

**DEVELOPING AND MANAGING INFORMATION TECHNOLOGY  
RISK MANAGEMENT FRAMEWORK - CASE STUDY OF A  
COMMERCIAL BANK**

**ABID HOSSEN**



**DEPARTMENT OF INDUSTRIAL AND PRODUCTION ENGINEERING (IPE)**

**BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY (BUET)**

**DHAKA, BANGLADESH**

**FEBRUARY 2019**

**DEVELOPING AND MANAGING INFORMATION TECHNOLOGY  
RISK MANAGEMENT FRAMEWORK - CASE STUDY OF A  
COMMERCIAL BANK**

**By**

**ABID HOSSEN**

A Thesis paper submitted to the  
Department of Industrial and Production Engineering,  
Bangladesh University of Engineering and Technology  
in partial fulfillment of the requirements for the degree of  
Master of Engineering (M. Engg.) in Advanced Engineering Management (AEM)



**DEPARTMENT OF INDUSTRIAL AND PRODUCTION ENGINEERING (IPE)  
BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY (BUET)  
DHAKA, BANGLADESH**

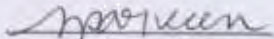
**FEBRUARY 2019**

## CERTIFICATE OF APPROVAL

---

The thesis entitled as “**Developing and Managing Information Technology Risk Management Framework – Case Study of a Commercial Bank**” submitted by Abid Hossen, Student No. 0411082110, Session- April 2011, has been accepted as satisfactory in partial fulfillment of the requirement for the degree of M.Engg. in Advanced Engineering and Management on February 26,2019.

### BOARD OF EXAMINERS



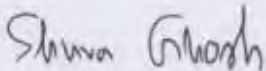
Dr. Sultana Parveen  
Professor  
Department of IPE, BUET, Dhaka

Chairman (Supervisor)



Dr. Syed Mithun Ali  
Associate Professor  
Department of IPE, BUET, Dhaka

Member



Dr. Shuva Ghosh  
Assistant Professor  
Department of IPE, BUET, Dhaka

Member

## CANDIDATE'S DECLARATION

---

It is hereby declared that this thesis or any part of it has not been submitted elsewhere for the award of any degree or diploma.

Abid Hossen

**THIS WORK IS DEDICATED TO MY FAMILY  
AND MY WELL-WISHERS**

## ACKNOWLEDGEMENT

---

At first, the author wants to convey his deepest gratefulness to the almighty God, the beneficial, the merciful for granting me to bring this research work into light. The author would like to express his sincere respect & gratitude to honorable teacher & thesis supervisor, Dr. Sultana Parveen, Professor, Department of Industrial and Production Engineering (IPE), Bangladesh University of Engineering and Technology (BUET), Dhaka, for his thoughtful suggestions, constant guidance and encouragement throughout the progress of this research work. The author also expressed his sincere gratitude to Dr. Syed Mithun Ali, Associate Professor and Dr. Shuva Ghosh, Assistant Professor, Department of IPE, BUET for their constructive remarks and evaluation of this research.

The author is especially thankful to different IT officials of National Bank Ltd in Bangladesh for their opinions and contribution during the questionnaire and data collection phase. It allows the author to have clear ideas about total risk Management in the Banking Sector.

The author is also grateful to all the writers and publishers of the books and journal papers that have taken as references while conducting this research. With a very special recognition, the author would like to thanks all the members of his family, who provided their continuous inspiration, sacrifice and support which encouraged in completing the research work successfully.

## ABSTRACT

---

The aim of this research is to establish a IT risk management framework for a commercial bank by which an organization can identify, measure, manage, monitor and report a risk. Framework helps the bank to manage its IT related risk I to evaluate, response and governance of risks. In order to prepare for IT related risk, organization must understand all domain, process goal and key activities under each process goal to handle risk effectively and efficiently.

This thesis is based on both qualitative and quantitative research methodology. A part of the report looks into the details of different framework and standard which are related to Information technology risk. Therefore, performing gap analysis, a suitable framework was selected for further usage in terms of governance, risk evaluation and risk mitigation.

The author used a survey among IT officials from different financial organizations in Bangladesh to determine whether they are acquainted with different framework and which is most appropriate framework for them. Survey suggests that Risk IT framework is the most suitable framework which is aligned with the gap analysis performed earlier. The author used AHP and FAHP method to identify the most important key activities of Risk IT framework by collecting expert opinion from a commercial bank.

Following the method, a commercial bank can be beneficial to identify the appropriate key activities among set of activities for establishing a framework to manage, evaluate and response the IT related risk.

## Table of Contents

<b>CHAPTER 1: INTRODUCTION.....</b>	<b>1</b>
1.2 OBJECTIVES OF THE STUDY.....	1
1.3 OUTLINE OF METHODOLOGY.....	1
<b>CHAPTER 2 : LITERATURE REVIEW.....</b>	<b>3</b>
2.1 RISK IT FRAMEWORK.....	3
2.2 AHP AND FUZZY AHP.....	5
<b>CHAPTER 3: METHODOLOGY.....</b>	<b>6</b>
3.1 RESEARCH METHOD.....	6
3.2 SAMPLING.....	6
3.3 TOOLS FOR ANALYSIS.....	6
3.4 DATA COLLECTION AND ANALYSIS.....	6
<b>CHAPTER 4 : THEORETICAL FRAMEWORK.....</b>	<b>7</b>
4.1 INTRODUCTION.....	7
4.2 IMPORTANCE OF IT RISK MANAGEMENT FRAMEWORK IN BANK.....	7
4.3 LIST OF RISK ANALYSIS STANDARD/Framework.....	8
4.4 COMPARATIVE ANALYSIS OF FRAME WORK.....	10
4.5 GAP ANALYSIS.....	10
4.6 CHOOSING AN APPROPRIATE IT FRAMEWORK.....	11
4.7 RISK IT FRAMEWORK.....	11
4.8 PURPOSE OF THE RISK IT FRAMEWORK.....	12
4.9 BENEFITS AND OUTCOMES.....	13
4.10 RISK IT PRINCIPLES.....	13
4.11 DETAILS OF RISK IT PROCESS MODEL.....	14
4.12 ANALYTIC HIERARCHY PROCESS (AHP).....	16
4.13 NECESSITY OF FAHP INSTEAD OF AHP?.....	18
4.14 FUZZY SETS AND ITS ARITHMETIC OPERATIONS.....	19
4.15 ASSESSMENT MODEL.....	19
4.16 CONSISTENCY INDEX.....	21
4.17 THE PROPOSED FUZZY AHP.....	21
<b>CHAPTER 5 : RESULT AND FINDINGS.....</b>	<b>23</b>
5.1 WEIGHT CALCULATION BY AHP PROCESS.....	23
5.1.1 PAIRWISE COMPARISON.....	23
5.1.2 CONSISTENCY RATIO CHECKING:.....	23
5.1.3 KEY ACTIVITIES PRIORITIZATION.....	24
5.1.4 KEY ACTIVITIES AND PROCESS GOAL.....	24
5.1.5 ALL KEY ACTIVITIES CALCULATED BY AHP PROCESS.....	25
5.2 ALL KEY ACTIVITIES CALCULATED BY FUZZY AHP PROCESS.....	26
5.2.1 COMPARISON OF WEIGHT OF KEY ACTIVITIES CALCULATED BY AHP AND FUZZY AHP .....	28



5.2.2 OUTCOME OF THE COMPARISON BETWEEN AHP AND FUZZY AHP.....	29
5.2.3 PROPOSED FRAMEWORK.....	29
<b>CHAPTER 6: DISCUSSION.....</b>	<b>31</b>
6.1 DISCUSSION.....	31
<b>CHAPTER 7 : CONCLUSION.....</b>	<b>32</b>
7.1 CONCLUSION.....	32
7.2 LIMITATION AND RECOMMENDATION FOR FURTHER RESEARCH.....	32
<b>REFERENCES.....</b>	<b>33</b>
<b>APPENDIX-A.....</b>	<b>35</b>
<b>APPENDIX-B.....</b>	<b>38</b>
<b>APPENDIX C.....</b>	<b>40</b>
<b>APPENDIX D.....</b>	<b>45</b>

## **List of Tables**

Table 4.1: List of Risk Analysis Standard/ Framework	09
Table 4.2: Randomly Generated Consistency Index for different size of matrix	18
Table 4.3: AHP Scale for Comparison	19
Table 5.1: Process Goal prioritization	25
Table 5.2: Key activities and Process Goal	26
Table 5.3 : Weight of Key Activities through AHP Process	27
Table 5.4: Weight of Key Activities through Fuzzy AHP Process	28
Table 5.5: Comparison of Fuzzy and AHP	29
Table 5.6: Weight Comparison between AHP and Fuzzy AHP	30

## LIST OF ABBREVIATIONS

<b>Symbol</b>	<b>Acronym</b>
IT	Information Technology
IS	Information System
COSO	Committee of Sponsoring Organizations of the Treadway Commission
COBIT	Control Objectives for Information and Related Technology
ERM	Enterprise Risk Management
ISACA	Information Systems Audit and Control Association
ISO	International Standardization Office
AHP	Analytical Hierarchy Process
CI	Consistency Index
CR	Consistency Ratio
RCI	Random Consistency Index
ICT	Information and Communication Technology
AS/NZS	Australian/New Zealand Standards
NIST	National Institute of Standard and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
RG	Risk Governance
RE	Risk Evaluation
RR	Risk Response

# CHAPTER 1: INTRODUCTION

## 1.1 Introduction

Now a days all Banks of Bangladesh and all over the world are totally dependent on Information technology. Information technology covers from Branch level to all divisions of Bank. Mostly all the business process is totally dependent on the IT. As per guideline of Bangladesh Bank there are seven core risks area in banking sector, IT security is one of the core risk. In this context, Information technology (IT) risk assessment plays an entirely exceptional role in each bank. IT integrates all different functional areas within an organization and thus it has a potential to integrate the risk assessment activities as well. Based on the assumptions, we can conclude that there is no need to make a difference between business risk and IT risk. IT risk is business risk – specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an Bank. The business value and IT risk are two sides of the same coin and risk is inherent to all enterprises.

There are a lot of risk assessment frameworks or standard like COSO ERM, AS/NZS 4360, ISO 31000, Basel II, Octave but they have not focus on IT risk assessment and management area. As well there are other framework which is focused on only the IT security like NIST, BS7799, and ISO 27000 family but for a financial institution we have to select a comprehensive framework where depth of coverage of IT and completeness of Business Risk Management scope will be fully covered. Moreover in the context of commercial Bank of Bangladesh, most of the bank does not follow any risk assessment framework, but it is absolutely necessary for every bank to follow a framework.

As risk is increasing day by day to commercial banks as all business operations are dependent on IT infrastructure so it is obvious to identify a suitable risk framework which will govern, evaluate and response of all kind of IT risk. Moreover this risk framework will provide a holistic approach for treating the risk and integrating the risk management framework in context of enterprise.

## 1.2 Objectives of the Study

The specific objectives of this project are

- To identify and select a IT Risk framework to manage a Bank's Risk in perspective of Enterprise Risk Management.
- To identify the most appropriate control or activities for development of an IT risk management framework using AHP and Fuzzy AHP.

## 1.3 Outline of Methodology

The proposed research methodology is outlined below:

- 1) First the report will discuss about the different risk framework and
- 2) Then this study will suggest the appropriate risk framework which seems fit for a commercial bank in terms of governance, risk evaluation and risk response.
- 3) Next the study will focus on key activities identification and prioritization by collecting the comparison data through expert interview

- 4) Then this study will identify and prioritize key risk activities under the different process area by Analytical Hierarchy Process and Fuzzy Analytical Hierarchy process based on the data of expert interview
- 6) And finally, this report will find out the prioritized risk activities and according to that it will propose a redefined IT risk management framework for a commercial bank.

## CHAPTER 2 : LITERATURE REVIEW

### 2.1 Risk IT Framework

Information Systems Audit and Control Association (ISACA) developed, The international risk IT model, which provides a comprehensive view of IT risks related to businesses. In 2012 Bakshi, stated that the premise of risk IT is that institution management can manage the risk associated with IT, identify business opportunities, and attain a greater return on investments [1]. The risk IT model became the foundation for this study. The risk IT model has two sections: the risk IT framework and the risk IT practitioner guide. In 2016 Barrett [2] stated that during 2008 and 2009, ISACA working groups consisting of 112 members from 18 countries worked with over 1700 other IT professionals to develop the risk IT model and specifically, the risk IT work groups comprised seven IT risk task forces, six development team members, 65 expert reviewers, 11 framework committee members, and 14 board members. The risk IT model addresses the gap in knowledge between enterprise risk management activities and IT risk management activities. This model provides business leaders with a comprehensive tool to manage IT-related business risks and delivers direction on decisions connecting to risks associated with IT .Risk governance, risk evaluation, and risk response are the key constructs of the risk IT model. IT risk is the absence of computer software and hardware due to events such as denial of service attack, lack of expertise of IT personnel, loss of company's data due to theft; system malfunction or system glitches . In other way ISACA defines IT risk management as the protection of information within the institution's technology infrastructure based on the organization's tolerance for risk and includes an assessment of the business impact of technology risks, the compliance requirements, and the alignment of technology with the organization's business strategy.

