

Anahtar Kelimeler: Operasyonel Risk, Pazar Riski, Sayisal Modelleme (Nicel Modelleme), Sistem.

To my parents

ACKNOWLEDGEMENT

First and foremost, I thank Allah Almighty for endowing me with health, patience, and knowledge to complete this work. Acknowledgement is due to the Fatih University for the support given to this research through its excellent facilities and for granting me the opportunity to pursue my graduate studies.

This study would not have been possible without the support and guidance of a number of people and organizations. I would like to express my gratitude to my supervisor, Prof. Dr. Nader NADA, for his continuous support, patience, motivation, enthusiasm and immense knowledge. I could not have imagined having a better advisor for my master thesis.

Likewise I am thankful to the other faculty members, Assoc. Prof. Dr. Ali TÜRKYILMAZ, Prof. Dr. Cevdet MERİÇ, Muhammet Enis BULAK, and Leyla TEMİZER for their help and assistance during the period of research and data analysis.

TABLE OF CONTENTS

LIST OF TABLES

TABLE

LIST OF FIGURES

FIGURE

LIST OF SYMBOLS AND ABBREVIATIONS

SYMBOL/ABBREVIATION

SMEs	Small and Medium Enterprises
BCBS	Basel Committee on Banking Supervision7
JMP	Jump Data Analysis Software
KOSGEB	Small and Medium Enterprise Development Organization
AVIAD	Eurasia Business Association
SMEDA	Small and Medium Enterprises Authority
KPI	Key Process Indicators
KRI	Key Risk Indicators
EIF	European Investment Fund
ICF	Internal Control Framework
HR	Human Resources
IT	Information Technology
OECD	Organization for Economic Co-operation and Development
SC	Strategic Capability
OC	Operational Capability
AC	Adaptive Capability
MC	Operational Capability
MC	Managerial Capability
ORMF	Operational Risk Management Framework
ORM	Operational Risk Management
VS	Visual Strategy
F	Finance
BS	Business Sustainability
PcM	Process Management

PrM	Performance Management
R	Resilience
HS	Horizon Scanning
SP	Succession Planning
DM	Decision Making
BIS	Bank for International Settlements

CHAPTER 1

INTRODUCTION

1.1 CONTEXT OF THESIS

The purpose of this research is to find a practical solution for measurement and implementation of operational risk management system in Small and Medium Enterprises (SMEs). Small and medium enterprises encounter many internal and external problems that distract SMEs from their main business goals. These problems create risk for market share, economic crisis, production and manufacturing of an SME. To overcome these problems, smooth running of an SME is a significant challenge. To deal with these disturbances SMEs need a systematic approach and tools to identify and treat these potential risks.

"Operational risk is defined as the risk of losses 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." (BCBS, 2005)

Micro, small and medium sized enterprises are the back-bone and engine of a country's economy. They play a vital role in creating opportunities for jobs, innovation and entrepreneurship. However, in the start up or during the running stage they are confronted with market imperfections, lack of obtaining capital, access to innovation and technology. So, listening to SME is a key to successful economy that reduces unemployment.

So far, operational risk management system has been studied and applied in large companies while a little knowledge is available for SMEs. Because SMEs has small number of employees and products, that's why it is considered difficult to implement operational risk management system in SMEs. The purpose of this research is to find a

practical solution for measurement and implementation of operational risk management system in SMEs that co-relates the presented model and operational risk management different dimensions.

1.2 THESIS FORMAT

There are five chapters that include Chapter 1 Introduction, Chapter 2 Literature Review, Chapter 3 Operational risk Management Model, Chapter 4 Data Collection and Results, Chapter 5 Conclusion. There are two questionnaires related to operational risk and operational risk management model respectively. These questionnaires are the primary source for collecting data through survey.

1.3 RESEARCH QUESTION

As we know that there few data is available on operational losses in SMEs. So, data is collected from the experts in SMEs who have sufficient knowledge to understand and answer the questions asked. The thesis gives a framework of operational risk management for SMEs that is effective and efficient.

The research aims to:

- Identify what the operational risks are for SMEs.
- Measure the frequency and severity of occurrence.
- Level of Operational Risk.
- Check the dependencies of operational risk within the created model.

After the literature review, following research questions have been formulated.

1. How should SME manage the operational risk?
2. What is the relationship of operational risk management with the capabilities of SMEs?

1.4 HYPOTHESIS

Hypothesis 1. High level of Operational Risk management is associated with improved Process/Operational performance.

Hypothesis 2. High level of Operational Risk management is associated with improved Managerial performance.

Hypothesis 3. High level of Operational Risk management is associated with improved Strategic Capability.

Hypothesis 4. High level of Operational Risk management is associated with improved Adaptive Capability.

1.5 METHODOLOGY

The development of the operational risk measurement and implementation framework is the main goal of the thesis. The empirical study starts from a questionnaire prepared for the middle level management of a company. The questionnaire is designed to explore the level of the capabilities of an SME and investigate the disturbances due to the lack of operational risk management. The questionnaire contains five areas that need to be focused. The following five areas will be explained in chapter 3.

1. Operational Risk
2. Strategic Capabilities
3. Adaptive Capabilities
4. Operational Capabilities
5. Managerial Capabilities

A multiple choice, online questionnaire was conducted through e-mail and meeting face to face with officials. The organizations which work for the development and consultancy of the SMEs were also contacted in every country of interest to conduct the survey.

Questionnaire was sent to more than 900 SMEs majorly Turkey, Pakistan and Denmark. All these 900 SMEs are a blend of different sector. There is no restriction of manufacturing or service industry. Out of 900 SMEs, with a response rate of 13 %, 119 companies participated in the research work. Out of these 119, some of these companies did not fully participated in filling out the survey form. So, the responses of 9 companies were excluded from the data analysis because of their missing values in questionnaire.

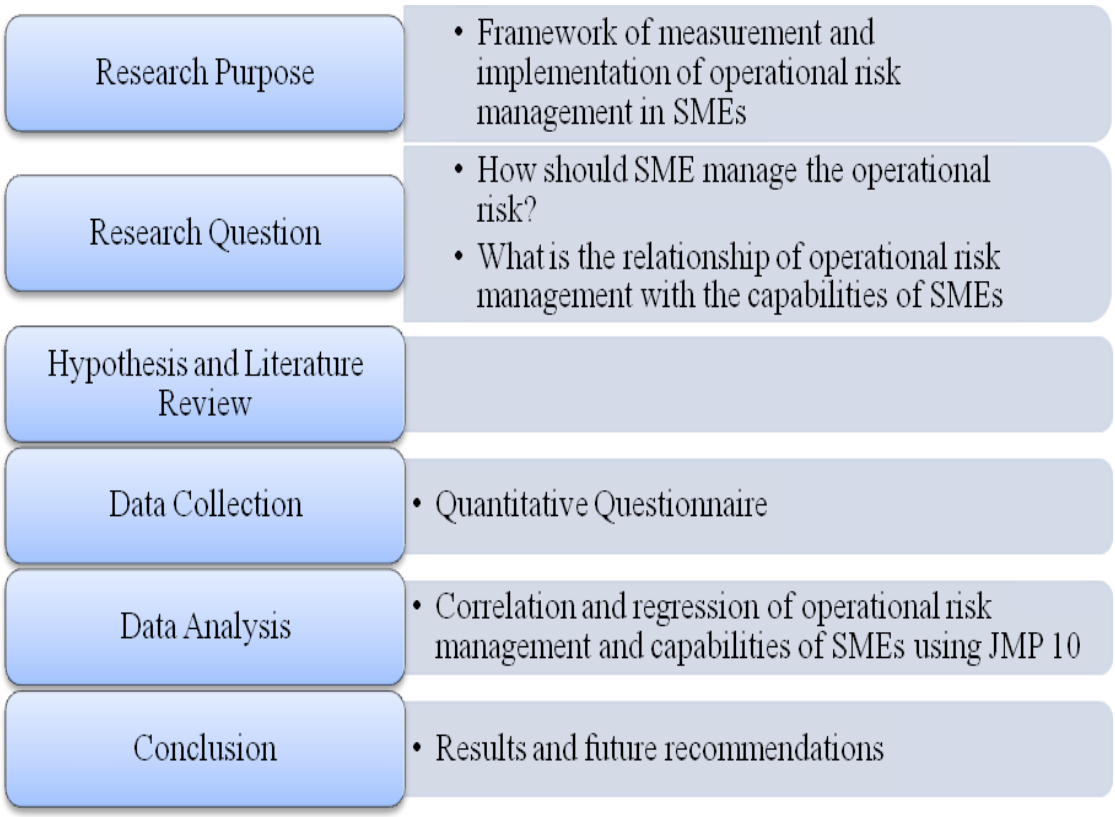


Figure 1.1 Outline of the research.

The questionnaire was designed in a way that can easily be understood and answered. The questionnaire also addresses the amount of internal and external losses in terms of money. This is the most difficult part of the questionnaire because companies do not want to share their financial information. The questionnaire is scaled from 1 to 5 and each question has the same weight. Because of this reason, the summation of the questions

makes one variable. Whereas 1 gives the minimum value and 5 gives maximum value. The questionnaire contains total of 184 questions, out of 184 there are 89 questions to access the level of operational risk and 95 questions to access the level of the capabilities of SMEs. The data was collected in the period of three months. After the data collection stage, multivariate statistical analyses via JMP 10 software package from SAS were conducted in order to validate the hypothesis. Occasional missing data were replaced by the average value through substitution method.

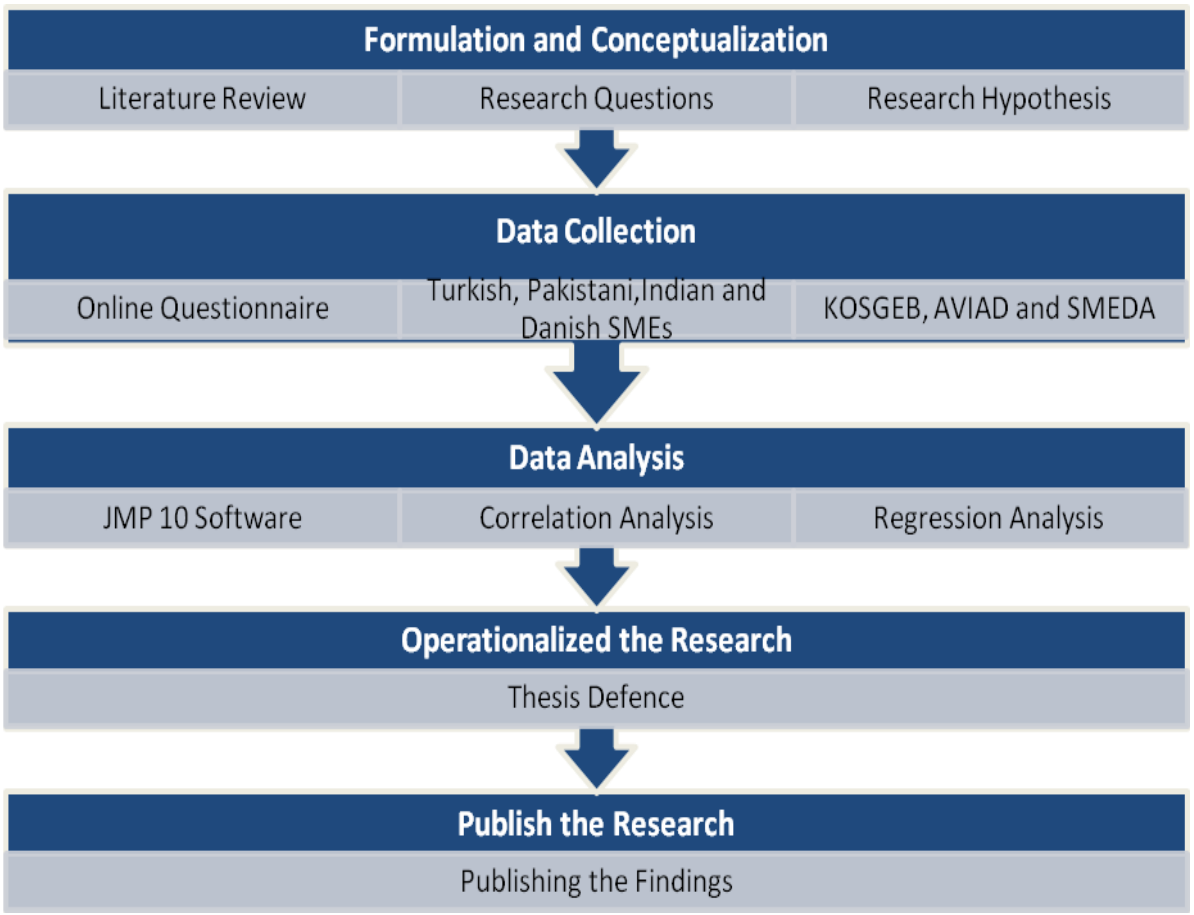


Figure 1.2 Research methodology.

1.6 LIMITATIONS AND DELIMITATIONS

The limitations that hindered to conduct the study are the time factor. The SMEs are not willing to share their financial information and other type of confidential data. The data collected and framework presented may predict that how big the risk will be but cannot predict the future. How much losses will occur is unpredictable because future could be different. As operational risk is mostly used in financial sectors, that's why it may differ from SME.

Operational risk is not a well known term in SMEs. Not too many SMEs really considering operational risk as part of procedure. It was a difficult task to conduct this survey because a few numbers of senior management know about the operational risk management. Being a foreigner here in Turkey, it was really a difficult task to convince a SME to participate in the study.

The framework of thesis accounts for both industries manufacturing and service. Operational risk may have a higher impact in manufacturing and production industries rather than service industry. The study addresses only operational risk, not other type of risks like insurance and credit risk. Also the thesis does not focus on the aftermath of the risk. This can be a different topic of crisis management.

