# A STUDY ON
# IMPACT OF INFORMATION TECHNOLOGY RISK AND RISK MANAGEMENT IN BANKS IN INDIA

*Thesis Submitted to*

*Cochin University of Science and Technology*

*For the award of the degree of*

*Doctor of Philosophy*

*Under the*

*Faculty of Social Sciences*


*By*

**Anil Kumar P.**

(Reg No 3096)

*Under the Guidance of*

**Dr. Jagathy Raj V. P.**

**School of Management Studies**

**Cochin University of Science and Technology**

Kochi - 682 022


December 2015

# A Study on Impact of Information Technology Risk and Risk Management in Banks in India

*Ph. D Thesis under the Faculty of Social Sciences*

*Author*

***Anil Kumar P.***
*School of Management Studies*
*Cochin University of Science and Technology*
*Cochin - 682 022, Kerala, India*
*email: anildfs@gmail.com*

*Supervising Guide*

***Dr. Jagathy Raj V.P.***
*Professor,*
*School of Management Studies*
*Cochin University of Science and Technology*
*Cochin - 682 022, Kerala, India*
*email: jagathyraj@gmail.com*

School of Management Studies
Cochin University of Science and Technology
Kochi - 682 022

*December 2015*

School of Management Studies
Cochin University of Science and Technology

*Dr. Jagathy Raj V.P.*
*Professor,*
*School of Management Studies*
*Cochin University of Science and Technology*
*Cochin - 682 022, Kerala, India*

*Ph: 9847220016*
*email: jagathyraj@gmail.com*

# Certificate

Certified that this thesis entitled "**A Study on Impact of Information Technology Risk and Risk Management in Banks in India"** submitted to the Cochin University of Science and Technology, Kochi for the award of the Degree of Doctor of Philosophy under the Faculty of Social Science, is the record of bona fide research carried out by **Mr. Anil Kumar P** under my supervision and guidance at School of Management Studies, CUSAT. This work did not form part of any dissertation submitted for the award of any degree, diploma, associate ship, fellowship or other similar title or recognition from this or any other institution. All the relevant corrections and modifications suggested by the audience during the pre-synopsis seminar and recommended by the Doctoral committee have been incorporated in the thesis.

Kochi,
03/12/2015

**Dr. Jagathy Raj V. P.**
(Supervising Guide)

# Declaration

I, **Anil Kumar P**, hereby declare that the work presented in the thesis "**A Study on Impact of Information Technology Risk and Risk Management in Banks in India"** being submitted to Cochin University of Science and Technology for award of Ph.D. degree under the Faculty of Social Science is the outcome of original work done by me under the supervision of **Dr. Jagathy Raj V. P.**, Professor, School of Management Studies, Cochin University of Science and Technology, Kochi. This work did not form part of any dissertation submitted for the award of any degree, diploma, associate ship, fellowship or other similar title or recognition from this or any other institution.

Kochi,
03/12/2015

**Anil Kumar P**

# Acknowledgement

*First of all, I would like to thank Almighty God, who has blessed and guided me during the course of this study for the successful completion of this thesis.*

*Apart from the efforts of self, the success of this thesis depends largely on the encouragement and guidelines of many others. I take this opportunity to express my gratitude to all those who have been instrumental in the successful completion of this thesis.*

*I take this opportunity to express my profound gratitude and deep regards to my research guide* ***Prof. Dr. Jagathy Raj V. P.****, School of Management Studies for his exemplary guidance, monitoring and constant encouragement throughout the course of this research work.*

*I also take this opportunity to express a deep sense of gratitude to* ***Dr. Moly P. Koshi,*** *Director, School of Management Studies and* ***Dr. James Manelel,*** *Member, Doctoral Committee for their cordial support, valuable information and guidance, which helped me in completing this task through various stages.*

*Furthermore, I would also like to acknowledge with much appreciation the crucial role of* ***Dr. Hareesh Ramanathan*** *for his useful comments, remarks and engagement throughout the learning phases of this thesis work.*

*Also, I express my deep sense of gratitude to the participants in my survey, who have willingly shared their precious time and information in responding to the research questionnaire.*

*I thank all my colleagues in School of Management Studies for their constant support and motivation during my study. I express a deep sense of gratitude to all the faculty members and office staff of School of Management studies for their guidance, support and information.*

*I would like to thank my loved ones, who have supported me throughout the process, both by keeping me harmonious and by helping me putting pieces together. I will be grateful forever for your love, constant encouragement, without which this thesis would not have been possible.*

*Last, but not the least, I would like to acknowledge the contribution of all others, who have played significant roles in helping me throughout my thesis work.*

***Anil Kumar P***

# Contents

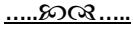
# List of Tables

# List of Figures

# List of Abbreviations

| | |
|---|---|
| IT | Information Technology |
| ITR | Information Technology Risk |
| ITRM | Information Technology Risk Management |
| FI | Financial Impacts |
| NFI | Non-Financial Impacts |
| SMS | Short Message Service |
| ANOVA | Analysis of Variance |
| GFI | Goodness Fit Index |
| AGFI | Adjusted Goodness Fit Index |
| CAGR | Cumulative Average Growth Rate |
| CFA | Confirmatory Factor Analysis |
| CFI | Comparative Fit Index |
| CMM | Capability Maturity Model |
| IRR | Interrater Reliability |
| IS | Information System |
| ISO | International Organization for Standardization |
| MIS | Management Information System |
| MTMM | Multi Trait Multi Method |
| RMSR | Root Mean Squared Residual |
| SPSS | Statistical Package for the Social Sciences |
| VIF | Variance Inflation Factor |
| RBI | Reserve Bank of India |
| ISO | International Standards Organization |
| IEC | International Electro Technical Commission |
| ISF | Information Security Forum |
| FI | Financial Institution |
| IS | Information System |
| COBIT | Control Objectives for Information and Related Technology |
| ORM | Operational Risk Management Framework |
| SEM | Structural Equation Modelling |

| | |
|---|---|
| NIST | National Institute of Standards and Technology |
| ISACA | Information Systems Audit and Control Association |
| CISA | Certified Information Systems Auditor |
| KYC | Know Your Customer |
| NIATEC | National Information Assurance Training and Education Center |
| LDAP | Lightweight Directory Access Protocol |
| BCP | Business Continuity Planning |
| CMMI | Capability Maturity Model Integration |
| CCTV | Closed-circuit television |
| VPN | Virtual Private Network |
| ITGI | IT Governance Institute |
| CIO | Chief Information Officer |
| STP | Straight Through Processing |
| SBI | State Bank of India |
| RMSEA | Root Mean Square Error of Approximation |
| ML | Maximum Likelihood |
| OLS | Ordinary Least Squares |
| NIST | National Institute of Standards and Technology |



# Chapter 1

# INTRODUCTION

Contents



## 1.1 Introduction to Information Technology Risks

Over the past twenty five years, as with any other industry, banks all over the world too have adopted to latest technologies for their day to day operations, customer services, interbank transactions, trading, housekeeping and also for regulatory reporting purposes. In today's banks, accounts and transactions are stored in electronic forms, most customer services are made online, payment transfers are done through electronic payment messaging, clearing is fully automated, statements are made downloadable any time, mobile access to account is enabled, instant SMS (Short Message Service)

alerts are provided to customer phones, and many more back office services are now using a straight through processing, without any manual intervention. Following this global technology enablement, scheduled commercial banks in India too achieved 100% computerization over the past few years for efficiency and excellence. The co-operative sector banks are now following the suite and are in the process of getting core banking systems implemented in their banks.

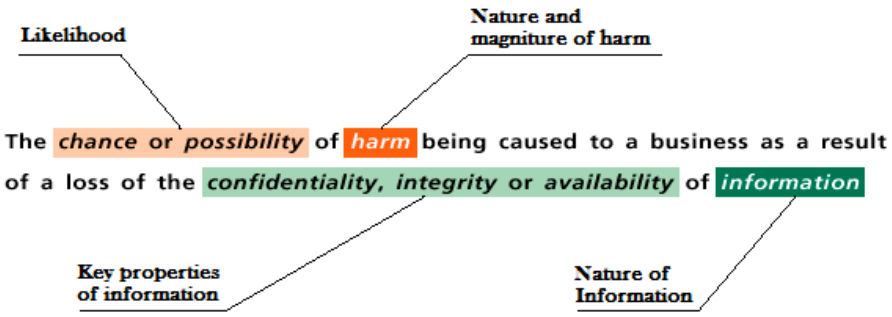
Commercial banks in India are broadly classified into scheduled and non-scheduled banks. The scheduled commercial banks in India include public sector banks, private sector banks and foreign banks. There are 26 nationalized banks including 6 in state bank group, 20 private sector banks and around 40 foreign banks operating in the country. Co-operative sector banks include state co-operative banks (31), regional rural banks (82) and other service co-operative banks (RBI List of Banks, 2013).

"*In today's Indian scenario, banking sectors are rapidly utilizing IT services for their operations. Automation of various processes no doubt has given lots of advantages to these banking and financial institutions, but has given rise to many risks as well*." (RBI, 2013). Increased reliance of customers on electronic banking channels and technologies can lead to customer dissatisfaction, loss of confidence, or even to account closure, if the banking services are disrupted for a while or the security is breached or the services did not meet the expectations. Such risks can also lead to reputational losses for the banks. On the other side, due to the extensive reliance of banks on technology, any inadequate implementation of technology can cause operational risks, reputational risks, compliance risks and business risks.

Moreover, in extreme cases, these issues can have a potential impact on safety and soundness of the banking system itself (systemic risk).

## 1.2 Information Technology Risks & its Impacts

A common definition for risk is "*the possibility of damage or loss, is described mostly in dependencies threat and vulnerability or impact and probability*" (Lheagwara, 2003). The long-standing (and still relevant) business requirement for information security is to maintain information's *confidentiality*, *integrity* and *availability* (ISO/IEC 17799, 2005). This is also an underlying requirement in the Information Security Forum's Standard of Good Practice (SOGP) (Information Security Forum, 2013), especially when risk and criticality standards are addressed. For example, many SOGP standards combine the word 'impact' with "loss of confidentiality, integrity, and availability." (SOGP sections referenced under 'Business Impact and Loss of' in the topic index). An excellent industry definition for information risk that combines the nature of risk (impact and probability) and the properties of information (confidentiality, integrity and availability) has been proposed by the Information Security Forum (ISF) and it is shown in Fig. 1.1 (Information Security Forum, 2007).




Source: The Standard of Good Practice, Information Security Forum, 20071

**Figure 1.1: Definition of IT Risk**

### 1.2.1 NIST SP 800-30 Definitions (NIST SP 800-30, 2002)

*Threat*: The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

*Threat-Source*: is either the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.

*Common Threat-Sources* - Natural Threats, Human Threats, Environmental Threats.

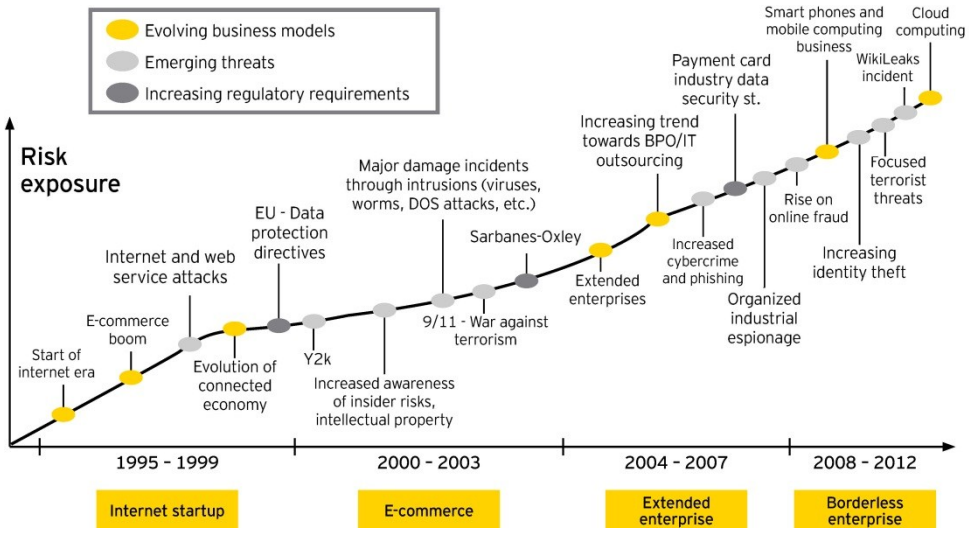
*Vulnerability*: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

*Technology risks are defined* as any potential adverse outcome, damage, loss, violation, failure or disruption arising from the use of or reliance on computer hardware, software, devices, systems, applications and networks. These risks are usually related to systems flaws, processing errors, software defects, operating mistakes, hardware breakdowns, systems failures, capacity inadequacies, network vulnerabilities, control weaknesses, security shortcomings, malicious attacks, hacking incidents, fraudulent actions and inadequate recovery capabilities (Monetary Authority of Singapore, 2002).

In the case of technology related risks, as the strategic importance of technology continues to increase for an organization, the type and number of risks too increases. Rapid deployments and deficiencies in controls too

add technology risks. In recent days, the way in which companies interact with their employees, customers and other organizations is changing drastically. Newer technologies like mobile computing, cloud computing, social media, etc are now breaking the old Information Technology risk paradigm and Information Technology risk is now considered as strategic business risk with an enterprise wide focus. According to *'The Ernst & Young Business Risk Report 2010'* (Ernst & Young, 2010), there is a strong relationship of Information Technology risks to business risks like financial risks, compliance risks, operations risks and strategic risks.

The risk exposure based on the change in business models, emerging threats and regulatory requirements are shown in Fig. 1.2. (Ernst & Young, 2011).




Source: Insights on IT Risks, Ernst & Young, 2011.

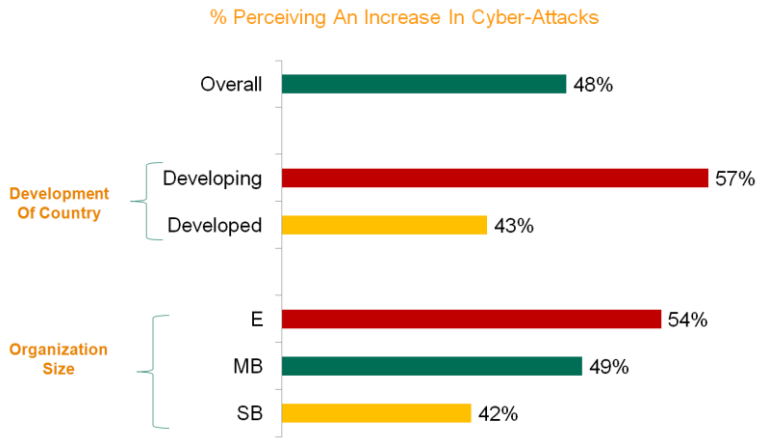
**Figure 1.2: Risk Exposure**

The Information Technology risk's 11 broad categories are shown as a Risk Universe in Fig. 1.3.


Source: Insights on IT Risks, Ernst & Young, 2011.

**Figure 1.3: The IT Risk Universe**

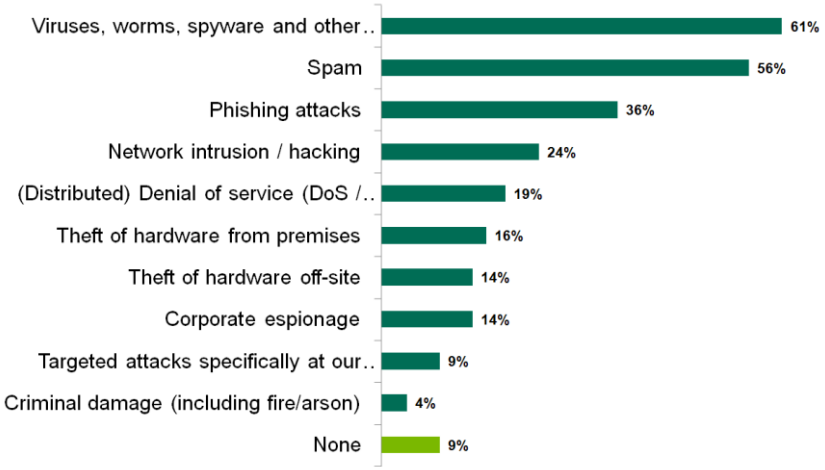
The *Global IT Security Risks* survey by *Kaspersky Lab* during June, 2011 (Kaspersky Lab, 2011) showed the following statistics on increase in cyber attacks, external threats and the consequent data losses.




Source: Global IT Security Risks Survey by Kaspersky Lab, June, 2011

**Figure 1.4: Cyber attacks based on development of country and organization size**

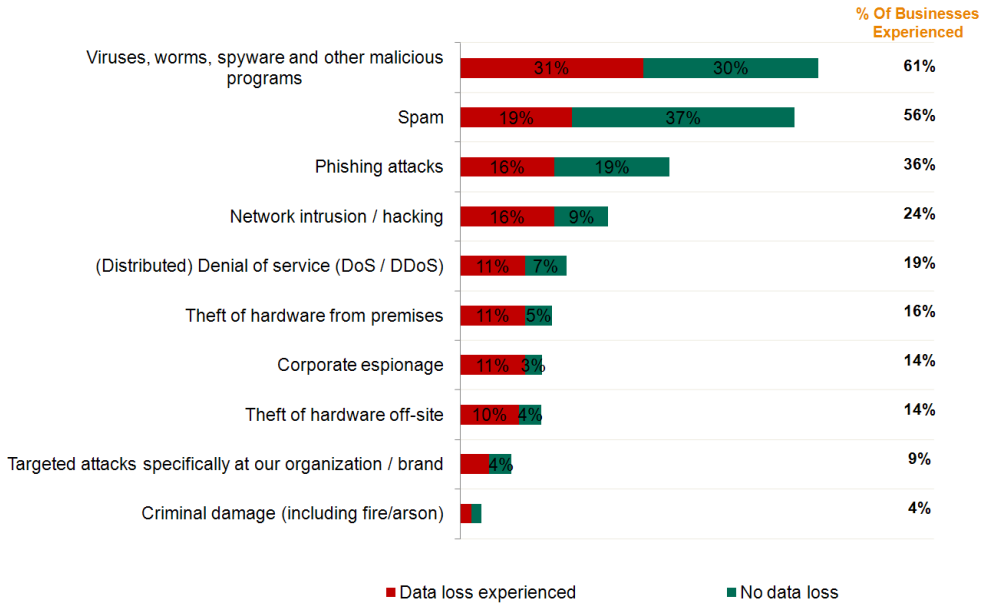
The Fig. 1.4 shows that, cyber attacks are more in developing countries compared to developed counties and it is also found that large enterprises are facing more attacks compared to small scale and medium scale enterprises.




Source: Global IT Security Risks Survey by Kaspersky Lab, June, 2011

**Figure 1.5: Types of external threats experienced**

Based on the Fig. 1.5, it is identified that the most common forms of the external threats are viruses and malware, followed by spams, phishing attacks, network intrusion and denial of service attacks. The percentage of data losses due to these attacks are also shown in Fig 1.6 below.




Source: Global IT Security Risks Survey by Kaspersky Lab, June, 2011

**Figure 1.6: Types of external threats experienced and data loss**

## 1.3 Information Technology Risks in Banking

The advancement of Information Technology has brought about rapid changes to the way businesses and operations are being conducted in the financial industry. IT is no longer a support function within a Financial Institution (FI) but a key enabler for business strategies including reaching out to and meeting customer needs (Monetary Authority of Singapore, 2013). Financial systems and networks supporting FI's business operations

have also grown in scope and complexity over the years. FIs offering a diversity of products and services could have their financial systems operating in multiple locations and supported by different service providers. Information Technology outsourcing has also become more attractive to FIs due to the abundance of outsourcing services. Against the backdrop of an increased reliance on complex IT systems and operations in the financial sector is the heightened risk of cyber attacks and system disruptions. In this regard, FIs are expected to continue to deepen their technology risk management capabilities and be ready to handle IT security incidents and system failures.

The growing dependence of banking organizations on Information Technology emphasizes one aspect of the need to identify and control this technology related risks. In banking organizations, based on Basel guidelines, Information Technology related risks are treated under operational risks. Operational risk arises from the potential that inadequate information systems, operational problems, breaches in internal controls, fraud, or unforeseen catastrophes will result in unexpected losses (Federal Reserve, 1995) Although, operational risk does not easily lend itself to quantitative measurement, it can result in substantial costs through error, fraud, or other performance problems.

Inadequate IT controls could result in cyber frauds and poor implementation of technology could lead to unsound decision making based on inaccurate information/data. The cyber threat landscape is also changing over the years and needs to be factored in while considering mitigating measures. (RBI, 2011)

## 1.4 The Impact of IT Risk in Banking

The impact of Information Technology risks in banking are financial (additional costs and/or reduction in earnings), operational (security, availability and integrity), business (reputational/strategic) and compliance (actions from central bank, reduced ratings, etc.) (Rechards, 2001).

Take an example of the IT risk: *Hacking*. The main cause of the risk is lack of or weakness in internal controls. This definitely has a direct effect on customer confidence and can cause financial losses. The related IT/operational risk is loss of integrity, the business risk is loss of reputation, and the regulatory impact could be legal actions from the regulatory authorities or reduced ratings.

NIST document SP800-30 (NIST SP 800-30, 2002) also considers Loss of integrity, Loss of Availability and Loss of Confidentiality as primary impacts of IT Risks.

## 1.5 Information Technology Risk Management

Banks' confidence in their ability to manage risk, especially technology and operations risk, is shaky at best (Deloitte, 2013). According to the survey, fewer than half of the firms surveyed rated themselves as extremely or very effective at managing operational and technology risk.

Managing Information Technology risk is a very important and challenging business concern now. Office of Government Commerce (OGC) definition for risk management is adapted to read as, "*Information Risk Management - the task of ensuring that the organization makes cost-*

*effective use of an information risk process*". The OGC definition goes on to say, "risk management requires: processes in place to monitor risk; access to reliable up-to-date information about risk; the right balance of control in place to deal with those risk; decision making processes supported by a framework of risk analysis and evaluation" (OGC, 2010).

It is generally neither feasible nor economically viable to protect against every known risk or threat. Even if it were possible, absolute security is still not attainable. Therefore, an effective risk mitigation approach means that a sound knowledge of the composition of risks – vulnerability, threat and the cost of consequences - is necessary in order to prioritise and focus resources on where the key risks are. The rapidity and frequency of systems and operational changes require an ongoing process of assessing new and existing risks and developing a proactive method of dealing with them. In today's fast-paced changing environment, there is no sufficient time to construct a risk mitigation plan between the time the first indication of a security incident is known and the time the consequences take effect. Advance planning and a fast incident response capability are necessary for such eventualities (Monetary Authority of Singapore, 2002).

The objective of the information risk management process is to enable decision makers who are responsible for information and systems to understand key information risks and agree upon the controls required to keep those risks within acceptable limits. A good systems control and security program should include implementation of sound security practices, system development controls and testing, compliance with legal and regulatory requirements and protection of business reputation (Monetary

Authority of Singapore, 2002). The various methods for managing technology risks include, internal processes and controls, Outsourcing and transferring risk through insurance.

## 1.6 IT Risks and Regulatory Guidelines

It is becoming increasingly apparent that information systems and technologies significantly influence business processes in the banking industry. The value of IS/IT depends widely on the way IS/IT is implemented and related to the banking activities. With regard to the dependency of business on IS/IT and due to the advanced stage of their penetration into the banking activities and products, the importance of IS/IT risk management is also growing. (Vlasta Svatá, 2011). This fact is reflected by banks themselves and obviously and also by regulators.

Except these general standards on IS/IT, like ISO 2700x, COBIT, ITIL etc. there are other relevant frameworks specific to banking and Basel II/III 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 IS/IT risk as an integral part (substantial subset) of operational risk. The approach is to how IT risk management is now treated within the banking industry all over the world is by the implementation of the so-called Operational Risk Management Framework.

## 1.7 Significance of the Study

Banks have faced both financial and non-financial losses due to IT risk incidents, which can even lead to failure of banking system, if not addressed properly. Literature review shows that there is not enough studies conducted

in the Indian context linking IT risks, IT risk management and its financial and nonfinancial impacts on banks. Regulators have issued only guidelines for banks to follow and build their own IT Risk Management models and controls. Since the areas of business operations, systems and technologies used could be relatively different in different banks, there could also be differences in the IT risk and IT risk management methods used by banks. The nature of the bank, geographical spread, technology used, volume in terms of customers/branches, certifications, outsourcing of services, training given to users/customers, etc. can also affect the IT risk profile of a bank. Linkages among IT risks, IT risk management methods and the impacts were not found to be studied in detail in a pan India context. It is very important to study and acquire insight into the various IT risk factors because each of which may affect differently the various dimensions of IT risk impacts. A particular control or risk management method reduces only certain aspects of IT risks and not all others. Linkages between the risks and its financial and nonfinancial impacts will help CIOs to identify and choose the right implementation strategies to achieve the desired outcome (ie. reduced financial or non-financial losses to the bank).