In 2013, Debreceny [3] opined that ISACA combined the risk IT framework along with other frameworks in Control Objectives for Information and Related Technology version5 (COBIT 5) to assist management in IT governance and risk management activities

Svatá and Fleischmann [4] graded the risk IT framework as the most suitable framework to manage IT risks and they also the risk IT framework provides detailed exposure of IT risk management activities, which institution leaders can use to accomplish IT risks.

Risk governance is the first of the three key constructs of the risk IT model. ISACA noted that risk governance is the governance of IT actions to manage risks associated with technology. According to ISACA, IT risk governance activities include (a) establishing and maintaining the institution's IT risk threshold by assessing the institution's risk appetite and tolerance, (b) establishing accountable and liable risk governance officers, and (c) providing self-governing assurances for the administration of IT risks.

In 2012, Haneef [5] stated that Financial institutions face business risks daily in normal activities. These risks include credit risk, liquidityrisk, regulatory risk, and operational risk. According to Bangladesh Bank (BPRD CIRCULAR NO: 17 Dated 07 October 2003, subject: "Guidelines on "Managing Core Risks in Banking") there were five core risks were identified which are a) Credit Risks; b) Asset and Liability/Balance Sheet Risks;c) Foreign Exchange Risks; d) Internal Control and Compliance Risks; and e) Money Laundering Risks. Thereafter additional another core risk was included in the name of IT Security risk [6] where risk tolerance and risk threshold was introduced related to IT. Risk tolerance is the level of

risk an institution can accept in other word risk tolerance as the acceptable deviation from the established risk appetite of the institution and risk appetite is the amount and type of risk an institution is willing to accept. Therefore, the establishment of an effective risk governance program to manage IT risks based on the institution's IT risk threshold is possible.

The second key construct of the risk IT model is risk evaluation Risk evaluation includes (a) identifying and assessing risk, (b) estimating the risk, and (c) maintaining a risk register . These risk evaluation activities form part of the risk evaluation process areas outlined in the risk IT model.

The first phase of risk management involves risk identification. Risk identification is the detection of possible events that may affect an institution from achieving the objectives. There are formal methods and techniques that aid in the identification of risks within an institution. These methods and techniques include using a risk breakdown structure (RBS) and a risk breakdown matrix (RBM) for identifying risk .The risk breakdown structure is a hierarchical grouping of identified risks arranged by risk categories and causes of the risks (Project Management Institute [PMI]). Researchers such as Loo, Abdul-Rahman, and Wang [7] and Mehdizadeh, Breysse, Tailandier, and Niandou [8] used RBS for risk identification in their studies involving construction, architectural, and engineering projects. Risk assessment involves reviewing the impact and likelihood of the occurrence of a risk.

In the year of 2013 Herrmann [9] studied risk estimation in IT and suggested that the Delphi method to estimate risk provides a more reliable estimate than other risk estimation methods. The Delphi method involves selecting a panel of experts to provide their opinions on an issue Despite its difficulty, risk estimation in IT is essential in supporting management to plan and rank risk management activities or prioritize IT requirements.

A risk register is a tool that captures the risk tolerance, the potential risk events, and the probability of occurrence of the risk. The risk register contains a list of threats, the probability of occurrence of these threats, and the impact of the threats. A risk register contains information such as the ranking of each identified risk, the estimated cost of the impact of the identified risk, and appropriate actions for each risk .

According to Kutsch, Browning, and Hall [10] Risk response is the third key construct of risk IT model. The four possible risk responses are (a) avoidance, (b) reduction, (c) sharing, and (d) acceptance. Risk response activities include (a) implementing controls, (b) communicating lessons learnt, and (c) monitoring risks .highlighted the importance of risk response in mitigating risks.

Implementing controls is a function of management in managing operations. An institution can manage operations by developing procedures, standards, policies, and systems to minimize or mitigate risks associated with any identified exposure .In the Year 2013 ,Ellul and Yerramilli [11] reviewed bank-holding institutions in United States and stated that institutions with sufficient risk controls had lower tail risks and higher return on asset (ROA) compared to institutions without adequate risk controls.

Monitoring risk is an essential activity for traditional and enterprise risk management program and involves ensuring that an established risk program is active .Active monitoring of risk fosters the development of appropriate risk management strategies and procedures to mitigate against identified risks Risks such as system failure and changing regulation are technology risks affecting institutions engaged in cloud services Babu &Sekhar [12]. Risk monitoring is part of the risk response activity and essential for IT risk management

In Year 2014 Igor Anikin [13] evaluated information security risk assessment on telecommunication network where they have considered information, host, server, telecommunication equipment's and IT services as their asset and based on pair wise comparison of question reached on probable threat based on information security risk level.

## **2.2 AHP and Fuzzy AHP**

In the year of 2015 MengMeng and Enping Liu [14] also used AHP method to identify the Information security risk factor based on the co factor of each criterion. In the research it used five criterion or factor and 15 sub factors for finding the most risk factor using AHP method. In the paper he showed Platform Security , Operation Security and Backup Security are the three major risk factors of the criterion layer in the hierarchy model of information security risk assessment of company He also used CI,RI and CR index to justify and ranking the risk.

Saman Amin bakhsh, Murat Gunduz, Rifat Sonmez [15] used AHP model to identify safety risks during planning and budgeting of construction projects . In this paper, a framework was proposed to assist in safety risk assessment and accident/injury prevention budgeting process; a framework that reduces biased decision making while facilitating consensus decision making by a group of decision makers. The proposed framework was applied to a real-life construction project to illustrate how the framework can guide the decision makers through safety risk assessment.

Shivani Sharma and Ravindra Pratap [16] has applied AHP for evaluation of risk related to supply chain management in a manufacturing firm. Five risks for the company are evaluated and defined. planning risk, product risk, environment risk, industrial risk, productivity risk. Dr A.C Shukla [17] stated that Analytical Hierarchy Process is one of the most inclusive system is considered to make decisions with multiple criteria because this method gives to formulate the problem as a hierarchical and believe a mixture of quantitative and qualitative criteria as well. The first step is to create a hierarchy of the problem. The second step is to give a nominal value to each level of the hierarchy and create a matrix of pairwise comparison judgment.

In the year 2016, Mingxiang He, XinAn [18] stated that By AHP, the relative weight of elements related to information security risk can be calculated. Then the optimal indicators, which can simplify the calculation of risk value, can be selected by sorting the weights of elements to reduce the number of indicators. According to these indicators, which have great influence on the risk, appropriate measures should be taken to control the risk. Moreover, AHP, a method of the combination of qualitative and quantitative assessment methods, can overcome the disadvantages of single qualitative or quantitative assessment method. The Analytic Hierarchy Process , a combination of quantitative and qualitative. analysis methods, is proposed by the famous American Operations Research Professor Saaty in the early 1970s. This method is more efficiently used to solve multiple complex problems. In the Analytic Hierarchy Process, elements related to decisions are divided into target, criteria and solutions. It breaks down complex problems into a number of levels based on dominance relations.

Mohsen Askari, Hamid Reza Shokrizadeh, Nina Ghane [19] also used Fuzzy AHP in risk ranking of a construction project to calculate global risk in perspective of global risk of the project. Mustafa Batuhan ayhan [20] also used fuzzy ahp for selection of supplier in the



supply chain management system. It has been also used in mining industry [21]. It has been also used to select apparel item for startup garments [22].

## **CHAPTER 3: METHODOLOGY**

### **3.1 Research Method**

This thesis paper concerns to define and manage a IT Risk Management Framework of a commercial bank about how to Govern, Evaluate and Response of Risks. The study was based on mixed method i.e based on qualitative and quantitative method. Qualitative method is based on the interview of focus group or expert group based on relative questions and therefore to quantify the outcome based on those answers is the quantitative method.

### **3.2 Sampling**

In this research the non-probability sampling technique specifically purposive and convenience sampling, has been applied. Non-probability sampling relies on the subjective judgment of the researcher and it is very cost and time-effective. It can also be used when it's impossible to conduct probability sampling (e.g. when we have a very small population to work with). Purposive sampling involves choosing people whose views are relevant to an issue because one makes judgment, and/or persuaded by collaborators or researcher, that their views are particularly worth obtaining and typify important varieties of viewpoint. For instance, case study is a purposive sampling where the research is limited to one group, often with a similar characteristic or of small size.

### **3.3 Tools for Analysis**

In this study, a quantitative analysis was done by AHP and Fuzzy AHP based on qualitative judgment of expert group. Qualitative judgment was mapped to comparison matrixes on predefined and standard scale and therefore after several mathematical calculation it was concluded in individual weight of those observations.

Overall, tools used in the whole research are Microsoft Excel, python based program for AHP and Fuzzy AHP. Apart from the research contextual data, the reference used in the research was recorded with the help of Mendeley Desktop software.

### **3.4 Data Collection and Analysis**

In this research, information collected from literature study and empirical investigations. An empirical study is investigations based on data, which was collected through surveys, interviews, telephonic conversations, and meetings. The case study aimed to develop and manage a IT risk frame work for a commercial bank. Here author had extensive repeated meeting, interview and discussion with Four IT Managers who are experienced more than 15 years in their respective field namely operation, infrastructure, system and techno business. Author discussed in detail about Nine process and all key activities under those process to exchange knowledge and with their group decision author recorded their comparison with

one metric to other metric. This was basis of building the comparison matrix. It can be mentioned that several times review meeting was done to review the comparison when author found major inconsistency.

## **CHAPTER 4 : THEORETICAL FRAMEWORK**

### **4.1 Introduction**

Risk assessment is regularly conducted by Risk Management unit of a bank to fulfill a variety of business and regulatory requirements. They rely on guidance from Bangladesh Bank to provide a framework for conducting the risk assessment which is focused on credit risk, market risk, operational risk, environmental and social risk. But according to guideline of Bangladesh bank ICT security guideline Bank has to follow ICT Risk Management. In this context, information systems and/or information technology(IT) risk assessment plays an entirely exceptional role in commercial bank for regulatory purpose. But in the guideline it was not mentioned which framework should be followed by commercial bank rather it was open. Now a days IT integrates all different functional areas within an bank and business area is totally dependent on the service of IT rather it is very much intertwined with each other. Based on the assumptions, we can conclude that there is no need to make a difference between business risk and IT risk. IT risk is business risk – specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. The business value and IT risk are two sides of the same coin and risk is inherent to all enterprises. So there is a need to manage all the risks.

### **4.2 Importance of IT Risk Management Framework in Bank**

It is becoming increasingly apparent that information systems and technologies significantly influence business processes in the banking industry. The value of IT depends widely on the way IT are implemented and related to the banking activities. The IT as such represent an important factor of competitiveness and commercial success of individual financial institutions. IT affect the banking business and its economic results in the following ways:

- 1) Contribution of IT to the business productivity;
- 2) making use of IT as a tool for banking innovations; and
- 3) IT as a banking risk mitigating (increasing) factor.

In accordance with the main focus of this article, we will hereafter highlight the relationship between IT and risk. This role of IT matters very much since drawbacks in risk control might lead not only to financial losses and a failure of individual institutions or threat to clients' deposits, but also to a negative impact on the whole economy both nationally and globally.

From this point of view, we can observe two relationships between risk management and IT:

- 1) IT support risk management in banks,
- 2) IT penetration into the banking processes causes dependency of business activities on IT.

This relationship increases the significance of IT risk management. Risk management is an inseparable part of business on financial markets. The core of an efficient and effective risk management lies in determining an optimal level of risks that are to be tolerated whereas risks above this level are suitable to be controlled. The ability to find the right balance between an inclination to risk and a tendency to its elimination is the very way to reach stable economic results. Therefore, investment in risk management does not automatically mean a negative item in a profit and loss

statement, but it might (and should) significantly contribute to the profitability of a bank. A bank's economic result is thus a common denominator of the business activity on the one hand and an efficient risk management on the other. With regard to the aforementioned dependency of business on IT and due to the advanced stage of their penetration into the banking activities and products, the importance of IT risk management is growing. This fact is reflected by banks themselves and obviously also by regulators. Leading regulators pay adequate attention to IT in banks and many of them, including the National Bank, have published prudential rules and carried out systematic supervision in this area. Regulatory requirements on IT in banks reflect the unique role of the banking industry for the national economy, general principles of banking risk management and the importance of IT in banking as such. Although this basis stresses the specifics mentioned above, IT regulation complies with the best practices and generally respected standards such as ISO 2700x, COBIT, ITIL etc. Except these general standards on IT, there are other relevant frameworks specific to banking, Basel II being the most important one. This framework has promoted operational risk among the three main banking risks besides credit and market risk, thus also highlighting IT risk as an integral part (substantial subset) of operational risk. The Basel II definition of operational risk regards systems as one of four operational risk drivers; however, the coverage of IT issues within Basel II is not deep. Although Basel II sets down only general principles and methods for operational risk capital requirement quantification, it establishes operational risk management as a separate risk discipline. However, no global operational standard, including guidance for the implementation of a bank's operational risk framework and particular operational risk management methods, has been established yet

### 4.3 List of Risk Analysis Standard/Framework

Table 4.1 ( List of Risk Analysis Standard/Framework)

General Information	identification	Users	Target Organization
COSO ERM Committee of Sponsoring organizations of the Treadway Commission •www.coso.org/Publications/ERM/COSO_ERM	COSO issued Internal Control – Integrated Framework to help businesses and other entities assess and enhance their internal control systems. COSO ERM views enterprise risk management as a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.	<ul style="list-style-type: none"> <li>• Executive Management</li> <li>• Internal auditors</li> </ul>	All organizations that are to be compliant with strict internal control regulations.