1.7 SIGNIFICANCE OF THE RESEARCH

The research is of significance to the reduction of losses due to operational risk in small and medium enterprises by proposing an ORMF. This study has been of significance to over 100 international SMEs mainly from Pakistan, Turkey and Denmark. The research is conducted through an online questionnaire to get quicker response. The concept of the operational risk is relatively new in majority of the small and medium enterprises. Therefore the handful of SMEs who have acknowledged about the ORM will help to raise the awareness among the others. The study is also important in terms of SMEs and operational risk management because operational risk is generally known in financial sectors. SMEs are not familiar with the operational risk and its losses.

CHAPTER 2

LITERATURE REVIEW

In this chapter seven frameworks of operational risk management during the period 2002 – 2013 have been described. Each framework has been discussed according to the researcher's perspective. All these seven frameworks are written with different perspective of operational risk in different fields. The content of each framework and its results, if any, finally all the seven frameworks are compared with each other. Through all this exercise a new framework has been developed that fits according to the activities of small and medium sized enterprises (SMEs). The frameworks reviewed and discussed in this chapter are;

1. Operational Risk Management Framework (Michael Haubenstock, 2002)
2. An Operational Risk Management Framework for Managing Agencies (John Thirlwell, 2004)
3. Operational Risk Management Framework for Service Outsourcing: Consideration of Risk Dimensions and their Application into the Framework (Zaw Zaw Aung, 2008)
4. Framework of Operational Risk for Information Security (ISRMC and LLC, 2009)
5. Operational Risk Management Charter (European Investment Fund, 2010)
6. Operational Risk Management in Practice: Implementation, Success Factors and Pitfalls (Dr. Daniel Imfelf and Dr. Claus Huber, 2011
7. Operational Risk Modeling Framework (Joshua Corrigan and Paola Rusachi, 2013)

In the last ten years, quality approaches to risk management have been developed and it has become an important issue for most responsible managers (KPMG, 2003). The financial crisis of 2008 - 09 showed how manifold risks are and that most companies and countries underestimated the complexity of risks. Poor risk management played a key role in the meltdown of the financial system (Fratianni & Marchionne, 2009). Operational risk is one of several risks a company faces. Other risks are market risk, credit risk, investment risk and insurance risks. The literature on operational risk has evolved tremendously and covers a wide spectrum of research topics (McNeil, Frey & Embrechts 2005).

2.1 FRAMEWORK 1

Michael Haubenstock has written this operational risk management framework in the perspective of terrorist attacks on United States of America. According to him, terrorist attacks on US gave birth to the different type of risk to the institutions. Business continuity, diversification and human resources are one of those risks which jumped suddenly. These are operational risks which need to be managed, control, access and mitigate.

According to Basel Committee on Banking Supervision (BCBS) ten qualitative principles of operational risk management will have to be implemented for a firm to be eligible to use the more advanced models. These ten qualitative principles are described as below:

1. The board of directors should be aware of the major aspects of operational risk, approve and periodically review the operational risk management framework.
2. The board of directors should ensure that the framework is subject to effective internal audit.
3. Senior management has responsibility for implementing the framework, and all levels of staff should understand their responsibilities.
4. Banks should identify the operational risk in all products, activities, processes and systems for both existing operations and new products.

5. Banks should establish the processes to regularly monitor operational risk profiles and material exposure to losses.
6. Banks should have policies, processes and procedures to control or mitigate operational risk. They should assess the feasibility of alternative strategies and adjust their exposures appropriately.
7. Banks should have in place contingency and business continuity plans to ensure their ability to operate as going concerns in the event of business disruption.
8. Bank supervisors should require banks to have an effective operational risk management strategy as part of an overall approach to risk management.
9. Supervisors should conduct regular independent evaluations of the related bank operational risk management strategies.
10. Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

This framework considers four major components of operational risk management framework; Strategy, Process, Infrastructure and Environment. These four major components are further divided into sub-components (see figure 2.1).

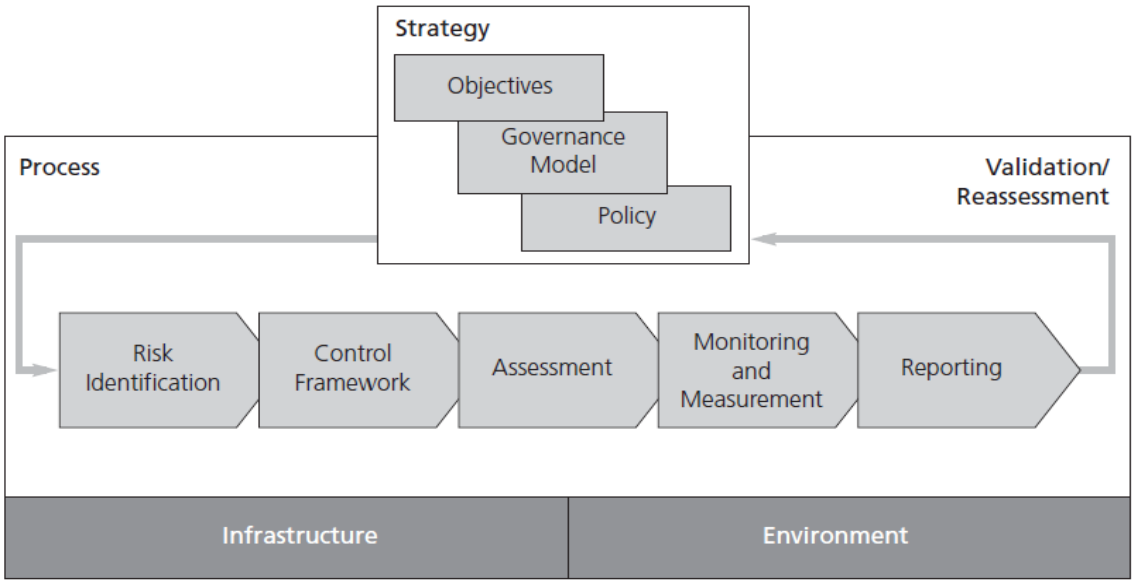


Figure 2.1 Operational risk management framework (Haubenstock, 2002).

2.1.1 Strategy

According to Haubenstock, strategy is the place where senior management starts to involve. Strategy is further categorized into business objectives, governance model and policy. Business objectives should define the risk appetite and what level of risk is acceptable. The definition of this governance model includes the roles, authority levels and accountabilities of each organizational component. Any organizational model requires the right people. The right skills base, combined with a training program for both operational risk staff and other affected people in the organization, becomes an important consideration for success. Corporate policy sets the overall strategy for operational risk management. Policies often start with the objectives of operational risk management. Also the policy might describe the expectations for the use of tools and reporting. A policy statement might discuss the governance model and related roles and responsibilities. This would include any committees that have operational risk as part of their scope, the roles of any central operational risk group, responsibilities of the business lines, and involvement with other staff groups such as compliance, legal, insurance, information technology and human resources.

2.1.2 The Operational Risk Process

The framework describes operational risk process as day-to-day activities required to understand and manage operational risks. The operational risk process includes risk identification, control framework, assessment, measurement and monitoring and reporting (see figure 2.2). In this framework six types of measure are applied to the operational risk.

1. Risk Indicators
2. Loss History
3. Capital Models
4. Performance Measures
5. Risk Drivers
6. Casual Models

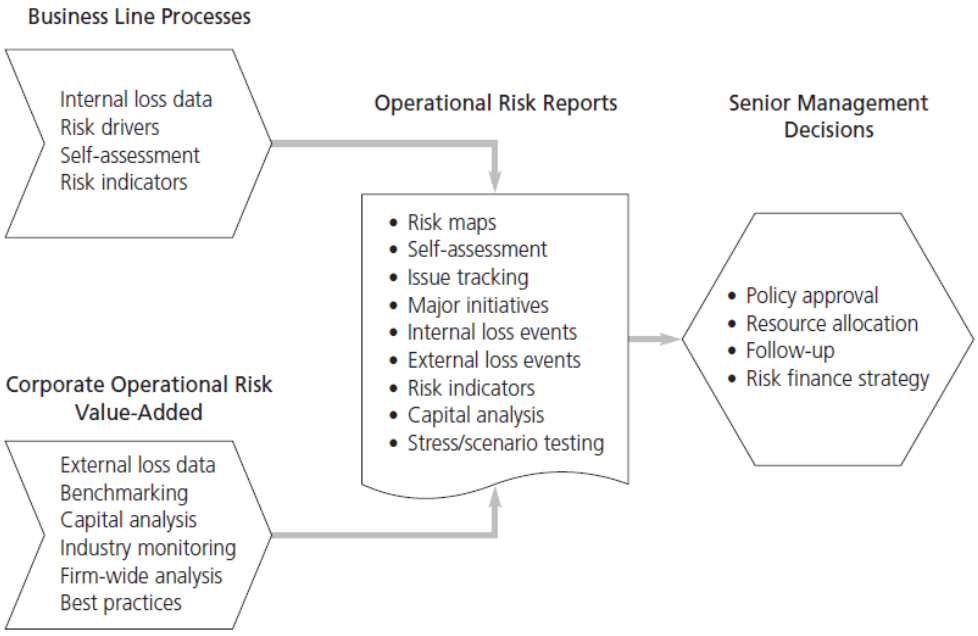


Figure 2.2 Operational risk management reporting process (Haubenstock, 2002).

2.1.3 Infrastructure

According to Haubenstock, infrastructure refers to the tools used to facilitate the entire risk management process. Infrastructure is the tangible components that are used to support decision-making in the process. Typical components of the infrastructure include systems, data, methodologies, and policies and procedures. While data are the core objectives and technology is a necessary enabler.

2.1.4 Environmental

The environment refers to the surroundings that set the tone and behavior of the organization. The primary component is the culture that supports the risk management objectives. We can define culture as the set of shared attitudes, values, goals and practices that characterize how a company considers risk in its day-to-day activities. Culture can either be explicitly formulated or be allowed to evolve over time. The definition of the entire risk management framework is an explicit communication of the desired culture.

Environment is also about communications. The institution's mission and strategy are clearly communicated, are understood, and individuals understand the overall mission and their individual organization's role in its achievement. Consideration of risk is an explicit part of business planning. Policies are also a type of communication. Comprehensive policies should exist, individuals should understand them and feel they provide constructive guidance, and the level of risk appetite must be understood and communicated. Individuals must receive timely, relevant and sufficient information to do their jobs.

2.2 FRAMEWORK 2

This framework is generally made for the banks. John Thirlwell describes how operational risk was evolved, what are the regulators and building blocks of operational risk. He mainly describes four dimensions of the operational risk. That is: Definition, Key Risk Indicators, Monitoring and reporting, Control and mitigation. He defines operational risk as;

> "The risk of loss resulting from inadequate or failed internal processes, people, system or from external events." (BBA/RMA/ISDA survey, 1999)

According to Thirlwell, operational risk is difficult to identify because it is soft risk not always linked to the transactions. Also it is difficult to identify because it is from people and external event. He explains evolution of operational risk as a result of financial crisis of 1990s. The companies like Barings, All First and NatWest had a great loss due to the operational risk. Also Bank regulators, the new Basel Capital Accord and the 'plug' factor (1998 – 2008) are the reasons of the evolution of operational risk. In this framework following dimensions of operational risk are considered;

Developing strategies to identify, assess, monitor and control and mitigate operational risk. Codify firm-level policies and procedures; design and implement assessment methodology; design and implement operational risk reporting system. Operational risk assessment system must play a prominent role in risk reporting, management reporting and risk analysis. He puts great emphasis on the documentations. Requirements for the

strategies of operational risk must be implemented consistently throughout the organization.

In the limitations of the operational risk management framework for banking sector, Thirlwell says that there are limitations for the quantitative analysis because of the lack of data. Also there is risk within the risk tolerance of an organization. Lack of awareness among staff, lack of senior management support are also the limitations of operational risk management. Then seven categories of operational are discussed with examples.

2.3 FRAMEWORK 3

This framework discusses on managing operational risks in an organization where one or more business processes are being outsourced. As outsourcing is becoming mandate for survival of the organizations, firms are compulsively outsourcing more and more of their business processes and services. Many organizations fail to give substantial attention to outsourcing related operational risks' complexity. The five-phase process of Bayesian-KRI networks development is discussed in the paper. The application of proposed framework is illustrated with a sample network reflecting actual business environments. Zaw Zaw Aung classifies operational risk into three main categories.

1. External Risk
2. Conduct Risk
3. Process Risk

He defines operational risk in outsourcing business as Basel Committee on Banking Supervision (BCBS) that

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

This study focuses on the framework that handles the risks arising from complexity of outsourcing processes. According to Aung, there are nine casual factors to risk

occurrence are; people, technology, external events, strategy or policy, corporate governance, organization culture, management, process and business conditions.

The development of the framework starts with the risk identification and justification that leads to critical success factors and then critical to non-critical activities. The figure 2.3 describes the idea of key risk identification. Finally it ends with the monitoring and reporting of the operational risk.

This paper discusses a number of fundamental building blocks for sound operational risk management and it demonstrate how operational manager can utilize the proposed framework in a variety of business condition. With this approach, an automated dynamic risk monitoring is highly expected as a future work.

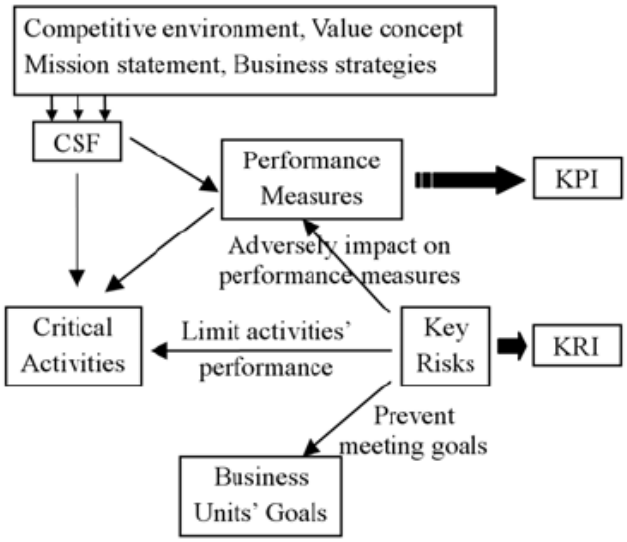


Figure 2.3 The process of key risk identification (Zaw Zaw Aung, 2009).