It is recognised that the approach for operational risk management that is chosen by an individual bank will depend on a range of factors, including size and sophistication, nature and complexity of its activities. However, despite these differences, clear strategies and oversight by the board of directors and senior management; a strong operational risk culture, i.e., the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a bank's commitment to and style of operational risk management; internal control culture (including

clear lines of responsibility and segregation of duties); effective internal reporting; and contingency planning are all crucial elements of an effective operational risk management framework (RBI, 2005).

Most of the studies in these domains have been done in developed countries and have come out with generalized conclusions on specific aspects of technology risks or technology risks on specific business lines. Some studies have focussed on IT security risks on internet banking, some others have on SMS banking and ATM banking. The studies linking the IT risk, IT risk management and its impacts, as per Basel and RBI guidelines, is rarely done in an Indian banking context. All these point to the need for more studies to be able to generalize across varying socio-economic contexts and also develop insights into the IT risk-IT risk management-impact models in different contexts.

India presents very unique characteristics which will have impact on IT risk and risk management. The types of banks, the technologies adopted, the geographical spread, volume of operation, standards followed, IT development methodologies used, outsourcing, level of automation, banking products offered are different in different banks across the globe. Hence a study is undertaken to establish the links between IT risk and IT risk management methods based on these parameters specific to Indian context.

## 1.8 Background of the Study

Information Technology risks and it's management are very critical for banks as any single incidence can even cause them to lose the trust and confidence of customers earned through several years.

Some of the previous studies and research reports showed that many firms are exposed to IT risks due to the lack of sufficient IT risk management practices (Kros, et al., 2004) and (Garg, et al., 2003).

In addition to financial losses, NIST in its security policy (NIST SP 800-30, 2002), has also listed out operational/security issues like *Confidentiality, Integrity* and *Availability* of information. Basel report on Banking Supervision (BCBS, 2003), had specified another two losses, namely the legal/compliance losses and reputational losses due to IT risks.

The Basel Committee for International Banking Supervision, considers IT risks under the category 'Operational Risk'. The Reserve Bank of India guidelines on Information Security (RBI, 2013) and the Basel II/III guidelines on Operational Risk Management provide high level of flexibility for individual banks on implementing proper IT risk management practices to identify, control and monitor IT risks and reduce the impacts to minimum.

BCBS (Basel Committee on Banking Supervision) recommended three approaches namely, basic indicator approach, standardized approach, advanced measurement approach, to measure and report operational risks in banks. Most of the banks in India are still using basic indicator approach or standardized approach. The BCBS has not included any treatment for nonfinancial risks in their recommendations.

Most of the Banks in India are now using core banking systems and other high end technologies to provide both online and branch based services to its local and international customers. Growing number of

internet and mobile users coupled with more and more banking services going online have caused an increase in the number of IT security threats and breaches worldwide. This implies the need for banks to have more effective in IT risk management, since the business impact of such security breaches can be extremely severe. Therefore, an in depth understanding of the growing IT risks in banks and the need for effective control systems for the IT risk management to reduce its financial and non-financial impact is very essential. Based on the literature review, it has been found that very limited studies have been conducted in India, to understand the nature and relationship between IT risks, IT risk management and impacts, across different type of banks in India.

## 1.9 Statement of the Problem

An ever increasing use of Information Technology coupled with the vulnerabilities and threats from internal and external sources in banking sector has brought in a lot of concerns to the regulatory authorities as well as the public. Use of advanced technologies and lack of sufficient risk management control methods can often lead to financial and nonfinancial losses to the banks.

RBI and Basel has provided only a set of general guidelines on effective risk management. At present, the IT risks, risk management and impacts are studied, managed and reported by individual banks based on these guidelines.

However, from the literature review, it is found that very limited research has been reported studying the nature and relationship of IT risk,

risk management and its financial and nonfinancial impacts present across different type of banks operating in India. So, this research tries provide an insight into the nature and relationship of IT risks, risk management and impacts present in the different type of banks in India.

## 1.10 Research Questions

IT risk and risk management are multidimensional constructs whose sub dimensions need to be studied and analysed. The literature review (covered in chapter 2) also indicates major gaps in research with respect to these constructs. This research tries to plug some of these gaps in research both in international as well as in Indian context. The following major research questions are addressed in this study.

a) Whether there exists a significant difference in the IT risks, IT risk management and it's financial and nonfinancial impacts based on the oraganizational characteristics of the banks in India

b) Whether there exists a significant variation in financial and non-financial impacts based on the IT risk present in the bank

c) Whether there exists a significant variation in financial and non-financial impacts based on the level of IT risk management practices used in the bank.

## 1.11 Scope of Study

Scope of study defines the boundaries of research. The four elements characterising the scope of the study are population, place of study, period of study and data sources.

Considering the importance of the subject under study and looking at the nature of the research problem, it was decided to conduct the research on pan India basis (112 banks). Banks operating in India were taken as the basic unit of analysis, namely sample unit. The period of study was between the year 2012 to 2014. Since the study was on Indian banks, the population was defined as all public sector banks (26), private sector banks (20), foreign sector banks (40) in India and cooperative banks in Kerala which have implemented core banking systems (26).

Based on the RBI guidelines, co-operative sector banks in India are now increasingly implementing computerised core banking systems for improved customer service, performance and regulatory reporting. To facilitate a comparative study, co-operative sector banks in Kerala, where core banking systems implemented, were also included in the scope of this study. The District (DCB) and Urban (UCB) co-operative banks are working under RBI and Basel guidelines.

## 1.12 Concepts and Definitions

**1.12.1 Banks in India**: are the banks operating in India (public sector banks, private sector banks, foreign banks and co-operative sector banks).

**1.12.2 Operational Risk**: is the risk of loss resulting from *inadequate or failed internal processes, people and systems, or from external events* (BCBS, 2013).

**1.12.3 IT Risks**: *is defined as the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise* (ISACA, 2009).

**1.12.4 IT Risk Management**: *is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization"* (CISA, 2006).

**1.12.5 Financial Impacts**: *is defined as the impact on capital and earnings.*

**1.12.6 Nonfinancial Impacts**: *are the direct and indirect impacts due to operational/security losses (NIST SP-800-30), compliance related losses (BCBS, 2003), reputational losses (BCBS, 2003) and business losses (Martina, 2014).*

**1.12.7 Public Sector Banks:** Public sector banks are those Indian banks in which the Government of India holds a majority stake.

**1.12.8 Private Sector Banks:** Private sector banks are those Indian banks in which the majority of stakes are held by private individuals or organizations, and not by the Government of India.

**1.12.9 Foreign Banks**: Foreign banks are those banks head quartered in other countries but having branches and operations in India.

**1.12.10 Cooperative Sector Banks**: Cooperative sector banks are the banks in India which are registered under the Co-operative Societies Act. The cooperative banks are also regulated by the RBI.

**1.12.11 Risk**: Risk is defined as a combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact. (NISTSSI).

**1.12.12 Threat**: Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization.

**1.12.13 Vulnerability**: Vulnerability is a weakness of an asset or group of assets that can be exploited by one or more threats.

**1.12.14 Risk Management**: Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization. Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication. (CISA, 2006).

**1.12.15 Risk Impact**: Impact is the likelihood that a vulnerability will be exploited or that a threat may become harmful. Risk impact indicates the potential adverse outcome(s) or consequences of risk events, if they are materialized.

## 1.13 Objectives of the Study

The main objective of the study is stated below,

a) *To study how IT risk and IT risk management impact the financial and non-financial aspects of different type of banks in India.*

In order to achieve this main objective, the following specific sub-objectives are stated.

a) *To study the nature and extend of IT risk in Indian banks.*

b) *To study the various IT risk management practices used in Indian banks.*

c) *To examine how IT risk, IT risk management and its financial and non-financial impacts varies based on the organizational characteristics of the banks in India.*

*d) To suggest ways and means for establishing effective IT risk management in banks in order to reduce the risk impacts.*

## 1.14 Conceptual Framework

The following conceptual model shown in Fig 1.7, which has an integrated and comprehensive view of Information Technology risk, risk management and its financial and nonfinancial impacts, was tested in this study.

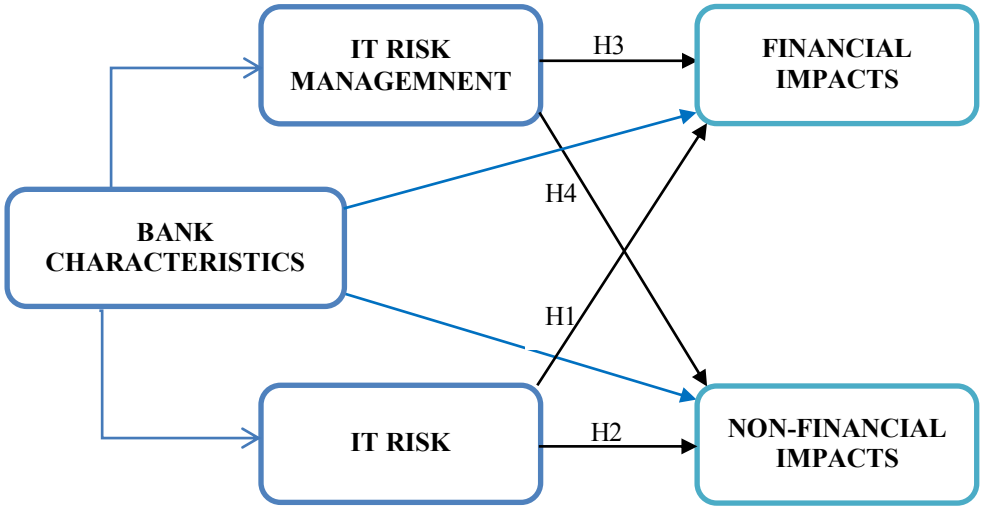



**Figure 1.7: Conceptual Framework linking IT Risk, IT Risk Management and Impacts**

## 1.15 Hypothesis

In line with objectives of the study, appropriate hypothesis were framed and tested statistically, for accepting and rejecting the same. The hypothesis of the study are,

- IT risk has significant positive relationship with financial impacts
- IT risk has significant positive relationship with nonfinancial impacts
- IT risk management has significant negative relationship with financial impacts
- IT risk management has significant negative relationship with nonfinancial impacts
- There is significant variation in IT risk, IT risk management and impacts across different organizational characteristics of the bank.

## 1.16 Limitation of Study

Research studies are exposed to inherent limitations while exploring, describing or explaining a phenomena, depending upon the nature of the research. This study also has got few limitations although the findings were statistically significant. The major limitations of the study were presented below.

IT risk and IT risk management are two emerging domains. Both of them are complex constructs which many researchers constantly work on. The technologies, technology related risks and its control mechanisms

constantly evolve and change. Hence it is quite possible that this research may not have captured every aspect of these constructs even though an extensive literature review was conducted and experts in the area were consulted for inputs.

Though the scales developed and used in the study were validated, there is always scope for further refinement in order to increase their level of reliability and their ability to explain the variance associated with the constructs they measure.

Basel and RBI guidelines were used as the sample frame for this study. The results should not be completely discounted for the possible extension to other financial institutions that does not come under the regulatory controls of RBI. The replication of the study across a broader sampling frame would provide additional validity for the findings and further empirical support for related theoretical studies.

A single-respondent or informant was used in this study. Although it is common to use a single respondent in academic research (Pinsonneault & Kraemer, 1993), it would be more desirable to have multiple respondents from each bank independently assessing risk and outcome in order to validate the results.

## 1.17 Content and Organization of the Thesis

The current research attempted to identify the various Information Technology risks present in banks, the various risk management controls and constructs used, and its financial and non-financial impacts, with a specific interest on Indian banks. Following the accepted procedures,

validated instruments were developed for measuring IT risks and the risk management controls. Comprehensive models linking IT risk, risk management and its impacts were proposed and statistically tested.

This research work is presented in the thesis in ten chapters and the remaining nine chapters are organized as follows:

In **Chapter 2**, a review of literature on IT risk, IT risk management and the financial and non-financial IT risk impacts are presented. A check list of IT risk and risk management controls are also presented based on the literature survey. Observations from the literature review and motivation for the present study are also discussed there.

**Chapter 3** presents the various aspects of the research methodology and instrument development. The initial part of the chapter presents concepts and definitions, research methodology, design, approach, research analysis and data sources. The second part explains the steps leading to the research instrument development, population of the study, variables of study, sampling method and conceptual models.

**Chapter 4** builds on the discussion in chapter 3 on instrument development and its empirical validation. It describes the profile of the final sample collected. The chapter also include results of the reliability analysis, validity and dimensionality analysis, generating the risk and risk management scores.

**Chapter 5** explores IT risk constructs further. It explores the link between IT risk factors with different bank types. The risk characteristics based on the analysis is also presented there.

**Chapter 6** explores IT risk management constructs further. It explores the link between IT risk management factors with respect to different bank types. The risk management based on the bank type (public, private and foreign) is analysed and reported there.

**Chapter 7** explores IT risk impact constructs (financial and non-financial) further. It explore the link between IT risk impacts with respect to different type of banks. The financial and non-financial impacts of IT risk based on different bank types (public, private and foreign) is analysed and presented.

**Chapter 8** IT risk, IT risk management, financial impact and non-financial impact constructs are analysed based on bank characteristics (like bank type, geographical spread) and technological characteristics (like technology used, data center model used, development methodology, etc.). Regression models connecting these four constructs are also presented here.

**Chapter 9** presents basic models showing relationship among IT risks, IT risk management and impacts. The model has each of the impact measures taken as the dependent variable and the IT risk dimensions as the independent variables. The models connecting IT risk and IT risk management to impacts is presented in this chapter. The various hypothesis formulated are also tested.

**Chapter 10** presents a summary of the results and findings of the research. The relevance of the research for practice is discussed. The limitations of this research work and scope for future research are also presented here.

# Chapter 2

# REVIEW OF LITERATURE

Contents



## 2.1 Introduction

Quality and success of research often a reflection of the time and effort invested in developing research ideas and concepts. The immediate goal of a literature survey is to determine whether the idea is worth pursuing or not. The first step of the procedure entails specifying the domain of the constructs (Pinder, et al., 2003). This includes outlining what is included and excluded from the concept under study (Churchill, 1979). Hence this study of IT risk and IT risk management began with an examination of the literature.

In order to obtain a better understanding of the nature of IT risk and IT risk management constructs, an extensive literature review was

performed. It was conducted mainly to identify those features of technologies used in banks which researchers and practitioners have pointed out as factors that increase the riskiness of a bank and the strategies they adopt to counter these factors. An extensive amount of literature survey was conducted to ensure that no important factor was overlooked. In order to identify as many factors as possible, the following general resources are considered.

The first source of literature was guidelines on Information Technology risk management from various central banks, which provided and explained a broad category of IT risks and IT risk management guidelines. The loss data published by these central banks and similar research institutions were also taken into account for understanding and categorizing the IT risks and its impacts. Some of these articles used empirical data to draw conclusions or build models as to the effects of particular risk factors in a business line with its financial or business impacts. These articles taken individually did not provide a detailed spectrum of risk constructs or risk control methods. The second source of literature was the Basel committee recommendations on banking laws and regulations issued by Basel Committee on Banking Supervision (BCBS) which includes Basel II and III. The third main source of literature was the various IS security and audit articles and reports. The fourth source of literature was articles written by practitioners in IT security, IT risk management and IT audit who detailed their experiences with IT risks, IT risk management and impacts. These kinds of resources and articles described mainly the authors experience and observations with a certain

bank or IT system. It also spoke about particular problems that appeared in IT systems in banks and how those risks were mitigated.

## 2.2 Theoretical Review

### 2.2.1 Information Technology Risk Definitions

Cambridge learner's dictionary defines "*risk*" as the possibility of something bad happening. Researchers and practitioners in various domains have conducted studies on this topic. Though there are differences in perceptions and approaches to the same, an examination of literature revealed a great deal of similarity in conclusions. Typically, risk is described as some kind of an event that may or may not occur, coupled with a consequence that follows if the event occurs (Dedolph, 2003).

Risk is the potential of losing something of value, weighed against the potential to gain something of value. Values such as physical, social or emotional wellbeing or financial wealth can be gained or lost when taking risk resulting from a given action, activity and/or inaction, foreseen or unforeseen. Risk can also be defined as the intentional interaction with uncertainty. Any human endeavour carries some risk, but some are much riskier than others (Hansson, 2012).

Risk is a combination of the likelihood of an occurrence of a hazardous event or exposure(s) and the severity of injury or ill health that can be caused by the event or exposure(s) (BS OHSAS, 2007). So, risk is also defined as the product of the likelihood of an event occurring and the impact that event would have on an Information Technology asset, i.e. *Risk = Likelihood * Impact*. Further, the impact of an event on an

information asset is usually taken to be the product of vulnerability in the asset and the asset's value to its stakeholders. To summarise, risk is a product of threat, vulnerability and asset value (Albert, 2009).

Committee on National Security Systems (CNSS), USA defined *risk as the possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability* (CNSS, 2010). In National Security Telecommunications and Information Systems Security Instruction (NSTISSI, 2012) No. 1000, risk is defined as: '*a combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact'*.

The classical decision theory states that risk is perceived as reflecting variations in the distribution of likely outcomes and their subjective values. Hence a risky alternative is one where the variance is large and risk forms an important factor in evaluating alternative options. Decisions are said to be taken under risk when there is the possibility of more than one outcome resulting from the selection of an option. Furthermore, it is assumed that the probability of occurrence of each is known to the decision maker in advance. The variation in outcomes is said to be a consequence of factors which are beyond his control (Radford, 1978).

IT risk is the risk related to Information Technology. The following sections explain in detail some of the standard IT risk definitions.

#### 2.2.1.1 ISO Definition

IT risk is *the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.*

*It is measured in terms of a combination of the probability of occurrence of an event and its consequence.*

#### 2.2.1.2 NIST Definition

*IT related risk is defined as the probability* that *a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and the resulting impact if this should occur* (NIST SP 800-30, 2002).

IT related risks arise from legal liability or mission loss due to:

a) Unauthorized (malicious or accidental) disclosure, modification, or destruction of information

b) Unintentional errors and omissions

c) IT disruptions due to natural or man-made disasters

d) Failure to exercise due care and diligence in the implementation and operation of the IT system.

#### 2.2.1.3 ISACA Definition

*IT risk is defined as the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise* (ISACA, 2009). ISACA published the "*Risk IT"* framework in order to provide an end-to-end, comprehensive view of all risks related to the use of IT.

#### 2.2.1.4 Basel Definitions

Except these general standards on IS/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 IS/IT risk as an integral part (substantial subset) of operational risk.

A widely used definition of **operational risk** is the one contained in the Basel II regulations. This definition states that *operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events* (BCBS, 2013).

The Basel II definition of operational risk regards systems as one of four operational risk drivers; however, the coverage of IS/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 (Fleischmann, 2011).

### 2.2.2 Risk Factors & Definitions

The extensive literature review resulted in the identification of several risk factors. The next step was to try to group similar factors together in order to get a clearer picture of the general types of IT risk factors. This study being focussed on IT risks in Banking organizations, RBI and Basel guidelines on operational risk management were followed in this process and which resulted in the creation of seven general types of software IT risk categories (RBI, 2005).

a) Internal fraud

b) External fraud

c) Employment practices and work place safety

d) Clients, products and business practices

e) Damage to physical assets

f) Business disruption and system failures

g) Execution, delivery and process management

These categories were identified and listed based on the risk categories listing under operational risk management of Basel recommendations. Each of these IT risks categories are explained in detail in the following sections.

### 2.2.2.1 Internal Fraud

***Fraud*** can loosely be defined as "*any behaviour by which one person intends to gain a dishonest advantage over another*". RBI working group on 'information security, electronic banking, technology risk management and cyber frauds' (RBI , 2013), defined fraud as *'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank'.*

*Internal fraud* is defined as the losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or

company policy, excluding diversity/discrimination events, which involves at least one internal party. For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account etc. are different types of internal fraud. Internal fraud, under Basel recommendations, is further divided into the following subcategories.

#### 2.2.2.1.1 Unauthorized Activity

Under this subcategory, employees perform unauthorized activities which can lead to financial losses to the organization. Such unauthorized activities include,

a) Transactions are not reported intentionally

b) Unauthorized transaction types are used which causes monetary losses

c) Intentional mismarking of positions

#### 2.2.2.1.2 Theft and Fraud

Multiple global economic crime studies show that approximately 50% of businesses experience workplace fraud or theft in a given year. Theft and fraud can cause financial damage and/or loss of reputation to banks too. The main subcategories of theft and frauds listed under the Basel framework are as follows.

a) Fraud, credit fraud, worthless deposits

b) Theft, extortion, embezzlement, robbery

c) Misappropriation of assets

d) Malicious destruction of assets

e) Forgery, cheque kiting, smuggling

f) Account takeover, impersonation

g) Tax noncompliance, evasion

h) Bribes, kickbacks

i) Insider trading.

#### 2.2.2.2 External Fraud

*External fraud* is defined as the losses due to acts of a type intended to defraud, is appropriate property or circumvent the law, by a third party. External fraud is carried out by an external party outside the organization. Robbery, forgery, cheque kiting, and damage from computer hacking are examples for this category. External fraud, under Basel recommendations, is further divided into subcategories as follows.

##### 2.2.2.2.1 Theft and Fraud

Theft and frauds by third parties, included in this subcategory are,

a) Theft/Robbery

b) Forgery

c) Cheque kiting (*Check kiting is a method of utilizing the time required for cheques to clear to obtain unauthorized funds without any interest charge).*

##### 2.2.2.2.2 System Security

Under system security, the following subcategories are included,

a) Theft of information

b) Hacking damage.

(*Hacking* is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose. The person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of their choice, is called a *hacker*).

#### 2.2.2.3 Employment practices and work place safety

*Employment practices and work place safety* risk is defined as the losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events. For example, workers compensation claims, violation of employee health and safety rules, organised labour activities, discrimination claims, and general liability come under this category. Any given company may have employment practices and standards regarding employee and workplace safety. These standards and practices are enforced to protect the safety of all employees in the business and to protect the business in case an accident occurs in the workplace. Basel had further classified this category into the following subcategories.

##### 2.2.2.3.1 Employee Relations

Employee relations deal with the risks that may arise due to the relationship issues between the organization and employees and also between employees of the organization. This includes,

a) Compensation benefit, termination issues

b) Organised labour activity.

#### 2.2.2.3.2 Environmental Safety

Environmental safety measures (policies and procedures) are implemented by every organization to protect people, environment, property, finance and other resources. Environmental safety risks can cause consequent losses to people, resources or environment. Basel committee considers the following items under environmental safety,

a) General liability (workplace accidents like slip, fall, etc.)

b) Employee health & safety rules events

c) Workers compensation.

#### 2.2.2.3.3 Diversity and Discrimination

Diversity refers to the fact that we are all different. Some are male, some female, some tall, some short, some dark skinned, some light skinned. Each one may come from different cultural backgrounds, different faiths, and different family groupings, and may have different learning styles, different personalities, etc. Discrimination refers to the practice of treating someone differently due to characteristics beyond their control, or for which they should not be treated in a negative manner. Some people discriminate against others because of their sex, their age, or the colour of their skin. The risk from diversity/discrimination events are considered under this subcategory. This include,

a) All types of discriminations.

b) Harassment

c) Equal employment opportunity.

#### 2.2.2.4 Clients, products and business practices

This is the losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product is. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorised products comes under this category.

##### 2.2.2.4.1 Confidentiality of customer information

Confidentiality refers to limiting information access and disclosure to authorized users (the right people) and preventing access by or disclosure to unauthorized ones (the wrong people). The risk categories considered under confidentiality of customer information (suitability, disclosure and fiduciary) are,

a) Fiduciary breaches/guideline violation.
b) Suitability of disclosure issues (KYC etc)
c) Retail customer disclosure violations
d) Breach of privacy
e) Aggressive sales
f) Account churning
g) Misuse of confidential information
h) Lender liability.

#### 2.2.2.4.2 Improper Business or Market Practices

Today's world of fast information makes it particularly risky for business to employ improper practices. The internet, social networking, television and radio media will spread the word quite quickly about product recalls, bad customer experiences or executive improprieties. Government "watchdog" agencies also alert consumers when a company uses any improper business or market practices. Risky business practices will be disclosed eventually, and the consequences can include fines, lawsuits and the potential for bankruptcy.

Under Basel recommendations for banks, the following subcategories are listed under improper business or market practices.

a) Antitrust
b) Improper trade or market practices
c) Market manipulation
d) Insider trading
e) Unlicensed activities
f) Money laundering.

#### 2.2.2.4.3 Product Flaws

Any flaws in banking products, models or even system flaws can affect the professional obligation of banks to meet client obligations and can cause losses. Product flaws category covers the following subcategories

a) Product/module defects, flaws (unauthorized etc) &
b) Model errors.