<ul style="list-style-type: none"> <li>AS/NZS 4360:2004</li> <li>Standards Australia and Standards New Zealand</li> <li><a href="http://www.standards.org.au">http://www.standards.org.au</a></li> </ul>	<p>The standard provides a generic guide to managing risk and specifies the elements of the risk management process. The standard does not propose a uniform risk management systems, rather the standard proposes that the design and implementation of the risk management system should be influenced by the varying needs of the organisation, its products and services, and the processes and specific practices employed</p>	<ul style="list-style-type: none"> <li>Management</li> </ul>	<ul style="list-style-type: none"> <li>Government agencies</li> <li>Large companies</li> <li>SME</li> <li>Commercial CIO</li> <li>Non-commercial CIO</li> </ul>
<ul style="list-style-type: none"> <li>ISO 31000:2009</li> <li>International Organization for Standardization</li> <li><a href="http://www.iso.org">www.iso.org</a></li> </ul>	<p>ISO 31000 is intended to be a family of standards relating to risk management Codified by the International Organization for Standardization. ISO 31000:2009 addresses the entire management system that supports the design, implementation, maintenance and improvement of risk management processes.</p>	<ul style="list-style-type: none"> <li>executive level stakeholders appointment holders in the enterprise risk management group</li> <li>risk analysts and management officers</li> <li>line managers and project managers</li> <li>compliance and internal auditors</li> <li>independent practitioners</li> </ul>	<ul style="list-style-type: none"> <li>Government agencies</li> <li>Large companies</li> <li>SME</li> <li>Commercial CIO</li> <li>Non-commercial CIO</li> </ul>
<ul style="list-style-type: none"> <li>ISO/IEC 27005:2009 (ISO 13335-2)</li> <li>Information security risk management</li> <li>ISO</li> </ul>	<p>Describes the complete process of information security Risk Management in a generic manner. The annexes contain examples of information security Risk Assessment approaches as well as lists of possible threats, vulnerabilities and security controls. It can be viewed at as the basic information Risk Management standard at international level, setting a framework for the definition of the Risk Management process</p>	<ul style="list-style-type: none"> <li>Management</li> <li>Operational</li> </ul>	<ul style="list-style-type: none"> <li>Government agencies</li> <li>Large companies</li> <li>SME</li> <li>Commercial CIO</li> <li>Non-commercial CIO</li> </ul>
<ul style="list-style-type: none"> <li>ISO Guide 73:2009 Risk Management Vocabulary</li> <li>International Organization for Standardization</li> <li><a href="http://www.iso.org">www.iso.org</a></li> </ul>	<p>Provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the</p>	<ul style="list-style-type: none"> <li>risk managers,</li> <li>developers of national or sector-specific standards, guides, procedures and codes of practice</li> </ul>	<ul style="list-style-type: none"> <li>Government agencies</li> <li>Large companies</li> <li>SME</li> <li>Commercial CIO</li> <li>Non-commercial CIO</li> </ul>

	management of risk.	relating to the management of risk	
<ul style="list-style-type: none"> <li>• BASEL II</li> <li>• BASEL II and IT control objectives</li> </ul>	Basel II is an international standard published by the Basel Committee on Banking Supervision in June 2004. It gives recommendations for banking regulators with regard to capital standards and risk management in banks. Basel II sets down risk and capital management principles to ensure a bank holds capital reserves appropriate to its risk exposure. It aims to make capital allocation more risk sensitive and gives wider range of approaches for risk and capital adequacy quantification	<ul style="list-style-type: none"> <li>• Stakeholders</li> <li>• Executive management</li> <li>• Management</li> <li>• Risk managers</li> <li>• Internal auditors</li> <li>• information risk managers</li> </ul>	<ul style="list-style-type: none"> <li>• Banks</li> <li>• Other credit institutions</li> <li>• Regulators</li> <li>• External auditors</li> <li>• Rating</li> </ul>
OCTAVE Method <a href="http://www.cert.org/octave/">http://www.cert.org/octave/</a>	OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning.	<ul style="list-style-type: none"> <li>• Management</li> <li>• Operational</li> </ul>	<ul style="list-style-type: none"> <li>• SME</li> </ul>
<ul style="list-style-type: none"> <li>• CRAMM (CCTA Risk Analysis and Management Method)</li> </ul> <a href="http://www.cramm.com">http://www.cramm.com</a>	CRAMM is a risk analysis method developed by the British government organization CCTA (Central Communication and Telecommunication Agency), now renamed the Office of Government Commerce (OGC).	<ul style="list-style-type: none"> <li>• Management</li> <li>• Operational</li> <li>• Technical</li> </ul>	<ul style="list-style-type: none"> <li>• Government agencies</li> <li>• Large companies</li> </ul>

#### 4.4 Comparative Analysis of Frame Work

Different risk management frameworks take into account the specifics of the IT area differently. COSO ERM, AS/NZS 4360, ISO 31000 and BASEL II are typical examples of not paying special attention to IT risk management. However, considering that Basel II is a very important standard for financial organizations, and at the same time these institutions introduce governance principles to their management systems, there is a need to integrate both the frameworks. In 2008, ISACA and ITGI introduced the document “Control Objectives for Basel II”. It provides a framework for managing the operational and information risk in the context of Basel II. It presents an outline of risk under Basel II, the links between the operational risk and the IT risk, and an approach for managing the information risk. The document addresses three groups: information risk managers, IT practitioners and financial services experts. The executive summary states that financial services organizations using the framework presented are able to apply recognized IT control objectives and management processes to address the role of IT in operational risk. On the other hand, focusing on the depth of the IT coverage within the risk management frameworks, we can furnish frameworks such as ISO 2700x, ISF and CRAMM. They are examples of frameworks covering IT risk management without any serious attempt to

integrate it with the business risk management. The framework OCTAVE is the only framework which deals with organizational risk in addition to IT risk.

#### **4.5 Gap Analysis**

If we position different types of risk assessment frameworks along the axis X – Depth of coverage of IT and axis Y – Completeness of risk management scope can help us understand both their relevance to the IT/IS area and the level of commonness in the understanding the phenomenon of risk. There is a whole range of different frameworks dealing with risk assessment, but these regulations either are too generic to be applicable to IT risk management or, although they deal with IT risk management, they narrow the area to IT security risk management. The area named “GAP” identifies the space which is not well supported by the available frameworks, however, at the same time it represents the key to more integrated IT/IS and business risk management.

#### **4.6 Choosing an appropriate IT framework**

With regard to filling the gap it is worth mentioning especially the generally oriented initiative of these organizations called meaningfully Risk IT. In our opinion, the key contribution of this initiative is the fact that the framework connects business with IT risk management as closely as possible. This set of principles leads an enterprise to align its management of IT related business risk with its overall risk management. As such, it tries to bridge the gap in the current array of risk management frameworks for IT. There is no known framework that both includes a holistic look at risk management and, at the same time, provides an adequate depth and detail when covering IT. This might promote Risk IT as a unique tool offering a coverage that is missing in COSO ERM, AS/NZS 4360 and security-oriented IT risk management frameworks. Risk IT complements ISACA’s COBIT, which provides a comprehensive framework for the control and governance of business-driven, IT-based solutions and services.

#### **4.7 Risk IT Framework**

Risk IT Framework is dedicated to helping enterprises manage IT-related risk. The collective experience of a global team of practitioners and experts, and existing and emerging practices and methodologies for effective IT risk management, have been consulted in the development of the Risk IT framework. Risk IT is a framework based on a set of guiding principles and featuring business processes and management guidelines that conform to some principles. The Risk IT framework complements ISACA’s COBIT<sup>1</sup>, which provides a comprehensive framework for the control and governance of business-driven information-technology-based (IT-based) solutions and services. While COBIT sets good practices for the *means* of risk management by providing a set of controls to mitigate IT risk, Risk IT sets good practices for the *ends* by providing a framework for enterprises to identify, govern and manage IT risk. The Risk IT framework is to be used to help implement IT governance, and enterprises that have adopted (or are planning to adopt) COBIT as their IT governance framework can use Risk IT to enhance risk management.

The COBIT processes manage all IT-related activities within the enterprise. These processes have to deal with events internal or external to the enterprise. Internal events can include operational IT incidents, project failures, full (IT) strategy switches and mergers. External events can include changes in market conditions, new competitors, new technology becoming

available and new regulations affecting IT. These events all pose a risk and/or opportunity and need to be assessed and responses developed. The risk dimension, and how to manage it, is the main subject of the Risk IT framework. When opportunities for IT-enabled business change are identified, the Val IT framework best describes how to progress and maximize the return on investment. The outcome of the assessment will probably have an impact on some of the IT processes and/or on the input to the IT processes.

It is important to keep this risk/benefit duality in mind during all risk-related decisions. For example, decisions should consider the exposure that may result if a risk is not treated vs. the benefit if it is addressed, or the potential benefit that may accrue if opportunities are taken vs. missed benefits if opportunities are foregone.

The Risk IT framework is aimed at a wide audience, as risk management is an all-encompassing and strategic requirement in any enterprise. The target audience includes.

- 1) Top executives and board members who need to set direction and monitor risk at the enterprise level.
- 2) Managers of IT and business departments who need to define
- 3) Risk Management professionals who need specific IT risk guideline.
- 4) External stakeholders.

The Risk IT framework is based on the principles of enterprise risk management (ERM) standards/frameworks such as COSO ERM2 and AS/NZS 43603 (soon to be complemented or replaced by ISO 31000) and provides insight on how to apply this guidance to IT. Risk IT applies the proven and generally accepted concepts from these major standards/frameworks, as well as the main concepts from other IT risk management related standards.

Although Risk IT aligns with major ERM frameworks, the presence and implementation of these frameworks is not a prerequisite for adopting Risk IT. By adopting Risk IT enterprises will automatically apply all ERM principles. In cases where ERM is present in some form, it is important to build on the strengths of the existing ERM programme—this will increase business buy-in and adoption of IT risk management, save time and money, and avoid misunderstandings about specific IT risks that may be part of a bigger business risk.

Risk IT defines, and is founded on, a number of guiding principles for effective management of IT risk. The principles are based on commonly accepted ERM principles, which have been applied to the domain of IT. The Risk IT process model is designed and structured to enable enterprises to apply the principles in practice and to benchmark their performance.

The Risk IT framework is about IT risk—in other words, business risk related to the use of IT. The connection to business is founded in the principles on which the framework is built, i.e., effective enterprise governance and management of IT risk.

#### **4.8 Purpose of the Risk IT Framework**

The all-encompassing use of IT can provide significant benefits to an enterprise, but it also involves risk. Due to IT's importance to the overall business, IT risk should be treated like other key business risks, such as strategic risk, environmental risk, market risk, credit risk, operational risks and compliance risk, all of which fall under the highest 'umbrella' risk category: failure to achieve strategic objectives. While these other risks have long been incorporated into corporate decision-making processes, too many executives tend to relegate IT risk to technical specialists outside the boardroom.

The Risk IT framework explains IT risk and enables users to:

- 1) Integrate the management of IT risk into the overall ERM of the enterprise, thus allowing the enterprise to make risk-return aware decision.
- 2) Make well-informed decisions about the extent of the risk and risk appetite and risk tolerance of the enterprise.
- 3) Understand how to respond to the risk

In brief, this framework allows the enterprise to make appropriate risk-aware decisions.

Practice has shown that the IT function and IT risk are often not well understood by an enterprise's key stakeholders, including board members and executive management. Yet, these are the people who depend on IT to achieve the strategic and operational objectives of the enterprise and, by consequence, should be accountable for risk management. Without a clear understanding of the IT function and IT risk, senior executives have no frame of reference for prioritizing and managing IT risk.

IT risk is not purely a technical issue. Although IT subject matter experts are needed to understand and manage aspects of IT risk, business management is the most important stakeholder. Business managers determine what IT needs to do to support their business; they set the targets for IT and consequently are accountable for managing the associated risks. In Risk IT, business management includes enterprise/corporate roles, business-line leaders and support functions (chief financial officer [CFO], chief information officer [CIO], human resources [HR], etc).

The Risk IT framework fills the gap between generic risk management frameworks such as COSO ERM, AS/NZS 4360, ISO 31000, the UK-based ARMS5 and domain-specific (such as security-related or project-management-related) frameworks. It provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues. In summary, the framework will enable enterprises to understand and manage all significant IT risk types.

The framework provides:

- 1) An end to end process framework for successful IT risk management.
- 2) Guidance for practitioners, including tools and techniques to understand and manage concrete risks to business operations. This includes a generic list of common, potentially adverse IT-related risk scenarios that could impact the realization of business objectives.

#### **4.9 Benefits and Outcomes**

The Risk IT framework addresses many issues that enterprises face today, notably their need for

- 1) An accurate view of significant current and near future IT related risk throughout the extended enterprise, and the success with which the enterprise is addressing them.
- 2) End –to-end guideline on how to manage IT-related risks, beyond both purely technical control measures and security.
- 3) Understanding how to capitalize on an investment made in an IT internal control system already in place to manage IT –related risk.
- 4) Understanding how effective IT risk management enables business process efficiency, improves quality, and reduce waste and costs.



- 5) A common framework/language to help communication and understanding amongst business, IT risk and audit management.
- 6) Promotion of risk responsibility and its acceptance throughout the enterprise.
- 7) A complete risk profile to better understand the enterprise full exposure, so as to better utilize company resources.