Then Aung comes to the three dimensions of risk that are, probability, severity and complexity. After identifying and ranking critical risk points, Aung is to construct risk monitoring networks based on underlying risk indicators using Bayesian Network methodology and Causal analysis to identify the major cause of risk. This framework can

also assist risk manager in a variety of analysis and forecasting tasks. Under causal analysis, new evidence of operational risk exposure can be used to calculate the updated probabilities.

2.4 FRAMEWORK 4

ISRMC and LLC were founded in 2008, and are privately held. The framework of operational risk management is prepared for the information security. According to ISRMC and LLC the operational risk framework is based on the following four-step process;

1. Assess the risks in the business
   Inventory the processes, technology and other business assets
   Determine the risk profile
   Assess the inherent risk for each process
2. Implement controls to mitigate those risks
   Inventory the existing controls
   Determine if the controls adequately address the risk or if modifications or additional controls are necessary
   Assess the residual risk of each process based on these controls
3. Monitor the performance of those controls
   Implement periodic testing and reporting to identify deficiencies in controls
4. Respond to instances where the controls are deficient
   Implement procedures to limit losses caused by control failures
   Create a process of continuous improvement that adjusts controls based on changes to the risk environment and repeat.

2.5 FRAMEWORK 5

European Investment Fund presented a charter on operational risk management during the board of directors meeting in 2010. According to this charter the management of

operational risk is a key feature of sound risk management practice in modern financial markets. The recognition of operational risk as a specific category next to market and credit risk by the Basel Committee on Banking Supervision in the Revised International Capital Framework demonstrates its growing importance. The Charter codifies European Investment Fund's approach to identifying, measuring, managing, reporting and controlling operational risk. The document also defines operational risk as the Basel Committee on Banking Supervision (BCBS).

> "Operational Risk is defined as the risk of loss or reputational damage resulting from inadequate or failed internal processes, people and systems or from external events."

The framework of operational risk management according to European Investment Fund is given below.

2.5.1 Operational Risk Management Tools

The main components of the Framework, supporting the identification, assessment, measurement and reporting of operational risk, and the objectives of each, are the following:

1. Process Risk & Control Assessment
2. The identification of the risks inherent to EIF's activities and environment, the assessment of the adequacy of the related internal controls to determine the residual risk for the organization and the classification of the risks according to their potential impact and likelihood.
3. Key Risk Indicators
4. These are the identification and analysis of parameters that can be considered as indicators of the level of operational risk within the organization. The Process Risk & Control Assessment enables a focus on indicators related to the most risky activities and processes.
5. Operational Risk Events

6. The collection and analysis of operational risk events, including the identification of the root cause that has led to their occurrence and the definition of a remediation plan.
7. Scenario Analysis
8. It enables he assessment of the impact and the likelihood of potential OREs and the proactive mitigation of the identified risks. Scenario analysis also enables an organization to gain a better understanding of the risks that it could face under extreme conditions.
9. New Mandates, Products & Processes
10. It includes the framework for the proactive identification and assessment of risks inherent to new products and mandates as well as to projects that have a material impact on EIF's operational processes.
11. Operational Risk Awareness Program

The organization of trainings, workshops and information sessions to build up an operational risk management culture within the organization and to inform EIF Staff about specific operational risk management tools and processes. The internal operational risk culture is the combined set of individual and corporate values, attitudes, competencies and behavior that determine a firm's commitment to and style of operational risk management.

2.5.2 Relationship with Stakeholders

The overall assessment of operational risk at EIF resulting from the implementation of the Framework, and particularly the Process Risk & Control Assessment, will be shared with the Audit Board in the form of the EIF Internal Control Framework (ICF).

2.6 FRAMEWORK 6

In this article, Huber and Imfeld focus on operational risk management for mid-sized asset management companies which are not part of a large international banking organization and hence will not have fully developed staff departments for operational risk.

As the operational risk management is increasingly important - not only for large companies but also for other asset management companies such as private equity companies, family offices or independent asset managers.

2.6.1 Risk Identification

According to Huber and Imfeld, mid size asset managers face many specific challenges. There are large asset base under management, but a small number of employees. The financial assets are comparable to large industrial corporations with several thousand employees. Segregation of duties in such small organizations is difficult. There is increase in regulatory focus and burden. Also there is a creative business environment for portfolio managers and product structures. Often young organizations do not have tradition of risk and control management or structured processes.

In this article the systematic operational risk starts from risk identification and risk reassessment to mitigation, controlling, reporting and to finally defining a risk strategy in line with the risk policy. Important points in risk assessment are that the risk is made visible to people in the organization, thereby raising awareness, naming an owner for the risk and clearly assigning responsibilities. In other risk identification instruments, Huber and Imfeld describe loss data collection on actual loss events and key risk indicators as an early warning system. The loss events may include;

1. Customer complaints
2. Internal fraud case
3. Loss of legal documents

Using key risk indicators as a method for risk identification is usually the case in organizations that have developed a few years of experience with risk assessments and systematic loss data collection. Based on the latter, some key risks might have been identified for which an early warning risk (Huber and Imfeld, 2010).

2.6.2 Risk Mitigation and Control System

In order to adequately assess the impact of an identified risk on the organization's business, one has to consider existing controls and mitigating measures that already reduce the likelihood and/or severity of the risk scenario identified. A risk mitigating measure, in contrast to a control, is usually a one-time measure for which an implementation dates and a responsible person is defined (Huber and Imfeld, 2010).

For the mitigation of risk both writers have given a four eye principle for transaction of more than one million Euros for a specific case in the article. In this article the risk mitigation technique is a strict screening process of all individuals who work in that particular portfolio management.

2.6.3 Risk Controlling and Reporting

The goal of the risk management process, regarding this article of Huber and Imfeld, is to keep identified risks in line with the risk policy and risk strategy approved by the board of directors and the executive team. For a successful flow of information about operational risk an integrated risk and control overview can help timely reporting and mitigation of operation risk. There should be a simple work flow to keep things simple. In this article a Dashboard idea is given for the successful mitigation and control of risk.

2.6.4 Risk Strategy

After making a plan of identification, controlling, mitigation and reporting the risk manager should find the answers of the following questions to make better strategy.

1. Which risks need further mitigation and a prioritized action plan with approved budget for implementation since they might endanger specific company goals?
2. Which risks can be accepted without further mitigation?
3. Where can the company save costs by giving up historically established mitigation measures or controls since the risks are not really threatening company goals? This will allow to save cost in insurance, hedging, unnecessary security measures or to save time by giving up unnecessary control activities.

4. Which risks diversify within the organization? Often risks seem important from one department's point of view, but for the organization as a whole the risk is diversified and acceptable.
5. Which risks or risk combinations need further analysis and investigation or the development of additional risk evaluation tools like an early warning system, detailed scenario modeling and stress testing or systematic loss tracking?
   (Huber and Imfeld, 2010)

2.7 FRAMEWORK 7

This is the most recent presented operational risk management framework by Joshua and Rusachi in 2013. Both authors of this research propose following components for an effective operational risk management framework in an organization.

1. Risk identification
2. Risk assessment
3. Risk capital assessment
4. Risk monitoring
5. Risk mitigation
6. Risk appetite and risk limit settings
7. Risk sensitivity analysis
8. Emerging risk assessment
9. Risk culture assessment
10. Risk reporting, distribution and communication

2.8 FRAMEWORK COMPARISON AND DISCUSSION

In this section, a comparison between the previous reviewed frameworks is presented as shown in table 2.1 and highlighting the weaknesses of these frameworks then a general discussion. The literature review shows that there some spaces for a comprehensive

operational risk management framework in every author's or organization's framework. This is because of the perspective or the interest of the author or organization. Every operational risk management framework discussed above has its own dimensions. One of the eight dimensions "Business Resiliency and Continuity" has not been discussed for a comprehensive operational risk management framework. Likewise some authors missed Role of Disclosure and Governance and strategy too.

1. Managerial Capability: Governance and Structure
2. Operational Capability: Monitoring and Reporting, Control and Mitigation, Key Risk Indicators, Identification and Assessment
3. Adaptive Capability: Business Resilience and Continuity, Role of Disclosure
4. Strategic Capability

For a comprehensive and effective framework of operational risk management all these dimensions must be included. The final framework created as a result of this study, contains all these dimensions which are converted into a model that is co-related with the operational risk management categories. It was realized that there is a lack of an integrated system that can be implemented and measured with respect to small and medium enterprises (SMEs). Following model includes all the dimensions for an effective operational risk management framework (see figure 2.4).

Table 2.1 Literature review.

Authors Dimensions	Michael Haubenstock 2002	John Thirlwell 2004	Zaw Zaw Aung 2008	ISRMC, LLC 2009	European Investment Fund (EIF) 2010	Dr. Daniel Imfeld, Dr. Claus Huber 2011	Joshua Corrigan, Paola Rusachi 2013	Muhammad Shahbaz 2013
Definition		x			x	x		x
Governance and Structure(culture)	x	x			x		x	x
Key Risk Indicators	x	x	x	x	x			x
Identification and Assessment	x		x		x	x	x	x
Monitoring and Reporting	x	x	x	x			x	x
Control and Mitigation	x	x		x	x	x	x	x
Resiliency and Continuity								x
Role of Disclosure					x			x

1. Adaptive Capability

   Resilience, Horizon Scanning
2. Operational Capability

   Process Management, Performance Measurement
3. Managerial Capability

   Governance/Structure
4. Strategic Capability

   Operational Model, Finance, Business Sustainability, Visual Strategy

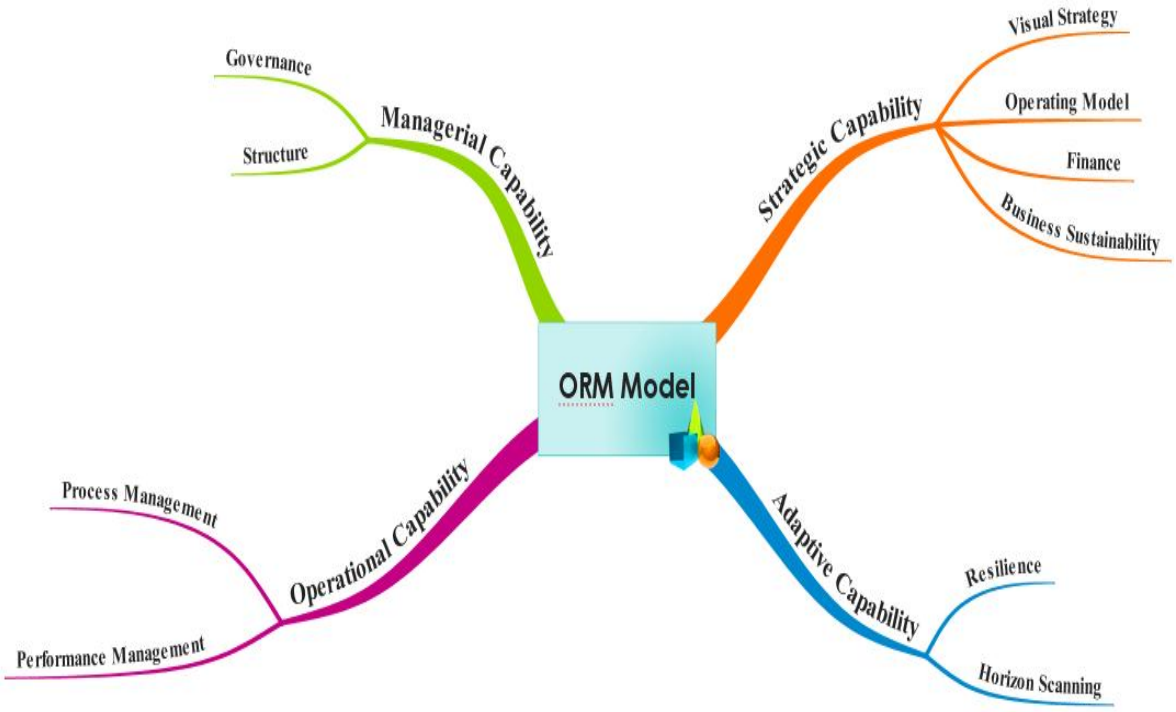


Figure 2.4 Operational risk management model (Shahbaz, 2013).

CHAPTER 3

OPERATIONAL RISK MANAGEMENT MODEL

This chapter represents the main contributions of this thesis. The main questions and hypothesis regarding operational risk management are discussed in chapter 1. The major frameworks of operational risk management are reviewed, presented and discussed in chapter 2. These frameworks are developed during the period 2002 - 2013 as mentioned in the previous chapter.

It has been explained that each of the developed frameworks has some weakness points. A comprehensive framework of operational risk management is proposed in this chapter. The proposed framework takes into consideration the key dimensions presented in other frameworks, the proposed operational risk management framework adds extra dimensions related to small and medium sized enterprises (SMEs).

3.1 OPERATIONAL RISK

The use of the term “operational risk” in banking first came to prominence in the mid-1990s and, along with the major banking scandals around that time. The list of risks faced by banks today includes fraud, system failures, terrorism and employee compensation claims. These types of risk are generally classified under the term operational risk. In June 1999, the Basel Committee on Banking Supervision7 decided to highlight the importance attributed to operational risk in banks by advocating an explicit regulatory capital charge

for other risks (BCBS, 1999). One of the reasons for doing so was the fact that the capital held as a cushion against residual risks, including operational risk, was increasingly reduced due to the more and more accurate measurement of credit risk (Oesterreichische Nationalbank). In January 2001, the Basel Committee narrowed down these other risks by drafting the first definition of operational risk that was eventually finalized in a working paper presented by the Basel Committee in September 2001 (BSBC, 2001). Operational risk is defined by the Basel Committee on Banking Supervision 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." (BCBS, 2005)

The following list explains the expressions used in the operational risk definition of BCBS. The description follows Mestchian (2003):

1. Internal Process risk: These include inefficiencies or ineffectiveness in the various business processes within the organization, value-driving processes (front-office) such as sales and marketing, product development and customer support, as well as value-supporting processes (back-office) such as Information Technology (IT), Human Resources (HR) and operations.
2. People risks: These include employee errors, employee misdeeds (like internal fraud), employee unavailability, inadequate employee development and recruitment.
3. System risks: These include system failures caused by breakdown, data quality and integrity issues, inadequate capacity and poor project management.
4. External risks: These include the risk of loss caused by actions of external parties such as competitor behavior, external fraud, regulatory change, and macro- and socio-economic events.
5. Legal risks: These include, but are not limited to, exposures to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

The interaction of these risks is shown in figure 3.1. Strategic and reputational risk is not included in this definition for the purpose of a minimum regulatory operational risk capital charge. This definition focuses on the causes of operational risk and the Committee believes that this is appropriate for both risk management and, ultimately, measurement (BCBS, 2001).