#### 2.2.2.4.4 Employee Relationship

Sound employee relationships within an organization can provide the capabilities to achieve greater performance and also to provide better customer services. Employee relationship covers the inter employee relationship in a bank

a) Sound and cordial employee relationship.

#### 2.2.2.4.5 Customer Identity Check (KYC)

KYC is an acronym for "*Know Your Customer*", a term used for customer identification process used by RBI and banks in India. It involves making reasonable efforts to determine true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the banks to manage their risks prudently. The objective of the KYC guidelines is to prevent banks being used, intentionally or unintentionally by criminal elements for money laundering. KYC has two components - identity and address. While identity remains the same, the address may change and hence the banks are required to periodically update their records.

As per regulatory guidelines the KYC norms are to be satisfied by every bank before a customer is allowed to make any banking transaction.

a) Failure to investigate client per guidelines.

#### 2.2.2.4.6 Client Exposures/Limits

Exposure indicates the extent to which the lender is exposed to the risk of loss in the event of the borrower's default. Banks do cap client

exposure with limits to control the risk of exposures. So, this client exposure/limits category enforces the need for strict checks for client limits manage exposures.

a) Exceeding client exposure limits.

**2.2.2.4.7 Advisory Activities**

Failed bank's advisory activities and services or disputes over the advisory activities can cause losses to the bank.

a) Disputes over performance of advisory activities.

**2.2.2.5 Damage to physical assets**

*Damage to physical assets* is defined as the losses arising from loss or damage to physical assets from natural disasters or other events. For example, terrorism, vandalism, earthquakes, fires and floods can cause damage to physical assets and losses to banks. The main subcategories under this category of risk are,

**2.2.2.5.1 Disaster and other events**

A disaster is a natural or man-made (or technological) hazard resulting in an event of substantial extent causing significant physical damage or destruction, loss of life, or drastic change to the environment. A disaster is defined as any tragic event stemming from events such as earthquakes, floods, catastrophic accidents, fires, or explosions. It is a phenomenon that can cause damage to life and property and destroy the economic, social and cultural life of people. The items considered under this category are as follows,

a) Losses due to natural disaster

b) Human losses from external sources (terrorism, vandalism, etc)

#### 2.2.2.6 Business disruption and system failures

*Business disruption and system failure* is defined as the losses arising from disruption of business or system failures. Hardware and software failures, telecommunication problems, and utility outages are examples of business disruption due to system failures.

##### 2.2.2.6.1 Systems Failures

A systems failure occurs when a system does not meet its requirements. A computer system failure occurs because of a hardware failure, software failure, network failure or power disruptions. A failure may cause the system to work slow, stop working and/or even malfunction, causing greater operational and business risks.

a) Hardware

b) Software

c) Telecommunications

d) Utility outrage/disruptions.

#### 2.2.2.7 Execution, delivery and process management

It is the risk of losses from failed transactions processing or process management, from relations with trade counterparties and vendors. For example: data entry errors, collateral management failures, incomplete legal documentation, and unauthorized access given to client accounts, non-client counterparty non/under performance, and vendor disputes. A detailed list of categories and subcategories are listed below.

#### 2.2.2.7.1 Transaction capture, execution and maintenance

A secure information system must preserve the confidentiality, integrity and availability of information. It protects the information from unauthorised access, use, disclosure, disruption, modification and destruction and thus minimised the risk of exposure of information to unauthorized parties. A properly implemented information system must keep the information free from threats throughout the information processing cycle (creation, storage, processing, transmission, maintenance and destruction).

a) Miscommunication

b) Data entry, maintenance, or loading error

c) Missed deadline or responsibility

d) Model/system malfunction

e) Accounting error/entity attribution error

f) Other task non performance

g) Delivery failure

h) Collateral management failure

i) Reference data maintenance.

#### 2.2.2.7.2 Monitoring and Reporting

It is mandatory for banks to provide various reports (ad hoc and regular) to regulatory authorities like central bank and other government agencies. Failing in providing timely reports and/or providing inaccurate reports may lead to legal actions and business risks to banks.

a) Failed mandatory reporting obligation

b) Inaccurate external report (loss incurred).

#### 2.2.2.7.3 Customer intake and documentations

Banks have to follow KYC (Know Your Customer) norms set by central banks and complete all required legal and other documentations before creating new customers, accounts or performing any financial transactions on these customer accounts. Banks also publishes disclaimers to restrict themselves on their legal liabilities on various products and services.

a) Client permissions/disclaimers missing

b) Legal documents missing/incomplete.

#### 2.2.2.7.4 Customer/Client account management

Customer/client account management lists out the following subcategories of risks,

a) Unapproved access to accounts

b) Incorrect client records

c) Negligent loss damage of client assets.

#### 2.2.2.7.5 Documentation

It is important for banks to make sure that all required documentations are completed before making financial transactions on client accounts. This is a regulatory requirement and can cause legal disputes and losses, if omitted/violated.

a) Incorrect, missing and/or partial documentation.

#### 2.2.2.7.6 Counter party under/non-performance and disputes

To accomplish various customer services and own functional requirements in a more efficient and cost effective way, banks sometimes

depend on external (third) parties for various products/services. In such cases, any under/non-performance of the third party or a dispute with the third party becomes a risk for the bank and may also cause losses.

a) Non client counter party under/non performance
b) Misc. non-client counter party disputes.

**2.2.2.7.7 Outsourcing**

Outsourcing is an example of assigning third parties for performing some of the bank's requirements/functions or self or clients.

a) Outsourcing of services/facilities.

## 2.2.3 Information Technology Risk Management Definitions

IT Risk Management is usually a sub component of an enterprise's risk management system. It deals with the application of risk management to Information Technology. The Certified Information Systems Auditor Review Manual, 2006, provides the following definition of risk management: *"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."* (CISA, 2006). The *process* of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerability emerge every day. Also, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

*Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives* (NIST SP 800-30, 2002).

National Information Assurance Training and Education Center (NIATEC, 2014) glossary of terms defines IT risk management as "*The total process to identify, control, and minimize the impact of uncertain events. Otherwise, an element of managerial science concerned with the identification, measurement, control, and minimization of uncertain events.* An effective risk management program encompasses of a risk assessment (evaluation of threats and vulnerabilities), management decision, control implementation and effectiveness review.

The financial services industry recognized during the financial crisis that boards needed to change focus from share price and profitability to the risks entailed in their strategies. Also, chief risk officers needed to be empowered to create cultural change within their organizations. With these shifts well underway, senior risk executives are focused on moving reputation and operational risk higher up the agenda. However, banks are still struggling to ensure that specific business decisions are consistent with risk appetite and are putting new programs in place to achieve this (Institute of International Finance and EY, 2013).

A thorough review of literature on risk management strategies for IT risks and discussions with experts in the field, helped to identify a range of risk resolutions techniques.

The NIST SP 800-26 (NIST , 2002), Security Self-Assessment Guide for Information Technology Systems, provides an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems are tested and measured. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. The goal of this document is to provide a standardized approach to assessing a system. This document strives to blend the control objectives found in the many requirement and guidance document. It lists out a set of Management Controls, Operational Controls and Technical Controls.

Based on NIST SP 800-30 guidelines (NIST SP 800-30, 2002), the following nine categories of IT risk management control objectives are formulated and discussed in detail below;

a) Policies and procedures

b) Data security

c) Access control and authentication

d) System logs and audit

e) Backup and recovery

f) Monitoring systems

g) Software development and deployment

h) Physical security

i) Network security.

Each of the above items is discussed elaborately in the following sections.

### 2.2.3.1 Policies and procedures

Policies and procedures are a very critical component of IT security. Banks need to frame a board approved information security policy and identify and implement appropriate information security management measures/practices keeping in view their business needs (RBI , 2013). The policies need to be supported with relevant standards, guidelines and procedures. A policy framework would, inter-alia, incorporate/take into consideration a strategy which is aligned with business objectives and legal requirements. The policy includes specifications covering the structure, roles and responsibilities, reviews, monitoring, exceptions, access rights, training, logging, audits, etc. There may be specific policies to certain areas included as part of this main policy, like the ones for logical access control, asset management, network access control, password management, backup, physical security, internet security, etc.

Bank needs a common language for describing loss-event types, causes, and effects according with regulatory requirements. The development of definitions, linkages, and structures can help enable banks to efficiently identify, assess, and report such operational risk-related information by forming the basis of consistent databases that can help enable banks to

maintain data that remains meaningful over time. (Basel II Operational Risk Advisory, KPMG).

RBI guidelines on operational risk mandates, each bank to have policies and procedures that clearly describe the major elements of the operational risk management framework including identifying, assessing, monitoring and controlling/mitigating operational risk. Operational risk management policies, processes, and procedures should be documented and communicated to appropriate staff i.e., the personnel at all levels in units that incur material operational risks. The policies and procedures should outline all aspects of the institution's operational risk management.

**2.2.3.2 Data security**

Data security means protecting data from unauthorized access, disclosure or destructive forces. In the context of computer science, security is the prevention of, or protection against,

a) Access to information by unauthorized recipients, and

b) Intentional but unauthorized destruction or alteration of that information (Dictionary of Computing, 1996).

Many countries have created regulations/acts in view of data security. Examples are, *Data Protection Act 1998* which governs the protection of personal data in United Kingdom, the *European Data Protection Regulation* jointly prepared by the European Union Agency for Fundamental Rights (FRA) and the Council of Europe together with the Registry of the European Court of Human Rights, The *Federal Privacy Act*

*1988* of Australia, *National privacy or data security laws* of USA, *Regulations of Federal Trade Commission* of USA, the *Information Technology Act 2000* of India (DLA Piper, 2014).

"With 2.5 quintillion bytes of data created every day, and with the average cost of security-related incidents in the era of big data estimated to be over USD 40 million, now is the time to keep customer, business, personally identifiable information (PII) and other types of sensitive data safe against internal and external threats." (IBM, 2013)

Data Security and Privacy help organizations in the following ways,

a) **Prevent data breaches:** Avoid disclosure or leakage of sensitive data to mitigate the cost of a data breach

b) **Ensure data integrity:** Prevent unauthorized changes to data, data structures, configuration files and logs to ensure complete visibility into data access patterns and trends

c) **Reduce cost of compliance:** Automate and centralize controls and simplify audit review processes

d) **Protect privacy:** Prevent disclosure of sensitive information by masking or de-identifying data in databases, applications, and reports on demand across the enterprise.

*Encryption* is a most commonly used technology to protect data from unauthorized access while storing or transmitting over networks. Encryption is a process of encoding messages or information using encryption algorithms and a key in such a way that only authorized parties can read it, if decrypted.

### 2.2.3.3 Access control and authentication

#### 2.2.3.3.1 Authentication

Authentication is any process by which a system verifies the identity of a user who wishes to access it. Authentication is a means for one party to verify another's identity. For example, a client gives a password to directory server during an LDAP bind operation.

#### 2.2.3.3.2 Access control

Access control refers to security features that control who can access resources in the system. Applications call access control functions to set who can access specific resources or control access to resources provided by the application (Microsoft, 2013).

While *authentication* provides proof of identity, it does not describe the privileges an entry processes. For example, you are authenticated before you access a database system, but this does not tell the database system which data you are entitle to access. This later function is known as the *authorization or access control* (Woo, 1992).

Central banks including RBI, was mandating additional factor of authentication for certain type of high risk transactions like online banking, card payments etc, through regulations (RBI, 2013). Login names and passwords are the most common kind of authentication method used by banks. Some banks do also provide an additional key in a digital medium or by SMS/Email to the client for increased security while making financial transactions. For access control, users in the system are grouped into user groups/roles (say admin, sales, HR, etc.) and each user group/role

is assigned with well defined access rights and privileges. Access control matrix is used to specify and control access to the system by many core banking systems.

#### 2.2.3.4 System logs and audit

An audit trail/log is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event (Committee on National Security Systems, 1996), (ATIS, 2012). Audit records typically result from activities such as financial transactions, data manipulations, communications, systems, accounts, or other entities. Audit trails are not accessible to normal users.

An information system audit is an examination of the management controls within an Information Technology infrastructure. The evaluation of obtained evidence determines whether the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews are normally done with the help of system logs. The system verified/ evaluated to identify the gaps, if any, with respect to the organization's access control specifications, security policies and procedures, etc.

It is important to provide necessary system logs and audit trails, which is used to locate the system risks, and alternatively to provide a method to identify and address the gaps in information security. RBI has issued guidelines on system audit in its circular, "Information systems audit policy for the banking and financial sector." (RBI Guidelines, 2012)

### 2.2.3.4 Backup and recovery

*Backup and recovery* refers to the various strategies and procedures involved in protecting your database against data loss and reconstructing the database after any kind of data loss (Romero, 2005). A backup is a copy of data from your database that is used to reconstruct that data. Backups are normally divided into physical backups and logical backups.

*Physical backups* are backups of the physical files used in storing and recovering your database, such as data files, control files, and archived redo logs. Ultimately, every physical backup is a copy of files storing database information to some other location, whether on disk or some offline storage such as tape. *Logical backups* contain logical data (for example, tables or stored procedures) exported from a database with an export utility and stored in a binary file, for later re-importing into a database using the corresponding import utility.

Hardware failures, terrorist attacks or natural calamities can destroy the entire data center as in September 11 attack. So, regular backup and recovery testing is a mandatory requirement for banks across the world in assuring business continuity and information security.

BCP (Business Continuity Planning) forms a part of an organisation's overall Business Continuity Management (BCM) plan, which is the "preparedness of an organisation", which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes, at an agreed level and limit the impact of the disaster

on people, processes and infrastructure (includes IT); or to minimise the operational, financial, legal, reputational and other material consequences arising from such a disaster (RBI , 2011). To ensure business continuity, banks should be having necessary backups for all resources, including data, systems, power, network, human resources, etc.

#### 2.2.3.6 Monitoring systems

A *system monitor* is a hardware or software component used for monitoring resources, activities or performance of a system. Monitoring systems help to detect various technology related risks in time and sometimes to prevent certain types of such risks from happening.

An effective monitoring process is essential for adequately managing technology related risks. 'Internal controls and the internal audit are used as the primary means to mitigate operational risk. Banks could also explore setting up operational risk limits, based on the measures of operational risk. The contingent processing capabilities could also be used as a means to limit the adverse impacts of operational risk' (RBI, 2013). Banks do deploy various monitoring systems as part of their core banking system to monitor transactions, detect and/or prevent any intrusion, protect against malicious software, etc. Systems and tools are also deployed for effective review and analysis of logs.

#### 2.2.3.7 Software development and deployment

Due to the lack of in house expertise, reduced cost, increased efficiency and also the need for providing better services to customers round the clock, Banks are now increasingly depending on outsourced products and services

for their IT requirements and operations. It is now very important that banks do select the right vendor and make sure that any of their in house or outsourced software developments and/or implementation follows proven industry standards. The Software Development Standards (SDS) document normally establishes the standard for the development, acquisition, and support of the software which will provide a concise and complete method for implementing a uniform software development process waterfall model, spiral model, agile development, rapid application development, are some of the example models used for software development in the Industry. CMMI, ISO 9000, ISO/IEC 15504 are some of the most commonly used international standards for software development processes by software development companies.

**2.2.3.8 Physical security**

Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks) (US Department of Army, 2001). Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, protective barriers, locks, access control protocols, and many other techniques. Physical security systems for protected facilities are generally intended to,

a) Deter potential intruders (e.g. warning signs and perimeter markings);

b) Distinguish authorized from unauthorized people (e.g. using key cards/access badges)

c) Delay, frustrate and ideally prevent intrusion attempts (e.g. strong walls, door locks and safes);

d) Detect intrusions and monitor/record intruders (e.g. intruder alarms and CCTV systems);

e) Trigger appropriate incident responses (e.g. by security guards and police).

(Garcia, 2007), (US Department of Army, 2001) and (Anderson, 2001)

Information and equipment stored in data centers are vulnerable to physical theft too, though. They are targeted by thieves for their resale value or, more likely, by criminals who want to exploit the data held on them. Banks in India are advised to implement suitable physical and environment controls taking into consideration threats, and based on the entity's unique geographical location, building configuration, neighbouring entities, etc. as part of a critical component to information security (RBI, 2011). Physical security strategies are based on (1) the concept of protection, detection, response, and recovery; (2) design based on a series of clearly discernible zones; (3) control of access to restricted areas; and (4) the capability to increase security during emergencies and increased threat situations ( MITS, 2013).

Physical security involves measures undertaken to protect personnel, equipment and property against anticipated threats. Passive measures include the effective use of architecture, landscaping and lighting to achieve improved security by deterring, disrupting or mitigating potential threats. Active measures include the use of proven

systems and technologies designed to deter, detect, report and react against threats (Lynda, 2012).

ISO 27001 defines the role of physical security as 'Protect the organization's assets by properly choosing a facility location, maintaining a security perimeter, implementing access control and protecting equipment'.

**2.2.3.9 Network security**

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources (Simmonds, et al., 2004). Network security refers to any activities designed to protect the network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network (CISCO, 2012). The most common network threats are, viruses, worms, Trojan horses, spyware, adware, zero hour attacks, hacker attacks, Denial of Service attacks (DoS), data interception and theft and identity theft.

The various network security management methods include, firewalls, antivirus software, secured and encrypted connections, strong passwords, physical security of network centers, network analysers/ monitors, use of VPN for connections, disabling all unwanted services and also user training to raise awareness on network security. User awareness is very important on security because, even though the data

centers and networks are equipped with sufficient security controls, any access by a user from inside the network to the internet using external modems or data cards can open vulnerabilities for an attacker/virus to enter the network.

### 2.2.4 Security Controls & Definitions

A comprehensive and effective IT risk management has to include sufficient technical security controls, methods, policies, procedures and trainings to users at all levels. The following sections lists out the various Technical security controls, namely supporting, preventive and detection and recovery type of controls.

#### 2.2.4.1 Technical Security Controls

The following are the *supporting technical controls*

a) Identification (ability to identify users, processes and information resources

b) Cryptographic key management (includes key generation, distribution, storage, and maintenance)

c) Security administration (Configurable features, operating system and application level security, add-on security systems/ products for additional security)

d) System protections (design processes, implementation process, system protection.

The following are the *preventive technical controls*

a) Authentication

b) Authorization

c) Access control enforcement

d) Non-repudiation

e) Protected communications

f) Transaction privacy.

The following are the *detection and recovery technical controls*

a) Audit

b) Intrusion detection and containment

c) Proof of wholeness

d) Restore secure state

e) Virus detection and eradication.

**2.2.4.2 Management Security Controls**

The following are the *Management Security Controls - Preventive*

a) Assign security responsibility for mission critical IT systems

b) Document security controls

c) Implement personnel security controls (separation of roles, access privileges)

d) Security awareness and technical training to employees and end users.

The following are the *Management Security Controls – Detection*

a) Periodic review of security controls

b) Periodic system audits

c) Ongoing risk assessment and mitigation.

The following are the *Management Security Control - Recovery*

a) Business continuity plans

b) Incident management systems.

### 2.2.4.3 Operational Security Controls

The following are the *Preventive Operational Controls*

a) Control data media access and disposal

b) Limit external data distribution

c) Control software viruses

d) Safeguard computing facility

e) Backup capability and offsite storage

f) Protect workstations

g) Protect IT resources form natural disasters and terrorist attacks

h) Provide backup power/network capabilities

i) Controlled environment (humidity, temperature).

The following are the *Detection Operational Controls*

a) Physical security (motion detectors, CCTV, sensors and alarms)

b) Environmental security (smoke/fire detectors, sensors and alarms).

### 2.2.5 IT Risk Impacts Definitions

The major impacts of IT risks are classified into financial and non-financial impacts. Financial impact of IT risks is defined as the impact of IT risks on capital and earnings. The other nonfinancial impacts are: loss of IT security, legal/compliance losses, loss of reputation and loss of business. IT Security mainly is concerned about the CIA triad - confidentiality, integrity and availability.

*Confidentiality* is the Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (NIST SP 800-30, 2002). *Availability* is defined as ensuring timely and reliable access to and use of information (NIST SP 800-30, 2002). *Integrity* is defined as guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity (NIST SP 800-30, 2002).

The expression "*compliance risk*" is defined in this paper as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities (together, "compliance laws, rules and standards") (BCBS, 2005).

## 2.3 Check Lists on IT Risk & IT Risk Management

One of the most common methods for identifying the presence of risk factors and risk management strategies in an Information Technology system has been the use of checklists. These checklists present a list of all

potential risks and risk management factors that might be applicable in an IT system.

### 2.3.1 IT Risk Check List

Information Technology risks are categorised under operational risk management by Basel Committee recommendations. On 16 January 2001, the Basel Committee on Banking Supervision announced a second consulting paper for the new Basel Capital Accord (Basel II). The new regulation about equity capital, which has become effective from 2005, also comprises approaches to measure operational risks. In the Basel papers operational risk is defined as "*the risk of losses resulting from inadequate or failed internal processes, people and systems or from external circumstances*." The reason for the inclusion of operational risks in the new Basel capital accord is the increasing importance of these risks. Basel Committee (BCBS, 2002) and RBI (the central bank or regulatory authority for banks in India) has provided the check list of operational risks (RBI, 2010) to be considered by banks and other financial institutions in India. The list is given in table Table 2.1. The 'guidance on management of operational risk' by Reserve Bank of India (RBI, 2005) loss event classification and list also provides a check list as follows.

**Table 2.1: Checklist of operational risk categories**

| No | Risk Category Level 1 | Category Level 2 | Category Level 3 |
|---|---|---|---|
| **1** | Internal fraud | 1.1 Unauthorised Activity | Transactions not reported (intentional) |
| | | | Trans type unauthorised (w/monetary loss) |
| | | | Mismarking of position (intentional |
| | | 1.2 Theft and Fraud | Fraud / credit fraud / worthless deposits |
| | | | Theft / extortion / embezzlement / robbery |
| | | | Misappropriation of assets |
| | | | Malicious destruction of assets |
| | | | Forgery |
| | | | Check kiting |
| | | | Smuggling |
| | | | Account take-over / impersonation / etc. |
| | | | Tax non-compliance / evasion (wilful) |
| | | | Bribes / kickbacks |
| | | | Insider trading (not on firm's account) |
| **2** | External fraud | 2.1 Theft and Fraud | Theft/Robbery |
| | | | Forgery |
| | | | Check kiting |
| | | 2.2 Systems Security | Hacking damage |
| | | | Theft of information (w/monetary loss) |
| **3** | Employment Practices and Workplace Safety | 3.1 Employee Relations | Compensation, benefit, termination issues |
| | | | Organised labour activity |
| | | 3.2 Safe Environment | General liability (slip and fall, etc.) |
| | | | Employee health & safety rules events |
| | | | Workers compensation |
| | | 3.3 Diversity & Discrimination | All discrimination types |

| No | Risk Category Level 1 | Category Level 2 | Category Level 3 |
|---|---|---|---|
| **4** | Clients, Products & Business Practices | 4.1 Suitability, Disclosure & Fiduciary | Fiduciary breaches / guideline violations |
| | | | Suitability / disclosure issues (KYC, etc.) |
| | | | Retail consumer disclosure violations |
| | | | Breach of privacy |
| | | | Aggressive sales |
| | | | Account churning |
| | | | Misuse of confidential information |
| | | | Lender Liability |
| | | 4.2 Improper Business or Market Practices | Antitrust |
| | | | Improper trade / market practices |
| | | | Market manipulation |
| | | | Insider trading (on firm's account) |
| | | | Unlicensed activity |
| | | | Money laundering |
| | | 4.3 Product Flaws | Product defects (unauthorised, etc.) Model errors |
| | | 4.4 Selection, Sponsorship & Exposure | Failure to investigate client per guidelines |
| | | | Exceeding client exposure limits |
| | | 4.5 Advisory Activities | Natural disaster losses |
| | | | Human losses from external sources (terrorism, |
| | | | vandalism) |
| **5** | Damage to Physical Assets | 5.1 Disasters and other events | Natural disaster losses |
| | | | Human losses from external sources (terrorism, vandalism) |
| **6** | Business disruption and system failures | 6.1 Systems | Hardware |
| | | | Software |
| | | | Telecommunications |
| | | | Utility outage / disruptions |

| No | Risk Category Level 1 | Category Level 2 | Category Level 3 |
|---|---|---|---|
| **7** | Execution, Delivery & Process Management | 7.1 Transaction Capture, Execution &Maintenance | Miscommunication |
| | | | Data entry, maintenance or loading error |
| | | | Missed deadline or responsibility |
| | | | Model / system mis-operation |
| | | | Accounting error / entity attribution error |
| | | | Other task mis-performance |
| | | | Delivery failure |
| | | | Collateral management failure |
| | | | Reference Data Maintenance |
| | | 7.2 Monitoring and Reporting | Failed mandatory reporting obligation |
| | | | Inaccurate external report (loss incurred) |
| | | 7.3 Customer Intake and Documentation | Client permissions / disclaimers missing |
| | | | Legal documents missing / incomplete |
| | | 7.4 Customer / Client Account Management | Unapproved access given to accounts |
| | | | Incorrect client records (loss incurred) |
| | | | Negligent loss or damage of client assets |
| | | 7.5 Trade Counterparties | Non-client counterparty mis-performance |
| | | | Misc. non-client counterparty disputes |
| | | 7.6 Vendors & Suppliers | Outsourcing |
| | | | Vendor disputes |

Source: Guidance on management of operational risk' by Reserve Bank of India, 2005

### 2.3.2 IT Risk Management Check List

Sources that are used in compiling Information Technology risk management checklist include, but are not limited to, the following government regulatory and security directives and sources applicable to the IT system processing environment: Computer Security Act of 1987 (Unites States Congress, 1987), Federal Information Processing Standards Publications (FIPS PUBS, 2010), OMB November 2000 Circular A-130 (OMB, 2000), Privacy Act of 1974 (US Federal Law, 1974), system security plan of the IT system assessed, the organization's security policies, guidelines, and standards, industry practices, etc. Expert opinions, RBI and other central bank guidelines, IT security standards/models and IS audit documents were also analysed in detail as this study is confined to banks in India.