#### **4.10 Risk IT Principles**

Risk IT defines, and is founded on, a number of guiding principles for effective management of IT risk. The principles are based on commonly accepted ERM principles, which have been applied to the domain of IT. The Risk IT process model is designed and structured to enable enterprises to apply the principles in practice and to benchmark their performance.

The Risk IT framework is about IT risk in other words, business risk related to the use of IT. The connection to business is founded in the principles on which the framework is built, i.e., effective enterprise governance and management of IT risk.

- 1) Always connect to business objectives
- 2) Align the management of IT-Related business risk with overall ERM (If applicable)
- 3) Balance the costs and benefits of managing IT risk
- 4) Promote fair and open communication of IT risk
- 5) Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well defined tolerance levels

#### **4.11 Details of Risk IT Process Model**

In risk IT Framework there are three main domain which are divided and subdivided by process goal and process activities. The domain, process and their key activities are described below:

##### **a. Risk Governance**

Risk Governance Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.

1. Integrate with ERM (IWER)
2. Establish and Maintain a Common Risk View
3. Make Risk-Aware Business Decision

##### **b. Risk Evaluation**

Risk Evaluation Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

1. Analysis Risk
2. Maintain Risk Profile
3. Collect Data

##### **c. Risk Response**

Risk Response Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

1. Manage Risk
2. Articulate Risk
3. React To Events

#### **A. Establish and Maintain a Common Risk View**

**Process Goal RG1:** Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it.

**Key Activities:**

- RG1.1 Perform enterprise IT risk assessment.
- RG1.2 Propose IT risk tolerance thresholds.
- RG1.3 Approve IT risk tolerance.
- RG1.4 Align IT risk policy.
- RG1.5 Promote IT risk-aware culture.
- RG1.6 Encourage effective communication of IT risk.

#### **B. Integrate with ERM**

**Process Goal RG2:** Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level.

**Key Activities:**

- RG2.1 Establish and maintain accountability for IT risk management.
- RG2.2 Co-ordinate IT risk strategy and business risk strategy.
- RG2.3 Adapt IT risk practices to enterprise risk practices.
- RG2.4 Provide adequate resources for IT risk management.
- RG2.5 Provide independent assurance over IT risk management

#### **C. Make Risk-aware Business Decisions**

**Process Goal RG3:** Ensure that enterprise decisions consider the full range of opportunities and consequences from reliance on IT for success.

**Key Activities:**

- RG3.1 Gain management buy-in for the IT risk analysis approach.
- RG3.2 Approve IT risk analysis.
- RG3.3 Embed IT risk considerations in strategic business decision making.
- RG3.4 Accept IT risk.
- RG3.5 Prioritize IT risk response activities.

#### **D. Collect Data**

**Process Goal :**Identify relevant data to enable effective IT-related risk identification, analysis and reporting.

**Key Activities:**

- RE1.1 Establish and maintain a model for data collection.
- RE1.2 Collect data on the operating environment.
- RE1.3 Collect data on risk events.
- RE1.4 Identify risk factors.

## **E. Analysis Risk**

**Process Goal :** Develop useful information to support risk decisions that take into account the business relevance of risk factors.

### **Key Activities:**

- RE2.1 Define IT risk analysis scope.
- RE2.2 Estimate IT risk.
- RE2.3 Identify risk response options.
- RE2.4 Perform a peer review of IT risk analysis.

## **F. Maintain Risk Profile**

**Process Goal :** Maintain an up-to-date and complete inventory of risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls the context of business products, services and processes.

### **Key Activities:**

- RE3.1 Map IT resources to business processes.
- RE3.2 Determine business criticality of IT resources.
- RE3.3 Understand IT capabilities.
- RE3.4 Update IT risk scenario components.
- RE3.5 Maintain the IT risk register and IT risk map.
- RE3.6 Develop IT risk indicators.

## **G. Articulate Risk**

**Process Goal :** Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response.

### **Key Activities:**

- RR1.1 Communicate IT risk analysis results.
- RR1.2 Report IT risk management activities and state of compliance.
- RR1.3 Interpret independent IT assessment findings.
- RR1.4 Identify IT-related opportunities.

## **H. Manage Risk**

**Process Goal :** Ensure that measures for seizing strategic opportunities and reducing risk to an acceptable level are managed as a portfolio.

### **Key Activities:**

- RR2.1 Inventory controls.
- RR2.2 Monitor operational alignment with risk tolerance thresholds.
- RR2.3 Respond to discovered risk exposure and opportunity.
- RR2.4 Implement controls.
- RR2.5 Report IT risk action plan progress

## **React To Events**

**Process Goal :**Ensure that measures for seizing immediate opportunities or limiting the magnitude of loss from IT-related events are activated in a timely manner and are effective.

**Key Activities:**

- RR3.1 Maintain incident response plans.
- RR3.2 Monitor IT risk.
- RR3.3 Initiate incident response.
- RR3.4 Communicate lessons learned from risk events

**4.12 Analytic Hierarchy Process (AHP)**

The Analytic Hierarchy Process (AHP) is a multi-criteria decision-making approach and was introduced by Saaty. AHP organizes the basic rationality by breaking down a problem into its smaller constituent parts. By decomposing the problem, the decision-maker can focus on a limited number of items at the same time. The AHP is carried out in two phases: the design of the hierarchy and the evaluation of the components in the hierarchy. AHP is a multi-criteria decision making process that is especially suitable for complex decisions which involve the comparison of decision elements which are difficult to quantify. It is based on the assumption that when faced with a complex decision the natural human reaction is to cluster the decision elements according to their common characteristics. It is a technique for decision making where there are a limited number of choices, but where each has a number of different attributes, some or all of which may be difficult to formalize. It is especially applicable when a team is making decisions. It involves building a hierarchy (Ranking) of decision elements and then making comparisons between each possible pair in each cluster (as a matrix). This gives a weighting for each element within a cluster (or level of the hierarchy) and a consistency ratio (useful for checking the consistency of the data).

Table 4.2(Randomly Generated Consistency Index for different size of matrix)

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	9	1.12	1.24	1.32	1.4	1.45	1.49

Randomly Generated Consistency Index for different size of matrix. The acceptable CR range varies according to the size of matrix i.e. 0.05 for a 3 by 3 matrix, 0.08 for a 4 by 4 matrix and 0.1 for all larger matrix,  $n \geq 5$ . If the value of CR is equal to, or less than that value, it implies that the evaluation within the matrix is acceptable or indicates a good level of consistency in the comparative judgments represented in that matrix. In contrast, if CR is more than the acceptable value, inconsistency of judgments within that matrix has occurred and the evaluation process should therefore be reviewed, reconsidered and improved. An acceptable consistency ratio helps to ensure decision-maker reliability in determining the priorities of a set of criteria. The AHP process can be described in the following phase.

**Phase 1.** Structuring the hierarchy model of factors

This phase involve formulating the hierarchy of AHP model consisting of goal ,factors & sub factors, the goal of our problem is risk management/optimization and various factors as Risk Governance , Risk Evaluation and Risk Response and those are further divided into several sub factors as key activities.

**Phase2.** Collecting the data through expert interview.

After building the AHP model the next step is measuring and collecting the data, which involves the group of expert and assigning pair wise comparison to the various risks, using the table of five point scale (this scale is called the Saaty Scale), a questionnaire set is

prepared that consists of all the process and key activities. The expert will assign a score to each risk compare to other risk from the range of 1 to 9.

Table 4.3: AHP Scale for Comparison

Intensity of Importance	Definition	Explanation
1	Equal importance	Two factors contribute equally to the objective.
3	Somewhat more important	Experience and judgment slightly favor one over the other.
5	Much more important	Experience and judgment strongly favor one over the other.
7	Very much more important	Experience and judgment very strongly favor one over the other. Its importance is demonstrated in practice.
9	Absolutely more important	The evidence favoring one over the other is of the highest possible validity.

AHP is used for prioritization of activities as it has the ability to capture both quantitative and qualitative decision criteria. The AHP allows decision maker to model a complex problem as a hierarchical structure that shows the relationship between the goal, primary criteria, sub-criteria and alternatives. It is used for multi-criteria problems in a number of application domains. The step by step algorithm used is shown below.

Step 1: The pair-wise comparisons among the key activities are developed on the basis of expert judgments. A scale of 1 to 9 as shown below Table 2 is used for pair-wise comparisons. The pair-wise comparisons are done in terms of which a key activities dominates another. These judgments are then expressed as integers. If key activity A dominates over key activity B, then the whole number integer is entered in row A, column B and reciprocal is entered in row B, column A. If the key factor is being compared are equal, a one is assigned to both positions.

Step 2: Construct several set of pair-wise comparison matrixes for key activities on the basis of the opinions of all pre decided number of experts.

Step 3: There are several methods for calculating the eigenvector. By making each column of matrix normalized by dividing each value of column by sum of column, this would normalize the values.

Step 4: The next stage is to calculate  $\lambda_{max}$  (max Eigen Value), multiply on the right the matrix of judgments by the eigenvector, obtaining a new vector. The product  $Ax$  and the AHP theory says that  $Ax = \lambda_{max}X$  (For such a  $AX$  Square matrix,  $X$  is said to be an eigenvector (of order  $n$ ) and  $\lambda$  is an eigenvalue).

Step5: In Analytic Hierarchy Process (AHP) method Finally, a Consistency Index can be calculated using formula  $(\lambda_{max} - n)/(n - 1)$ . That needs to be assessed against judgments made completely at random and Saaty has calculated large samples of random matrixes of increasing order and the Consistency Indices of those matrixes. A true Consistency Ratio is calculated by dividing the Consistency Index for the set of judgments by the Index for the corresponding random matrix. Saaty suggests that if that ratio exceeds 0.1 the set of judgments may be inconsistent to be reliable. In practice, CRs of more than 0.1 sometimes

have to be accepted. If CR equals 0 then that means that the judgments are perfectly consistent.

**Phase 3.** Following the above phases we have to create comparison matrix for key activities under nine process goals. Nine comparison matrix will be built of forty three key activities under nine process goal area.

#### 4.13 Necessity of FAHP instead of AHP?

In the conventional AHP, the pair wise comparisons for each level with respect to the goal of the Best alternative selection are conducted using a nine-point scale. So, the application of Saaty's AHP has some shortcomings as follows(1) The AHP method is mainly used in nearly crisp decision applications, The AHP method creates and deals with a very unbalanced scale of judgment, The AHP method does not take into account the uncertainty associated with the mapping of one's judgment to a number, Ranking of the AHP method is rather imprecise, The subjective judgment, selection and preference of decision-makers have great influence on the AHP results. In addition, a decision-maker's requirements on evaluating alternatives always contain ambiguity and multiplicity of meaning. Furthermore, it is also recognized that human assessment on qualitative attributes is always subjective and thus imprecise. Therefore, conventional AHP seems inadequate to capture decision maker's requirements explicitly .In order to model this kind of uncertainty in human preference, fuzzy sets could be incorporated with the pairwise comparison as an extension of AHP. A variant of AHP, called Fuzzy AHP, comes into implementation in order to overcome the compensatory approach and the inability of the AHP in handling linguistic variables. The fuzzy AHP approach allows a more accurate description of the decision making process [23].

#### 4.14 Fuzzy Sets and its arithmetic operations

Fuzzy set theory was introduced by zedah [24] to deal with uncertainty and fuzziness information. The application of fuzzy set theory has been established to solve many real world problems. The definition of fuzzy set theory is Let  $X$  be universe of discourse,  $\tilde{A}$  is a fuzzy subset of  $X$  such that for all  $x \in X, \mu_{\tilde{A}}(x) \in [0,1]$  which is assigned to stand for the membership of  $x$  to  $\tilde{A}$ , and  $\mu_{\tilde{A}}(x)$  is Called the membership function of set  $\tilde{A}$

Informally, fuzzy sets are the concept of a continuum of grades of membership ranging between zero and one. If the assigned value is zero, the element does not belong to the set and if the value assigned is one, then the element belongs completely to the set. Lastly, the value which lies between 0 and 1 belongs to the fuzzy set only partially. The commonly used fuzzy numbers are triangular fuzzy numbers and trapezoidal fuzzy numbers. The triangular fuzzy numbers is the generalized form of trapezoidal fuzzy numbers if the two most promising values of the trapezoidal fuzzy number are same. In addition, triangular fuzzy numbers have been used in many applications as its intuitive appeal and computational efficiency. Triangular fuzzy numbers are applied to deal with the fuzziness and vagueness that exist in the decision problem. A triangular fuzzy number of  $\tilde{M}$  is represented as  $\tilde{M} = (l, m, u)$  and its membership function is described as in (1).

$$\mu_{\tilde{M}}(x) = \begin{cases} 0 & x < l \\ \frac{x-l}{m-l} & l \leq x < m \\ \frac{u-x}{u-m} & m \leq x < u \\ 0 & x \geq u \end{cases} \quad (4.1)$$

The parameters  $l, m, u$ , indicate the smallest possible value, the most promising value, and the largest possible value that describe a fuzzy amount respectively

#### 4.15 Assessment Model

In the following, the outlines of the Chang's extent analysis method [25] on Fuzzy AHP are given:

Let,  $U = \{u_1, u_2, \dots, u_m\}$  be a goal set and  $X = \{x_1, x_2, \dots, x_n\}$  be the object set. Each object is taken and extent analysis for every goal is performed, respectively. Therefore,  $m$  extent analysis values for each goal can be obtained, with the following signs

$$\widetilde{M}_{g_i}^1, \widetilde{M}_{g_i}^2, \dots, \dots, \widetilde{M}_{g_i}^m, i=1,2,3,\dots,n \quad (4.2)$$