This definition is deceptively short for such a broad area. To elaborate, the Basel Committee issued a July 2002 consultative paper, "Sound Practices for the Management and Supervision of Operational Risk," where they defined the following seven types of operational risk loss events.

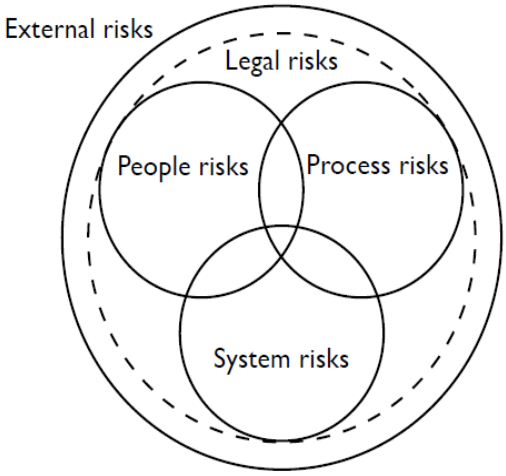


Figure 3.1 Taxonomy of operational risk (Meschian, 2003).

3.1.1 Categories of Operational Risk

All seven types of operational risk are explained below. (Guy Carpenter & Company, LLC, 2007) pp. 144-172.

1. Internal Fraud

   Acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involve at least one internal party. Examples include intentional misreporting of positions, employee theft and insider trading on an employee's own account.

2. External Fraud

   Acts by a third party, of a type intended to defraud, misappropriate property or circumvent the law. Examples include robbery, forgery, check kiting and damage from computer hacking.

3. Employment Practices and Workplace Safety

   Acts inconsistent with employment, health or safety laws or agreements, or which result in payment of personal injury claims, or claims relating to diversity/discrimination issues. Examples include workers compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims and general liability (for example, a customer slipping and falling at a branch office).

4. Clients, Products and Business Practices

   Unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product. Examples include fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering and sale of unauthorized products.

5. Damage to Physical Assets

   Loss or damage to physical assets from natural disaster or other events. Examples include terrorism, vandalism, earthquakes, fires and floods.

6. Business Disruption and System Failures

   Disruption of business or system failures. Examples include hardware and software failures, telecommunication problems and utility outages.

7. Execution, Delivery and Process Management

   Failed transaction processing or process management, and relations with trade counterparties and vendors. Examples include data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance and vendor disputes.

3.2 SMALL AND MEDIUM ENTERPRISES (SMEs)

In Europe, there are three broad parameters which define SMEs: micro-entities are companies with up to 10 employees; small companies employ up to 50 workers, whilst medium-sized enterprises have up to 250 employees (European Commission (2003-05-06)). SMEs are defined as non-subsidiary, independent firms which employ less than a given number of employees. This number varies across national statistical systems. The most frequent upper limit is 250 employees, as in the European Union. However, some countries set the limit at 200 employees, while the United States considers SMEs to include firms with fewer than 500 employees. Small firms are generally those with fewer than 50 employees, while micro-enterprises have at most ten, or in some cases five, workers. Financial assets are also used to define SMEs. In the European Union, SMEs must have an annual turnover of EUR 40 million or less and/or a balance-sheet valuation not exceeding EUR 27 million (OECD, 200).

3.3 OPERATIONAL RISK MANAGEMENT MODEL

After reviewing all the frameworks as discussed in chapter 2 it was realized that there is a lack of an integrated system that can be implemented and measured with respect to the small and medium enterprises (SMEs). Following model includes all the dimensions for an effective operational risk management framework for small and medium sized enterprises (SMEs). The proposed model is explained below categorically. The proposed model of operational risk management in small and medium enterprises is co-related with the categories of operational risk management. The study demonstrates how quantitative modeling of risk can be undertaken for SMEs based on opinions provided by experts within the organization.

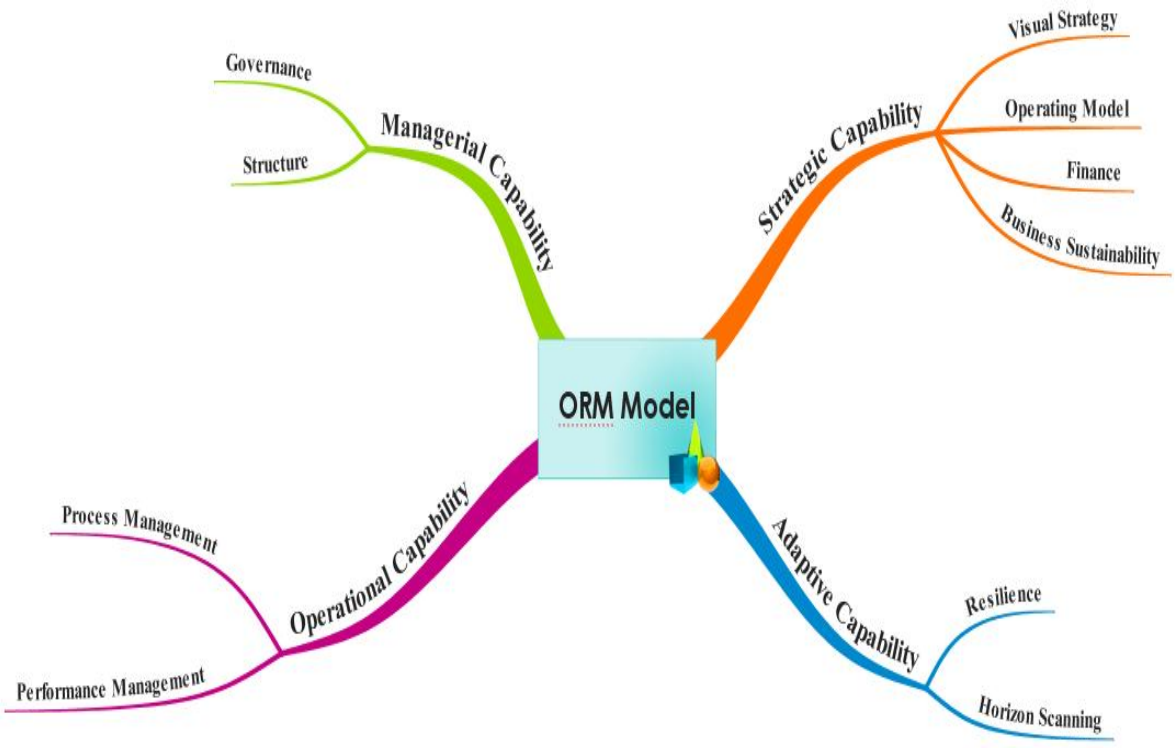


Figure 3.2 Operational risk management model.

3.3.1 Adaptive Capability

The essence of management is coping with change (Chakravarthy, 1982). This capability of an SME can produce the ability to shape itself according to the emerging environment in operational risk. It focuses on managerial, operational and strategic capabilities of an organization. 80% of companies without a comprehensive crisis plan vanish within 2 years of suffering a major disaster (Penrose, 2000).

1. Resilience

   Lengnick-Hall and Beck (2005) propose that resilience capacity influences an organization's response to environmental change. To make plan according to the future opportunities and threats is called resilience. It also makes an SME to absorb negative impacts on the business.

There are three central features of organizational resilience:

a) The ability of organization to absorb or buffer disturbances and still maintain its core functioning.
b) The ability of organization to self-organize
c) The capacity for learning and adaptation in the context of change.

2. Horizon Scanning

The organizations encounter with the interconnected and changing world. To cope with uncertain future risks and opportunities, organizations have to take active notice. The task of horizon scanning requires three steps.

a) Long term policies
b) Focused policies
c) Sustainable policies

Horizon scanning as a policy tool aims to broadly explore information about novel and unexpected issues and trends as well as persistent problems in an organization's external environment (Aguilar (1967); Choo (2001).

Horizon scanning is a process to identify the area that can be improved in an operational environment and then gathering all the information required and making this as a part of the strategy to make decisions. Horizon scanning is the tool to be aware with the external environment of the operations. It helps to compete in the market, knowing the behavior of the customer, their preferences and to anticipate with the relevant technologies.

Horizon scanning facilitates a systematic and structured evidence-gathering process and provide an understanding what is happening and why in an organization's environments, what processes produce and support change, the relations between these processes, the main actors and their objectives, the anticipation of change, and the required capacities and resources Aguilar (1967), Choo (2002, 1999), Lang (1995), or Morrison (1992).

3.3.2 Operational Capability

Operational capability is the ability of aligning technology available in the market, resources and operations effectively to the vision of the organization. Continuous process improvement makes organizations more competitive and effective. Those organizations who improve their resources, technologies and operations faster are more successful in the market.

1. Process Management

   In a business point of view, process management is the important tool to reduce cost of the product, customer satisfaction and the new product development. Every product coming out of a company is based on number of operations that are performed while creating this product. Process management organizes these operations and the relationship of these operations with each other and improves

them. Continuous improvement is the main element of the operational risk management. Efficient processes provide you faster and low cost products with fewer resources.

Management process consists of a set of activities that are performed in coordination with the organizational and technical environment. These activities jointly realize a business goal (M. Weske 2012). Each business process is enacted by a single organization, but it may interact with business processes performed by other organizations (M. Weske 2012). A company can achieve its goals more easily if the people and other resources in the organization have collaboration.

2. Performance Measurement

Performance is a contextual concept associated with the phenomenon being studied (Hofer, 1983). Performance measures give a quantitative measure of our processes, product and operations being performed in an organization. According to Oak Ridge Associated Universities, performance measures are a tool to help us understand, manage, and improve what our organizations do. Performance measures let us know:

a) How well we are doing
b) If we are meeting our goals
c) If our customers are satisfied
d) If our processes are in statistical control
e) If and where improvements are necessary

It includes design, implementation and management of a performance system. Performance measurement ensures that the measures used throughout your organization align to its overall goals. This helps you achieve results in a systematic way (Rober B. Carton).

3.3.3 Strategic Capability

"Where there is equilibrium between the strategy and strategic capability the performance of the organization is optimized for a particular business environment" (Ansoff, 1984). The ability to change the organization and create business environments is called strategic capability. If a capability has a potential to change or actually brings change, can be a strategic capability. Competence, quality and strategic resources can analyze strategic capability of an organization (Jokull Johannesson, 2010). Strategic capability includes visual strategy, finance, business sustainability and operating model of an organization. "Strategic analysis creates a massive amount of information that is difficult to absorb by any individual manager or group" (Leaderer and Sethi, 1996).

1. Visual Strategy

   Clear thinking and proper communication is needed while planning a strategy because all the parties are involved while gathering data and making it information within the organization. To make an action plan, clear understanding of information is necessary so that an appropriate strategy can be developed to handle the operational losses. Visual strategy is the best way bring a data into information and then from information to strategy.

2. Operating Model

   Operating model of an organization includes all the operations being performed in that particular organization. These operations provide strength to the vision of the organization. Operations include supply chain, production, buying, selling products, manufacturing and all the daily routine practices. Operating model is created generally to support the organization so that it can achieve its goals and changes rapidly. Sometimes change in the operating model may reduce its rapidness to support the business. To avoid different types of frauds within or outside of the organization, operating model is the best tool to cope.

3. Finance

   This is all about the finance running inside the organization or outside. It may also include some cash flows, profiting, business plans and sources of finance. Regularly monitoring of projected cash flows and source of the funding of the organization may reduce financial losses.

4. Business Sustainability

   Considering environmental and social aspects of a business while operation is called sustainability of the business. Business is not just financial management. In other ways we can say it is a model for green business because it includes operational losses, environmental legislations, and cost of the performance of a product or service.

3.3.4 Managerial Capability

"Integrating the managerial knowledge of individuals, a firm achieves its managerial capabilities" (Frans A.J. Van Den Bosch, Raymond Van Wikj, 2000). "Integrating individual managerial knowledge in, for example, a constellation of people such as a team, can provide additional services as the ones rendered by individual managers, because working with each other 'enables them to provide services that are uniquely valuable for the operations of the particular group with which they are associated" (Penrose, 1959). So, "they become individually and as a group more valuable to the firm in that the services they can render are enhanced by their knowledge of their fellow-workers, of the methods of the firm, and the best way of doing things in the particular set of circumstances in which they are working" (Penrose, 1959).

1. Governance/ Structure

   "Organizational governance concerns how agents, pursuing their own interests, and with different preferences, knowledge or information, and endowments, use instruments of control to regulate their transactions to avoid problems of coordination and motivation they confront when interacting within or through the

purposefully designed social systems known as organizations." (Nicolai J. Foss, Peter G. Klein, 2008). Actually it is a way in which operational risk is governed and structured to pursue its losses. Consistent, social responsible and sustainable management is required for governance and structure of a company. Governance and structure are the tools to optimize operational performance of an organization.

So the comprehensive operational risk management framework containing Adaptive capabilities, Managerial capabilities, Operational capabilities and Strategic capabilities of SMEs are to be compared with the operational risk level. Moreover each capability is compared separately to know the relationship with operational risk so that it can be visualized that which capability has the greatest effect on operational in an SME.

Figure 3.3 Operational risk management framework.