*Solarwinds* white paper on *IT security management check list* (Solarwinds, 2013) included key recommendations to keep the network safe, which included logs, firewalls and monitoring tools for network security. The *NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems* (Swanson, 2001), provides an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems are tested and measured. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy.

The *NIST SP 800-30, Risk Management Guide For Information Technology Systems* (NIST SP 800-30, 2002) and other NIST standards have classified the controls into technical security controls, management

security controls and operational security controls. The security controls are further divided into support, prevent and detect & recover groups. The following IT Security standards also serve as a baseline for defining security controls. ISO 17799 (Information Technology -- Code of practice for information security management.) is a starting point for developing policies, ISO 13335 (Information Technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security) assists with developing baseline security.

Organizations must implement appropriate IT Governance (Jochum, 2006) in order to provide a controlled IT framework to the business processes. The common information control models used by organizations are like CobiT (by ISACA and ITGI), BS7799 (by BSI, IEC), ISO 27001 (by IEC, ISO), ITIL (by OGC) and COSO. (Önal, 2008). *Mehmet Zeki Onal* had also listed the following control objectives for IT risks in banking.

a) *Internal fraud*: user account and identity management, logging mechanism

b) *External fraud*: personnel security, physical security, network security, trusted and secure data exchange

c) *Employment practices and workplace safety*: staffing, staff evaluation and training

d) *Clients, products and business practices*: IT models, delivery, resource management, database management, data classification and data confidentiality

e) *Damage to physical assets*: site facilities, offsite storage/ backups, access to physical assets, sensitive documents, document/ data disposal

f) *Business disruption and system failures*: disaster recovery plan, business continuity plan, configuration, infrastructure, problem and change management, backup and recovery, deployment

g) *Execution, delivery & process management*: data integrity, data processing, reporting.

RBI in its *standardised checklist for IS Audit* (Committe on Computer Audit, RBI, 2001), provided a list of items to be considered during computer audit. This included the need for controls like, policies and procedures, proven software development processes, physical access controls, application level controls and network management controls. Also, RBI on its *guidelines on information security, electronic banking, technology risk management and cyber frauds* (RBI , 2013) enumerated the controls like Information Technology governance, information security, IT operations, IS Audit, business continuity planning, customer education and legal issues, which is a main source of IT risk management constructs for this research study.

RBI has the following groups on IS Security:-

a) Internet banking committee (important security issues on internet banking and audit)

b) Working group for Information System Security for the Banking and Financial Sector (Checklists for IS audit)

c) Working Group on Information Security (Recommendations on information security systems in banks)

d) Department of Banking Supervision (Guidelines on information security, electronic banking, technology risk management and cyber frauds).

The risk control matrix and risk assessment questionnaires from various banks and other institutions also helped in preparing a check list of IT risk controls. (Habib Bank AG Zurich, 2010), (RBI, 1998).

Based on the above literature reviews ((Solarwinds, 2013), (Swanson, 2001), (NIST SP 800-30, 2002), (Önal, 2008), (Committe on Computer Audit, RBI, 2001), (Monetary Authority of Singapore, 2002) (BCBS, 2011) (RBI , 2013)) for IT risk management controls and also based expert opinions, the following nine first level constructs were identified as Information Technology risk management controls to be evaluated in banks. Microsoft also provides a check list of organizational, operational and technological controls which are preventive, detection and management controls in its Security Risk Management Guide (Microsoft, 2006).

Based on NIST SP 800-30 guidelines (NIST SP 800-30, 2002), the following nine categories of IT risk management control objectives were formulated and discussed in Table 2.2;

**Table 2.2: Checklist of operational risk management controls**

| No | Control Level 1 | Control Level 2 |
|---|---|---|
| **1** | Policies and procedures | IT Security Policies and Procedures |
| **2** | Data security | Encryption for storage and transfer |
| | | Proper disposal of media/storage/data |
| **3** | Access control and authentication | User Access Control |
| | | Authentication |
| | | Multi-factor authentication |
| | | Multi-Stage Transaction Processing |
| **4** | System logs and audit | System Logs |
| | | Audit Entries |
| | | Internal Audit |
| | | Reconciliations |
| **5** | Backup and recovery | Backup |
| | | Disaster Recovery |
| | | Business Continuity Planning |
| | | Incident Response System |
| **6** | Monitoring systems | Transaction Monitors |
| | | Intrusion Detection and Prevention Systems |
| | | Protection Software |
| | | Log monitors/review |
| **7** | Software development and deployment | Standardised Development Process |
| | | Source Code Management |
| | | Centralized Controls |
| **8** | Physical security | Physical Security |
| | | Redundancy |
| | | Environmental Controls |
| **9** | Network security | Network Security |
| | | Access Restrictions |

Source: NIST SP 800-30, 2002

The National Institute of Standards and Technology (NIST) provides a foundation for the development of a risk management program and is particularly prevalent in the government sector. Their *Risk Management Guide for Information Technology Systems* (NIST SP 800-30, 2002) is considered the seminal work in this area. It is credited with establishing widely accepted definitions of key risk terms. This document is primarily a guidance document, though, geared towards informing risk managers about the key concepts needed for risk management at a high level.

### 2.3.3 IT Risk Impacts Check List

The financial impacts of Information Technology risks are quite obvious. Recent IBM global study on the economic impact of IT risks also reveals the top IT threats to reputation and quantifies the cost of IT events that disrupt business. Legal or compliance risks may cause an organization to loose its license to operate legally, thus affecting its business continuity. Sometimes, legal disputes may also incur huge penalties which in turn may affect the performance and/or share value of the company itself (PWC, 2013). So the major impacts of IT risk considered for this study are listed below.

i) Financial Loses: impact of IT risks on capital and earnings

ii) Non-Financial Losses:

IT risk can also cause other risks or losses to happen. Operational events (especially internal fraud events) can produce reputational effects on the financial institution which can also cause an abnormal depreciation of stock prices (Marco & Giovanni, 2008).

Protecting a firm's reputation is the most important and difficult task facing senior risk managers. In a survey of 20 companies, reputational risk emerged as the most significant threat to business out of various choices of categories of risk. (Mercy, 2011). "Reputation risk is risk of indirect loss (current or prospective) arising from one or multiple stake holder's adverse experience while dealing with the institution or which resulted in an adverse perception of the institution (as a standalone entity or as a part of major corporate group)."

Basel defined legal risk as follows. The risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities (Basel, 2005).

a) Operational/Security Losses (NIST SP 800-30, 2002)
   i. Confidentiality
   ii. Integrity
   iii. Availability
b) Compliance related losses (BCBS, 2003)
c) Loss of Reputation (BCBS, 2003), (Martina, 2014)
d) Loss of Business (Martina, 2014).

## 2.4 Review of Studies on IT Risk, IT Risk Management & Impacts

IT assets are exposed to risk of damage or losses. IT security involves protecting information stored electronically. That protection implies data integrity, availability and confidentiality. Nowadays, there are many types

of computer crimes: money theft 44%, damage of software 16%, theft of information 16%, alteration of data 12%, theft of services 10%, trespass 2% (Boran, 2003).

Statistics quoted in a recent report by the Association of Certified Fraud Examiners' titled "*Report to the Nation on Occupational Fraud and Abuse"* (ACFE, 2012) may have some answers. The report has estimated that a typical organization loses 5% of its revenues to fraud each year and cumulative annual fraud loss globally during 2011 could have been of the order of more than $3.5 trillion. The amount involved in the frauds reported by the banking sector in India has more than quadrupled from Rs. 2038 crore during 2009-10 to Rs. 8646 crore during 2012-13.

A comparative picture of total number of fraud cases and amount involved as on March 31, 2013 for scheduled commercial banks, NBFCs, Urban Cooperative banks, and Financial Institutions is as under: (Chakrabarty, 2013) is shown in Table 2.3.

**Table 2.3: Number of Fraud Cases Reported by RBI Regulated Entities**

| **(No. of cases in absolute terms and amount involved in Rs. crore) Category** | **No. of Cases** | **Amount Involved (crores)** |
|---|---|---|
| Commercial Banks | 169190 | 29910.12 |
| NBFCs | 935 | 154.78 |
| UCBs | 6345 | 1057.03 |
| FIs | 77 | 279.08 |
| **TOTAL** | **176547** | **31401.01** |

Source: Conference Proceedings on National Conference on Financial Fraud, Jul, 2013

Table 2.4, shows the number of fraud causes reported and the amount involved bank group wise. (Chakrabarty, 2013).

**Table 2.4: Number of Fraud Cases Reported by RBI Bank Group Wise**

| Bank Group | No. of cases | % to Total Cases | Amount Involved | % to Total Amount |
|---|---|---|---|---|
| Nationalised Banks including SBI Group | 29653 | 17.53 | 24828.01 | 83.01 |
| Old Pvt. Sector Banks | 2271 | 1.34 | 1707.71 | 5.71 |
| New Pvt. Sector Banks | 91060 | 53.82 | 2140.48 | 7.16 |
| Sub Total (Private Banks) | 93331 | 55.16 | 3848.19 | 12.87 |
| Foreign Banks | 46206 | 27.31 | 1233.92 | 4.12 |
| **Total** | **169190** | **100** | **29910.12** | **100** |

Source: Conference Proceedings on National Conference on Financial Fraud, Jul, 2013

Table 2.5, shows the technology related number of fraud causes reported and the amount involved bank group wise during the period from 2009 to 2013 (Chakrabarty, 2013).

**Table 2.5: Bank Group Wise Technology Related Frauds**

| (Number of cases in absolute terms and amount involved in ₹ Crore.) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 2009-2010 | | 2010-2011 | | 2011-2012 | | 2012-2013 | | Cumulative Total (As on March 2013) | |
| **Bank Group** | **No. Of Cases** | **Amount Involved** | **No. Of Cases** | **Amount Involved** | **No. Of Cases** | **Amount Involved** | **No. Of Cases** | **Amount Involved** | **No. Of Cases** | **Amount Involved** |
| Nationalized Banks including SBI Group | 118 | 1.82 | 143 | 3.39 | 172 | 7.26 | 190 | 9.85 | 824 | 25.6 |
| Old Private Sector Banks | 9 | 0.15 | 4 | 0.46 | 9 | 0.06 | 6 | 1.09 | 55 | 2.3 |
| New Private Sector Banks | 14387 | 34.53 | 9638 | 21.41 | 6552 | 16.54 | 3408 | 33.97 | 74321 | 183.48 |
| Sub Total | **14396** | **34.68** | **9642** | **21.87** | **6561** | **16.6** | **3414** | **35.06** | **75200** | **211.38** |
| Foreign Banks | 5273 | 26.88 | 4486 | 14.77 | 3315 | 14.6 | 5161 | 22.45 | 36455 | 145.95 |
| **Grand Total** | **19787** | **63.38** | **14271** | **40.03** | **10048** | **38.46** | **8765** | **67.36** | **1E+05** | **357.33** |

Source: Conference Proceedings on National Conference on Financial Fraud, Jul, 2013

While the number of frauds reported each year is actually coming down, the amount involved is going up substantially. The increase in amount involved is largely attributable to the few large value advance related frauds that come to light each year. The small value technology related and other transactional frauds, as a proportion to the number of daily banking transactions, are very miniscule and are manageable (Chakrabarty, 2013).

The literature review showed that, various researchers have studied the interrelationship of IT risks and the IT risk management methods in specific technology domains like internet banking, eCommerce etc. These studies were focused on specific products, it's risks and risk management methods used to control those risks. This thesis is intended for the study of IT risk categories specified by RBI as per Basel guidelines and the IT risk management controls used by Indian banks and its impact on financial and non-financial assets.

There are studies linking Information Technology risks and risk management in specific areas like Mobile Banking, Internet Banking, SMS Banking, etc. For example, there were studies like, Managing the Risk of Mobile Banking Technologies (Banable Frontier Associates, 2008). Some studies focused on risk management in banking as whole in their studies (Kanchu & Manoj Kumar, 2013). There were comparison studies which linked the risk management between different groups of banks (The Journal of Risk Finance, 1999). The study of risk management in commercial banks was another case study between public and private sector banks (Arunkumar & Kotreshwar, 2006).

COBIT had done case studies on IT risk management in banks. This case study was a real-life example of using COBIT® for IT risk management within a global bank. COBIT was used effectively for managing risk within the technology teams to ensure that appropriate IT governance and IT assurance processes were utilised throughout the bank (Barve, 2013).

A review of studies on IT risk, risk management and impacts showed that there were no detailed study done in an Indian context, linking the various factors of IT risk, IT risk management and its impacts. Hence, this thesis work is a study of these three factors and it's inter relationships.

## 2.5 Observations from the Literature Review

Deregulation and globalisation of financial services, together with the growing sophistication of financial technology, are making the activities of banks and thus their profiles more complex. Evolving banking practices suggest that risks other than credit risks and market risks can be substantial. Examples of these new and growing risks faced by banks include: highly automated technologies, emergence of e-Commerce, large volumes handled, outsourcing, acquisitions and mergers (RBI, 2005).

The organizations are increasingly exposed to various operational risks related to the use of IT, since IT is now intrinsic to and pervasive within enterprises (ISACA, 2007), e.g. virus attacks, unauthorized access to data, breakdown of infrastructure, system and infrastructure contingency, performance problems. In order to prevent such risks efficiently, the banks are forced to identify, analyze and evaluate potential IT related operational

risks. They should implement appropriate IT Governance (Jochum, 2006) in order to provide a controlled IT framework to the business processes since IT Governance enables an organization to attain three vital objectives: regulatory and legal compliance, operational excellence, and risk optimization.

Since Basel II requires a supervisory review process including the assessment of the control environment, it was also required that supervisors should consider the quality of the bank's management information reporting and systems, the manner in which business risks and activities are aggregated, and the management's record in responding to emerging or changing risks (Basel Committee, 2004). In addition, Basel II requires that banks should have clear and effective policies, procedures, and information systems to monitor compliance (Basel Committee, 2004), that supervisors should develop detailed review procedures to ensure that banks' systems and controls are adequate to serve (Basel Committee, 2004), and that management must also ensure, on an ongoing basis, that the rating system is operating properly (Basel Committee, 2004). These requirements shows that the banks should have a sound ORM structure, and IT related operational risks should be covered in a comprehensive way. In addition to Basel II itself, ITGI published the document entitled "Information Technology Control Objectives for Basel II" in October 2007 (ITGI, 2007b). (ITGI, 2007b) which was taking the proactive step of addressing risk in financial service organizations considering that information risk and Information Technology have become decisive factors in shaping modern business, and many financial service organizations have undergone a fundamental

transformation in terms of IT infrastructures, applications, and IT related internal controls. Since IT related components such as applications, infrastructure elements and controls are all defined as parts of operational risk, (ITGI, 2007b) maps Basel II principles for operational risk against Information Technology risk.

Operational risk is by far the most extensive risk category and therefore demands the most general approach (Marshall, 2001), (Hussain, 2000). Thus operational risks consist of threats coming from factors such as people, processes and internal systems, as well as external events. Unlike market and credit risk, the data concerning operational risk is difficult to grasp. A lot of the data is instead qualitative and subjective while credit risk and market risk data is more quantitative related (Marshall & Haffes, 2003). Information Technology includes risks on different levels and since it is constantly evolving it does not provide a complete coverage of all those risks. Further, the information systems and transfers are not totally reliable. Errors can easily appear in unstable environments and any missing information is a source of risk. There are many potential causes for deficiencies. Broadly, information might be improperly disclosed, modified in an inappropriate way or destroyed or lost (Vilhelm & Frida, 2004). Any deficiency in information risk management potentially generates losses of an unknown magnitude. Given the information- and knowledge-intense characteristics of the modern world, there is no surprise that information risks and security is a growing concern among most companies and the managing of these risks are therefore increasing in significance (Bessis, 1998 ).

Global survey found that large banks and other financial institutions are suffering multimillion-dollar losses as a result of poor risk management. For example, a survey by Risk Waters Group and SAS found that one of five financial companies still did not had an information risk management program, yet 90% of these companies lost more than $10 million a year because of poor risk control practices. The losses could be caused by transaction error or fraud, system failures and resulting downtime as well as by inefficiencies or mismatching of transactions (Marshall & Haffes, 2003); (Computergram Weekly, 2003).

Information Technology systems have become critical to every aspect of business, resulting in a fact that IT risk, once a minor component of operational risk, is emerging as a major hazard for organisations to identify and manage. IT risk includes security, availability, performance and compliance elements, each with its own origins (Ans, 2008). Ans Savic classified IT risks based on their impact on the organization.

Mehmet Zeki Onal in his study (Önal, 2008) of the various ORM related to IT risks and listed an aggregated Information Technology check list for operational risk management. The study sheds light into various control objectives recommended by various institutions and regulatory authorities for the management of IT risks. In addition to Basel II itself, ITGI published the document entitled "Information Technology Control Objectives for Basel II" in October 2007 (ITGI, 2007b). ITGI (2007b) is taking the proactive step of addressing risk in financial service organizations considering that information risk and Information Technology have become decisive factors in shaping modern business, and

many financial service organizations have undergone a fundamental transformation in terms of IT infrastructures, applications, and IT related internal controls. Since IT related components such as applications, infrastructure elements and controls are all defined as parts of operational risk, ITGI (2007b) maps Basel II principles for operational risk against Information Technology risk.

A research on the banking sector (Hood & Yang, 1998) studied the impact of banking information systems security on banking in China. The aim of that research is to study the information systems security in the Chinese banking industry in comparison with the UK, so as to suggest changes that need to be made, as Chinese banking is transformed to become more market-oriented.

The CAIS security check-list included security controls elements under the following ten main security control groups: namely organisational information security controls, hardware and physical access security controls, software and electronic access security controls, data and data integrity security controls, off-line programs and data security controls, utility security controls, bypassing of normal access security controls, user programming security controls, division of duties; and output security controls (Ahmad & Abu-Musa, 2004).

Anand Singh in his thesis Improving Information Security Risk Management (Anand, 2009) studied the various IT risk controls objects used by NIST, COBIT, etc. A study by Semantec Corporation during Feb 2007 examined IT risk, along with the technology and process controls used to mitigate it, in a year-long study based on in-depth structured

interviews with more than 500 IT professionals around the world. The study identified substantial differences in the ways IT operational personnel and executives view their IT risk exposure, and examined these in detail. (Semantec, 2007). While acknowledging the relevance of Risk Management to IT, organizations often struggle to put its principles into practice. Participants' ratings of their organizations' effectiveness deploying processes and technologies for IT Risk Management depend not only on their organizations' industry, size, range of operation and other demographic factors, but on the differing perceptions of professionals within the organizations. Semantec had also identified eight technology and eight process controls that represent best practices for managing IT Risk in this study.

Homolaya Daniel in his thesis 'operational risks and firm size' (Homolya, 2011), studied in detail about the Hungarian banking system for operational risks and the risk losses based on the bank size. Another study by Dr. Yogieta S. Mehra (Yogieta, 2011), University of Delhi, aimed to explore the range of practices used by Indian banks in the management of operational risk essential for achievement of Advanced Measurement Approach (hereafter referred to as AMA) for a *cross –section of Indian Banks* and perform a comparative analysis with AMA compliant banks worldwide. The study also analyses the impact of size and ownership of banks on the range of operational risk management practices used by the banks.

Laker (Laker, 2006) argues that greater complexity of banking activity and increasing dependence on technology and specialist skills has

made operational risk as one of the most important risk facing banking institutions of which outsourcing and technology risk are two major sources of operational risk. (Davis, 2009) observed that the September 11 terrorist attacks changed the debate around operational risk. It had an impact on firms' operations, as well as economic and regulatory fallout, it raised questions about business continuity, financial crime and processing automation.

A study conducted by (Edin & Sejfudin, 2013) on the Perception of Information Security of Management of Banking and Insurance Companies in Countries of Western Balkans stated that there is a big gap in the perception of IT risk management managers and auditors.

Pavel and Simona (Pavel & Simona, 2013) has stated on the implications of the operational risk practices applied in the banking sector on the information system area. The work presents the risks within banking industry as described by the Basel Committee on Banking Supervision and tries to capture the relevance and implications of the recommended practices for the management and supervision of operational risk upon the information systems area.

Operational and Technology Risk identification and measurement is still in evolutionary stage as compared to the maturity that market and credit risk measurements have achieved. The Basel Committee requires the banking institutions to implement a framework to manage the operational risk. An effective risk management is facilitated by an organization wide risk philosophy, materialized in a set of strategies, processes, enablers and tools used in the business. Through operational risk management, the

organization identifies the inherent operational risks, treats them in accordance with its business objectives and monitors the residual risk (Pavel & Simona, 2013).

In financial services organizations, the degree of automation is usually high, while the human intervention low. Banks depend on Information Technology and information management, complex infrastructure and applications, thus controls are required to support the business processes. Furthermore, the information used by financial institution is often entirely IT generated, managed and controlled, therefore the confidentiality, availability and reliability of financial information is crucial. Having this in our mind, it is said that the risks introduced by the use of information systems play a significant role in the operational risk. (Pavel & Simona, 2013).

The study conducted by (Roopadarshini & Shilpa, 2014) describes and analyse the impact of IT innovation in banking and also to analyse the impact of banking technologies. Another study conducted by Sartaj to assess and analyse the present framework and management practices of J&K Bank Ltd towards operational risk (Sartaj, 2013) provided the following results. "As per the research results, various objectives of operational risk management identified as highly significant are not in line with the present state of affairs of the operational risk management framework of the bank". "Technology and infrastructure deficiencies, lack of skilled or professionally qualified people, i.e. lack of proper awareness and education about operational risk represent the significant hurdles in the operational risk management framework development, particularly operational risk loss database of the bank".

While considering the non-financial impacts of the IT risks, the study by (Mercy, 2011) covers the concepts of how reputation risk is identified, measured, managed and resolved, if any events takes place. Another study by Infosys, (Infosys, 2012) considers reputation or goodwill, that invaluable asset of the banking industry, is also probably its most fragile one. Reputation risk or the risk of loss of reputation is also called "risk of risks", as it often comes on the heels of other risks in banking, but differs from them in that it is intangible and hard to measure. Unfortunately, most banks view the risk of reputation loss as a standalone problem, failing to recognize that all other risks, namely credit, market, operational, liquidity etc., feed into it. For instance, the operational risk of data theft by employees, the credit risk associated with heavy lending exposure to a single industry, the market risk inherent in instruments like credit swaps or stocks, can all snowball to hit banks' hard-built reputation (Infosys, 2012).

Growing number of high-profile operational loss events worldwide have led banks and supervisors to increasingly view operational risk management as an integral part of the risk management activity. Management of specific operational risks is not a new practice; it has always been important for banks to try to prevent fraud, maintain the integrity of internal controls, reduce errors in transaction processing, and so on. However, what is relatively new is the view of operational risk management as a comprehensive practice comparable to the management of credit and market risk. 'Management' of operational risk is taken to mean the 'identification, assessment, and / or measurement, monitoring and control / mitigation' of this risk (RBI, 2005).

## 2.6 Motivations for the Research Work.

Information Technology risks and it's management are very critical for banks as any single incidence can even cause them to lose the trust and confidence of customers earned through several years. The RBI (Reserve Bank of India) guidelines on Information Security (RBI, 2013) and the Basel II/III guidelines on Operational Risk Management (ORM) provide high level of flexibility for individual banks on implementing proper IT risk management practices to identify, control and monitor IT risks and reduce the impacts to minimum.

BCBS (Basel Committee on Banking Supervision) recommends there approaches to measure and report operational risks in banks. Basic Indicator Approach (based on annual revenue of the financial institution), Standardized Approach (based on annual revenue of each of the broad business lines of the financial institution) and Advanced Measurement Approach (based on the internally developed risk measurement framework of the bank adhering to the standards prescribed (methods include IMA, LDA, Scenario-based, Scorecard etc.). Most of the banks in India are still using BIA or SA. Basel recommendations contains no treatment for nonfinancial impacts like reputational risk, business risk, etc. Based on the size, sophistication, areas of business operations, systems and technologies used, geographical spread, outsourcing etc. each bank is exposed to a different IT risk profile. And hence, the IT risk management controls employed could also be different.