Where all the  $\widetilde{M}_{g_i}^j$  ( $j=1,2,\dots,m$ ) are triangular fuzzy numbers  $g_i$  (TFNs) and  $g_i$  is the corresponding goal. The value of fuzzy synthetic extent with respect to the  $i^{th}$  object is defined as

$$S_i = \sum_{j=1}^m \widetilde{M}_{g_i}^j \otimes \left[ \sum_{i=1}^n \sum_{j=1}^m \widetilde{M}_{g_i}^j \right]^{-1} \quad (4.3)$$

To obtain  $\sum_{j=1}^m \widetilde{M}_{g_i}^j$ , the fuzzy addition operation of  $m$  extent analysis values is performed such as

$$\sum_{j=1}^m \widetilde{M}_{g_i}^j = \left( \sum_{j=1}^m l_j, \sum_{j=1}^m m_j, \sum_{j=1}^m u_j \right) \quad (4.4)$$

In order to obtain  $\sum_{i=1}^n \sum_{j=1}^m \widetilde{M}_{g_i}^j$ , the fuzzy addition operation of  $\widetilde{M}_{g_i}^j$  ( $j = 1, 2, \dots, m$ ) values is carried out as below:

$$\sum_{i=1}^n \sum_{j=1}^m \widetilde{M}_{g_i}^j = \left( \sum_{i=1}^n l_i, \sum_{i=1}^n m_i, \sum_{i=1}^n u_i \right) \quad (4.5)$$

And then the inverse of the vector in (4.5) is computed such that

$$\left[ \sum_{i=1}^n \sum_{j=1}^m \widetilde{M}_{g_i}^j \right]^{-1} = \left( \frac{1}{\sum_{i=1}^n u_i}, \frac{1}{\sum_{i=1}^n m_i}, \frac{1}{\sum_{i=1}^n l_i} \right) \quad (4.6)$$

The degree of possibility of  $\widetilde{M}_2 = (l_2, m_2, u_2) \geq \widetilde{M}_1 = (l_1, m_1, u_1)$  is defined as

$$V(\widetilde{M}_2 \geq \widetilde{M}_1) = \begin{cases} 1 & \text{if } m_2 \geq m_1 \\ 0 & \text{if } l_1 \geq u_2 \\ \frac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)} & \text{otherwise} \end{cases} \quad (4.7)$$

And it can be expressed as follows:

$$V(\widetilde{M}_2 \geq \widetilde{M}_1) = \begin{cases} 1 & \text{if } m_2 \geq m_1 \\ 0 & \text{if } l_1 \geq u_2 \\ \frac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)} & \text{otherwise} \end{cases} \quad (4.8)$$

The degree of possibility for a convex fuzzy number to be greater than  $k$  convex fuzzy numbers

$\widetilde{M}_i(i=1,2,\dots,k)$  can be defined by

$$V(\widetilde{M} \geq \widetilde{M}_1, \widetilde{M}_2, \dots, \widetilde{M}_k) = \min V(\widetilde{M} \geq \widetilde{M}_i) \quad (4.9)$$

Assume that

$$d'(A_i) = \min V(S_i \geq S_k) \quad (11)$$

For  $k=1,2,\dots,n \wedge k \neq i$ , then the weight vector is given by

$$W'(A_i) = (d'(A_1), d'(A_2), \dots, d'(A_n))^T \quad (4.10)$$

where  $A_i(i=1,2,\dots,n)$  are  $n$  elements.

Via normalization, the normalized weight vectors are

$$W = (d(A_1), d(A_2), \dots, d(A_n))^T \quad (4.11)$$

#### 4.16 Consistency Index

The following formula [26] are implemented to check for consistency of all pairwise comparison matrixes in this Fuzzy AHP.

$$\text{Lamda max} = N + \det \begin{bmatrix} m_{11} & m_{12} & m_{1n} \\ m_{21} & m_{22} & m_{2n} \\ m_{41} & m_{42} & m_{4n} \end{bmatrix}$$

$$\text{Consistency Index: CI} = \frac{\text{Lamda max} - N}{N-1}$$

$$\text{Consistency Ratio CR} = \text{CI/RI}$$

#### 4.17 The Proposed Fuzzy AHP

The proposed Fuzzy AHP model to assess the key activities is composed in a systematic flow of framework which follow following steps

Step 1. Construct a hierarchical structure of the problem

Developing a hierarchical structure is the most crucial step in AHP approach in which can provide a clear representation of the whole problem. The hierarchical structure consists of main goal, factors, sub-factors and alternatives.

Step 2. Select the decision makers

A group of decision makers is formed which consist of the experts from the related field. In order to obtain a reliable result, it is important to consider the decision makers' background. The decision makers must be someone who has experience with the research



topic as each of them needs to give judgment in the evaluation process. The relative weights of factors and sub-factors are then obtained from the decision makers' judgments.

### Step 3. Decide the suitable linguistic variables

Linguistic variables are applied to describe the relative importance of factors and sub-factors. In addition, they are able to express words or sentences of human language. The evaluation process is done through questionnaires which are in the form of linguistic variables. In order to proceed with mathematical operations, linguistic variables should be converted into fuzzy scales. In AHP approach, the nine-point ratio scale is used to perform pair-wise comparison while in this study, triangular fuzzy numbers are used to represent fuzzy pair-wise comparisons.

### Step 4. Create comparison matrixes

Pair-wise comparison matrixes are constructed to transform the linguistics variables into triangular fuzzy numbers

### Step 5. Check for consistency

Consistency needs to be measured to assure that the decision makers' judgments are reliable and also to avoid any misleading solutions.

### Step 6. Compute the factors and sub-factors priority weights

The weights of factors and sub-factors can be obtained by performing the extend analysis Fuzzy AHP method from the group fuzzy pairwise comparison matrixes

## CHAPTER 5 : RESULT AND FINDINGS

To develop and manage a IT risk Framework for Bank a focused group discussion was made to carry out pairwise comparison of the the process and key activities of the all the process. Four IT managers from different unit of IT division of National Bank Ltd who participated in this discussion. Total Nineteen matrix's were compared based on the Nine control of three domain and Key activities of those nine control. Here author focused to identify which key activity has most priority than other in context of the Bank. Analytical hierarchical process and Fuzzy AHP was used based on the fundamental scale developed by T. L .Satty. Here we will focus on detail construction of AHP and Fuzzy AHP process on forty three key activities to prioritize them.

### 5.1 Weight Calculation by AHP Process

#### 5.1.1 Pairwise Comparison

Pairwise comparison was carried out for all the components and the components were coded for simplicity and clarity. Manage Risk as MR, Articulate risk as ARTR, React to event as RE, Analysis risk as AR, Maintain risk profile as MRP, collect data as CD, Integrate with ER IWER, Establish and maintain a common risk view CRV and make risk aware business decision RABD. Consequently key activities under nine processes were marked sequentially RG 1.1 to RG 1.6, RG2.1 to RG 2.5, RG 3.1 to RG 3.5, etc.

During pairwise comparison each metrics formed a square matrixes of the order of nxn for  $A=[a_{ij}]$  where  $a_{ij}$  represents the comparison between two factors I and j and n= number of items compared . During pairwise comparison it was taken care to ensure that formed matrix satisfy three conditions

Reciprocity: For  $a_{ij}=x$  then  $a_{ji}=1/x$

Homogeneity: when two factors are judged to be equally important then  $a_{ij}=a_{ji}=1$  and  $a_{ii}=1$  for all i.

Consistency:  $a_{ik} * a_{kj} = a_{ij}$  is satisfied

The pairwise comparison exercise started by comparing the constructs in a 9 x 9 pairwise matrix of the risk IT process. Subsequently, the pairwise comparison of the key activities in their respective categories was carried out.

#### 5.1.2 Consistency Ratio Checking:

By making each column of matrix normalized by dividing each value of column by sum of column, this would normalize the matrixs. Thereafter Row wise sum has to be done on the matrixs and Sum of The Row has to be divided by no of Matrixs ( Here it would be 9) and result is called eigenvector or priority vector(X). The next stage is to calculate  $\lambda_{max}$  (max Eigen Value), AHP theory says that  $AX = \lambda_{max}X$  (For such a AX Square matrix, X is said to be an eigenvector (of order n) and  $\lambda$  is an eigenvalue). The consistency index and the consistence ratio were obtained from following formula.

Consistence index =  $CI = \frac{\lambda_{max} - N}{N - 1}$

The consistency ratio = CR = CI/RCI

Obtaining RCI value from table 4.2 we obtain value of CR, CI and  $\lambda_{max}$  which is 0.82, 1.2 and 18.67 accordingly. Detail calculation on Nine process goal is given in appendix and final result of the calculation is Table 4.3. Subsequently same calculation was carried over for other key activities matrixes which summarized result is given in Table 5.2.

Table 5.1 (Process goal prioritization)

	MR	ARTR	RE	AR	MRP	CD	IWER	CRV	RABD	Eigen Vector
MR	0.2690	0.7435	0.4923	0.3745	0.2651	0.1355	0.0682	0.0822	0.0227	0.2726
ARTR	0.0384	0.0929	0.3517	0.1498	0.2651	0.2371	0.2047	0.0822	0.0909	0.1681
RE	0.0384	0.0186	0.0703	0.2996	0.2209	0.2033	0.2388	0.0822	0.1818	0.1504
AR	0.0538	0.0465	0.0176	0.0749	0.1767	0.1016	0.0682	0.2192	0.1591	0.1020
MRP	0.0448	0.0155	0.0141	0.0187	1.0000	0.2710	0.2388	0.1370	0.1364	0.2085
CD	0.0672	0.0133	0.0117	0.0250	0.1250	0.0339	0.1365	0.1918	0.1818	0.0874
IWER	0.1345	0.0155	0.0100	0.0374	0.1429	0.2500	0.0341	0.1644	0.1591	0.1053
CRV	0.0897	0.0310	0.0234	0.0094	0.2000	0.0048	0.0057	0.0274	0.0455	0.0485
RABD	0.2690	0.2500	0.0088	0.0107	0.1667	0.0042	0.0049	0.0137	0.0227	0.0834

### 5.1.3 Key activities Prioritization

Depending on the eigen value obtained from eigen vector we prioritize the key activities accordingly. Table 5.1 shows the list of process goal and corresponding value of that process. Similarly the other key activities are listed in Table 5.2 along the weight or eigen value associated with the CI and CR value.

### 5.1.4 Key activities and Process Goal

In table 4 we see that all nine process along with highest and lowest value key activities were recorded though weight of the process will not be considered in this research only weight of all key activities will be considered and compared with further Fuzzy AHP calculation to obtain the lowest one. Though there are CR values more than 0.1 but we consider them for further analysis through fuzzy AHP

Table 5.2 ( Key activities and Process Goal)

Process	Highly ranked attribute	Eigenvector Value	Low Ranked attribute	Eigenvector Value	$\lambda_{max}$	CI	CR
Integrate with ERM	RG2.1	0.417	RG2.5	0.058	5.47	0.118	0.0941
Common Risk View	RG1.1	0.336	RG1.6	0.0595	5.39	0.0921	0.0866
Risk Aware Business Decision	RG3.1	0.397	RG3.5	0.0518	5.31	0.0981	0.0879
Analysis Risk	RE2.1	0.464	RE2.4	0.0513	4.15	0.0570	0.0513
Risk Profile	RE2.1	0.464	RE2.4	0.115	4.56	0.0981	0.0776
Collect Data	RE1.1	0.442	RE1.5	.0525	5.77	0.1934	0.172
Manage Risk	RR2.1	0.405	RR2.2	0.281	5.6	0.405	0.1342
Articulate risk	RR1.1	0.464	RR1.2	0.279	4.15	0.6513	0.057
React To Events	RR3.1	0.4567	RR3.2	0.324	4.385	0.1284	0.142

### 5.1.5 All key activities calculated by AHP process

In Table 5.2 weight of all key activities along with CI and CR value have been recorded where CR value has value greater than 0.1 but it is not too high so we are considering those three process goal for further analysis in Fuzzy AHP. From Table 5.2 we find that there are total nine key activities which have very less significant value considering the other key activities so if we omit those key activities from this framework then it should not have much effect on this framework. Each key activity has less than 5% to 8 % on the total value. Moreover if we analyze those activities in more details we find that RG1.5 (Promote IT risk Culture),RG1.6 (Encourage effective communication of IT risk),RG2.5(Provide independent assurance over IT risk Management),RR2.5(Report IT Risk action plan progress),RG3.5 (Prioritize IT Risk response activities),RE3.1(Map IT resources to business process,RR3.4 (Communicate lessons learn from risk events) have less impact.