CHAPTER 4

DATA COLLECTION AND ANALYSIS

This chapter describes the relationship between operational management framework and operational risk management in small and medium enterprises. On the basis of analysis of the data collected through a comprehensive survey and analyzed by JMP.10 software package, at the end of this chapter we will also be able to figure out which capability of SMEs has a strong relationship with the operational risk management. This chapter also gives information about what type of SMEs are involved, their work force, annual turnover and how many customers do they have.

As described in the methodology of the conducted quantitative study in chapter 1 that the online comprehensive survey was conducted in more than five countries mainly Turkey, Pakistan and Denmark. The organizations that develop small and medium enterprises were contacted to conduct the survey in respective countries. In this regard KOSGEB and Aviad from Turkey while SMEDA from Pakistan have the largest contribution in conducting the survey. Moreover, some data was also collected by personally visiting SMEs in Turkey.

The quantitative survey contains 184 questions in three different sections. First section of the questionnaire assesses the capabilities of small and medium enterprises; second section of the questionnaire is about the losses in terms of money and occurrence of that particular loss. While the third section is to judge the frequency of disturbances due to operational activities.

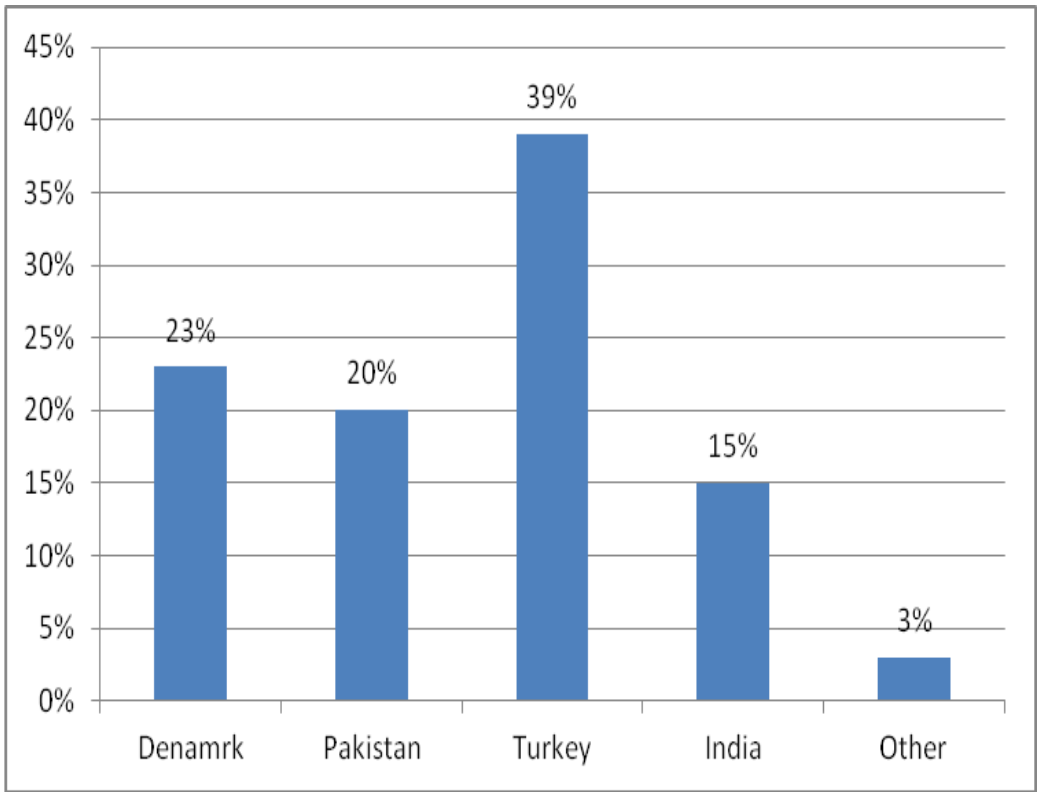


Figure 4.1 Percentage of participating countries.

There are a total of 110 small and medium enterprises, out of them 39% are from Turkey, 20% from Pakistan, 23% from Denmark, 15% from India and 3% from other countries.

A large number of SMEs responded from manufacturing and textile sector. As the objective of the survey is to develop an operational risk management framework for small and medium enterprises, 80% of the SMEs which responded to the survey are small and medium sized.

Figure 4.2 shows the percentage of the involvement of different sectors.

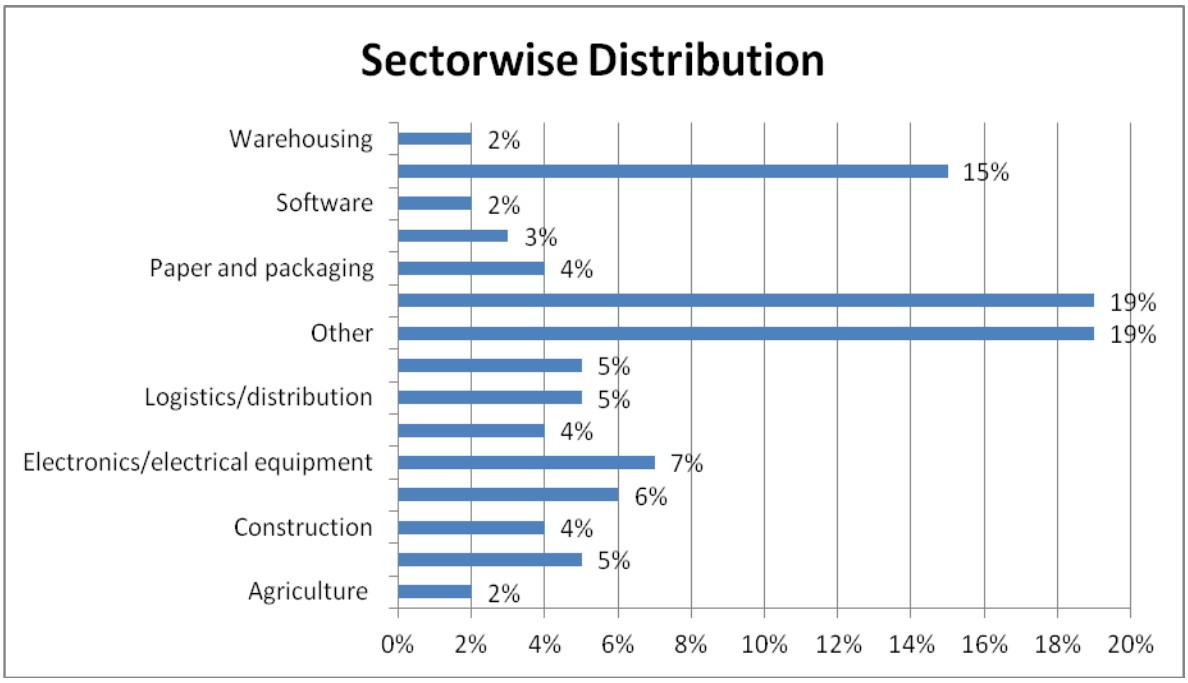


Figure 4.2 Sector-wise percentage of participating SMEs.

Following table gives the detailed information about the size, number of customers, annual turnover of the enterprise and their percentage of the contribution in this survey.

Table 4.1 Size, number of customers, annual turnover of participating SMEs.

Size of the Enterprise	%age of Contribution	No. of Customers	%age of Contribution	Annual Turnover	%age of Contribution
Large sized	12	More than 100	37	More than 7.5 Million Dollars	17
Medium sized	43	50 to 99	32	2.5 to 7.5 Million Dollars	27

Table 4.1 (Cont.)

Small sized	37	20 to 49	21	0.25 to 2.5 Million Dollars	Small sized
Micro	8	0 to 19	10	0 to 0.5 Million Dollars	27

4.1 THE SUREVY

The first section of the survey addresses four capabilities of an SME that are Strategic capability, Operational Capability, Managerial Capability and Adaptive Capability. Actually these capabilities are the framework that will validate the research hypothesis either operational risk can be managed with the high level of these capabilities or not. Each capability is divided into sub sections get the detailed information about the level of SMEs. There are seven categories of operational risk in the second part of the survey. Each category of questionnaire contains a set of question about the amount of loss in terms of US Dollars per year and frequency of the loss due to that particular category of the operational risk. Thirdly, there are some routine activities in an SME if those are not performed well we name them disturbances. So, third section is about those disturbances which are part of the operational risk but being so small that SMEs mostly do not keep their loss data. Actually our main goal is to figure out and give awareness to the SMEs about those disturbances which are being ignoring because of their small impact.

4.2 ANALYSIS AND RESULTS

The questionnaire is scaled from 1 to 5 and each question has the same weight. Because of this reason, the summation value of the questions makes one variable. Whereas 5 being the minimum loss (best) and 1 maximum loss (worst). The 9 SMEs out of 119 that

were excluded of the data analysis had a lot of missing data. For the still remaining missing data was treated by substitution method i.e by replacing with the average of that particular question. Following table gives the amount of loss per year due to each category of operational risk in terms of simple numbers according to scale of the questionnaire.

More than 75 thousand Dollars = 1

50 to 75 thousand Dollars = 2

25 to 50 thousand Dollars = 3

10 to 25 thousand Dollars = 4

0 to 10 thousand Dollars = 5

Similarly in the case frequency of occurrence of the loss is assigned values from worst 1 to best 5.

More than 30 times = 1

20 to 30 time = 2

10 to 20 times = 3

6 to 10 times = 4

1 to 6 times = 5

By taking sum of all these values we can find the level of loss due to each category of operational risk.

Table 4.2 Level of losses and frequency of occurrence of operational risk.

Category of Operational Risk	Level of the losses	Frequency of Occurrence
Internal Fraud	446	457
External Fraud	430	452
Employment Practices and Workplace Safety	438	439
Clients, Products and Business Practices	455	457
Damage to Physical Assets	426	443
Business Disruption and System Failures	445	451
Execution, Delivery and Process Management	460	456

So, the picture of the first part of the questionnaire is clear by viewing the above table. It clearly shows that Damage to Physical Assets has gained the lowest value. According to our scale, Damage to Physical Assets has highest level of loss as compared to the other six categories of operational risk. Similarly if we see the frequency of occurrence Employment Practices and Workplace Safety has gained the minimum value. Which shows that Employment Practices and Workplace Safety occur frequently as compared to other six categories of operational risk.

Also, we have a question regarding the most important risk in SMEs. Each category of the operational risk is assigned a number from least important 1 to the most important 7. After the analysis of that question we have found that also shows that Damage to Physical Assets is the most important category of operational risk in the eyes of top management.

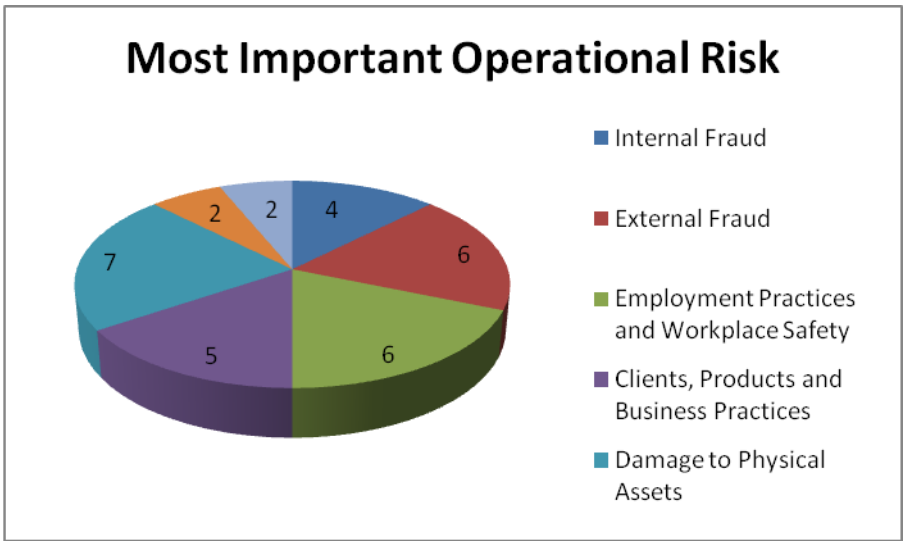


Figure 4.3 Categorical importance of operational risk.

4.3 RELATIONSHIP OF ORM WITH THE CAPABILITIES OF SMEs

4.3.1 Introduction to Correlation

a) To discover whether there is a relationship between variables.
b) To find out the direction of the relationship –whether it is positive, negative or zero.
c) To find the strength of the relationship between the two variables.

The test statistic called the 'correlation coefficient r' measures the strength of the relationship between the variables. This relationship varies from +1 to -1. Zero shows no relationship, while +1 shows strong relationship and -1 shows weak relationship.

For any two variables X and Y, the coefficient of correlation is calculated by the following formula:

$$\Gamma = \frac{\sum (X - \overline{X}) \bullet (Y - \overline{Y})}{\sqrt{\sum (X - \overline{X})^2 \bullet \sum (Y - \overline{Y})^2}} \qquad (4.1)$$

The data collected for the empirical analysis is analyzed by Pearson Correlation (+1 - 1) Method using JMP.10 software package.

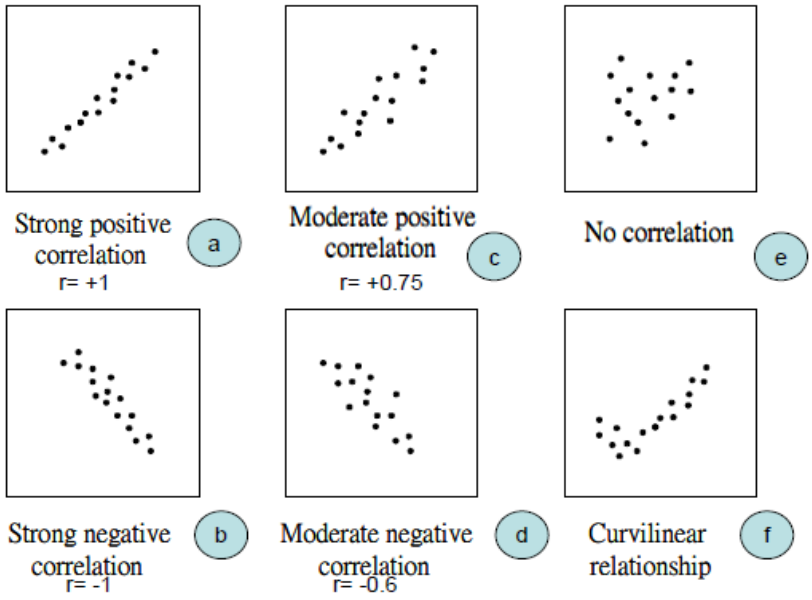


Figure 4.4 Example figure of correlation.