Literature review also shows that, there is not enough studies conducted in the Indian context linking IT risks, IT risk management and

the impacts on assets in banks. Most of the studies in these domains have been done in developed countries and have come out with generalized conclusions on specific aspects of technology or business line. Some studies have focussed on IT security risks on internet banking, some others have on SMS banking and ATM banking. The studies linking the IT risks and IT risk management as per Basel and RBI guidelines is rarely done in Indian banking context. All these point to the need for more studies to be able to generalize across varying socio-economic contexts and also develop insights into the IT risk-IT risk management-impact models in different contexts.

## 2.7 Hypothesis Development

The previous sections of this chapter have already presented a detailed review of the IT risk and risk management literature. Various studies on IT risk and IT risk management practices have reported the financial and some of the non-financial impacts separately or collectively.

Researchers have studied the different types of IT risks and its impacts in different industries separately. Study of different type of IT security related risks (Boran, 2003) has shown the different types of computer crimes: money theft 44%, damage of software 16%, theft of information 16%, alteration of data 12%, theft of services 10%, trespass 2%. Report by Association of Certified Fraud Examiners (ACFE, 2012), has estimated that a typical organization loses 5% of its revenues to fraud each year and cumulative annual fraud loss globally during 2011 could have been of the order of more than $3.5 trillion. The amount involved in the frauds reported by the banking sector in India has more than

quadrupled from Rs. 2038 crore during 2009-10 to Rs. 8646 crore during 2012-13. A comparative picture of the total number of fraud cases and the amount involved as on March 31 2013, when reported by RBI (Chakrabarty, 2013), was in the order of Rs 31401 crores. The report had also shown that technology related losses in the Indian banks, was almost doubled from 2012 to 2013. A bank type wise (private, public, foreign, UCBs, FIs and NBFCs) technology related fraud cases report (Chakrabarty, 2013), had also shown that there was significant difference in the number of fraud incidents and the total losses incurred by banks.

Several studies were also done on the risk management aspects, considering the various risks of banks as a whole or separately. The study on 'Risk of Mobile Banking Technologies' by (Banable Frontier Associates, 2008) studies the risk of using a particular channel (mobile) for transacting with banks, while the study 'Risk Management in Banking Sector – An empirical Study' (Kanchu & Manoj Kumar, 2013), focused on risk management in banking as a whole. COBIT studies on IT risk management in banks, verified thatwhen COBIT was used effectively for managing risk within the technology teams to ensure that appropriate IT governance and IT assurance processes were utilized throughout the bank (Barve, 2013).

The report on 'Management of Non-Financial Risks' by Bank for International Settlements (Central Bank Governance Group, 2009) focuses on the opportunities available to central banks to enhance, and thus gain more benefits from, their management of non - financial risks, like operational risks, policy risk, reputational risk, etc. Damage to reputation and/or brand has moved up to No. 4 from No. 6 among the Top 10 risks

identified in Aon's 2011 Global Risk Management Risk Ranking. Reputation risk, perhaps it is of greater significance and importance to banks due to the fact that banks deal more with others' (other than owners') money, be it that of depositors, customers, counterparties, investors, among others. This paper (Sumit, 2013) makes an attempt to understand the gamut of reputational risks and understand the challenges, opportunities and possible responses from banks towards this new risk.

A study of impact of technology (mobile devices) on information security on IT professionals (Dimensional Research, 2013) revealed that, securing corporation information, including customer information is a challenge and the related security incidents are very expensive. These incidents and the impacts of such greater security risk than reported to be worse than cybercriminals. The costs and consequences of non-compliance too within financial services firms are greater than ever before. Other than monitory fines, organization may fire senior managers, may experience expensive and disruptive operational consequences and customer distrusts (Stacey & Susannah, 2013).

Based on the literature analysis and previous studies considering the factors of IT risks, IT risk management and its impacts, suitable hypotheses were for formulated and is tested in the respective chapters.

## 2.8 Conclusion

The chapter has reviewed previous research studies on Information Technology risk, Information Technology risk management methods and how it impacts a bank financial assets and non-financial assets. The literature

still lacks a comprehensive and validated study linking IT risk, risk management and its impacts. Also no major studies on these constructs are reported from India. The motivation for the present research is derived from these limitations.

.....ꕥ.....

# Chapter 3

# METHODOLOGY AND INSTRUMENT DEVELOPMENT

Contents



## 3.1 Introduction

Banks all over the world are facing increased risks due to Information Technology adoption. The Basel Committee for International Banking Supervision (BCBS), considers IT risks under the category of 'Operational Risk'. Basel Committee, Central Banks & IT experts in the area recommend that risk associated with Information Technology and systems be identified and managed properly so as to reduce both financial and non-financial impacts to the banks.

IT risk and IT risk management are two important constructs for both researchers and practitioners in the area of software development. Any risk

assessment involves identifying, analyzing and prioritizing the risk items that are likely to cause losses and the risk management involves managing these risk items so as to eliminate or control them.

Most of the past research has taken independent views of IT risk and risk management. The combined impact of risk and risk management on the financial and non-financial losses were rarely studied. No major studies on this topic were reported from India. The need was felt for more studies in order to generalize the findings of risk research across varying socio-economic contexts, and also to develop insights into the IT risk, risk management and its impacts on banks.

Literature survey and experience in the field of financial systems and banking has shown potential gaps in technology risk management in banking industry. The growing concerns on fraud, errors, identity thefts, disclosures, service disruptions and legal requirements, combined with the lack of sufficient knowledge and expertise at the bank level to identify and manage potential technology risks have prompted this study and the development of a model for technology risk assessment in banking. The study also aims to find out the effectiveness of Information Technology risk management methods practiced in Indian banks.

## 3.2 Research Methodology

The following sections details the methodology used for conducting the research and the various activities carried out for the collection of the relevant data.

The course study was descriptive in nature. A descriptive study is a fact-finding investigation with adequate interpretation. This study was initiated by reviewing the available literature in the arenas of Information Technology risk, risk management and its financial and nonfinancial impacts in banking industry. The relevant literature detailing the various dimensions of Information Technology risk, risk management and its impacts in Indian banking industry were critically reviewed. The scholarly interactions with practising professionals from the banking industry and Information Technology domain were highly beneficial. Based on the knowledge gained from the review of literature and the feedback from the IT and bank professionals, appropriate tools for data collection and analysis have been adopted and, suitably modified for the purpose of the study, in line with the derived objectives. The initial version of the instrument was reviewed for the content validity by four Information Technology specialists and four other banking domain experts. The instrument was also checked for its content validity, non-intrusiveness and further modified accordingly.

The questionnaire was then administered to the senior managers of all the eighty six banks (public, private and foreign) in India, with sufficient knowledge of Information Technology and Basel II operational risk management in the Bank. The data collection activity was extended for a year. The researcher also collected data from co-operative sector banks in Kerala, which implemented core-banking system in their bank, for a comparative study. The data collected was analysed using appropriate statistical tools. The theoretical and practical knowledge gained from the research was used to

bring out the inferences in line with the objectives of the study. The various phases of methodology followed is show in Fig 3.1.

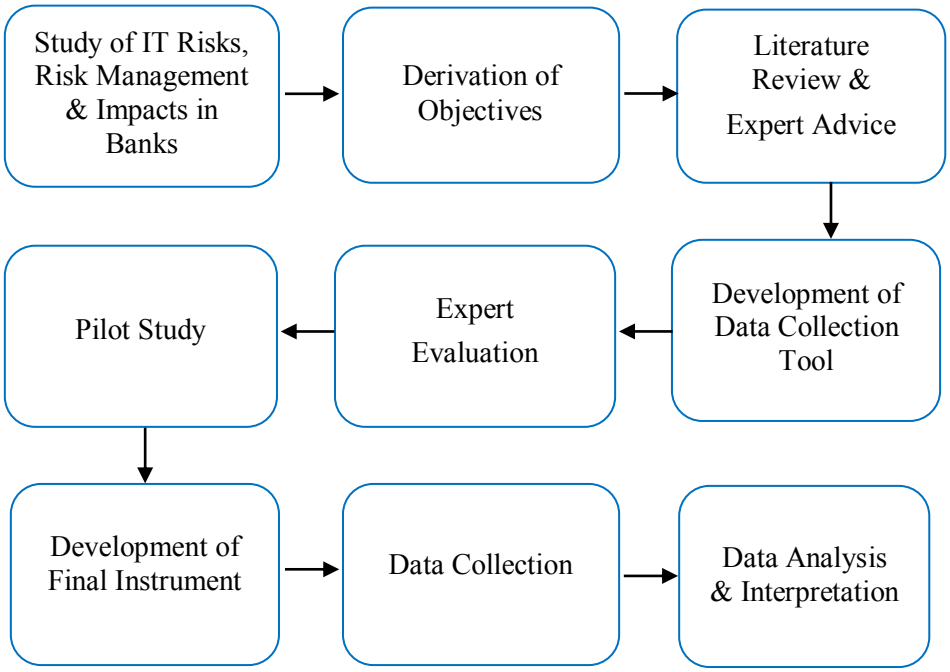



**Figure 3.1: Various phases of the methodology followed in the study.**

## 3.3 Research Design

This research provides background information and a relatively detailed description with an accurate picture about the IT risk, IT risk management practices and the risk impacts in the Indian banks. As the research questions indicate, the study was primarily descriptive in nature. The purpose of this study was to present and establish the current position of the IT risk, IT risk management practices and its financial and non-financial impacts and to further suggest ways and means for establishing effective risk management and controls to reduce the impacts. In order to

identify the cause-and-effect relationships, between IT risks, IT risk management and its impacts, causal design was also used.

## 3.4 Research Approach

A survey research using a structured questionnaire was adopted in this study. The data was collected from the bank professionals who are directly responsible for Basel II risk management activities and reporting.

## 3.5 Population of the Study

All the public, private and foreign banks in India constituted the population of the study. Hence, the 26 public sector banks, 20 private sector banks and 40 foreign sector banks in India were considered for the study. In addition to these Indian banks, there were other co-operative sector banks in India, where core banking system was implemented and also came under RBI and Basel guidelines. So, for a comparative study, all district cooperative banks (7) and urban cooperative banks (17) in Kerala which had implemented CBS (core banking systems) were also considered for this study.

## 3.6 Unit of Study

The respondents of the study were the public sector, private sector and foreign banks in India. The Table 3.1 provides details about the population in this research. There were total of 86 scheduled commercial banks (RBI List of Banks, 2013) out of which public sector banks are 26 (SBI and associates - 6, Nationalized banks - 20), private sector banks were 20 (Old - 13 and New - 7) and foreign banks were 40. The cooperative sector banks in Kerala which implemented CBS were 20.

**Table 3.1: Banks in India**

| Sl No | Bank Type | Number Of Banks |
|---|---|---|
| 01 | Public Sector (SBI Associates and Nationalized Banks) | 26 |
| 02 | Private Sector Banks (Old and New) | 20 |
| 03 | Foreign Banks | 40 |
| 04 | Cooperative Sector Banks in Kerala (with CBS implemented) | 26 |
| | Total | 112 |

Source: RBI & NABARD website

## 3.7 Sampling Method

The study reported in this thesis was contemplated as a form of census and the original proposal was to include all the banks in the public, private and foreign sectors in India. However, some of the banks refused to divulge information regarding the information security management of their bank. Out of the 112 banks, complete information was received from 53 willing banks. 59 banks refused to respond to the request in providing relevant information.

Hence, the researcher considered the universe to be consisting of all banks, which were ready to divulge and share information about the IT risk management practices of their bank. In this context, the 53 banks that were willing to share information constitute the universe. Therefore, the practical analysis was reduced to the analysis of 53 banks instead of 112 banks, due to non-response, limiting the study to a reduced size of the population.

Naturally, the research should address, the question of whether the results of the study would have been the same, if a 100% response rate had

been achieved. In spite of approaching all the items in the universe, only 53 banks were willing to divulge information. The results could be inclusive of a certain degree of error. These kinds of errors are called coverage errors, which is an accepted type of error, in census studies. The other type of errors are non-response errors, response errors and processing errors.

High level efforts were taken to eliminate response and non-response errors. To control processing errors, efforts were taken to use valid software directed by logical requirements. However, coverage error, ie the error that occurs when items are missed for some reason in the study, could be eliminated. When the universe is very large, there are accepted methods for balancing the final result for non-inclusion, if items like vacancy check, reverse record check and over coverage study exists. Since the universe was too small in this study, there was no scope for validation using these accepted procedures.

In this study, as stated earlier, there was a possibility of coverage error. The situation is best explained in the following lines. There are only 112 banks in the population. Information on technology risk management could be obtained only from 53 out of 112 banks. The reason for not getting the information from some of the banks was a matter of policy of those banks. Such banks do not allow sensitive information being shared even for research purposes. Thus, this study has been limited to the responding banks and the results obtained have been true with respect to these 53 banks as the universe. In that case, the results need no statistical validation since the study turns out to be like a census study.

An effort was taken to ensure that the results are more acceptable with a better level of generality. This effort started with a basic question, whether the 53 responses could be considered as responses from a random sample of 112 banks from a population of 112 banks using the available information about the non-responding banks. A break up of the responding and non-responding banks is shown in Table 3.2.

**Table 3.2: Responded and Non-Responded Banks**

| Type of Bank | Total No of Banks | No of Banks Responded | Percentage of response | No of Non Responding Banks | Percentage of Non-responding banks |
|---|---|---|---|---|---|
| Public Sector Banks | 26 | 11 | 42.3 | 15 | 57.7 |
| Private Sector Banks | 20 | 13 | 65.0 | 7 | 35.0 |
| Foreign Banks | 40 | 15 | 37.5 | 25 | 62.5 |
| Cooperative Banks | 26 | 14 | 53.84 | 12 | 46.15 |

Source: Survey Data

From the table 3.2, it shows that 42.3 percent of the public sector banks and 65 percent of the private sector banks, 37.5 percent of the foreign sector banks and 53.8 percent of the cooperative sector banks responded to the study. The average rate of response for these different types of bank is 49.66 percent.

This situation results in a possible coverage error, while considering it as a census study. At the same time, this cannot be treated as a random sample in a strict sense of random sampling. Assuming that the different

kinds of risk problems are almost similar for every bank in modern times, the study can be preceded, after establishing a correspondence between the responding and non-responding banks.

For the available and usable data based on the general information provided by the banks, it is concluded that the size of the bank in terms of the number of branches is a useful variable to study the correspondence between responding and non-responding banks. The number of branches of the two sets of banks, responding (32854) and non-responding (55708), represented in Table 3.3 reveals the following characteristics.

**Table 3.3: Branches of Responded and Non Responded Banks**

| Group Statistics | | | | | |
|---|---|---|---|---|---|
| | **Bank Type** | **N** | **Mean** | **Std. Deviation** | **Std. Error Mean** |
| No of Branches | Non Responded Banks | 59 | 644.2157 | 1108.18883 | 155.17748 |
| | Responded Banks | 53 | 1428.4103 | 2592.91911 | 415.19935 |

Source: RBI Site & Bank Websites

Considering these two groups as two samples (using random-effect concept), a t-test has been carried out to observe whether there exists any difference between the two sets of banks in their sizes assessed with the number of branches. A hypothesis was framed and tested using the t-test for understanding the equality of the means of the number of branches for the two types of banks as shown below.

**Ha**: Mean number of branches for responding and non-responding banks are same

**Hb**: Mean number of branches for responding and non-responding banks are not the same

The statistical results are shown in Table 3.4

**Table 3.4: Independent Samples Test**

| | | t-test for Equality of Means | | | | |
|---|---|---|---|---|---|---|
| | | **t** | **df** | **Sig. (2-tailed)** | **Mean Difference** | **Std. Error Difference** |
| No of Branches | Equal variances assumed | -1.943 | 88 | .065 | -784.19457 | 403.65899 |

Since the p-value is 0.065, (>0.05) the hypothesis was accepted. This implied that the average size of the responding and non-responding banks were the same.

Hence, the responses shall be treated as coming from a random sample of size 53 from a population of 112, as the distribution of size of responding banks and non-responding banks are seen to be equal. When we consider these responses as from a random sample, it is noted that the associated population is finite. While employing statistical techniques, care will have to be taken to apply 'Finite Population Correction'. The finite population correction will be,

$\sqrt{(N-n)/(N-1)}$ , where N is the size of the population and '**n**' is the size of the sample. This correction was applied to the statistics used for

tests, in the event of the population being finite. For example, the standard error of sample mean will be $\left(\frac{\sigma}{\sqrt{n}}\right)$ $(\sqrt{(}\frac{N-n}{N-1})$. Thus, the results obtained were validated, taking into consideration the kind of difficulties associated with this kind of studies.

Therefore, the research argument is that the study can be continued with the available data and the results can be generalized in more than one way.

a) The study with 53 banks will provide answers to the entire public, private, foreign and co-operative sector banks under the assumption that the two sets (responding and non-responding banks) of banks are the same size

b) These 53 banks can be considered as a random sample from the total 112 banks in the population and

c) Necessary corrections should be made to the summary statistics using finite population corrections

d) In addition to the scheduled commercial banks in India, co-operative sector banks in Kerala, which are directly under RBI/Basel guidelines (DCBs and UCBs) and those implemented core banking systems, are also included for a comparative study in this thesis.

Thus the primary data for the study was collected through a structured questionnaire administered to the designated officer responsible for the risk management in these banks

(Knapp, 2005) has also observed that previous researches on Information Security reported low response rates due to the intrusive nature of the subject and the respondent's unwillingness to answer. However, the present study received a good response rate of 49.66 percent, as adequate precaution was taken to ensure the active participation of the respondents. The data collection process took almost 12 months to collect relevant data from the respondents.

It is referred by some studies that SEM may not be very effective when data size is relatively small. But here the researcher don't have the luxury of increasing the sample size. However, some of the most recent studies recommend rather small sample sizes as enough for attempting SEM

Wolf, E. J., Harrington, K. M., Clark, S. L., & Miller, M. W. (2013). Sample size requirements for structural equation models an evaluation of power, bias, and solution propriety. Educational and Psychological Measurement, 73(6), 913-934. doi: 10.1177/0013164413495237

They found sample size requirements ranging from 30 (Simple CFA with four indicators and loadings around .80) up to 45 cases (mediation models).

Sideridis, G., Simos, P., Papanicolaou, A., & Fletcher, J. (2014). Using Structural Equation Modeling to Assess Functional Connectivity in the Brain Power and Sample Size Considerations. Educational and Psychological Measurement, dpi: 10.1177/0013164414525397. They found that a sample size of 50-70 would be enough for a model of functional brain connectivity involving 4 latent variables.

Muthén, L. K., & Muthén, B. O. (2002). How to use a Monte Carlo study to decide on sample size and determine power. Structural Equation Modeling, 9(4), 599-620. These references shows that, SEM can be applied with small sample sizes too and the technicalities associated with small sample size may be considered as the limitation of this study.

## 3.8 Data Sources

The study relied on both primary as well as secondary data. The primary data was collected from managers of banks with sufficient knowledge of Basel risk management guidelines and involved in operational risk management and reporting. For obtaining primary data, a structured questionnaire was designed to collect data from the managers of the bank.

The source of secondary data were drawn from Reserve Bank of India publications and Basel Committee publications. Various central bank publications and guidelines along with national and international IT security policies, procedures and standards were referenced for understanding the background of the study.

## 3.9 Research Instrument

A structured questionnaire was prepared with an objective to collect all relevant information required for meeting the research objectives. Interactions with the practicing IT experts and risk management experts in the banking domain helped in identifying some critical issues while designing the final questionnaire. The prepared questionnaire was pre-tested with a pilot study before being used for the final data collection.

Therefore, the initial focus was to develop a comprehensive questionnaire in order to capture the required data for the purpose of the study. Basel II guidelines on operational risk and risk management, RBI guidelines on information security and technology risk management and other IT security and management guidelines and policies worldwide were used to design the questionnaire. The major sections of the questionnaire are shown Table 3.5.

**Table 3.5: Sections of Questions in the Survey Instrument**

| Section | Content |
|---|---|
| Section A | Bank Characteristics |
| Section B | Technology Characteristics |
| Section C | Information Technology Risks |
| Section D | Information Technology Risk Management |
| Section E | Non-Financial Impact of Technology Risks |
| Section F | Financial Impact of Technology Risks |
| Section G | Background Information of the Respondent |

In the instrument, items on specific aspects of banks in line with the objectives of the study were also included. These items were added to get information about the type of the bank, geographical spread of the bank, size of the bank in terms of the number of branches and employees, the technological adoption level of the banks, technological characteristics and the respondents profile in terms of experience and capacity in the organizational structure. All this information was vital for the interpretation and discussion of the results.

### 3.9.1 Variables of Study

The theoretical and operational definitions of the variables in the study are given below. The scales used for measurement were either taken from published inventories or developed by the researcher. The scales were tested for their validity and reliability. The scale development process and the associated statistics are described in the subsequent sections

#### 3.9.1.1 Information Technology Risk

ISO has defined IT risk as "*the potential barrier that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence*." (ISO/IEC FIDIS, 2008). ISACA defined IT risk as "*the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise*" (ISACA, 2009). Basel considered Information Technology risks under operational risk and is defined as "*the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk*."

One of the most common methods for risk identification has been the use of risk factor checklists (Barki, et al., 1993). Since the study was focused on Indian banks, the researcher had developed a valid and reliable measure of the technology risk adopting the Basel and RBI guidelines. The tool had 26 items measuring the risks under the following sub dimensions: internal fraud, external fraud, employment practices and workplace safety, clients, products and business practices,

damage to physical assets, business disruption and system failures and execution delivery and process management (Table 3.6). The respondent had to indicate the level of presence of each risk item on a five point *Likert* scale.

**Table 3.6: IT Risk Variables**

| No | IT Risk Variables |
|---|---|
| **1** | Internal Fraud |
| **2** | External Fraud |
| **3** | Employment Practices and Workplace Safety |
| **4** | Clients, Products and Business Practices |
| **5** | Damage to Physical Assets |
| **6** | Business Disruption and System Failures |
| **7** | Execution, Delivery and Process Management |

Source: Basel & RBI guidelines

### 3.9.1.2 Information Technology Risk Management

Risk management is concerned with a phased and systematic approach to analyse and control risks occurring in a specific context (Charette, 1996). IT risk management is the application of risk management to Information Technology context in order to manage IT risks. Different methodologies have been proposed to manage IT risks, each of them divided in processes and steps (Katsicas, 2009).

The Certified Information Systems Auditor Review Manual 2006 provides the following definition of risk management: *"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the*

*organization* (ISACA, 2006). NIST risk management guide defines risk management as "*the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives*" (NIST SP 800-30, 2002).

Researcher had developed a valid and reliable measure of IT risk management drawing from the works of various researchers in this domain, regulatory guidelines and IT security standards (NIST). The scale had 25 items measuring IT risk management under the nine sub dimensions policies and procedures, data security, access control and authentication, system logs and audit, backup and recovery, monitoring systems, software development and deployment, physical security and network security (Table 3.7) . The respondent had to indicate the level of presence of each risk management item in the project on a five point *Likert* scale.

**Table 3.7: IT Risk Management Variables**

| No | IT Risk Management Variables |
|---|---|
| **1** | Policies and Procedures |
| **2** | Data Security |
| **3** | Access Control and Authentication |
| **4** | System Logs and Audit |
| **5** | Backup and Recovery |
| **6** | Monitoring Systems |
| **7** | Software Development and Deployment |
| **8** | Physical Security |
| **9** | Network Security |

Source: NIST-SP 800-30

### 3.9.1.3 Impact of IT Risks

The impacts of IT risks based on the various definitions include harm to the organization (ISO) like loss of information security, loss of reputation, non-compliance and regulatory issues, customer loss and other financial losses. These impacts and losses of IT risk are grouped into financial losses and nonfinancial losses (Table 3.8). The respondents were asked to rate these losses on a five point Likert scale. The average score on these parameters was taken as a measure of the overall effectiveness of the IT risk management controls used.

**Table 3.8: IT Risk Impacts**

| No | IT Risk Variables |
|---|---|
| **Financial Impacts** | |
| **1** | Financial Losses |
| **Non-Financial Impacts** | |
| **1** | Operational/Security Losses |
| **2** | Compliance Related Losses |
| **3** | Loss of Reputation |
| **4** | Loss of Customers/Business |

Source: RBI, NIST-SP 800-30, BCBS, PWC

### 3.9.1.4 Bank Characteristics

a) **Type of the Bank:** The type of bank was measured by checking whether the bank developed belonged to any of the following categories:- public sector, private sector, foreign bank and cooperative banks.

b) **Geographical Spread of the Bank**: The geographical spread was measured by checking whether the bank belonged to any of the following categories:- single location, multiple location -

single state, multiple location - multiple state, multiple location - multiple countries and others.

c) **Number of Branches of the Bank**: The approximate number of branches on the bank was measured using this item.

d) **Number of Customers of the Bank**: The approximate number of customers of the bank was measured here.

e) **Number of Employees of the Bank**: The approximate number of employees of the bank was measured here.

f) **Certifications of the Bank**: The certifications was measured by checking whether the bank possess any of the following category of certifications:- ISO 27001, BS7799, Basel II/III, ISO 9001:2000 and any others.