Table 5.3 (Weight of Key Activities through AHP Process)

<b>Risk Governance</b>					<b>Risk Evaluation</b>					<b>Risk Response</b>				
<b>Establish and Maintain a Common Risk View</b>	Eigen Vector Values	CR	CI	$\lambda_{max}$	<b>Collect Data</b>	Eigen Vector Values	CR	CI	$\lambda_{max}$	<b>Articulate Risk</b>	Eigen Vector Values	CR	CI	$\lambda_{max}$
RG1.1	0.336	0.0866	0.0921	5.39	RE1.1	0.442	0.172	0.1934	5.77	RR1.1	0.464	0.0571	0.651	4.15
RG1.2	0.266				RE1.2	0.246				RR1.2	0.279			
RG1.3	0.139				RE1.3	0.153				RR1.3	0.139			
RG1.4	0.115				RE1.4	0.104				RR1.4	0.115			
RG1.5	0.083													
RG 1.6	0.0595													
<b>Integrate with ERM</b>					<b>Analysis Risk</b>					<b>Manage Risk</b>				
RG2.1	0.417	0.0941	0.118	5.47	RE2.1	0.464	0.05706	0.0513	4.15	RR2.1	0.405	0.1343	0.15	5.6
RG2.2	0.183				RE2.2	0.279				RR2.2	0.281			
RG2.3	0.206				RE2.3	0.139				RR2.3	0.138			
RG2.4	0.134				RE2.4	0.115				RR2.4	0.112			
RG2.5	0.058									RR2.5	0.062			
<b>Make Risk-aware Business Decisions</b>					<b>Maintain Risk Profile</b>					<b>React To Events</b>				
RG3.1	0.397	0.0876	0.0981	5.39	RE3.1	0.052	0.0776	0.0981	4.56	RR3.1	0.4567	0.142	0.128	4.385
RG3.2	0.296				RE3.2	0.916				RR3.2	0.324			
RG3.3	0.128				RE3.3	0.654				RR3.3	0.151			
RG3.4	0.125				RE3.4	0.032				RR3.4	0.067			
RG3.5	0.0518				RE3.5	0.852								
					RE3.6	0.784								

### 5.2 All key activities calculated by Fuzzy AHP process

In Table 6 all weight of all key activities along with CI and CR value have been recorded where CR value (of three process are where sixteen key activities are attached) have value greater than 0.1 among them CR value for RG 1.1 to RG 1.6 is too high so there is high inconsistency in data which we cannot avoid. Here it can be mentioned that this table is constructed upon further discussion with expert. From Table 6 we find that there are total eight key activities which have very less significant value considering the other so if we omit those key activities from this framework then it should not have much effect on this framework. Each key activity has less than 5% to 8 % on the total value. So doing the Fuzzy AHP process we find that all our finding in AHP process exists here and extra another key activity is added here for low impact which is RE 3.5 (Maintain IT Risk register and IT Risk Map).

Table 5.4 (Weight of Key Activities through Fuzzy AHP Process)

<b>Risk Governance</b>					<b>Risk Evaluation</b>					<b>Risk Response</b>				
<b>Establish and Maintain a Common Risk View</b>					<b>Collect Data</b>					<b>Articulate Risk</b>				
weights	CR	CI	$\lambda_{max}$		weights	CR	CI	$\lambda_{max}$		weights	CR	CI	$\lambda_{max}$	
RG1.1	0.2319	3.06	3.8	25	RE1.1	0.3136	0.33	0.375	6.5	RR1.1	0.441	0.047	0.042	4.12
RG1.2	0.2525				RE1.2	0.2945				RR1.2	0.29			
RG1.3	0.2293				RE1.3	0.171				RR1.3	0.1598			
RG1.4	0.1713				RE1.4	0.1449				RR1.4	0.10141			
RG1.5	0.0809													
RG1.6	0.034													
<b>Integrate with ERM</b>					<b>Analysis Risk</b>					<b>Manage Risk</b>				
RG2.1	0.3545	0.027	0.031	5.124	RE2.1	0.35	0.047	0.0427	4.128	RR2.1	0.3362	0.814	0.911	8.645
RG2.2	0.2422				RE2.2	0.3				RR2.2	0.2392			
RG2.3	0.2127				RE2.3	0.2				RR2.3	0.2069			
RG2.4	0.1438				RE2.4	0.13				RR2.4	0.1573			
RG2.5	0.0469									RR2.5	0.0603			
<b>Make Risk-aware Business Decisions</b>					<b>Maintain Risk Profile</b>					<b>React To Events</b>				
RG3.1	0.3104	0.133	0.14	5.59	RE3.1	0.2474	0.837	1.038	5.19	RR3.1	0.372	0.38	0.35	5.05
RG3.2	0.2651				RE3.2	0.2371				RR3.2	0.3846			
RG3.3	0.2069				RE3.3	0.2293				RR3.3	0.1768			
RG3.4	0.1573				RE3.4	0.1713				RR3.4	0.0664			
RG3.5	0.0603				RE3.5	0.0809								
					RE3.6	0.034								

## 5.2.1 Comparison of weight of key activities calculated by AHP and Fuzzy AHP

After calculating the key activities by AHP and fuzzy AHP process, weight and ranking of each activity are given in below table

Table 5.5 (Comparison of fuzzy AHP and AHP process)

Risk Governance					Risk Evaluation					Risk Response				
<b>Establish and Maintain a Common Risk View</b>					<b>Collect Data</b>					<b>Articulate Risk</b>				
AHP weight	Rank	Fuzzy weight	Rank		AHP weight	Rank	Fuzzy weight	Rank		AHP weight	Rank	Fuzzy weight	Rank	
RG1.1	0.336	1	0.2319	1	RE1.1	0.442	1	0.3136	1	RR1.1	0.464	1	0.44	1
RG1.2	0.266	2	0.2525	2	RE1.2	0.246	2	0.2945	2	RR1.2	0.279	2	0.29	2
RG1.3	0.139	3	0.2293	3	RE1.3	0.153	3	0.171	3	RR1.3	0.139	3	0.16	3
RG1.4	0.115	4	0.1713	4	RE1.4	0.104	4	0.1449	4	RR1.4	0.115	4	0.1	4
RG1.5	0.083	5	0.0809	5										
RG 1.6	0.059	5	0.034	6										
<b>Integrate with ERM</b>					<b>Analysis Risk</b>					<b>Manage Risk</b>				
RG2.1	0.417	1	0.3545	1	RE2.1	0.464	1	0.35	1	RR2.1	0.405	1	0.34	1
RG2.2	0.183	3	0.2422	2	RE2.2	0.279	2	0.3	2	RR2.2	0.281	2	0.24	2
RG2.3	0.206	2	0.2127	3	RE2.3	0.139	3	0.2	3	RR2.3	0.138	3	0.21	3
RG2.4	0.134	4	0.1438	4	RE2.4	0.115	4	0.13	4	RR2.4	0.112	4	0.16	4
RG2.5	0.058	5	0.0469	5						RR2.5	0.062	5	0.06	5
<b>Make Risk-aware Business Decisions</b>					<b>Maintain Risk Profile</b>					<b>React To Events</b>				
RG3.1	0.397	1	0.3104	1	RE3.1	0.052	5	0.2474	1	RR3.1	0.4567	1	0.37	1
RG3.2	0.296	2	0.2651	2	RE3.2	0.916	1	0.2371	2	RR3.2	0.324	2	0.38	2
RG3.3	0.128	3	0.2069	3	RE3.3	0.654	4	0.2293	3	RR3.3	0.151	3	0.18	3
RG3.4	0.125	4	0.1573	4	RE3.4	0.032	6	0.1713	4	RR3.4	0.067	4	0.07	4
RG3.5	0.051	8	0.0603	5	RE3.5	0.852	2	0.0809	5					
					RE3.6	0.784	3	0.034	6					

### 5.2.2 Outcome of the comparison between AHP and Fuzzy AHP

If we look into the comparison table then we will find that there are Seven Key activities which weight are lowest among other in AHP process and same six key activities are also ranked lowest in Fuzzy AHP process. One extra key activity was identified by both AHP and Fuzzy AHP which has also lowest weight. So author is considering these set of lowest ranked/weighted data for excluding from main set. For the sake of further research and giving emphasis on risk response author decided not to exclude an activity which is RR 3.4.

Table 5.6 (Weight Comparison between AHP and Fuzzy AHP)

Low Ranked /weight by AHP	Low Ranked /weight by Fuzzy AHP
RG1.5 (Promote IT risk Culture)	RG1.5 (Promote IT risk Culture)
RG 1.6 ( Encourage effective communication of IT risk)	RG 1.6 ( Encourage effective communication of IT risk)
RG2.5 ( Provide independent assurance over IT risk Management)	RG2.5 ( Provide independent assurance over IT risk Management)
RR2.5 (Report IT Risk action plan progress)	RR2.5 (Report IT Risk action plan progress)
RG3.5 (Prioritise IT Risk response activities)	RG3.5 (Prioritise IT Risk response activities)
RR3.4 ( Communicate lessons learn from risk events)	RR3.4 (Communicate lessons learn from risk events)
RE3.4	RE3.6(Maintain IT risk register and Risk map)

### 5.2.3 Proposed Framework

After analyzing different framework, standard and procedure and therefore performing AHP, Fuzzy AHP total thirty six activities have been selected. Modified and optimized diagram of the Risk IT framework is presented below



# Risk Management Framework

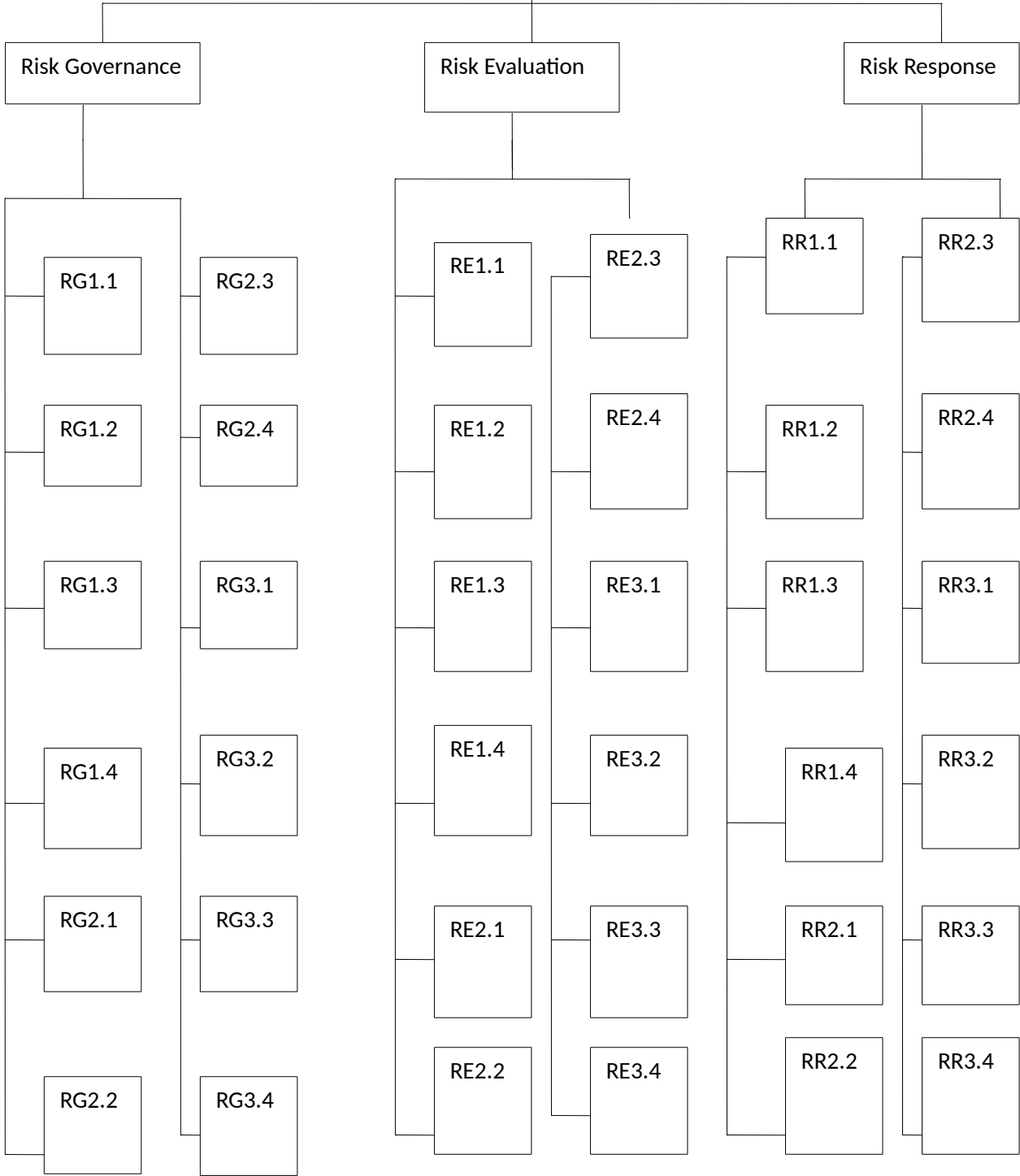




Figure-1

## CHAPTER 6: DISCUSSION

The key concept that was guiding the research for this project was to build a IT risk management framework for a commercial Bank comparing among all the existing framework. By keeping in mind of that research aimed to find a feasible way by using AHP, Fuzzy AHP and coefficient correlation to build a customized framework for a commercial bank.

### 6.1 Discussion

During research it was found that lot of research has been done by the help of AHP and Fuzzy ahp at different like project management, construction, mining, supply chain as well as Information security management system but none of ahp and fuzzy ahp was used for selecting a IT risk management framework. In that sense it can be treated as unique research. Moreover during my interview or discussion session it was clear that they were not aware of all process goal and key activities of Risk management framework. As we know that all banks are heavily dependent on Information technology for rendering all kind of their customer service. So any kind of threat or vulnerability to IT platform is also a threat to the business which directly or indirectly hampers the revenue of the bank. To handle such kind of risk all bank should follow the risk management framework. BIBM may play a significant role in this regard. They may arrange a round table discussion where participant will be higher management of different bank including Information Technology personal to have open discussion on the subject. Then it may be possible to select or develop a standard framework as guideline for all bank and others bank may follow the guideline depending on their strategic goal and mission of the bank.