4.3.2 Introduction to Regression Analysis

Correlation analysis allows us to conclude how strongly two variables relate to each other (both magnitude and direction); Linear regression analysis answers the question 'How much will y change, if x changes?' In other words: If x changes by a certain amount, we will be able to estimate how much y will change.

Regression line is described by the equation;

$$y = a + bx \tag{4.2}$$

where 'b' is the slope of the line and 'a' is the intercept i.e. where the line cuts the y axis.

The actual purpose of the regression analysis is;

a) What is the average error?

b) How strong is the relationship?

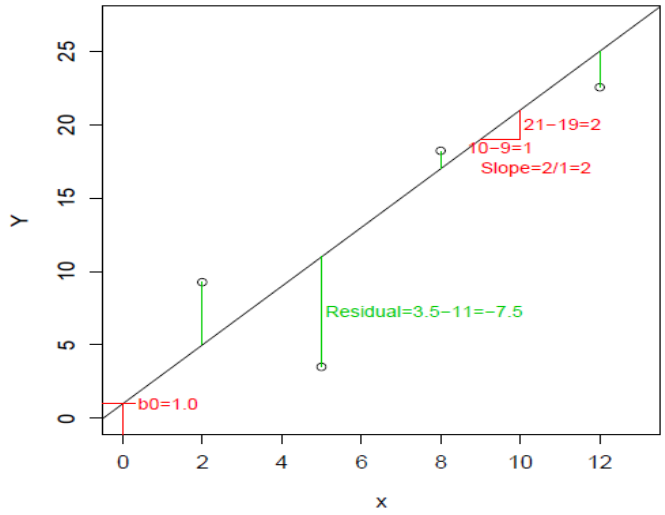


Figure 4.5 Example figure of regression analysis.

For the second part of the survey, data is analyzed according to the ordinal dependent and independent variables. There are a total of fourteen variables. While Operational Risk Management Framework is the collective sum of four main capabilities.

Table 4.3 Analyzed variables.

Name of the Variable	Category
Operational Risk Management	Dependent
Strategic Capability	Independent
Adaptive Capability	Independent

Table 4.3 (Cont.)

Operational Capability	Independent
Managerial Capability	Independent
Operational Risk Management Framework	Independent
Visual Strategy	Independent
Finance	Independent
Business Sustainability	Independent
Process Management	Independent
Performance Management	Independent
Resilience	Independent
Horizon Scanning	Independent
Succession Planning	Independent
Decision Making	Independent

4.4 DISTRIBUTIONS

After validating the data obtained by survey, to check either data is normally distributed or not, normal distribution test is applied and the values of mean, median, standard deviation and standard error mean are given in the following table.

Table 4.4 Distribution values of variables.

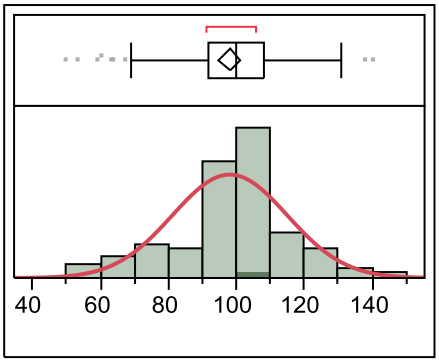
Ordinal Variable	Mean (μ)	Std Dev (σ)	Std Err Mean	Median
Strategic Capabilities	98.081	16.913	1.612	100
Operational Capabilities	63.981	13.440	1.281	64
Adaptive Capabilities	28.563	5.314	0.506	29

Table 4.4 (Cont.)

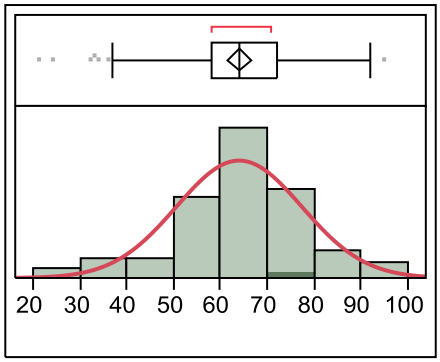
Managerial Capabilities	32.763	5.451	0.519	33.5
Visual Strategy	31.681	5.659	0.539	32
Finance	27.763	6.083	0.580	28
Business Sustainability	38.636	8.937	0.852	39
Process Management	46.045	10.032	0.956	47.5
Performance Management	17.936	5.183	0.494	19
Resilience	15.918	3.251	0.310	16
Horizon Scanning	12.645	2.916	0.278	13
Succession Planning	11.581	2.836	0.270	12
Decision Making	21.181	4.408	0.420	22
Operational Risk Management Framework	223.393	35.065	3.343	227
Operational Risk Management	84.172	10.065	0.959	43

By looking at the curves of normal distribution, in the figures given below, it can be realized that data is normally distributed.

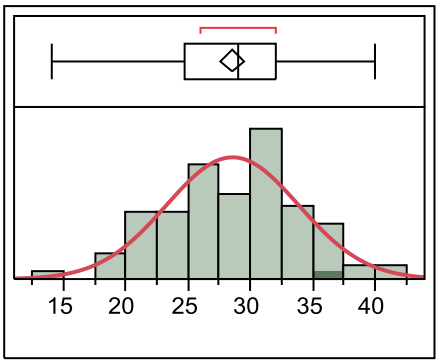
For the categorical ordinal variables, the histogram shows a bar for each level of the ordinal or nominal variable. For continuous variables, the histogram shows a bar for grouped values of the continuous variable.



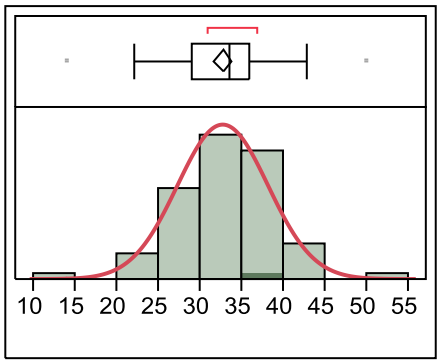
Strategic Capability



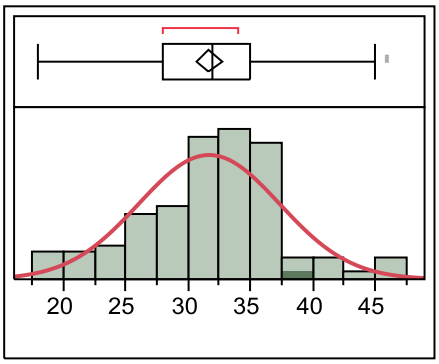
Operational Capability



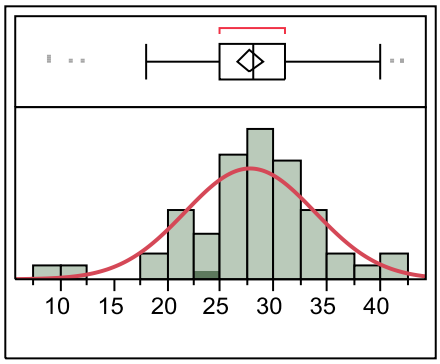
Adaptive Capability



Managerial Capability

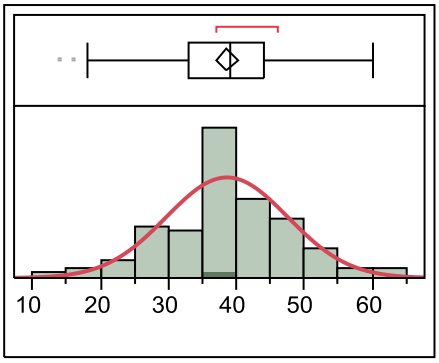


Visual Strategy

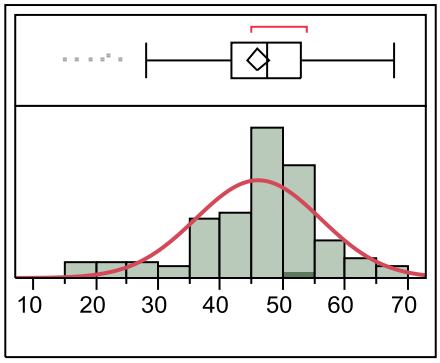


Finance

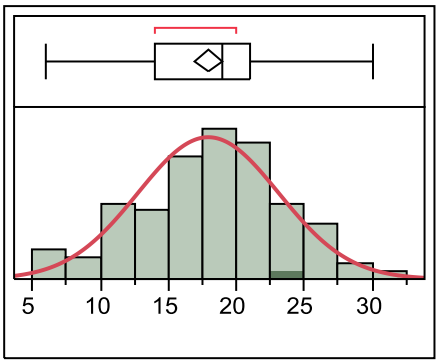
Figure 4.6 Distribution curves of variables.



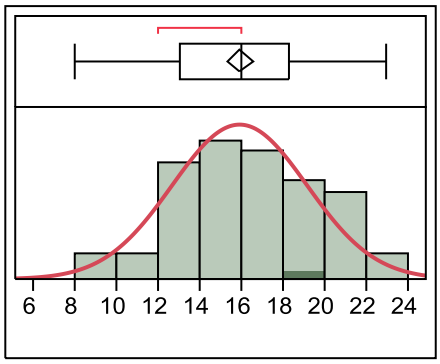
Business Sustainability



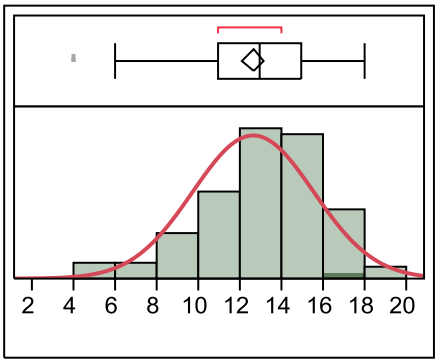
Process Management



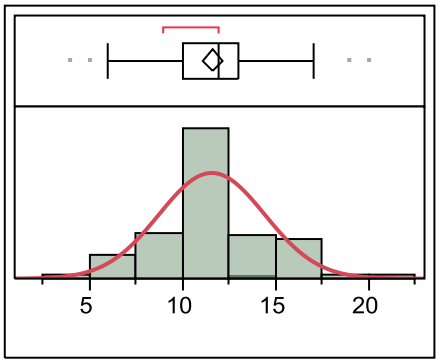
Performance Management



Resilience

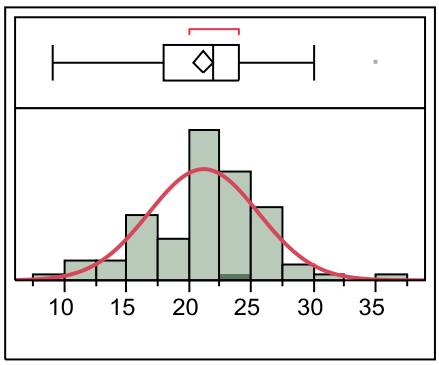


Horizon Scanning

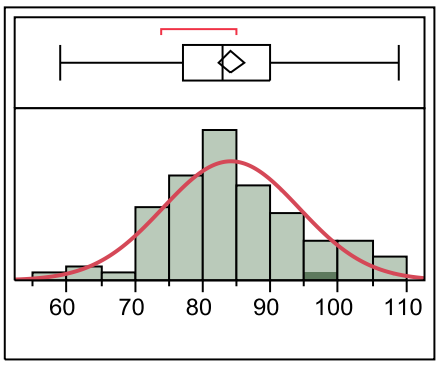


Succession Planning

Figure 4.6 (Cont.)



Decision Making



Operational Risk Management

Figure 4.6 (Cont.)

4.5 CORRELATIONS

After plotting the distribution curves variables are defined. There are total of fourteen variables out of these 14, one is the dependent variable. This dependent ordinal variable is correlated one by one with all the fourteen ordinal variables.

As the framework shows that all the independent variables are related with the operational risk management of SME, a correlation table is designed to show the strength of relationship.

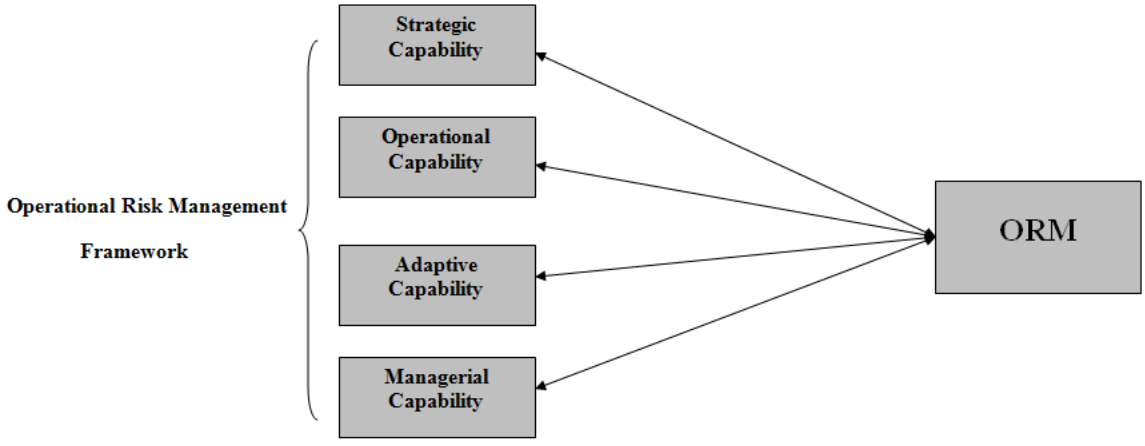


Figure 4.7 Correlation of main variable.