### 3.9.1.5 Technology Characteristics

a) **IS Development Methodology**: The development methodology was measured by checking whether the bank has used any of the following category:- outsourced IS development, in house developed information system, shared IS system with other banks, IS system shared with sister organizations and others.

b) **IS System Provider/Vendor** (if outsourced): The name of the outsourced vendor was entered by the respondent for this section.

c) **Level of Automation/STP**: The level of automation was measured on a three point scale with the categories as:- high, medium, low.

d) **Level of Skilled Man Power**: The level of skilled man power was measured by checking whether the bank posses any of the following category:- In house IT development team, branch level IT support team, centralised IT support team, IT support by external vendors.

e) **Frequency of IT Training to Employees**: The frequency of IT training to employees of the bank was measured directly as the numbers of times per year.

f) **Frequency of IT Training to Customers**: The frequency of IT training to end users or customers of the bank was measured directly as the numbers of times per year.

g) **Type of Software Used**: The type of software used was measured by checking whether the bank uses any of the following category of software:- open source based, Microsoft based, both open source based and Microsoft based and any other, to be specified by the respondent.

h) **Data Center Model:** The data center model used was measured by checking whether the bank uses any of the following data center model categories:- hosted with own data center, third party data center, hosted in cloud, shared data center facility and any other to be specified by the respondents.

### 3.9.1.6 Demographic Variables of the Respondent

Data was collected on the following items from the respondent:- years of service, service period with the current bank, how long is he

involved with the IT operations, designation, any IT certifications possessed by the respondent.

### 3.9.2 Instrument Development

#### 3.9.2.1 Validity and Reliability of the Instrument

Validity is defined as the extent to which any measuring instrument measures what it is intended to measure (Carmines & Zeller, 1990). Different validity terms are used to illustrate the various aspects of validity. Any research instrument should be tested for validity, so that it could be used for meaningful analysis. The initial validity tests, namely content validity and face validity were performed for the draft questionnaire as explained below.

#### 3.9.2.2 Content Validity

Content validity of an instrument refers to the degree to which it provides an adequate depiction of the conceptual domain that it is designed to cover (Hair, et al., 1998). In the case of content validity, the evidence is subjective and logical, rather than statistical. Content validity can be ensured if the items representing the various constructs of an instrument are substantiated by a comprehensive review of the relevant literature (Bohrnstedt, 1983). The instrument had been developed on the basis of a detailed review and analysis of the prescriptive, conceptual, practitioner and empirical literature, so as to ensure the content validity.

#### 3.9.2.3 Face validity

Generally, a measure is considered to have 'face validity' if the items are reasonably related to the perceived purpose of the measure (Kaplan & Scauzzo, 1993). Face validity is the subjective assessment of

the correspondence between the individual items and the concept through rating by expert judges (Hair, et al., 1998). In face validity, one looks at the measure and judges whether it seems a good translation of the construct under study. Face validity is also a subjective and logical measure, similar to content validity. The face validity can also be established through review of the instrument by experts in the field (Hair, et al., 1998).

The draft questionnaire was given to six senior software and security experts from the IT industry and four risk management experts from banking industry. They were briefed about the purpose of the study and its scope. The experts were requested to scrutinize the questionnaire and to give their impressions regarding the relevance of contents of the questionnaire. They were requested to critically examine the questionnaire, and to give objective feedback and suggestions with regard to the comprehensiveness/coverage, redundancy level, consistency and number of items in each variable. They had to suggest necessary changes by simplifying, rewording, removing, replacing and supplementing the items. Based on the feedback from experts, the researcher modified the draft questionnaire. This resulted in a new questionnaire, referred to as 'pilot questionnaire', containing 26 items under IT risk construct and 25 items under risk management construct. The project outcome questions were retained without any change.

In this study IRR is addressed in totality. Reliability analysis was done after the pilot study and after the final data collection. The reliability analysis of the pilot study is explained in section 3.9.2.5 and that of the final study is explained in section 4.3 of this thesis.

### 3.9.2.4 Convergent & Discriminant Validity

Convergent and discriminant validity are both considered as subcategories or subtypes of construct validity. Construct validity refers to the degree to which inferences can legitimately be made from the operationalizations in the study to the theoretical constructs on which those operationalizations were based.

Discriminant validity or divergent validity tests whether concepts or measurements that are not supposed to be related are, in fact, unrelated. Evidence for 'convergent validity' is obtained when a measure correlates well with other measures that are believed to measure the same construct (Kaplan and Scauzzo, 1993). In other words, convergent validity is the degree to which various approaches to construct measurements are similar to (converge on) other approaches that they theoretically should be similar to (Sureshchander et al., 2001).

The final instrument was developed after checking the essentials of the above mentioned tests and results of convergent and discriminant validity tests are furnished in Table 3.9 below.

**Table 3.9: Discriminant Validity - Information Technology Risk**

| | Average loading | Variance extracted | Variance extracted across all the factors | Correlation Matrix Average | Squared Correlation | Condition for Discriminant Validity |
|---|---|---|---|---|---|---|
| Factor 1 | 0.872 | 0.760837 | 0.808 | 0.144 | .020 | Variance extracted across all the factors > Squared correlation 0.808>0.020 |
| Factor 2 | 0.962 | 0.926397 | | | | |
| Factor 3 | 0.789 | 0.622498 | | | | |
| Factor 4 | 0.907 | 0.823297 | | | | |
| Factor 5 | 0.873 | 0.76273 | | | | |
| Factor 6 | 0.976 | 0.952315 | | | | |

Source: Pilot Study Data

All average loading are above 0.70, which indicate good convergent validity. The condition for discriminant validity is Variance extracted across all the factors should be greater than the squared correlation. In the first set of variables, Variance extracted across all the factors is greater than the squared correlation (0.808 > 0.020)

**Table 3.10: Discriminant Validity - Information Technology Risk Management**

| | Average loading | Variance extracted | Variance extracted across all the factors | Correlation Matrix Average | Squared Correlation | Condition for Discriminant Validity |
|---|---|---|---|---|---|---|
| Factor 1 | 0.860 | 0.760 | 0.723 | 0.318 | .101 | Variance extracted across all the factors > Squared correlation 0.723>0.101 |
| Factor 2 | 0.890 | 0.926 | | | | |
| Factor 3 | 0.802 | 0.622 | | | | |
| Factor 4 | 0.854 | 0.823 | | | | |
| Factor 5 | 0.921 | 0.762 | | | | |
| Factor 6 | 0.823 | 0.952 | | | | |
| Factor 7 | 0.853 | 0.727 | | | | |
| Factor 8 | 0.794 | 0.630 | | | | |
| Factor 9 | 0.808 | 0.652 | | | | |

All average loading are above 0.70, which indicate good convergent validity. The condition for discriminant validity is Variance extracted across all the factors should be greater than the squared correlation. In the first set of variables, Variance extracted across all the factors is greater than the squared correlation > 0.101)

### 3.9.2.5 Pilot Test

The pilot questionnaire was administrated to a convenient sample of 20 banks with respondents having 10+ years of experience in banking (managers and above) and familiar with IT/risk operations. The goal of this exercise was to obtain a general assessment of the instruments' appearance, to

further eliminate items that did not contribute significantly to the value of the instrument, and to understand the underlying dimensions of the constructs under study.

The data collected from the pilot group was first scrutinized to identify the no response questions. If more than 80% of the respondents did not respond to a question, it was identified as a candidate to be removed or reworded. Bank type wise and geographical spread wise respondent details are shown in Table 3.11 and 3.12 respectively.

**Table 3.11: Bank type wise respondents for the pilot study**.

| | Frequency | Percent | Actual Numbers | %Responded |
|---|---|---|---|---|
| Foreign | 5 | 25 | 40 | 12.5 |
| Private | 5 | 25 | 20 | 25.0 |
| Public Sector | 5 | 25 | 26 | 21.0 |
| Cooperative | 5 | 25 | 26 | 19.2 |
| **Total** | **20** | **100.0** | **112** | |

Source: Pilot Study Data

**Table 3.12: Geographical spread wise respondents for pilot study**

| | Frequency | Percent |
|---|---|---|
| Multiple Location, Single State | 5 | 25 |
| Multiple Location, Multiple State | 7 | 35 |
| Multiple Location, Multiple Countries | 8 | 40 |
| **Total** | **20** | **100.0** |

Source: Pilot Study Data

### 3.9.2.6 Reliability Analysis

Reliability of an instrument is defined as the extent to which any measuring instrument yields the same result on repeated trials (Carmines & Zeller, 1990). It is the degree to which the instrument yields a true score of

the variable (factor) under consideration. The instrument is not considered as reliable to the extent to which it contains measurement error (Neale & Liebert, 1986).

There are several methods to establish the reliability of a measuring instrument. These include test-retest method, equivalent forms, split-halves method and internal consistency method. Of all these methods, the internal consistency method is the most popular method, especially in field studies. The advantage of this method is that it requires only one administration, and consequently this method is considered to be the most general form of reliability estimation (Sureshchander, et al., 2001). In this method, reliability is operationalized as 'internal consistency', which is the degree of inter-correlation among the items that constitute the scale (Nunnally, 1978). The internal consistency is estimated using a reliability coefficient called Cronbach's alpha (α) (Cronbach, 1951). An alpha value of 0.70 or above is considered to be the criterion for demonstrating strong internal consistency of established scales (Nunnally, 1978).

The reliability of the instrument developed in the current study was tested by computing Cronbach alpha (α) value for each of the IT risk factors as well as for the entire set. The item-total correlation was tested for each risk item under each factor.

The final values of Cronbach alpha for the IT risk factors are presented in Table 3.13. As seen from the table, all the factors had Cronbach alpha value above 0.7, which testified the reliability of the instrument. Here in this case no statements were deleted since all have loading above 0.7 and the cronbach's Alpha is 0.909 which is relatively very high.

**Table 3.13: Results of Reliability Analysis of IT Risk**

| Reliability Statistics (Pilot Study) | |
|---|---|
| **Cronbach's Alpha** | **N of Items** |
| .909 | 26 |

| IT Risk Item-Total Statistics (Pilot Study) | | | | |
|---|---|---|---|---|
| | **Scale Mean if Item Deleted** | **Scale Variance if Item Deleted** | **Corrected Item-Total Correlation** | **Cronbach's Alpha if Item Deleted** |
| VAR00001 | 34.5000 | 143.167 | .695 | .914 |
| VAR00002 | 34.3000 | 136.900 | .664 | .912 |
| VAR00003 | 34.6000 | 148.267 | .623 | .918 |
| VAR00004 | 33.6000 | 138.711 | .505 | .917 |
| VAR00005 | 33.1000 | 141.656 | .429 | .919 |
| VAR00006 | 32.5000 | 141.611 | .480 | .917 |
| VAR00007 | 32.8000 | 125.067 | .782 | .908 |
| VAR00008 | 32.8000 | 133.956 | .619 | .914 |
| VAR00009 | 32.4000 | 128.711 | .794 | .907 |
| VAR00010 | 33.7000 | 130.678 | .593 | .916 |
| VAR00011 | 33.5000 | 132.944 | .704 | .911 |
| VAR00012 | 33.8000 | 125.511 | .812 | .906 |
| VAR00013 | 33.7000 | 129.789 | .655 | .913 |
| VAR00014 | 34.0000 | 132.000 | .826 | .907 |
| VAR00015 | 31.9000 | 146.100 | .614 | .916 |
| VAR00016 | 33.7000 | 137.711 | .504 | .916 |
| VAR00017 | 32.5000 | 141.611 | .480 | .917 |
| VAR00018 | 32.8000 | 125.067 | .782 | .908 |
| VAR00019 | 32.8000 | 133.956 | .619 | .914 |
| VAR00020 | 33.7000 | 129.789 | .655 | .913 |
| VAR00021 | 34.0000 | 132.000 | .826 | .907 |
| VAR00022 | 31.9000 | 146.100 | .614 | .916 |
| VAR00023 | 34.3000 | 136.900 | .664 | .912 |
| VAR00024 | 34.6000 | 148.267 | .623 | .918 |
| VAR00025 | 34.0000 | 132.000 | .826 | .907 |
| VAR00026 | 33.8000 | 125.511 | .812 | .906 |

Source: Survey Data

Cronbach alpha (α) values were computed for the IT risk management factors also. The results are listed in Table 3.14. No statements were excluded because of high loading and the Cronbach's alpha was reported to be 0.934 for IT risk management.

**Table 3.14: Results of Reliability Analysis of IT risk management**

| Reliability Statistics (Pilot Study) | |
|---|---|
| **Cronbach's Alpha** | **N of Items** |
| .934 | 25 |

| IT Risk Management Item-Total Statistics (Pilot Study) | | | | |
|---|---|---|---|---|
| | **Scale Mean if Item Deleted** | **Scale Variance if Item Deleted** | **Corrected Item-Total Correlation** | **Cronbach's Alpha if Item Deleted** |
| VAR00001 | 74.3000 | 226.678 | .804 | .952 |
| VAR00002 | 74.0000 | 228.444 | .793 | .952 |
| VAR00003 | 74.3000 | 220.678 | .905 | .950 |
| VAR00004 | 74.3000 | 223.344 | .838 | .951 |
| VAR00005 | 74.0000 | 246.000 | .611 | .955 |
| VAR00006 | 73.8000 | 248.178 | .593 | .955 |
| VAR00007 | 73.6000 | 256.044 | .328 | .957 |
| VAR00008 | 73.9000 | 241.656 | .758 | .953 |
| VAR00010 | 73.8000 | 247.733 | .614 | .955 |
| VAR00011 | 74.0000 | 226.222 | .853 | .951 |
| VAR00012 | 74.3000 | 232.900 | .750 | .952 |
| VAR00013 | 74.4000 | 240.933 | .615 | .954 |
| VAR00014 | 73.9000 | 232.322 | .876 | .951 |
| VAR00015 | 73.4000 | 250.711 | .812 | .955 |
| VAR00016 | 74.1000 | 228.767 | .704 | .954 |
| VAR00017 | 74.5000 | 232.944 | .856 | .951 |
| VAR00018 | 74.7000 | 228.233 | .685 | .954 |
| VAR00019 | 74.2000 | 230.622 | .638 | .955 |
| VAR00020 | 74.1000 | 231.878 | .855 | .951 |
| VAR00021 | 73.6000 | 256.044 | .328 | .957 |
| VAR00022 | 74.1000 | 228.767 | .704 | .954 |
| VAR00023 | 74.0000 | 226.222 | .853 | .951 |
| VAR00024 | 74.2000 | 230.622 | .638 | .955 |
| VAR00025 | 74.3000 | 223.344 | .838 | .951 |

Source: Survey Data

Cronbach alpha (α) values were computed for the nonfinancial impact factors also. The results are listed in Table 3.15. No statements were excluded because of high loading and the Cronbach's alpha was reported to be 0.816 for nonfinancial impact.

**Table 3.15: Results of Reliability Analysis of Financial Impacts**

| **Reliability Statistics – Nonfinancial Impact (Pilot Study)** | |
|---|---|
| **Cronbach's Alpha** | **N of Items** |
| .816 | 6 |

| **Nonfinancial Impact - Item Total Statistics (Pilot Study)** | | | | |
|---|---|---|---|---|
| | **Scale Mean if Item Deleted** | **Scale Variance if Item Deleted** | **Corrected Item-Total Correlation** | **Cronbach's Alpha if Item Deleted** |
| VAR00001 | 9.569 | 24.530 | .829 | .864 |
| VAR00002 | 9.569 | 25.370 | .771 | .873 |
| VAR00003 | 9.216 | 24.613 | .690 | .882 |
| VAR00004 | 8.961 | 22.838 | .696 | .884 |
| VAR00005 | 8.961 | 22.838 | .728 | .877 |
| VAR00006 | 9.020 | 24.500 | .668 | .885 |

Source: Survey Data

Cronbach alpha (α) values were computed for the financial impact factors also. The results are listed in Table 3.16. No statements were excluded because of high loading and the Cronbach's alpha was reported to be 0.81 for financial impact.

**Table 3.16: Results of Reliability Analysis of Nonfinancial Impacts**

| Reliability Statistics- Financial Impact (Pilot Study) | |
|---|---|
| **Cronbach's Alpha** | **N of Items** |
| .810 | 7 |

| Financial Impact – Item Total Statistics | | | | |
|---|---|---|---|---|
| | **Scale Mean if Item Deleted** | **Scale Variance if Item Deleted** | **Corrected Item-Total Correlation** | **Cronbach's Alpha if Item Deleted** |
| VAR00001 | 11.765 | 22.344 | .600 | .844 |
| VAR00002 | 11.333 | 21.387 | .555 | .847 |
| VAR00003 | 11.098 | 20.050 | .573 | .846 |
| VAR00004 | 11.627 | 22.438 | .581 | .846 |
| VAR00005 | 11.275 | 18.283 | .733 | .821 |
| VAR00006 | 10.725 | 17.643 | .700 | .829 |
| VAR00007 | 11.235 | 19.944 | .707 | .826 |

Source: Survey Data

### 3.9.2.7 Exploratory and Confirmatory Factor Analysis (EFA and CFA)

The scale used for IT Risk is based on the Basel II guidelines on Operational Risk and that for IT Risk Management is based on the guidelines provided by Reserve Bank of India (RBI) to the Banks in India. The study was intended to evaluate the risk and risk management practices based on these guidelines and the CFA and EFA was not attempted, since items cannot be eliminated.

### 3.9.2.8 Generating the Risk Scores and Risk Management Scores

The next step was to generate appropriate scores to represent these factors for further statistical analysis. There were three popular methods availables for the researcher. 1. Use one variable from the set of variables loading on to a factor as a surrogate to represent that factor. 2. Use

summated scale formed by combining all variables loading heavily onto that factor. 3. Use factor score computed by the statistical package based on the rotated factor loading matrix.

For an instrument whose validity, reliability and dimensionality have been proven, summated scales are recommended (Hair, et al., 1998) from the following considerations. (a) These scales are easily replicated across studies. (b) They are easy to interpret. (c) They represent multiple aspects of the concept under measure.

The researcher used summated scales for this study. The score was calculated for each risk factor (dimension) by taking the average of all items included under that risk factor. Similarly risk management scores were also calculated for each of the four factors of risk management by taking the average of all items included under that risk management factor.

## 3.10 Data Collection

The study reported in this thesis was contemplated as a form of census and the original proposal was to include all the banks in the public, private and foreign sectors in India. However, some of the banks refused to divulge information regarding the information security management of their bank. Out of the 112 banks, complete information was received from 53 willing banks. 59 banks refused to respond to the request in providing relevant information.

Hence, the researcher considered the universe to be consisting of all banks, which were ready to divulge and share information about the IT risk management practices of their bank. In this context, the 53 banks that were

willing to share information constitute the universe. Therefore, the practical analysis was reduced to the analysis of 53 banks instead of 112 banks, due to non-response, limiting the study to a reduced size of the population.

## 3.11 Instrument for Final Survey

The final instrument was developed from the pilot study questionnaire, incorporating all the modifications and corrections mentioned above. The respondent was asked to indicate to what extent these risk and risk management items were present in his/her bank. The respondent had to indicate the presence of each risk/risk management item on a five point Likert scale.

IT Risk impact was measured in terms of financial losses and non-financial losses. Non-financial impacts were measured for information security (confidentiality, integrity and availability), reputation, non-complaints and customer loss. The financial losses were also measured through a five point rating scale where the respondent rated the looses due to the seven IT risks namely internal fraud, external fraud, employment practices and work place safety, clients, products and business practices, damage to physical assets, business disruption and system failures, and execution, delivery and process management. The average score on these seven dimensions was taken as a measure of financial loss.

A single informant, self reporting methodology was adopted for data collection. Though this method has potential reporting bias, it is very commonly used in academic research (Pinsonneault & Kraemer, 1993) (Wallace, et al., 2004) (Barki, et al., 1993) (Deephouse, et al., 2005). Inter-

rater reliability tests and Harman's one factor tests also showed favourable results.

The important classification/demographic variables included in the instrument were:

a) **Bank Characteristics**

Bank type, geographical spread, number of branches of the bank, number of customers of the bank, number of employees of the bank and certifications of the bank.

b) **Technology Characteristics**

Development methodology, outsourcing, level of automation, man power, employee and user training, type of software used and the data center model.

c) **Personal details**

Total experience, experience in the current bank, experience in IT operations and certifications.

The instrument was organized in 7 parts. Section A had 6 questions related to bank characteristics, Section B had 8 questions related to technology characteristics of the bank, Section C had 26 questions related to the IT risks, Section D had 25 questions related to the IT risk management, Section E had 6 questions related to non-financial impacts, Section F had 7 questions related to financial impacts/losses and Section G has 5 questions related to background information of the respondent. The instrument is shown in Appendix 1.

## 3.12 Analysis Design

Appropriate statistical techniques were used for the analysis and interpretation of the data collected, for the purpose of the research. Descriptive analytical techniques like averages, percentages and frequencies have been performed on data. The data was presented in charts, figures and tables in order to analyse the background information about the banks and the respondents.

The statistical package IBM SPSS 22.0 was used for data editing, coding and basic analysis. ANOVA, t-tests and correlation analysis were used for hypothesis testing. The basic models linking IT risk, IT risk management and impacts were tested by using structured equation modelling (SEM) and path analysis, performed with AMOS.

## 3.13 Conclusion

This chapter presented various aspects of research methodology used in the study. It also explained the questionnaire development process. The draft questionnaire prepared based on literature review was edited by experts to improve its content and face validity. Exploratory factor analysis was performed on the pilot data to understand the underlying factor structure. This exercise helped in variable reduction and also to identify items for further editing based on the level of loading.

After incorporating the modifications and corrections from this exercise, the final instrument to be used for the final survey was developed

Chapter 4

# DATA COLLECTION & VALIDATION OF THE INSTRUMENT

Contents



## 4.1 Introduction

IT risk and risk management are multidimensional constructs whose sub dimensions need to be studied and analysed. The literature review in chapter 2 had identified major gaps in research with respect to these constructs in Indian banks. This research tries to plug some of these gaps in research both in international as well as in Indian context. Hence the study focused on IT risk factors, IT risk management methods and it's financial and non-financial impacts on the banks. The major variables of study are IT risk factors, IT risk management factors and its financial and non-financial impacts on banks. Questionnaire was prepared and data was collected from various banks in India and this chapter does the analysis and validation of the data collected.

## 4.2 Sample Profile

The sampling design is described in chapter 3. The researcher distributed 86 questionnaires to various banks in India and another set of 20 questionnaires to selected co-operative banks having multiple branches and also core banking system implemented. After two rounds of reminders

through telephone interviews and direct interviews 58 filled questionnaires were collected back from 112 banks. Detailed examination of the data based on grossly missing or inappropriate values resulted in the deletion of 5 records resulting in final data set of 53.

### 4.2.1 Bank Characteristics

On checking the data of bank characteristics – namely type of the bank - the final data set of 53 records were spread as 15 foreign banks, 13 private banks, 11 public sector banks and 14 cooperative sector banks. And the geographical spread of the banks based on area of operation were containing 14 multiple location - single state banks, 24 multiple location - multiple state banks and 15 banks operating in multiple location - multiple country. Table 4.1, 4.2 shows the details.

**Table 4.1: Frequency table – Bank Type**

| Bank Type Wise | | | | |
|---|---|---|---|---|
| | **Frequency** | **Percent** | **Actual Numbers** | **% Responded** |
| Foreign | 15 | 28.3 | 40 | 37.5 |
| Private | 13 | 24.5 | 20 | 65.0 |
| Public Sector | 11 | 20.8 | 26 | 42.3 |
| Cooperative | 14 | 26.4 | 26 | 53.8 |
| Total | 53 | 100.0 | 112 | |

Source: Survey Data

**Table 4.2: Frequency table – Geographical Spread**

| Geographical Spread | | |
|---|---|---|
| | **Frequency** | **Percent** |
| Multiple Location, Single State | 14 | 26.4 |
| Multiple Location, Multiple State | 24 | 45.3 |
| Multiple Location, Multiple Countries | 15 | 28.3 |
| **Total** | **53** | **100.0** |

Source: Survey Data

On checking the data of bank characteristics for certifications/standards followed by banks in India are listed in Table 4.3. Based on the data, it showed that most of the banks follow Basel II/III and ISO 9001:2000 standards. Very few banks had implemented ISO 27001 and BS 7799 standards.