## **CHAPTER 7 : CONCLUSION**

### **7.1 Conclusion**

Information Technology risk has become a top priority issue in the banking sector for the last few years and there are lot of risk management standard or framework but author tried to customize the existing Risk IT framework depending on the feedback of industry expert. Author used analytical hierarchy process and Fuzzy analytical hierarchy process to select key activities of risk management depending on their weight and finally checked the coefficient correlation to describe their relationship among themselves.

### **7.2 Limitation and Recommendation for Further Research**

One of the limitations of this research study was about the consistency of the data as we have collected the data based on the comparison scale from the expert so sometimes consistency of data was not maintained despite our repeated effort to correct the data by the help of expert. Though that scale of inconsistency was lower or close to acceptable range so those data had been considered. For further research we may use group AHP process so result will be more accurate. Further research may be conducted on the relationship between size of institution, revenue and IT Risk framework using the path diagram.

## REFERENCES

- [1] B. S. Bakshi, "Risk IT Framework for IT Risk Management : A Case Study of National Stock Exchange of India Limited," vol. 1, no. January, 2012.
- [2] D. Shaun and K. Barrett, "Effects of Information Technology Risk Management and Institution Size on Financial Performance," 2016.
- [3] R. Debreceeny, "Research on IT Governance , Risk , and Value : Challenges and Opportunities," vol. 27, no. 1, pp. 129–135, 2013.
- [4] V. Svatá and M. Fleischmann, "IS / IT Risk Management In Banking Industry," pp. 42–60, 2009.
- [5] S. Haneef, M. A. Rana, and Y. Karim, "Impact of Risk Management on Non-Performing Loans and Profitability of Banking Sector of Pakistan Hailey College of Commerce University of the Punjab Hafiz Muhammad Ishaq Federal Urdu University of Arts , Science and Technology," vol. 3, no. 7, pp. 307–315, 2012.
- [6] Bangladesh Bank, "Guideline on ICT Security For Scheduled Banks and Financial Institutions," *Govt. of Bangladesh*, 2015.
- [7] Y. Liu, L. Wang, and Z. Zhu, "Experimental and numerical studies on the effect of inlet pressure on cavitating flows in rotor pumps," *J. Eng. Res.*, vol. 4, no. 2, pp. 151–171, 2016.
- [8] R. Mehdizadeh, D. Breysse, and F. Taillandier, "Civil Engineering and Environmental Systems Dynamic and multi perspective risk management in construction with a special view to temporary structures," no. August 2013, pp. 37–41.
- [9] A. Herrmann, "The Quantitative Estimation of IT-Related Risk Probabilities," vol. 33, no. 8, pp. 1510–1531, 2013.
- [10] E. Kutsch, T. R. Browning, and M. Hall, "Bridging the Risk Gap : The Failure of Risk Management in Information Systems Projects Bridging the Risk Gap The Failure of Risk Management in Information Systems Projects," vol. 6308, no. January, 2016.
- [11] A. Ellul and V. Yerramilli, "Stronger Risk Controls , Lower Risk : Evidence from U . S . Bank Holding Companies," vol. LXVIII, no. 5, 2013.
- [12] M. S. Babu and M. C. Sekhar, "Enterprise Risk Management Integrated framework for Cloud Computing," vol. 1950, pp. 1939–1950, 2013.
- [13] I. Anikin, "Based on AHP and Fuzzy Sets," 2014.
- [14] M. Meng and E. Liu, "The Application Research of Information Security Risk Assessment Model Based on AHP Method," vol. 6, no. 4, pp. 201–206, 2015.
- [15] S. Aminbakhsh, M. Gunduz, and R. Sonmez, "Safety risk assessment using analytic hierarchy process ( AHP ) during planning and budgeting of construction projects," *J. Safety Res.*, vol. 46, pp. 99–105, 2013.
- [16] S. Sharma and R. Pratap, "A Case Study of Risks Optimization Using AHP Method,"

- vol. 3, no. 10, pp. 1–6, 2013.
- [17] A. C. Shukla, “Virendra Rajput,” no. 2277, pp. 6–7, 2014.
- [18] C. Science, M. He, and X. An, “Information Security Risk Assessment Based on Analytic Hierarchy Process,” vol. 1, no. 3, pp. 656–664, 2016.
- [19] M. Askari, H. R. Shokrizadeh, and N. Ghane, “A Fuzzy AHP Model in Risk Ranking,” vol. 6, no. 14, pp. 194–203, 2014.
- [20] Mustafa Batuhan ayhan, “A Fuzzy AHP Approach for Supplier Selection Problem: A Case Study in a Germotor Company,” vol. 4, no. 3, pp. 11–23, 2013.
- [21] S. Verma and S. Chaudhri, “Integration of Fuzzy Reasoning approach ( FRA ) and Fuzzy Analytic Hierarchy Process ( FAHP ) for Risk Assessment in Mining Industry,” vol. 7, no. 5, pp. 1347–1367, 2014.
- [22] A. Ishizaka, “No Title,” vol. 9, no. 1991, pp. 1–22, 2014.
- [23] T. K. Biswas, S. M. Akash, and S. Saha, “A Fuzzy-AHP Method for Selection Best Apparel Item to Start-Up with New Garment Factory : A Case Study in Bangladesh,” vol. 7, no. 1, pp. 32–50, 2018.
- [24] D. M. A. A. H. Golam Kabir, “Comparative Analysis Of Ahp And Fuzzy AHP Models Formulticriteria Inventory Classification,” vol. 1, no. 1, pp. 1–16, 2011.
- [25] A. Awang, A. Termimi, A. Ghani, L. Abdullah, and M. F. Ahmad, “Fuzzy Analytic Hierarchy Process ( FAHP ) with Cosine Consistency Index for Coastal Erosion Problem : A Case Study of Setiu Wetlands,” vol. 7, no. 4, 2017.

## Appendix-A

### AHP Process

#### 1) Comparison Matrix:

	MR	ARTR	RE	AR	MRP	CD	IWER	CRV	RABD
MR	1	8	7	5	6	4	2	3	1
ARTR	1/8	1	5	2	6	7	6	3	4
RE	1/7	1/5	1	4	5	6	7	3	8
AR	1/5	1/2	1/4	1	4	3	2	8	7
MRP	1/6	1/6	1/5	¼	1	8	7	5	6
CD	¼	1/7	1/6	1/3	1/8	1	4	7	8
IWER	½	1/6	1/7	1/2	1/7	1/4	1	6	7
CRV	1/3	1/3	1/3	1/8	1/5	1/7	1/6	1	2
RABD	1	1/4	1/8	1/7	1/6	1/8	1/7	1/2	1
	3.71	10.75	14.21	13.35	22.63	29.51	29.30	36.5	44

#### 2) Normalized Matrix:

Step1: Colum wise Sum has to be done

	MR	ARTR	RE	AR	MRP	CD	IWER	CRV	RABD
MR	1	8	7	5	6	4	2	3	1
ARTR	1/8	1	5	2	6	7	6	3	4
RE	1/7	1/5	1	4	5	6	7	3	8
AR	1/5	1/2	1/4	1	4	3	2	8	7
MRP	1/6	1/6	1/5	¼	1	8	7	5	6
CD	¼	1/7	1/6	1/3	1/8	1	4	7	8
IWER	½	1/6	1/7	1/2	1/7	1/4	1	6	7
CRV	1/3	1/3	1/3	1/8	1/5	1/7	1/6	1	2
RABD	1	1/4	1/8	1/7	1/6	1/8	1/7	1/2	1
	3.71	10.75	14.21	13.35	22.63	29.51	29.30	36.5	44

Step2: Each Column has to be divided by the sum of the column

	MR	ARTR	RE	AR	MRP	CD	IWER	CRV	RABD
MR	0.268972	0.743527	0.492339	0.374498	0.265082	0.135511	0.068237	0.082192	0.022727
ARTR	0.038425	0.092941	0.35167	0.149799	0.265082	0.237145	0.204712	0.082192	0.090909
RE	0.038425	0.018588	0.070334	0.299599	0.220901	0.203267	0.23883	0.082192	0.181818
AR	0.053794	0.04647	0.017584	0.0749	0.176721	0.101633	0.068237	0.219178	0.159091
MRP	0.044829	0.01549	0.014067	0.018725	1	0.271022	0.23883	0.136986	0.136364
CD	0.067243	0.013277	0.011722	0.024967	0.125	0.033878	0.136474	0.191781	0.181818
IWER	0.134486	0.01549	0.010048	0.03745	0.142857	0.25	0.034119	0.164384	0.159091
CRV	0.089657	0.03098	0.023445	0.009362	0.2	0.00484	0.005686	0.027397	0.045455
RABD	0.268972	0.25	0.008792	0.0107	0.166667	0.004235	0.004874	0.013699	0.022727



### 3) Creation of Priority Vector(X)

Step1: Row wise sum has to be done on the matrixes

Step2 : Sum of The Row has to be divided by no of Matrixes ( Here it would be 9) and result is called eigenvector or priority vector

	MR	ARTR	RE	AR	MRP	CD	IWER	CRV	RABD	Sum of Row
MR	0.26897	0.74353	0.4923386	0.3745	0.265082	0.135511	0.068237	0.082192	0.022727	2.453085756
ARTR	0.03842	0.09294	0.3516704	0.1498	0.265082	0.237145	0.204712	0.082192	0.090909	1.512874178
RE	0.03842	0.01859	0.0703341	0.2996	0.220901	0.203267	0.23883	0.082192	0.181818	1.353954072
AR	0.05379	0.04647	0.0175835	0.0749	0.176721	0.101633	0.068237	0.219178	0.159091	0.917608878
MRP	0.04483	0.01549	0.0140668	0.0187	1	0.271022	0.23883	0.136986	0.136364	1.876313123
CD	0.06724	0.01328	0.0117223	0.025	0.125	0.033878	0.136474	0.191781	0.181818	0.786160432
IWER	0.13449	0.01549	0.0100477	0.0374	0.142857	0.25	0.034119	0.164384	0.159091	0.947924011
CRV	0.08966	0.03098	0.0234447	0.0094	0.2	0.00484	0.005686	0.027397	0.045455	0.436822768
RABD	0.26897	0.25	0.0087918	0.0107	0.166667	0.004235	0.004874	0.013699	0.022727	0.750665239

	Eigen Vector
MR	0.272565084
ARTR	0.168097131
RE	0.150439341
AR	0.101956542
MRP	0.208479236
CD	0.087351159
IWER	0.10532489
CRV	0.048535863
RABD	0.083407249

### 4) Consistency Check

For consistency check we follow the below formula

$$\text{Consistence Index}=\text{CI}=(\tilde{\lambda}_{\max}-N)/ N-1 \quad (1)$$

$$\text{Consistency ratio}=\text{CI}/\text{RI} \quad (2)$$

To find the consistence index we have to find the value of  $\tilde{\lambda}_{\max}$

$$\tilde{\lambda}_{\max}=AX/X \quad (3)$$

Where A is the criteria matrix and X is the priority Vector.

Now we will find the value of  $\tilde{\lambda}_{\max}$  by solving the equation 3

A =

	MR	ARTR	RE	AR	MRP	CD	IWER	CRV	RABD
MR	1	8	7	5	6	4	2	3	1
ARTR	0.125	1	5	2	6	7	6	3	4
RE	0.14286	0.2	1	4	5	6	7	3	8
AR	0.2	0.5	0.25	1	4	3	2	8	7
MRP	0.16667	0.1667	0.2	0.25	1	8	7	5	6
CD	0.25	0.1429	0.1667	0.333	0.125	1	4	7	8
IWER	0.5	0.1667	0.1429	0.5	0.1429	0.25	1	6	7
CRV	0.33333	0.3333	0.3333	0.125	0.2	0.143	0.167	1	2
RABD	1	0.25	0.125	0.143	0.1667	0.125	0.143	0.5	1

$$\lambda_{\max} = AX/X = 2.544/0.1362 = 18.67$$

Now we put the value of the  $\lambda_{\max}$  in equation 1 to find the CR value of equation 1

$$CI = (\lambda_{\max} - n) / (n - 1) = (18.67 - 9) / (9 - 1) = 1.2$$

$$CR = CI / RI = 1.2 / 1.45 = 0.82$$

## Appendix-B

### Fuzzy AHP Calculation

We have calculated total nine matrix in fuzzy method as described in the theoretical framework where we have followed some steps and calculation here we have taken Risk Evaluation controls. Which pair wise comparison matrix in fuzzy method is given below:

### 1) Comparison Matrix

	RE2.1	RE2.2	RE2.3	RE2.4
RE2.1	(1,1,1)	(1,2,3)	(3,4,5)	(2,3,4)
RE2.2	(1/3,1/2,1/1)	(1,1,1)	(2,3,4)	(1,2,3)
RE2.3	(1/5,1/4,1/3)	(1/4,1/3,1/2)	(1,1,1)	(1,2,3)
RE2.4	(1/4,1/3,1/2)	(1/3,1/2,1/1)	(1/3,1/2,1/1)	(1,1,1)