Table 4.5 Correlation values of main variables.

	SC	OC	AC	MC	ORMF	ORM
SC	1.000					
OC	0.670	1.000				
AC	0.582	0.661	1.000			
MC	0.460	0.554	0.595	1.000		
ORMF	0.899	0.893	0.778	0.680	1.000	
ORM	0.062	0.107	0.221	0.272	0.147	1.000

It is clear from the table given above that operational risk management has the least relationship r = 0.0623 with Strategic Capabilities and the strongest relationship is between operational risk management and Managerial Capabilities r = 0.2724 among all the variables for operational risk management framework.

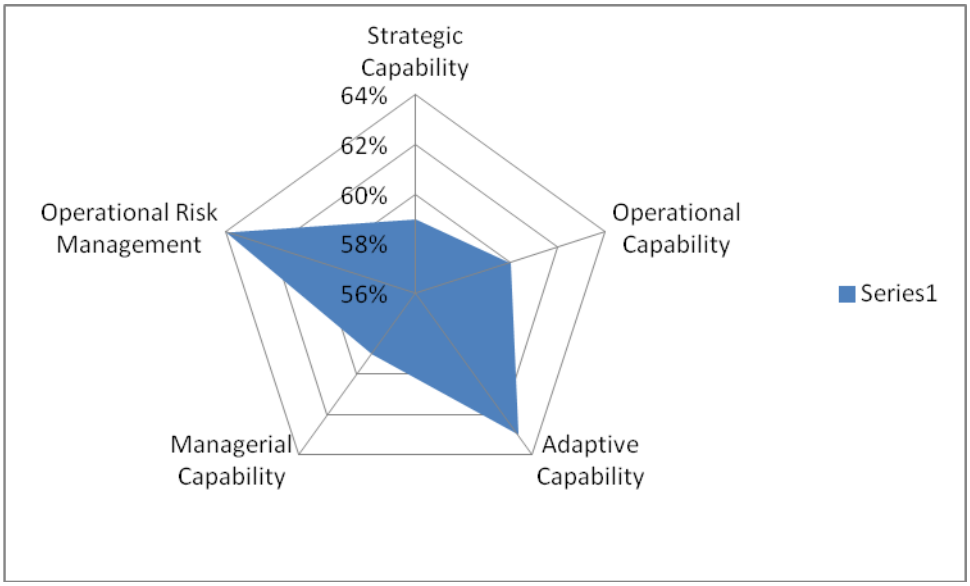


Figure 4.8 Spider diagram of main variables.

Spider diagrams are drawn by taking the percentage from 0% to 100% of the variable in SMEs. Above figure shows that Operational Risk Management has the highest value among all other variables. It means that the surveyed SMEs has strong grip on operational risk management as compared to other capabilities.

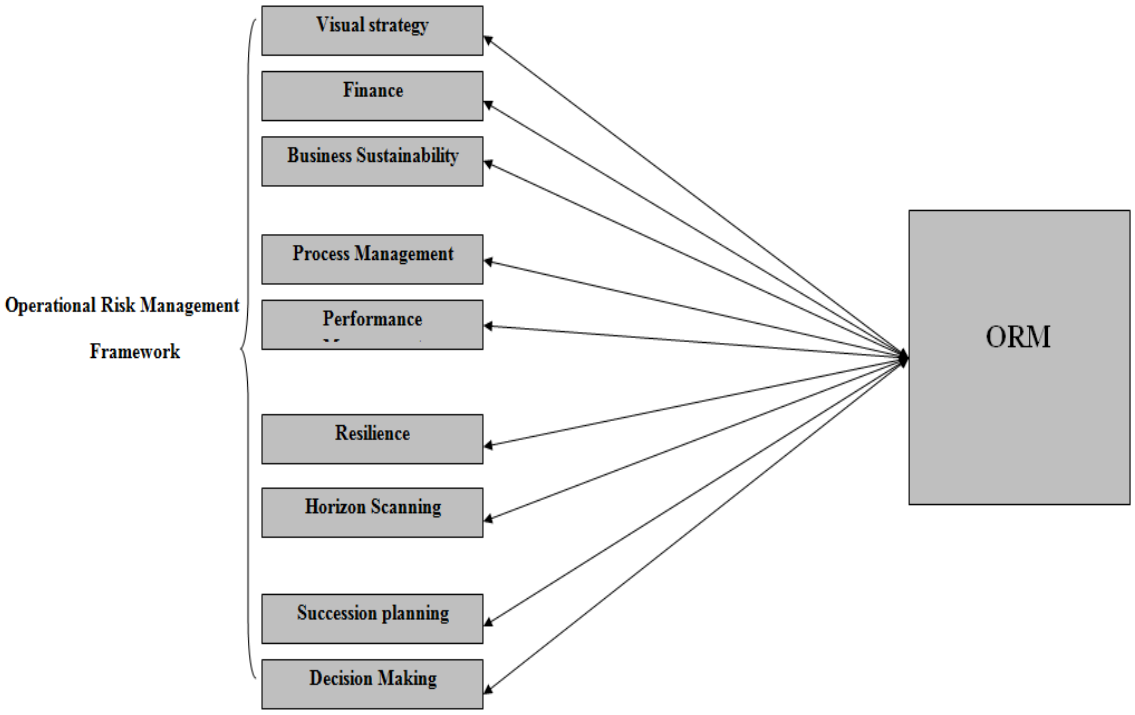


Figure 4.9 Correlations of sub-variables.

Table 4.6 Correlation values of sub-variables.

	VS	F	BS	PcM	PrM	R	HS	SP	DM	ORM
VS	1.000									
F	0.606	1.000								
BS	0.461	0.447	1.000							
PcM	0.505	0.459	0.603	1.000						
PrM	0.491	0.353	0.345	0.510	1.000					
R	0.457	0.460	0.357	0.488	0.484	1.000				

Table 4.6 (Cont.)

HS	0.444	0.387	0.393	0.544	0.480	0.483	1.000			
SP	0.370	0.246	0.236	0.386	0.486	0.422	0.367	1.000		
DM	0.375	0.368	0.177	0.374	0.261	0.333	0.429	0.089	1.000	
ORM	0.127	0.206	-0.103	0.049	0.183	0.224	0.153	0.082	0.283	1.000

For the sub-variables, it is also clear from the table given above that operational risk management has the least relationship r = -0.1035 with Business Sustainability and the strongest relationship is between operational risk management and Decision Making r = 0.2838 among all the sun-variables for operational risk management framework.

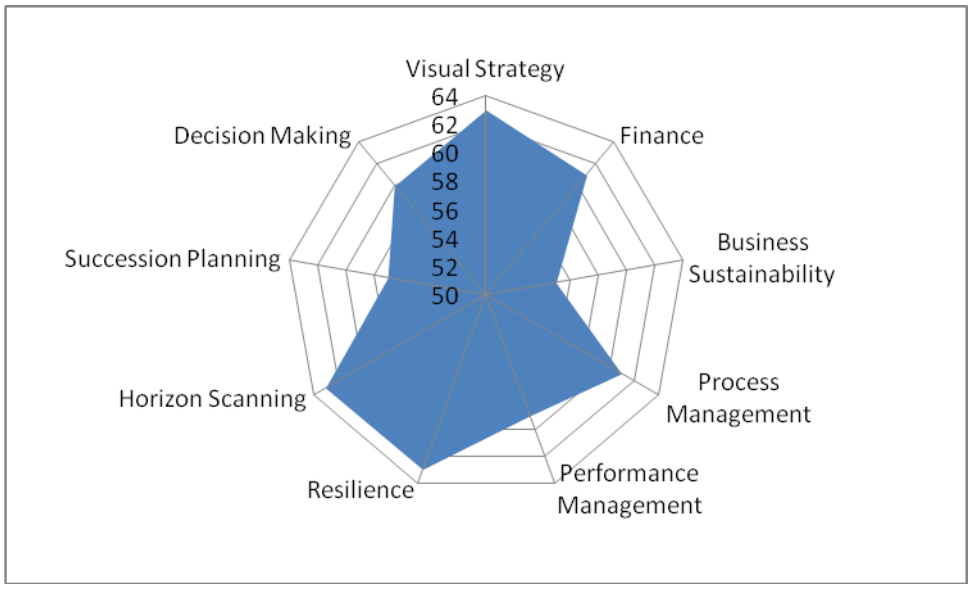


Figure 4.10 Spider diagram of sub-variables.

By looking at the above spider diagram, it is clear that SMEs has strong grip on Resilience, Horizon Scanning and Visual Strategy as compared to other nine sub-variables.

Similarly country wise correlations are given below;

Table 4.7 Correlation values of SMEs of Turkey.

	SC	OC	AC	MC	ORMF	ORM
SC	1.000					
OC	0.655	1.000				
AC	0.601	0.457	1.000			
MC	0.561	0.380	0.554	1.000		
ORMF	0.922	0.819	0.749	0.695	1.000	
ORM	0.122	0.064	0.336	0.392	0.222	1.000

Strongest: ORM and Managerial Capability

Weakest: ORM and Operational Capability

Table 4.8 Correlation values of SMEs of Pakistan.

	SC	OC	AC	MC	ORMF	ORM
SC	1.000					
OC	0.052	1.000				
AC	-0.005	0.696	1.000			
MC	-0.303	0.462	0.529	1.000		
ORMF	0.478	0.850	0.731	0.465	1.000	
ORM	-0.479	-0.333	-0.025	0.061	-0.429	1.000

Strongest: ORM and Managerial Capability

Weakest: ORM and Strategic Capability

Table 4.9 Correlation values of SMEs of Denmark.

	SC	OC	AC	MC	ORMF	ORM
SC	1.000					
OC	0.795	1.000				
AC	0.774	0.869	1.000			
MC	0.580	0.635	0.649	1.000		
ORMF	0.936	0.941	0.902	0.728	1.000	
ORM	0.415	0.407	0.378	0.417	0.450	1.000

Strongest: ORM and Managerial Capability

Weakest: ORM and Adaptive Capability

Table 4.10 Correlation values of SMEs of India.

	SC	OC	AC	MC	ORMF	ORM
SC	1.000					
OC	0.734	1.000				
AC	0.464	0.361	1.000			
MC	0.602	0.605	0.534	1.000		
ORMF	0.933	0.889	0.585	0.756	1.000	
ORM	-0.175	-0.023	-0.098	0.041	-0.103	1.000

Strongest: ORM and Adaptive Capability

Weakest: ORM and Strategic Capability

As we know that correlation analysis allows us to conclude how strongly two variables relate to each other but linear regression analysis answers the question 'How much will y change, if x changes?'

So, the ordinal variables of the operational risk management framework are analyzed by linear regression method to understand the dependency of variables. Also p- value, i.e level of significance is calculated by ANOVA (Analysis of variance) test. The independent variable has a number attached to it in the regression result, its "p-value" or significance level. The p-value is a percentage. It tells that how likely it is that the coefficient for that independent variable emerged by chance and does not describe a real relationship.

4.6 BIVARIATE FIT OF ORM BY ORMF

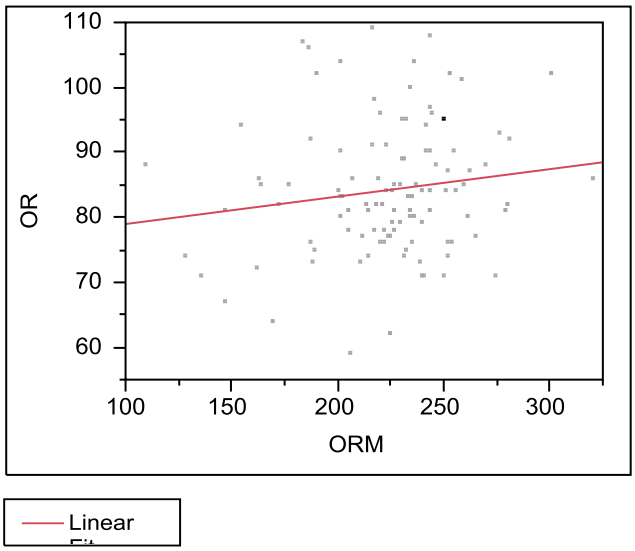


Figure 4.11 Regression analyses of ORM and ORMF.

Linear Fit

$$ORM = 74.732569 + 0.0422585*ORMF \quad (4.3)$$

Summary of Fit

RSquare	0.021671
RSquare Adj	0.012613
Root Mean Square Error	10.00203
Mean of Response	84.17273
Observations (or Sum Wgts)	110

Analysis of Variance

Source	**DF**	**Sum of Squares**	**Mean Square**	**F Ratio**
Model	1	239.334	239.334	2.3924
Error	108	10804.384	100.041	**Prob > F**
C. Total	109	11043.718		0.1249

The result of ANOVA test gives p = 0.12. So, p-value of 0.12 means that there is a 12% chance that the relationship between Operational risk management and Operational risk Management Framework emerged randomly and 88% chance that the relationship is real.

As with the p-value, the significance F value is also lower than p-value, it shows that the relationships in the model are real.

Regression equation between operational risk management and framework shows that we have;

a = 74.73 and b = 0.042.

It means there is a weak positive relationship between Operational Risk Management and Operational Risk Management Framework. For every unit increase in Operational Risk Management Framework, Operational Risk Management increases 4 % only.

The R-squared and adjusted R-squared values are estimates of the 'goodness of fit' of the line. As RSquare is the correlation coefficient between outcomes and the predicted values, it represents that 2.1 % variation of the data explained by the fitted line. So we can clearly say that Operational risk management varies 2.1% with respect to Operational Risk Management framework.

Similarly regression equations of main variables show that managerial capability has the highest relation with operational risk management.