**Table 4.3: Frequency table – Standards followed**

| **ISO 27001** | | |
|---|---|---|
| | **Frequency** | **Percent** |
| Certified | 1 | 01.9 |
| Not Certified | 52 | 98.1 |
| **Total** | **53** | **100.0** |
| **BS 7799** | | |
| Certified | 1 | 1.9 |
| Not Certified | 52 | 98.1 |
| **Total** | **53** | **100.0** |
| **BASEL II/III** | | |
| Certified | 37 | 69.8 |
| Not Certified | 16 | 30.2 |
| **Total** | **53** | **100.0** |
| **ISO 9001:2000** | | |
| Certified | 23 | 43.4 |
| Not Certified | 30 | 56.6 |
| **Total** | **53** | **100.0** |

Source: Survey Data

**Table 4.4: Statistics – Size of the bank (branches, customers, employees)**

| | **Branches** | **Customers** | **Employees** |
|---|---|---|---|
| Mean | 835.32 | 17473333.33 | 11095.42 |
| Std. Deviation | 1253.551 | 62880173.915 | 15128.688 |
| Minimum | 5 | 10000 | 40 |
| Maximum | 4100 | 400000000 | 60000 |

Source: Survey Data

### 4.2.2 Technology Characteristics

On checking the data of technology characteristics, the following frequency table were obtained. Table 4.5 shows the level of automation in various banks. 32 banks were reported to have high level of automation used in their banks, 14 banks reported medium level of automation and 5 banks reported very low level of automation in their banks. 2 Banks did not respond to this question.

**Table 4.5: Frequency table – Level of automation**

| | | Frequency | Percent | Valid Percent |
|---|---|---|---|---|
| **Valid** | High | 32 | 60.4 | 62.7 |
| | Medium | 14 | 26.4 | 27.5 |
| | Low | 5 | 9.4 | 9.8 |
| | Total | 51 | 96.2 | 100.0 |
| **Missing** | Not Responded | 2 | 3.8 | |
| **Total** | | **53** | **100.0** | |

Source: Survey Data

Table 4.6 shows the level of in house development team in various banks. 15 banks reported to have in house developments and 38 banks reported that they did not have any in house developments.

**Table 4.6: Frequency table – In house development team**

| | | Frequency | Percent |
|---|---|---|---|
| **Valid** | Opted | 15 | 28.3 |
| | Not Opted | 38 | 71.7 |
| | **Total** | **53** | **100.0** |

Source: Survey Data

Table 4.7 shows the presence of branch level technical support team in various banks. 8 banks opted to have branch level technical support

team and 45 banks reported that they did not have any branch level technical support team. Frequency tables for banks with centralised tech support team and outsourced support teams are also shown in tables 4.8 and 4.9.

**Table 4.7: Frequency table – Branch level tech support team**

| | Frequency | Percent |
|---|---|---|
| **Opted** | 8 | 15.1 |
| **Not Opted** | 45 | 84.9 |
| **Total** | **53** | **100.0** |

Source: Survey Data

**Table 4.8: Frequency table – Centralised support team**

| | Frequency | Percent |
|---|---|---|
| Opted | 32 | 60.4 |
| Not Opted | 21 | 39.6 |
| **Total** | **53** | **100.0** |

Source: Survey Data

**Table 4.9: Frequency table – External support team**

| | Frequency | Percent |
|---|---|---|
| **Opted** | 33 | 62.3 |
| **Not Opted** | 20 | 37.7 |
| **Total** | 53 | 100.0 |

Source: Survey Data

The next set of tables reported the frequency tables for banks related to technology training given to their employees as well as to their customers. Training plays an important role in security. Table 4.10 reports the frequency of training provided by banks to their employees. Most of the banks (34), provide training to their employees at least once in a year. Two banks reported that they were not giving any technology training to

employees. Table 4.11 shows whether banks provide any training to their customers. Training to customers on information security is important as the use of online channels are increasing day by day.

**Table 4.10: Frequency table – Training to employees**

| | Frequency | Percent | Valid Percent |
|---|---|---|---|
| Not Provided | 2 | 3.8 | 3.9 |
| One time an Year | 34 | 64.2 | 66.7 |
| Two Times an Year | 9 | 17.0 | 17.6 |
| Three Times an Year | 2 | 3.8 | 3.9 |
| > than 3 Times | 4 | 7.5 | 7.8 |
| **Total** | **51** | **96.2** | **100.0** |
| Not Responded | 2 | 3.8 | |
| **Total** | **53** | **100.0** | |

Source: Survey Data

**Table 4.11: Frequency table – Training to customers**

| | Frequency | Percent |
|---|---|---|
| No | 20 | 37.7 |
| Yes | 28 | 52.8 |
| Not Responded | 5 | 9.4 |
| **Total** | 53 | 100.0 |

Source: Survey Data

Table 4.12 shows the frequency table for the type of data center model used by banks and table 4.13 shows the frequency table for type of software used by the banks for building their core banking and other related systems. Table 4.14 shows the frequency table for the type of software used for the development of Information Technology systems in the bank.

**Table 4. 12: Frequency table – Data center model**

| | Frequency | Percent |
|---|---|---|
| Hosted with Third Party | 24 | 45.3 |
| Own Data Center | 29 | 54.7 |
| **Total** | 53 | 100.0 |

Source: Survey Data

**Table 4.13: Frequency table – Type of software used**

| | Frequency | Percent | Valid Percent |
|---|---|---|---|
| **Open Source** | 20 | 37.7 | 40.0 |
| **Microsoft Based** | 16 | 30.2 | 32.0 |
| **Both** | 14 | 26.4 | 28.0 |
| Total | **50** | **94.3** | **100.0** |
| **Not Responded** | 3 | 5.7 | |
| Total | **53** | **100.0** | |

Source: Survey Data

**Table 4.14: Frequency table – Software development methodology**

| | Frequency | Percent |
|---|---|---|
| **Outsourced IS Development** | 39 | 73.6 |
| **In-house Developed** | 10 | 18.9 |
| **Total** | 49 | 92.5 |
| **Not Responded** | 4 | 7.5 |
| **Total** | 53 | 100.0 |

Source: Survey Data

## 4.3 Reliability Analysis

The reliability of the final instrument developed in the current study was tested by computing Cronbach alpha (α) value for each of the IT risk factors as well as for the entire set. The item-total correlation was tested for each risk item under each factor.

The final values of Cronbach alpha for the IT risk factors are presented in Table 3.15. As seen from the table, all the factors had Cronbach alpha value above 0.7, which testified the reliability of the instrument. Here in this case no

statements were deleted since all have loading above 0.7 and the cronbach's Alpha is 0.919 which is relatively very high.

**Table 4.15: Results of reliability analysis of IT risk**

| Reliability Statistics | |
|---|---|
| **Cronbach's Alpha** | **N of Items** |
| .919 | 26 |

| RISK Item-Total Statistics | | | | |
|---|---|---|---|---|
| | **Scale Mean if Item Deleted** | **Scale Variance if Item Deleted** | **Corrected Item-Total Correlation** | **Cronbach's Alpha if Item Deleted** |
| VAR00001 | 34.5000 | 143.167 | .695 | .914 |
| VAR00002 | 34.3000 | 136.900 | .664 | .912 |
| VAR00003 | 34.6000 | 148.267 | .623 | .918 |
| VAR00004 | 33.6000 | 138.711 | .505 | .917 |
| VAR00005 | 33.1000 | 141.656 | .429 | .919 |
| VAR00006 | 32.5000 | 141.611 | .480 | .917 |
| VAR00007 | 32.8000 | 125.067 | .782 | .908 |
| VAR00008 | 32.8000 | 133.956 | .619 | .914 |
| VAR00009 | 32.4000 | 128.711 | .794 | .907 |
| VAR00010 | 33.7000 | 130.678 | .593 | .916 |
| VAR00011 | 33.5000 | 132.944 | .704 | .911 |
| VAR00012 | 33.8000 | 125.511 | .812 | .906 |
| VAR00013 | 33.7000 | 129.789 | .655 | .913 |
| VAR00014 | 34.0000 | 132.000 | .826 | .907 |
| VAR00015 | 31.9000 | 146.100 | .614 | .916 |
| VAR00016 | 33.7000 | 137.711 | .504 | .916 |
| VAR00017 | 32.5000 | 141.611 | .480 | .917 |
| VAR00018 | 32.8000 | 125.067 | .782 | .908 |
| VAR00019 | 32.8000 | 133.956 | .619 | .914 |
| VAR00020 | 33.7000 | 129.789 | .655 | .913 |
| VAR00021 | 34.0000 | 132.000 | .826 | .907 |
| VAR00022 | 31.9000 | 146.100 | .614 | .916 |
| VAR00023 | 34.3000 | 136.900 | .664 | .912 |
| VAR00024 | 34.6000 | 148.267 | .623 | .918 |
| VAR00025 | 34.0000 | 132.000 | .826 | .907 |
| VAR00026 | 33.8000 | 125.511 | .812 | .906 |

Source: Survey Data

Cronbach alpha (α) values were computed for the IT risk management factors also. The results are listed in Table 3.16. No statements were excluded because of high loading and the Cronbach's alpha was reported to be 0.955 for IT risk management.

**Table 4.16: Results of Reliability Analysis of IT risk management**

| **Reliability Statistics** | | | | |
|---|---|---|---|---|
| **Cronbach's Alpha** | | **N of Items** | | |
| .955 | | 25 | | |
| **RISK MANAGEMENT Item-Total Statistics** | | | | |
| | **Scale Mean if Item Deleted** | **Scale Variance if Item Deleted** | **Corrected Item-Total Correlation** | **Cronbach's Alpha if Item Deleted** |
| VAR00001 | 74.3000 | 226.678 | .804 | .952 |
| VAR00002 | 74.0000 | 228.444 | .793 | .952 |
| VAR00003 | 74.3000 | 220.678 | .905 | .950 |
| VAR00004 | 74.3000 | 223.344 | .838 | .951 |
| VAR00005 | 74.0000 | 246.000 | .611 | .955 |
| VAR00006 | 73.8000 | 248.178 | .593 | .955 |
| VAR00007 | 73.6000 | 256.044 | .328 | .957 |
| VAR00008 | 73.9000 | 241.656 | .758 | .953 |
| VAR00010 | 73.8000 | 247.733 | .614 | .955 |
| VAR00011 | 74.0000 | 226.222 | .853 | .951 |
| VAR00012 | 74.3000 | 232.900 | .750 | .952 |
| VAR00013 | 74.4000 | 240.933 | .615 | .954 |
| VAR00014 | 73.9000 | 232.322 | .876 | .951 |
| VAR00015 | 73.4000 | 250.711 | .812 | .955 |
| VAR00016 | 74.1000 | 228.767 | .704 | .954 |
| VAR00017 | 74.5000 | 232.944 | .856 | .951 |
| VAR00018 | 74.7000 | 228.233 | .685 | .954 |
| VAR00019 | 74.2000 | 230.622 | .638 | .955 |
| VAR00020 | 74.1000 | 231.878 | .855 | .951 |
| VAR00021 | 73.6000 | 256.044 | .328 | .957 |
| VAR00022 | 74.1000 | 228.767 | .704 | .954 |
| VAR00023 | 74.0000 | 226.222 | .853 | .951 |
| VAR00024 | 74.2000 | 230.622 | .638 | .955 |
| VAR00025 | 74.3000 | 223.344 | .838 | .951 |

Source: Survey Data

Cronbach alpha (α) values were computed for the nonfinancial impact factors also. The results are listed in Table 3.17. No statements were excluded because of high loading and the Cronbach's alpha was reported to be 0.896 for nonfinancial impact.

**Table 4.17: Results of Reliability Analysis of Financial Impacts**

| Reliability Statistics – Nonfinancial Impact | | | | |
|---|---|---|---|---|
| **Cronbach's Alpha** | | **N of Items** | | |
| .896 | | 6 | | |
| **Item-Total Statistics** | | | | |
| | **Scale Mean if Item Deleted** | **Scale Variance if Item Deleted** | **Corrected Item-Total Correlation** | **Cronbach's Alpha if Item Deleted** |
| VAR00001 | 9.569 | 24.530 | .829 | .864 |
| VAR00002 | 9.569 | 25.370 | .771 | .873 |
| VAR00003 | 9.216 | 24.613 | .690 | .882 |
| VAR00004 | 8.961 | 22.838 | .696 | .884 |
| VAR00005 | 8.961 | 22.838 | .728 | .877 |
| VAR00006 | 9.020 | 24.500 | .668 | .885 |

Source: Survey Data

Cronbach alpha (α) values were computed for the financial impact factors also. The results are listed in Table 3.18. No statements were excluded because of high loading and the Cronbach's alpha was reported to be 0.858 for financial impact.

**Table 4.18: Results of Reliability Analysis of Nonfinancial Impacts**

| Reliability Statistics- Financial Impact | | | | |
|---|---|---|---|---|
| **Cronbach's Alpha** | | **N of Items** | | |
| .858 | | 7 | | |
| **Item-Total Statistics** | | | | |
| | **Scale Mean if Item Deleted** | **Scale Variance if Item Deleted** | **Corrected Item-Total Correlation** | **Cronbach's Alpha if Item Deleted** |
| VAR00001 | 11.765 | 22.344 | .600 | .844 |
| VAR00002 | 11.333 | 21.387 | .555 | .847 |
| VAR00003 | 11.098 | 20.050 | .573 | .846 |
| VAR00004 | 11.627 | 22.438 | .581 | .846 |
| VAR00005 | 11.275 | 18.283 | .733 | .821 |
| VAR00006 | 10.725 | 17.643 | .700 | .829 |
| VAR00007 | 11.235 | 19.944 | .707 | .826 |

Source: Survey Data

### 4.3.1 Comparison of Reliability (Cronbach's Alpha) – Pilot Study Vs Final Study

The following Table 4.19 shows a comparison of the Cronback's Alpha values for pilot study and final study. The reliability values got higher for final study.

**Table 4.19: Comparison of Reliability Pilot Study Vs Final Study**

| Reliability Statistics For | Pilot Study | Final Study | Number of Items |
|---|---|---|---|
| IT Risk | 0.809 | 0.919 | 26 |
| IT Risk Management | 0.834 | 0.955 | 25 |
| Nonfinancial Impact | 0.816 | 0.896 | 6 |
| Financial Impact | 0.810 | 0.858 | 7 |

Source: Survey Data

## 4.4 Conclusion

The final sample had sufficient number of banks represented from public sector, private sector, foreign banks and cooperative sector banks. The data showed that the responses came from different organizations showing considerable diversity in sample. There was a good mix of responses from banks having operations in single location, multiple states and multiple countries.

.....ꕥ.....

Chapter 5

# ANALYSIS OF INFORMATION TECHNOLOGY RISK CONSTRUCTS

Contents

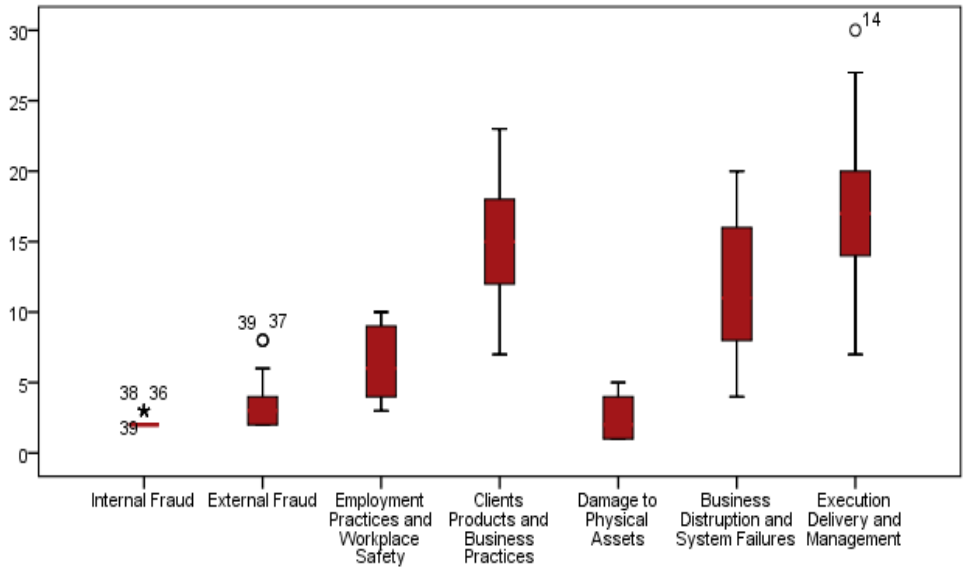


## 5.1 Information Technology Risk Variables

As explained in chapter 3, extensive literature review resulted in the identification of several IT risk factors. The next step was to try to group similar factors together in order to get a clearer picture of the general types of IT risk factors present. This study being focussed on IT risks in Indian banking organizations, Basel and RBI guidelines were followed in this process and which resulted in the creation of the following seven general types of software IT risk categories. The following categories are identified and listed based on the risk categories listing under operational risk management guidelines of Basel recommendations.

a) Internal fraud
b) External fraud
c) Employment practices and work place safety
d) Clients, products and business practices
e) Damage to physical assets
f) Business disruption and system failures
g) Execution, delivery and process management

Figure 5.1 shows the box plot for the above listed Information Technology risk variables.




Source: Survey Data

**Figure 5.1: Box Plot – Information Technology risk variables**

There are actually seven sub components in the measurement of information technology risk. After the computation of variables, a box plot was generated to check the spread of the data and to find out outliers if any. Data analysis involves the use of statistical techniques to identify patterns that may be hidden in a group of numbers. One of these techniques is the "box plot," which is used to visually summarize and compare groups of data (Williamson & Parker, 1989). The box plot uses the median, the approximate quartiles, and the lowest and highest data points to convey the level, spread, and symmetry of a distribution of data values. It can also be easily refined to identify outlier data values. Figure 5.1 shows the box plot

diagram which reminds the presence of some outliers in some of the variables.

Currently there are several technical ways of dealing with outliers which are in practice worldwide. Major among the treatment techniques are data transformations (Hamilton, 1992) (Osborne, 2002), usage of robust methods like trimmed mean (Anscombe, 1960), outlier removal (Barnett & Lewis, 1994) and merging with immediate lower/ upper value (Lornez, 1987). These methods were used to adjust the outliers according to the need of the data and merit of the method to arrive in producing the descriptive statistics as shown in Table 5.1

**Table 5.1: Descriptive Statistics - Information Technology Risk**

| | Internal Fraud | External Fraud | Employment Practices and Workplace Safety | Clients Products and Business Practices | Damage to Physical Assets | Business Disruption and System Failures | Execution Delivery and Management |
|---|---|---|---|---|---|---|---|
| Mean | 2.189 | 3.245 | 6.340 | 14.774 | 2.453 | 11.151 | 17.377 |
| Std. Deviation | .3950 | 1.6279 | 2.3854 | 4.0792 | 1.4619 | 4.1575 | 4.7686 |
| Range | 1.0 | 6.0 | 7.0 | 16.0 | 4.0 | 16.0 | 23.0 |
| Minimum | 2.0 | 2.0 | 3.0 | 7.0 | 1.0 | 4.0 | 7.0 |
| Maximum | 3.0 | 8.0 | 10.0 | 23.0 | 5.0 | 20.0 | 30.0 |

Source: Survey Data

Table 5.1 explains the descriptive statistics of all the seven sub components of Information Technology risk and is explained as under.

Instead of cut-off, mean is used in this thesis for the analysis and to state where the concentrations is. The mean is interpreted based on the scale min and max as explained below.

*Internal fraud* measure was reported with a mean of 2.18 with a standard deviation of 0.39 on a one to ten scale. The spread was observed very low (1) with a minimum of 2 and maximum of 3. The mean of 2.18 on ten point scale indicates that the average internal fraud risk in banks is **low** (disagree). The standard deviation of 0.39 shows that, fairly large number of respondents have indicated that risks due to internal fraud is low in their banks. Thus we can say that the distribution is not diverse.

*External fraud* measure was reported with a mean of 3.24 with a standard deviation of 1.62 on a one to ten scale. The spread was observed as (6) with a minimum of 2 and maximum of 8. The mean of 3.24 on a ten point scale indicates that the average external fraud risk in banks is again **low**, but slightly more than the risk of internal fraud. The standard deviation of 1.62 shows that, fairly large number of respondents have indicated low risks due to external fraud. Thus we can say that the distribution is only slightly diverse.

*Employment practices and workplace safety* measure was reported with a mean of 6.34 with a standard deviation of 2.38 on a one to fifteen scale. The spread was observed as (7) with a minimum of 3 and maximum of 10. The mean of 6.34 on a fifteen point scale indicates that the average risk due to employment practices and work place safety in banks is **below average**. When compared to the risks of internal fraud an external fraud, the risk in this category more. The standard deviation of 2.38 shows that, fairly large number of respondents have indicated average risks due to employment practices and workplace safety and the distribution is slightly diverse.

*Clients products and business practices* measure was reported with a mean of 14.77 with a standard deviation of 4.07 on a one to thirty five

scale. The spread was observed as (16) with a minimum of 7 and maximum of 23. The mean of 14.77 on a thirty five point scale indicates that the average risk due to employment practices and work place safety in banks is **below average**. The standard deviation of 4.07 shows that, fairly large number of respondents have indicated that risks due to clients, products and business practices is below average in their banks. Thus we can say that the distribution is not diverse.

*Damage to physical assets* measure was reported with a mean of 2.45 with a standard deviation of 1.46 on a one to five scale. The spread was observed as (4) with a minimum of 1 and maximum of 5. The mean of 2.45 shows that the risk of 'damage to physical assets' is **average or below average**. Standard deviation of 1.46 shows that most of the respondents indicated that the risks in this category are below average. So the distribution is not diverse.

Business disruption and system failures measure was reported with a mean of 11.15 with a standard deviation of 4.15 on a one to twenty scale. The spread was observed as (16) with a minimum of 4 and maximum of 20. The mean of 11.15 on a one to twenty scale shows that the risk of business disruption and systems failures is **above average**. The standard deviation of 4.15 shows that, that the distribution relatively diverse.

Execution delivery and management measure was reported with a mean of 17.37 with a standard deviation of 4.76 on a one to thirty five point scale. The spread was observed as (23) with a minimum of 7 and maximum of 30. The mean of 17.37 on a one to thirty five point scale shows that the risk of

execution, delivery and management is **average**. The standard deviation of 4.76 shows that, that the distribution is relatively diverse.

A summary of the scale based IT risk level is shown in Table 5.2

**Table 5.2: Summary of Scale Based IT Risk Levels Across Banks**

| No | IT Risk Category | Mean | Scale | Decision |
|---|---|---|---|---|
| **1** | Internal Fraud | 2.189 | 2-10 | Very Low |
| **2** | External Fraud | 3.245 | 2-10 | Very Low |
| **3** | Employment Practices and Work Place Safety | 6.340 | 3-15 | Low |
| **4** | Clients, Products and Business Practices | 14.774 | 7-35 | Low |
| **5** | Damage to Physical Assets | 2.453 | 1-5 | Low |
| **6** | Business Disruption and System Failures | 11.151 | 4-20 | Low |
| **7** | Execution Delivery and Management | 17.377 | 7-35 | Low |

Source: Survey Data

## 5.2 IT Risk Variations across Types of Banks

The next part of the analysis was oriented towards finding the variations in information technology risk across different type of banks. Table 5.3 explains that, internal fraud was found to be more in cooperative banks (2.28) followed by foreign sector banks (2.2) and the lowest was observed among public sector banks (2.09). The external fraud is found to be more in cooperative sector banks (4.64) followed by foreign banks (2.86) and the lowest in public sector banks (2.455). The risk related to employment practices and workplace safety public sector banks scored high (7.27) followed by private sector banks (6.1), foreign banks (6.0) and the lowest is cooperative sector banks (5.71). For clients products and

business practices related risks, cooperative banks (18.0) being the highest and public sector banks being the lowest (11.45).

**Table 5.3: Information Technology risk across types of banks**

| | | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Internal Fraud | Foreign | 15 | 2.200 | .4140 |
| | Private | 13 | 2.154 | .3755 |
| | Public Sector | 11 | 2.091 | .3015 |
| | Cooperative | 14 | 2.286 | .4688 |
| | Total | 53 | 2.189 | .3950 |
| External Fraud | Foreign | 15 | 2.867 | .8338 |
| | Private | 13 | 2.846 | 1.1435 |
| | Public Sector | 11 | 2.455 | 1.0357 |
| | Cooperative | 14 | 4.643 | 2.2051 |
| | Total | 53 | 3.245 | 1.6279 |
| Employment Practices and Workplace Safety | Foreign | 15 | 6.000 | 2.0000 |
| | Private | 13 | 6.615 | 2.5344 |
| | Public Sector | 11 | 7.273 | 2.5334 |
| | Cooperative | 14 | 5.714 | 2.4939 |
| | Total | 53 | 6.340 | 2.3854 |
| Clients Products and Business Practices | Foreign | 15 | 14.667 | 3.4572 |
| | Private | 13 | 14.231 | 4.6216 |
| | Public Sector | 11 | 11.455 | 3.4457 |
| | Cooperative | 14 | 18.000 | 2.0000 |
| | Total | 53 | 14.774 | 4.0792 |

Source: Survey Data

Analysis of Variance (ANOVA) is used to uncover the effects of categorical independent variables (called "factors") on an interval dependent variable. The key statistic in ANOVA is the F-test of difference of group means, testing if the means of the groups formed by values of the independent are different enough not to have occurred by chance. If the

group means do not differ significantly then it is inferred that the independent variable(s) do not have an effect on the dependent variable. If the F test shows that, overall, the independent variable(s) are related to the dependent variable, then *multiple comparison tests* of significance are used to explore which values of the independent variable(s) have the most to do with the relationship.