### 2) Consistency Check

$$\lambda_{max} = \frac{1}{N} \det \begin{bmatrix} m_{11} & m_{12} & m_{1n} \\ m_{21} & m_{22} & m_{2n} \\ m_{41} & m_{42} & m_{4n} \end{bmatrix}$$

$$\text{Consistency Index: } CI = \frac{\lambda_{max} - N}{N-1}$$

$$\text{Consistency Ratio } CR = CI/RI$$

From above matrix we find N=4, determinant of matrix  $\lambda_{max} = 4.12$

So value of CI and CR is 0.042 and 0.047 and clearly  $CR \leq 0.1$  so data is consistent

### 3) Finding the Weight

$$S_i = \sum_{j=0}^m \tilde{M}_{g_i}^j \otimes \left[ \sum_{i=1}^n \sum_{j=1}^m \tilde{M}_{g_i}^j \right]^{-1} \quad (1)$$

$$\sum_{j=1}^m \tilde{M}_{g_i}^j = \left( \sum_{j=1}^m l_j, \sum_{j=1}^m m_j, \sum_{j=1}^m u_j \right) \quad (2)$$

We get values by using formula 2

SER2.1 (7,10,13), SRE2.2( 4.33,6.5,9),SRE 2.3(2.45,3.58, 4.38), SRE2.4(1.91,2.33,3.5)

$$\sum_{i=1}^n \sum_{j=1}^m \tilde{M}_{g_i}^j = \left( \sum_{i=1}^n l_i, \sum_{i=1}^n m_i, \sum_{i=1}^n u_i \right) \quad (3)$$

From formula 3 we get the values (30.33,22.41,15.70)

$$\left[ \sum_{i=1}^n \sum_{j=1}^m \tilde{M}_{g_i}^j \right]^{-1} = \left( \frac{1}{\sum_{i=1}^n u_i}, \frac{1}{\sum_{i=1}^n m_i}, \frac{1}{\sum_{i=1}^n l_i} \right) \quad (4)$$

From formula 4 we get the values (0.032,0.044,0.063)

Now putting the value from formula 2 and formula 4 in formula 1 we get

$$\begin{aligned} \text{SRE2.1} (7,10,13) \times (0.032,0.044,0.063) &= (0.23,0.44,0.82) \\ \text{SRE2.2} (4.33,6.5,9) \times (0.032,0.044,0.063) &= (0.14,0.28,0.57) \\ \text{SRE2.3} (2.45,3.58, 4.38) \times (0.032,0.044,0.063) &= (0.08,0.15,0.30) \\ \text{SRE2.4} (1.91,2.33,3.5) \times (0.032,0.044,0.063) &= (0.063,0.10,0.22) \end{aligned}$$

Now the degree of possibility  $\widetilde{M}_2 = (l_2, m_2, u_2) \geq \widetilde{M}_1 = (l_1, m_1, u_1)$  is defined as

$$V(\widetilde{M}_2 \geq \widetilde{M}_1) = \int_{y \geq x} \min(\mu_{\widetilde{M}_1}(x), \mu_{\widetilde{M}_2}(y)) dx$$

And it can be expressed as

$$V(\widetilde{M}_2 \geq \widetilde{M}_1) = \begin{cases} 1 & \text{if } m_2 \geq m_1 \\ 0 & \text{if } l_1 \geq u_2 \\ \frac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)} & \text{otherwise} \end{cases} \quad (5)$$

Considering the formula (5) we may calculate the following

$$\begin{aligned} V(\text{SRE2.1} \geq \text{SRE2.2}) &= 1 \\ V(\text{SRE2.1} \geq \text{SRE2.3}) &= 1 \\ V(\text{SRE2.1} \geq \text{SRE2.4}) &= 1 \end{aligned}$$

$$\begin{aligned} V(\text{SRE2.3} \geq \text{SRE2.1}) &= 0.19 \\ V(\text{SRE2.3} \geq \text{SRE2.2}) &= 0.55 \\ V(\text{SRE2.3} \geq \text{SRE2.4}) &= 1 \end{aligned}$$

$$\begin{aligned} V(\text{SRE2.2} \geq \text{SRE2.1}) &= 0.68 \\ V(\text{SRE2.2} \geq \text{SRE2.3}) &= 1 \\ V(\text{SRE2.2} \geq \text{SRE2.4}) &= 1 \end{aligned}$$

$$\begin{aligned} V(\text{SRE2.4} \geq \text{SRE2.1}) &= 0 \\ V(\text{SRE2.4} \geq \text{SRE2.2}) &= 0.31 \\ V(\text{SRE2.4} \geq \text{SRE2.3}) &= 0.73 \end{aligned}$$

There for according the below formula which was described in theoritacal framework we may select the minimum value

$$V(\widetilde{M} \geq \widetilde{M}_1, \widetilde{M}_2, \dots, \widetilde{M}_k) = \min V(\widetilde{M} \geq \widetilde{M}_i)$$

$$\begin{aligned} \min V(\text{SRE2.1} \geq \text{SRE2.2, SRE2.3, SRE2.4, S2.1}) &= \min(1, 1, 1) \\ \min V(\text{SRE2.2} \geq \text{SRE2.2, SRE2.3, SRE2.4, S2.1}) &= \min(0.68, 1, 1) \\ \min V(\text{SRE2.3} \geq \text{SRE2.2, SRE2.1, SRE2.4, S2.3}) &= \min(0.19, 0.55, 1) \\ \min V(\text{SRE2.4} \geq \text{SRE2.2, SRE2.1, SRE2.4, S2.3}) &= \min(0, 0.31, 0.73) \end{aligned}$$

Therefore we obtain weight

$W = (1, 0.68, 0.55, 0)$  and the normalized weight are

$W = (0.35, 0.30, 0.20, 0.13)$  which is the ranking of the four criteria under Risk Evaluation process.

## Appendix C

Dear Colleague,

I am Abid Hossen, a student of Department of Industrial & Production Engineering of BUET, doing M. Engineering in Advanced Engineering Management (AEM) program. Along with Dr. Parven Sultana, Professor, BUET, I am doing research in Developing and Managing Information Technology Risk Management Framework of commercial Bank. On that note, Group discussion is needed and your feedback is also needed for the research purpose. I assure you that the information you provide will remain confidential and it will be used only for this research purpose. Here we will need to compare a set of questions depending on their necessity you have to provide some relative points on the corresponding matrices. All the questions will be discussed in details and you will provide relative importance of those criteria in scale of 1 to 9. After the details discussion your combined feedback will be noted in front of you so that we can avoid any miscommunication.

Thanks,  
Abid Hossen  
VP , IT Division  
National Bank Limited

## RISK GOVERNANCE

The purpose of Risk Governance is to identify IT risk governance initiatives adapted by your institution.

1. Perform enterprise IT risk assessment [RG1.1]
2. Propose IT risk tolerance threshold [RG1.2]
3. Approve IT risk tolerance threshold [RG1.3]
4. Align IT risk policy [RG1.4]
5. Promote IT risk aware culture [RG1.5]
6. Encourage effective communication of IT risk [RG1.6]

		C1	C2	C3	C4	C5	C6
		RG1.1	RG1.2	RG1.3	RG1.4	RG1.5	RG1.6
C1	RG1.1	1	3	2	3	2	4
C2	RG1.2	0.33	1	3	2	5	5
C3	RG1.3	0.5	0.33	1	4	3	6
C4	RG1.4	0.33	0.25	0.25	1	5	4
C5	RG1.5	0.5	0.33	0.33	0.2	1	3
C6	RG1.6	0.25	0.2	0.25	0.5	0.33	1

7. Establish and manage accountability for IT risk management [RG2.1]
8. Coordinate IT risk strategy and business risk strategy [RG2.2]
9. Adapt IT risk practices to enterprise risk practices [RG2.3]
10. Provide adequate resource for IT risk management [RG2.4]
11. Provide independent assurance over IT risk management [RG2.5]

		C1	C2	C3	C4	C5
		RG2.1	RG2.2	RG2.3	RG2.4	RG2.5
C1	RG2.1	1	4	2	3	5
C2	RG2.2	0.25	1	2	4	3
C3	RG2.3	0.50	0.5	1	2	5
C4	RG2.4	0.33	0.25	0.5	1	4
C5	RG2.5	0.2	0.33	0.2	0.25	1

12. Gain management buy-in for IT risk approach [RG3.1]
13. Approve IT risk analysis [RG3.2]

- 25. Map IT resource to business process [RE3.1]
- 26. Determine business critic ability of IT resources [RE3.2]
- 27. Understand IT capability [RE3.3]
- 28. Update IT risk scenario components [RE3.4]
- 29. Maintain IT risk register and IT risk map [RE3.5]
- 30. Develop IT risk indicators [RE3.6]

		RG1.1	RG1.2	RG1.3	RG1.4	RG1.5	RG1.6
	RG1.1	1	2	4	5	3	2
	RG1.2	0.5	1	4	2	5	4
	RG1.3	0.25	0.25	1	3	2	3
	RG1.4	0.2	0.5	0.33	1	4	2
	RG1.5	0.33	0.2	0.5	0.25	1	4
	RG1.6	0.5	0.25	0.33	0.5	0.25	1

**Risk Response**

- 31. Communicate IT risk analysis results [RR1.1]
- 32. Report IT risk management activities and state of compliance [RR1.2]
- 33. Interpret independent IT assessment findings [RR1.3]
- 34. Identify IT related opportunities [RR1.4]

		RR1.1	RR1.2	RR1.3	RR1.4
	RR1.1	1	2	4	3
	RR1.2	0.5	1	3	2
	RR1.3	0.25	0.33	1	2
	RR1.4	0.33	0.5	0.5	1

- 35. Inventory controls [RR2.1]
- 36. Monitor operational alignment with risk tolerance threshold [RR2.2]
- 37. Respond to discovered risk exposure and opportunity [RR2.3]
- 38. Implement controls [RR2.4]

39. Report IT risk action plan progress [RR2.5]

		RR2.1	RR2.2	RR2.3	RR2.4	RR2.5
	RR2.1	1	4	2	4	2
	RR2.2	0.25	1	2	3	3
	RR2.3	0.5	0.5	1	2	4
	RR2.4	0.25	0.33	0.5	1	4
	RR2.5	0.5	0.33	0.25	0.25	1

40. Maintain incidents response plan [RR3.1]

41. Monitor IT risk [RR3.2]


42. Initiate incident response [RR3.3]

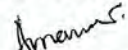
43. Communicate lessons learnt from incidents [RR3.4]


		RR3.1	RR3.2	RR3.3	RR3.4
	RR3.1	1	3	2	4
	RR3.2	0.33	1	4	5
	RR3.3	0.5	0.25	1	3
	RR3.4	0.25	0.2	0.33	1

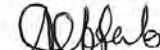
Matrices of Nine Process

	MR	ARTR	RE	AR	MRP	CD	IWER	CRV	RABD
MR	1	8	7	5	6	4	2	3	1
ARTR	1/8	1	5	2	6	7	6	3	4
RE	1/7	1/5	1	4	5	6	7	3	8
AR	1/5	1/2	1/4	1	4	3	2	8	7
MRP	1/6	1/6	1/5	1/4	1	8	7	5	6
CD	1/4	1/7	1/6	1/3	1/8	1	4	7	8
IWER	1/2	1/6	1/7	1/2	1/7	1/4	1	6	7
CRV	1/3	1/3	1/3	1/8	1/5	1/7	1/4	1	2
RABD	1	1/4	1/8	1/7	1/6	1/8	1/7	1/2	1

  
**Mohammad Sirajul Islam**  
 Senior Vice President

  
**Amanur Rahman**  
 SAVP

  
**Mahadi Hasan**  
 Vice President

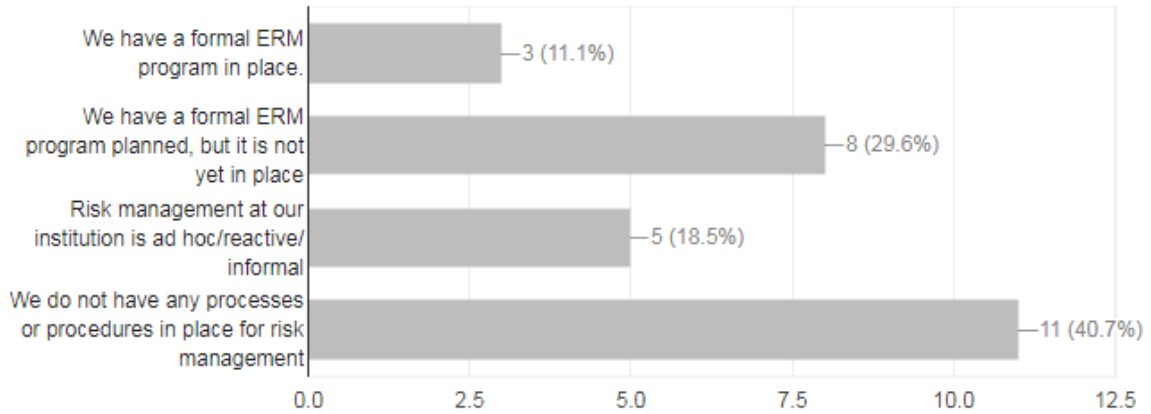
  
**Aftab Hossen**  
 SAVP



## Appendix D

### 1. To what extent does your institution have an enterprise risk management (ERM) program in place?

0 / 27 correct responses



### 16. Your opinion on Risk IT framework of ISACA

27 responses