ORM = 80.538347 + 0.0370546*SC (4.4)

ORM = 79.017956 + 0.0805662*OC (4.5)

ORM = 72.18446 + 0.4197038*AC (4.6)

ORM = 67.694195 + 0.5029519*MC (4.7)

ORM = 74.732569 + 0.0422585*ORMF (4.8)

CHAPTER 5

CONCLUSION

In this chapter results and analysis are connected to the hypothesis and research question of the study. The chapter is enclosed with the limited issues and future research. The research shows that there is a big difference between previous research and this research. Mostly one case study SME is considered in that particular country, but this research was conducted in four different countries.

From the regression line we can see that data is dispersed, missing and scars, the reason of scars data could be the unwillingness of the SMEs to share their financial information. The lack of loss data and time constraints have always been the main problem of the study. Because of the missing data, large numbers of values are substituted by the mean values. The reason for missing data could be the procedure of conducting the survey. Considering large amount of missing values especially amount of losses in terms of money, it can be assumed that the questionnaire was sent online in different countries, SMEs are not willing to share their financial information. The survey contains questions about frequency and level of losses due to operational risk. The survey shows that mostly questions from the level of losses due to operational risk were left empty. So, it is recommended that online survey is not a reasonable method to conduct or evaluate operational risk. Only face to face interviews are recommended with the top level of management or through a trusted body or organization to which SMEs willingly share the information.

This research recommends a quantitative framework of data collection for operational risk. Following two questions were formulated at beginning of the research.

1. How should SME manage the operational risk?
2. What is the relationship of operational risk with the capabilities of SMEs?

Answer to the first question lies in following points;

1. There should be awareness of operational risk management from bottom to top level management of SMEs.
2. Establishment of information and communication process in SMEs.
3. Establishment of dynamic structure and advisory board.
4. Proper collaboration and training the communication department.

Answer to the second question lies in the data analysis phase which proved that the proposed framework for operational risk management in SMEs has a weak relationship. The strongest relationship was recorded 0.27 with Managerial capabilities.

The hypothesis proposed in the beginning of this study cannot be falsified because there is no negative relationship between the capabilities of an SME and operational risk management. The overall relationship with the framework and operational risk management is 0.14. The proposed operational risk management framework was in general for the top level management of SMEs. Strategic capability, operational capability, adaptive capability and managerial capability collectively improve operational risk management by small amount.

By the regression analysis of all the capabilities of SME with operational risk Management it is concluded that Managerial Capability has a greater impact on operational risk management as compared to the operational risk management framework. Managerial capability improves operational risk management by 50 % while the overall framework improves by 4 % for every one unit increase in managerial capability and framework respectively.

Result 1. 3 % of Operational Risk management is associated with one unit improved Strategic Capability.

ORM = 80.538347 + 0.0370546*SC (5.1)

Result 2. 8 % of Operational Risk management is associated with one unit improved Process/Operational performance.

ORM = 79.017956 + 0.0805662*OC (5.2)

Result 3. 41 % of Operational Risk management is associated with improved Adaptive Capability.

ORM = 72.18446 + 0.4197038*AC (5.3)

Result 4. 50 % of Operational Risk management is associated with improved Managerial performance.

ORM = 67.694195 + 0.5029519*MC (5.4)

We can conclude that by improving Managerial and Adaptive capability of an SME, we can mitigate Operational risk.

Most of the times risk process lack of action plan. Mitigation activities should list all the activities that reduce risk to achieve the required level of risk. There are many rules to the practice of risk communication in SMEs. According to Covello & Allen 1988;

1. Accept and involve the public as a legitimate partner.
2. Plan carefully and evaluate your efforts.
3. Improve risk issues.
4. Listen to the public's specific concerns.
5. Listen to your employees concerns.
6. Be honest, frank, and open.
7. Be agreed to and implemented.

8. Be honest, frank, and open.
9. Co-ordinate and collaborate with other credible sources.
10. Meet the needs of the media.
11. Speak clearly and with compassion.

5.1 FURTHER RESEARCH

Future research in Managerial capabilities may continuously enhance the operational management framework. On the basis of this research and possible highest relationship of Managerial Capabilities, we can recommend following points as future recommendations;

Operational risk management should be integrated into the managerial structure and then its effect on operational risk management should be observed.

Crisis management can also be included to handle the losses due to operational risk.

REFERENCES

A.J. Van Den Bosch and Raymond Van Wijk, Erim, *Creation Of Managerial Capabilities Through Managerial Knowledge Integration: A Competence-Based Perspective,* ERS-2000-19-STR, February 2000.

Aguilar, Choo, Lang, and Morrison, *For studies on horizon scanning* , 1967, 2002, 1999, 1992.

Aguilar, Francis J. *Scanning the Business Environment*. New York: McMillan, 1967.

Airmic, Alarm, IRM *A Risk Management Standard*, 2002.

Ali Samad Khan, *Modern Operational Risk Management*, 2008.

Ansoff, H. I. *Implanting strategic management.* Englewood Cliffs: Prentice-Hall International, 1984.

Australian National Audit Office, "Business Continuity Management", *Building Resilience in Public Sector Entities, Best Practice Guide*–June 2009.

Bank for International Settlements and Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk,* July 2002.

Bank for International Settlements and Basel Committee on Banking Supervision , *Working Paper on the Regulatory Treatment of Operational Risk*. 2001, July 2002.

Bank for International Settlements, *Sound Practices for the Management and Supervision of Operational Risk,* Basel Committee on Banking Supervision, 2003.

Barton, T., Shenkir, W. and Walker, P., *Making Enterprise Risk Management Pay Off,* Morristown, NJ: Financial Executives Research Foundation, Inc 2001.

Basel Committee on Banking Supervision, *International convergence of capital measurement and capital standards,* A revised framework comprehensive version, June 2006.

Ian Storkey, Basel Committee on Banking Supervision, Consultative Document: *Operational Risk, Operational risk management and business continuity planning for modern state treasuries,* Fiscal Affairs Department, 2001.

Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards*, BIS, 2004.

Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards – A Revised Framework*, Part 2, Section V-A November 2005.

Basel II - *A Guide to Capital Adequacy Standards for Lenders*. The United Kingdom Council of Mortgage Lenders, February 2008.

Beat Habegger, *Horizon Scanning in Government, Concepts, Country Experiences and Models for Switzerland*, Center for Security Studies Seilergraben 45-49 ETH Zentrum / SEI CH-8092 Zurich, 2009.

Bryan J. Balin, *Basel I, Basel II, and Emerging Markets*, A Nontechnical Analysis, Washington DC 6, USA 2003.

Canadian Institute of Actuaries, *A New Approach for Managing Operational Risk*, 2009.

Chakravarthy, B.S., Adaptation: *A Promising Metaphor for Strategic Management*, Academy of Management Review, **7**:35-44, 1982.

Choo, Chun Wei, *Environmental Scanning as Information Seeking and Organizational Learning*, Information Research, 7(1), December 2008.

Choo, Chun Wei, Information Management for the Intelligent Organization*: The Art of Scanning the Environment.* Medford: Information Today, 2002.

Bank for International Settlements and Basel Committee on Banking Supervision, *Consultative Document Operational Risk*, July 2002.

Covello, VT & Allen, FH., *Seven Cardinal Rules of Risk Communication*, U.S. Environmental Protection Agency, OPA-87-020, Washington, DC 1988.

Deloitte and I.VW-HSG., *Management of Operational Risk in Insurance*, University of St. Gallen June 2007.

Dr. A Williams, *Division of Child Dental Health*, University of Bristol Dental School, Lower Maudling Street, Bristol, BS1 2LY, UK.

Dr. B Yarram Raju, *Operational Risk Management*, Professional Risk Managers' International association.

Dr. Daniel Imfeld, Dr. Claus Huber, *Operational Risk Management in Practice: Implementation, Success Factors and Pitfalls*, 2011.

Dr. Madhu Acharya, *Why the current practice of operational risk management in insurance is fundamentally flawed - evidence from the field*, The Business School, Bournemouth University.

Emerald Group Publishing Limited , *Strategy & Leadership,* Vol. 34 No. 1, pp. 4-10, ISSN 1087-8572, 2006.

European Commission (2003-05-06). *Recommendation 2003/361/EC: SME Definition*. Retrieved 2009-04-05.

European Investment Fund, Board of Directors Meeting on *Operational Risk Management Charter*, 2010.

FAA, "System Safety Handbook", *Chapter 15: Operational Risk Management.*

Financial Services Authority (FSA), *Building a Framework for operational Risk Management,* 2003.

Fratianni, MU & Marchionne, F., *The Role of Banks in the Subprime Financial Crisis,* SSRN., 2009.

Guy Carpenter & Company, LLC., *Enterprise Risk Analysis*, pp. 144-172. 2007.

Hans-Ulrich Doerig, *Operational Risks in Financial Services an Old Challenge in a New Environment,* 2001.

Hofer, C. W. ROVA: "A new measure for assessing organizational performance", R. Lamb (Ed.), *Advances in Strategic Management,* Vol. 2: 43-55. New York: JAI Press, 1983.

Ian Carey, Kate O'Reilly, *Operational Risk Management and Measurement*, Society of Actuaries in Ireland, 2004.

Organizational Resilience Perspective: Facilitating Organizational Adaptation Analysis, *International Conference on Economics Marketing and Management*, IPEDR Vol.28 IACSIT Press, Singapore, 2012.

Ir Stephen W.K Pang, *An Integrated Operational Risk Management Framework for power Generation.*

ISRM., LLC., *Information Security handbook*, 2009.

James Lam, *A Unified Management and Capital Framework for Operational Risk*, 2003

John Thirlwell,, Operational Risk Research Forum Lloyd's Risk Forum, *An Operational Risk Management Framework for Managing Agencies,* 28 May, 2004.

Jokull Johannesson, International Business Research, *The Dynamics of Strategic Capability*, Northampton Business School, January, 2010.

Jonathan Davies and Michael Haubenstock, RMA Journal, *Building Effective Indicators to Monitor Operational Risk*, 2002.

Jonathan Davies, Mike Finlay, Tara McLenaghen, Duncan Wilson, *Key Risk Indicators Their Role in Operational Risk Management and Measurement*, 2006.

Joshua Corrigan, Paola Rusachi, *Operational Risk Modeling Framework*, 2013.

KPMG., *Integriertes Risikomanagement*, KPMG. Deutschland, Berlin, 2006.

KPMG. "Global Financial Services", *Risk and capital management for insurers*, no:302054, 2003.

Lang, Trudi, *An Overview of Four Futures Methodologies: Delphi, Environmental Scanning, Issues Management, and Emerging Issue Analysis* (Occasional Paper 7). Hawai'i Research Center for Future Studies, Hawai, 1995.

Lederer, A.L. and V. Sethi, *Key Prescriptions for Strategic Information Systems Planning*, Journal of Management Information Systems, Vol. 13, pp. 35-62, 1996.

Lengnick-Hall, C.A., & Beck, T.E., "Adaptive fit versus robust transformation", *how organizations respond to environmental change*. Journal of Management, **31**: 738-757, 2005.

M. Weske, *Business Process Management*, DOI 10.1007/978-3-642-28616-2 1, Springer-Verlag Berlin Heidelberg, 2012.

Mango, Donald and Venter, Gary Guy Carpenter & Co., LLC., *Enterprise Risk Analysis* (Guy Carpenter & Company), 2007.

Martin J. Eppler et al. Paper #7/2006, *Visual Strategizing The Systematic Use of Visualization in the Strategy Process*, December, 2006.

McNeil, AJ., Frey, R. & Embrechts P., *Quantitative risk management: Concepts, techniques and tools*, Princeton University Press, Princeton, NJ, 2005.

Mestchian, P. Makarov, M & Mirzai B., *Operational risk - COSO reexamined*, Journal of Risk Intelligence, vol. 1, pp. 19-22, SAS International, 2005.

Mestchian, P., "Operational risk management" *The solution is in the problem, Advances in Operational Risk Management,* RISK Books, 2nd edition, Risk Waters Group, London, 2003.

Michael Haubenstock, *The operational Risk Management Framework*, 2002.

Morris A. Cohen, Howard Kunreuther, *Operations Risk Management*: Overview of Paul Kleindorfer's Contributions, 2007.

Morrison, James L., *Environmental Scanning*, In Meredith A. Whitely, John D. Porter, and Robert H. Fenske (eds.), A Primer for New Institutional Researchers. Tallahassee: The Association for Institutional Research, pp. 86–99. 1992.

Nicolai J. Foss. Peter G. Klein, *Organızational Governance*, Revised version: 8 June, 2008.

Oesterreichische Nationalbank in cooperation with the Financial Market Authority. *Guidelines on Operational Risk Management*.

Penrose E., *The theory of the growth of the firm* (3 Ed. consulted). Oxford: Oxford University Press, 1957.

Policy Brief, *Small and Medium-sized Enterprises: Local Strength, Global Reach*, June, 2000.

Robert B. Carton, *Measuring Organizational Performance*: an exploratory study, MBA The University of Georgia, 2004.

Smart Draw , *Visual Strategic Planning Thinking and Communicating Visually in the Strategic Planning Process,* Version 1.5, 2009.

Springer, *ACM Computing Classification* J.1, H.4.1, D.2.2 ISBN 978-3-540-73521-2 Berlin Heidelberg New York, 1998.

"The Firm as an Epistemic Community" The Knowledge Based View Revisited, *Opening Up Innovation: Strategy, Organization and Technology*, Imperial College London Business School, June 16 - 18, 2010.

The GARP Risk Series, *Operational Risk Management*, Chapter 12.

Tony Jaques Citation , "Issue Management and Crisis Management", An *Integrated, Non-linear, Relational Construct*, Public Relations Review, 33(2), pp 147-157, 2007.

Wilson, D., "Operational Risk" *in L. Borodovsky and M. Lore (eds) The Professional's Handbook of Financial Risk Management*, Oxford: Butterworth- Heinemann, pp. 377–413, 2001.

Yousef Paganeh, *Quantifying Operational Risk within Banks According to Basel II* (Applying Loss Distribution Method) University of Miskolc, 2010.

Zaw Zaw Aung, *Operational Risk Management for Service Outsourcing*. International Journal of Electronic Business Management, Vol. 6, No. 3, pp. 120 130, 2008.