Some key ANOVA assumptions are that the groups formed by the independent variable(s) are relatively equal in size and have similar variances on the dependent variable ("homogeneity of variances"). Like any other parametric tests, ANOVA also assumes normality.

In the present study, the assumption of equal sizes were not met for most of the subgroups as evident from respondent attributes analysis in chapter 4. But ANOVA implemented in SPSS has built- in mechanism to support unequal group sizes. Hence this will not affect the interpretation very much. The assumption that the dependent variable should have the same variance in each category of the independent variable was tested through Levene's test of homogeneity of variance.

The test failed to indicate equal variance in certain cases. However failure to meet the assumption of homogeneity of variances is not fatal to ANOVA. Moore (1995) suggested a rule of thumb that the ratio of largest to smallest group variances should be 4:1 or less. This condition was met in all cases in this study.

**Table 5.4: ANOVA - Information Technology risk across types of banks**

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Internal Fraud | Between Groups | .255 | 3 | .085 | .529 | .664 |
| | Within Groups | 7.859 | 49 | .160 | | |
| | Total | 8.113 | 52 | | | |
| External Fraud | Between Groups | 38.444 | 3 | 12.815 | 6.319 | .001 |
| | Within Groups | 99.367 | 49 | 2.028 | | |
| | Total | 137.811 | 52 | | | |
| Employment Practices and Workplace Safety | Between Groups | 17.771 | 3 | 5.924 | 1.044 | .382 |
| | Within Groups | 278.116 | 49 | 5.676 | | |
| | Total | 295.887 | 52 | | | |
| Clients Products and Business Practices | Between Groups | 270.915 | 3 | 90.305 | 7.445 | .000 |
| | Within Groups | 594.368 | 49 | 12.130 | | |
| | Total | 865.283 | 52 | | | |

Source: Survey Data

Table 5.4 details the test result for internal fraud across different banks. It is observed that the test was not found to be significant ($p>0.05$) and should conclude that there is no sufficient evidence to believe that internal fraud varies significantly across different bank groups and thus can say that the internal fraud threat is almost similar for all the banks irrespective of their category.

A significant F value indicates that there are differences in the means, but it does not tell you where those differences are and therefore, various methods have been developed for doing multiple comparisons of group means. Multiple comparisons will allow a researcher to compare all the group means with each other providing an in depth understanding of the differences in the mean. From Table 5.5, it was observed that only two variables were found to be significant namely External Fraud and Clients

Products and Business Practices and hence multiple comparisons were executed with an LSD model.

**Table 5.5: Multiple Comparisons**

| Dependent Variable | (I) Bank Type | (J) Bank Type | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| External Fraud | Foreign | Private | .0205 | .5396 | .970 |
| | | Public Sector | .4121 | .5653 | .469 |
| | | Cooperative | -1.7762 | .5292 | **.002** |
| | Private | Foreign | -.0205 | .5396 | .970 |
| | | Public Sector | .3916 | .5834 | .505 |
| | | Cooperative | -1.7967 | .5485 | **.002** |
| | Public Sector | Foreign | -.4121 | .5653 | .469 |
| | | Private | -.3916 | .5834 | .505 |
| | | Cooperative | -2.1883 | .5738 | **.000** |
| | Cooperative | Foreign | 1.7762 | .5292 | **.002** |
| | | Private | 1.7967 | .5485 | **.002** |
| | | Public Sector | 2.1883 | .5738 | **.000** |
| Clients Products and Business Practices | Foreign | Private | .4359 | 1.3197 | .743 |
| | | Public Sector | 3.2121 | 1.3825 | **.024** |
| | | Cooperative | -3.3333 | 1.2943 | **.013** |
| | Private | Foreign | -.4359 | 1.3197 | .743 |
| | | Public Sector | 2.7762 | 1.4268 | .057 |
| | | Cooperative | -3.7692 | 1.3415 | **.007** |
| | Public Sector | Foreign | -3.2121 | 1.3825 | **.024** |
| | | Private | -2.7762 | 1.4268 | .057 |
| | | Cooperative | -6.5455 | 1.4033 | **.000** |
| | Cooperative | Foreign | 3.3333 | 1.2943 | **.013** |
| | | Private | 3.7692 | 1.3415 | **.007** |
| | | Public Sector | 6.5455 | 1.4033 | **.000** |

Source: Survey Data

The case of *external fraud* was explained first and was observed from Table 5.5 that the external fraud differ significantly ($p< 0.05$) for the cooperative banks alone when we compare it with all the other groups viz foreign, private and public sector banks. Hence we can conclude that the

external fraud is treated same for foreign, private and public sector banks but cooperative banks behave significantly different.

In the case of *clients, products and business practices*, it differ significantly ($p< 0.05$) for the cooperative banks alone when we compare it with all the other groups viz foreign, private and public sector banks. Hence we can conclude that the clients, products and business practices for cooperative banks are significantly different from for foreign, private and public sector banks. It was also found that this risk factor (clients, products and business practices) differ significantly for foreign banks with respect to public sector banks.

**Table 5.6: Information Technology risk across types of banks (contd..)**

| | | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Damage to Physical Assets | Foreign | 15 | 2.533 | 1.3020 |
| | Private | 13 | 1.769 | 1.1658 |
| | Public | 11 | 1.818 | 1.4013 |
| | Cooperative | 14 | 3.500 | 1.4005 |
| | Total | 53 | 2.453 | 1.4619 |
| Business Disruption and System Failures | Foreign | 15 | 9.200 | 4.3622 |
| | Private | 13 | 10.846 | 3.8911 |
| | Public | 11 | 9.364 | 3.5006 |
| | Cooperative | 14 | 14.929 | 1.6392 |
| | Total | 53 | 11.151 | 4.1575 |
| Execution Delivery and Management | Foreign | 15 | 17.400 | 5.4746 |
| | Private | 13 | 17.769 | 5.3565 |
| | Public | 11 | 14.364 | 3.2023 |
| | Cooperative | 14 | 19.357 | 3.4996 |
| | Total | 53 | 17.377 | 4.7686 |

Source: Survey Data

Table 5.6 explains that, *damage to physical assets* was found to be more in cooperative banks (3.5) followed by foreign banks (2.533) and the

lowest was observed among private sector banks (1.769). The business disruption and system failures was found to be more in cooperative sector banks (14.929) followed by private banks (10.846) and the lowest was in foreign banks (9.2). The risk related to execution, delivery and management in cooperative sector banks scored high (19.357) followed by private sector banks (17.769), foreign banks (14.40) and the lowest was in public sector banks (14.364).

**Table 5.7: ANOVA - Information Technology risk across types of banks**

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Damage to Physical Assets | Between Groups | 25.955 | 3 | 8.652 | 4.977 | **.004** |
| | Within Groups | 85.177 | 49 | 1.738 | | |
| | Total | 111.132 | 52 | | | |
| Business Disruption and System Failures | Between Groups | 293.226 | 3 | 97.742 | 7.909 | **.000** |
| | Within Groups | 605.566 | 49 | 12.358 | | |
| | Total | 898.792 | 52 | | | |
| Execution, Delivery and Management | Between Groups | 156.785 | 3 | 52.262 | 2.497 | .071 |
| | Within Groups | 1025.667 | 49 | 20.932 | | |
| | Total | 1182.453 | 52 | | | |

Source: Survey Data

Table 5.7 details the test result for *execution, delivery and management* across different banks. It was observed that the test was not found to be significant ($p>0.05$) and should conclude that there was no sufficient evidence to believe that execution, delivery and management varies significantly across different bank groups and thus can say that the execution, delivery and management threat is almost similar for all the banks irrespective of their category.

A significant F value indicates that there are differences in the means, but it does not tell you where those differences are and therefore,

various methods have been developed for doing multiple comparisons of group means. Multiple comparisons will allow a researcher to compare all the group means with each other providing an in depth understanding of the differences in the mean. From Table 5.8, it was observed that only two variables are found to be significant namely damage to physical assets and business disruption and system failures and hence multiple comparisons were executed with an LSD model.

**Table 5.8: LSD - Multiple comparisons – IT risks across bank types**

| Dependent Variable | (I) Bank Type | (J) Bank Type | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| Damage to Physical Assets | Foreign | Private | .7641 | .4996 | .133 |
| | | Public Sector | .7152 | .5234 | .178 |
| | | Cooperative | -.9667 | .4900 | .054 |
| | Private | Foreign | -.7641 | .4996 | .133 |
| | | Public Sector | -.0490 | .5401 | .928 |
| | | Cooperative | -1.7308 | .5078 | .001 |
| | Public Sector | Foreign | -.7152 | .5234 | .178 |
| | | Private | .0490 | .5401 | .928 |
| | | Cooperative | -1.6818 | .5312 | .003 |
| | Cooperative | Foreign | .9667 | .4900 | .054 |
| | | Private | 1.7308 | .5078 | .001 |
| | | Public Sector | 1.6818 | .5312 | .003 |
| Business Disruption and System Failures | Foreign | Private | -1.6462 | 1.3321 | .222 |
| | | Public Sector | -.1636 | 1.3955 | .907 |
| | | Cooperative | -5.7286 | 1.3064 | .000 |
| | Private | Foreign | 1.6462 | 1.3321 | .222 |
| | | Public Sector | 1.4825 | 1.4402 | .308 |
| | | Cooperative | -4.0824 | 1.3540 | .004 |
| | Public Sector | Foreign | .1636 | 1.3955 | .907 |
| | | Private | -1.4825 | 1.4402 | .308 |
| | | Cooperative | -5.5649 | 1.4164 | .000 |
| | Cooperative | Foreign | 5.7286 | 1.3064 | .000 |
| | | Private | 4.0824 | 1.3540 | .004 |
| | | Public Sector | 5.5649 | 1.4164 | .000 |

Source: Survey Data

In the case of damage to physical assets, it differ significantly ($p < 0.05$) for the cooperative banks alone when we compare it with the other groups viz private and public sector banks. Hence we can conclude that the damage to physical assets for cooperative banks was significantly different for private and public sector banks. But damage to physical assets for cooperative banks was not significantly different from foreign banks.

In the case of business disruption and system failures, it differ significantly for the cooperative banks alone when we compare it with the other groups viz foreign, private and public sector banks. Hence we can conclude that the damage to physical assets for cooperative banks is significantly different from for foreign, private and public sector banks.

**Table 5.9: IT Risk Constructs – Variations across Different Bank Types**

| No | It risk Across Bank types | High | | | Low |
|---|---|---|---|---|---|
| **1** | Internal Fraud | COB (2.28) | FB (2.2) | PVT (2.1) | PSB (2.09) |
| **2** | External Fraud | COB (4.6) | FB (2.86) | PVT (2.84) | PSB (2.45) |
| **3** | Employment Practices and Work Place Safety | PSB (7.27) | PVT (6.61) | FB (6.00) | COB (5.71) |
| **4** | Clients, Products and Business Practices | COB (18.00) | FB (14.66) | PVT (14.23) | PSB (11.46) |
| **5** | Damage to Physical Assets | COB (3.50) | FB (2.53) | PSB (1.82) | PVT (1.77) |
| **6** | Business Disruption and System Failures | COB (14.93) | PVT (10.85) | PSB (9.36) | FB (9.20) |
| **7** | Execution Delivery and Management | COB (19.36) | PVT (17.77) | FB (17.40) | PSB (14.36) |

Source: Survey Data

*COB – Cooperative Bank, FB – Foreign Bank, PVT – Private Bank, PSB – Public Sector Bank*

## 5.3 Conclusion

This chapter has analysed the various IT risk constructs and how each of it varies with different bank types like public banks, private sector banks, foreign banks and cooperative sector banks. The analysis of each of the IT risk constructs against each of these type of banks are explained in detail under the respective sections. The major findings from the analysis include - *external fraud* differs significantly for cooperative sector banks when compared with other bank groups, *external fraud* and *business disruption* significantly differs for cooperative sector banks when compared with other bank groups, *clients, products and business practices* differs significantly for cooperative sector banks when compared with other bank groups, it also differs significantly between public sector banks and foreign banks.

Chapter 6

# ANALYSIS OF IT RISK MANAGEMENT CONSTRUCTS

Contents

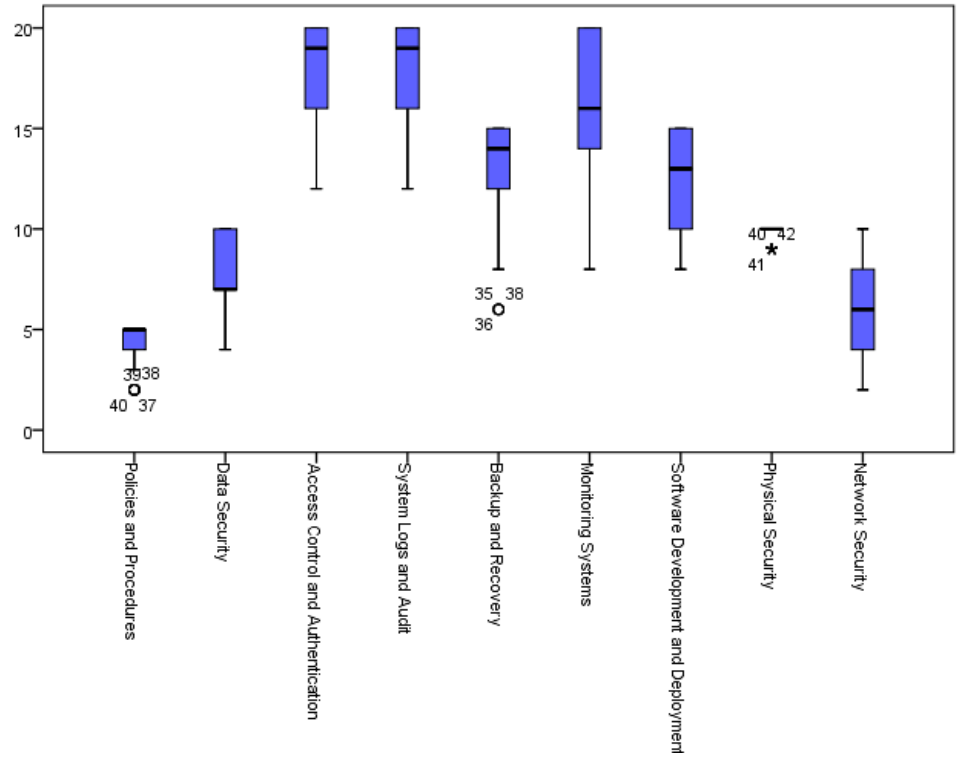


## 6.1 IT Risk Management Variables

As explained in chapter 3, extensive literature review resulted in the identification of several IT risk management factors. The next step was to try to group similar factors together in order to get a clearer picture of the general types of IT risk management factors present. This study being focussed on IT risk management in Indian banking organizations, Basel and RBI guidelines were followed in this process and which resulted in the creation of the following nine general types of software IT risk management categories. The following categories are identified and listed

a) Policies and procedures
b) Data security
c) Access control and authentication
d) System logs and audit
e) Backup and recovery
f) Monitoring systems
g) Software development & deployment
h) Physical security
i) Network security

Figure 6.1 shows the box plot for the above listed Information Technology risk management variables.




Source Data: Survey Data

**Figure 6.1: Box Plot – Information Technology risk management variables**

There are actually nine sub components in the measurement of Information Technology risk management. After the computation of variables, a box plot was generated to check the spread of the data and to find out outliers if any. Outliers were identified and treated based on the methods explained in section 5.1. Suitable methods were used to adjust the outliers according to the need of the data and merit of the method to arrive in producing the descriptive statistics as shown in Table 6.1.

**Table 6.1: Descriptive Statistics – Information Technology risk management**

| | Policies and Procedures | Data Security | Access Control and Authentication | System Logs and Audit | Backup and Recovery | Monitoring Systems | Software Development and Deployment | Physical Security | Network Security |
|---|---|---|---|---|---|---|---|---|---|
| Mean | 4.226 | 7.717 | 18.170 | 17.943 | 12.943 | 15.642 | 12.623 | 9.774 | 6.377 |
| Std. Deviation | 1.1032 | 1.7908 | 2.1815 | 2.4762 | 2.7204 | 3.5631 | 2.3141 | .4225 | 2.3552 |
| Variance | 1.217 | 3.207 | 4.759 | 6.131 | 7.401 | 12.696 | 5.355 | .179 | 5.547 |
| Minimum | 2.0 | 4.0 | 12.0 | 12.0 | 6.0 | 8.0 | 8.0 | 9.0 | 2.0 |
| Maximum | 5.0 | 10.0 | 20.0 | 20.0 | 15.0 | 20.0 | 15.0 | 10.0 | 10.0 |

Source: Survey Data

Table 6.1 explains the descriptive statistics of all the nine sub components of Information Technology risk management and is explained as under.

Policies and procedures for risk management were reported with a mean of 4.226 with a standard deviation of 1.1032 on a one to five scale. The spread was observed as (3) with a minimum of 2 and maximum of 5. The mean of 4.226 on a five point scale indicates that the average policies and procedure implementation in banks is very high. The standard deviation of 1.1032 shows that, fairly large number of respondents has indicated that banks do have well documented and implemented policies and procedures for IT risk management. Thus we can say that the distribution is not very diverse.

Data security measures were reported with a mean of 7.717 with a standard deviation of 1.79 on a one to ten scale. The spread was observed

as (6) with a minimum of 4 and maximum of 10. The mean of 7.717 on a ten point scale indicated that the average data security measures in banks were again high. The standard deviation of 1.79 showed that, fairly large number of respondents has indicated high level of data security in banks. The standard deviation also showed that distribution was not diverse.

Access control and authentication controls were reported with a mean of 18.17 with a standard deviation of 2.1815 on a one to twenty scale. The spread was observed as (8) with a minimum of 12 and maximum of 20. The mean of 18.17 on a twenty point scale indicated that the average access control and authentication controls in banks were very high. The standard deviation of 2.1815 showed that, fairly large number of respondents had indicated high level of access control and authentication controls in banks. The standard deviation also showed that distribution is not very diverse.

System logs and audit controls were reported with a mean of 17.943 with a standard deviation of 2.4762 on a one to twenty scale. The spread was observed as (8) with a minimum of 12 and maximum of 20. The mean of 17.943 on a twenty point scale indicated that the average system logs and audit controls in banks were a very high. The standard deviation of 2.4762 showed that, fairly large number of respondents had indicated high level of system logs and audit controls in banks. The standard deviation also showed that distribution is not very diverse.

Backup and recovery management were reported with a mean of 12.943 with a standard deviation of 2.7204 on a one to fifteen scale. The spread was observed as (9) with a minimum of 6 and maximum of 15. The

mean of 12.943 on a fifteen point scale indicated that the average backup and recovery management in banks was very high. The standard deviation of 2.7204 showed that, fairly large number of respondents had indicated high level of backup and recovery management practices in banks and the distribution was not very diverse.

Monitoring systems were reported with a mean of 15.642 with a standard deviation of 3.5641 on a one to twenty scale. The spread was observed as (12) with a minimum of 8 and maximum of 20. The mean of 15.642 on a twenty point scale indicated that the average use/deployment of monitoring systems in banks was high. The standard deviation of 3.5641 showed that, fairly large number of respondents had indicated increased use of monitoring systems in banks and the distribution was slightly diverse.

Software development and deployment practices were reported with a mean of 12.623 with a standard deviation of 2.3141 on a one to fifteen scale. The spread was observed as (7) with a minimum of 8 and maximum of 15. The mean of 12.623 on a fifteen point scale indicated that the average software development and deployment practices in banks were very high. The standard deviation of 2.3141 showed that, fairly large number of respondents had indicated high use of standard software development and deployment practices and the low standard deviation (2.3141) showed that distribution was not very diverse.

Physical security is reported with a mean of 9.774 with a standard deviation of 0.4225 on a one to ten scale. The spread was observed as (1) with a minimum of 9 and maximum of 10. The mean of 9.774 on a ten

point scale indicated that the average physical security controls in banks was very high. The low standard deviation of 0.4225 showed that, fairly large number of respondents had indicated good physical security systems in banks and the distribution was not diverse.

Network security was reported with a mean of 6.377 with a standard deviation of 2.3552 on a one to ten scale. The spread was observed as (8) with a minimum of 2 and maximum of 10. The mean of 6.377 on a ten point scale indicates that the average network security controls in banks were above average. The standard deviation of 2.3552 shows that, fairly large number of respondents had indicated average or good network security systems in their banks and the distribution was slightly diverse.

**Table 6.2: Summary of Risk Management Controls in Banks**

| No | It Risk Management | Mean | Scale | decision |
|---|---|---|---|---|
| **1** | Policies and procedures | 4.226 | 1 - 5 | High |
| **2** | Data security | 7.717 | 2 - 10 | High |
| **3** | Access control and authentication | 18.170 | 4 - 20 | Very High |
| **4** | System logs and audit | 17.943 | 5- 25 | High |
| **5** | Backup and recovery | 12.943 | 3 - 15 | High |
| **6** | Monitoring systems | 15.642 | 4 - 20 | High |
| **7** | Software development & deployment | 12.623 | 3 - 15 | High |
| **8** | Physical security | 9.774 | 2 - 10 | Very High |
| **9** | Network security | 6.377 | 2 - 10 | High |

Source: Survey Data

## 6.2 Analysis of IT Risk Management across Different Type of Banks

The following sections analyse how each of the IT risk management variables varies with different type of banks. The descriptive statistics is given in table 6.3.

**Table 6.3: Information Technology risk management across different types of banks**

| | | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Policies and Procedures | Foreign | 15 | 4.733 | .4577 |
| | Private | 13 | 4.538 | .6602 |
| | Public Sector | 11 | 5.000 | .0000 |
| | Cooperative | 14 | 2.786 | 1.0509 |
| | Total | 53 | 4.226 | 1.1032 |
| Data Security | Foreign | 15 | 8.333 | 1.5430 |
| | Private | 13 | 7.923 | 1.6053 |
| | Public Sector | 11 | 8.182 | 1.4709 |
| | Cooperative | 14 | 6.500 | 1.9904 |
| | Total | 53 | 7.717 | 1.7908 |
| Access Control and Authentication | Foreign | 15 | 18.467 | 1.7674 |
| | Private | 13 | 18.846 | 1.8640 |
| | Public Sector | 11 | 19.909 | .3015 |
| | Cooperative | 14 | 15.857 | 1.8752 |
| | Total | 53 | 18.170 | 2.1815 |
| System Logs and Audit | Foreign | 15 | 18.733 | 1.5796 |
| | Private | 13 | 18.385 | 2.5013 |
| | Public Sector | 11 | 19.636 | 1.2060 |
| | Cooperative | 14 | 15.357 | 2.0979 |
| | Total | 53 | 17.943 | 2.4762 |
| Backup and Recovery | Foreign | 15 | 13.933 | 1.0998 |
| | Private | 13 | 13.615 | 1.5021 |
| | Public Sector | 11 | 14.909 | .3015 |
| | Cooperative | 14 | 9.714 | 3.1727 |
| | **Total** | **53** | **12.943** | **2.7204** |

Source: Survey Data

Table 6.3 explains that, policies and procedures were found to be followed more in public sector banks (5.000) followed by foreign banks (4.733) and the lowest was observed among co-operative sector banks (2.786). Data security measures were best in foreign banks (8.333) followed by public sector banks (8.182) and the least in cooperative sector banks (6.5). Access control and authentication mechanisms were found to be the best in public sector banks (19.909), followed by private sector banks (18.846), foreign banks (18.467) and the lest in cooperative sector banks (15.857). System logs and audit controls were very good in public sector banks (19.636), followed by foreign banks (18.733), private banks (18.385) and the least in cooperative banks (15.357). Backup and recovery measures were found to be best in public sector banks (14.909), followed by foreign banks (13.933), private banks (13.615) and the least in cooperative sector banks (9.714).

Table 6.4 details the test result for IT risk management across different type of banks. It was observed that for all the five risk management controls (policies and procedures, data security, access control and authentication, system logs and audit, backup and recovery), the test was found to be significant ($p<0.05$) and should conclude that there was sufficient evidence to believe that these controls varies significantly across different bank groups.

**Table 6.4: ANOVA - Information Technology risk management across types of banks**

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Policies and Procedures | Between Groups | 40.762 | 3 | 13.587 | 29.562 | **.000** |
| | Within Groups | 22.521 | 49 | .460 | | |
| | Total | 63.283 | 52 | | | |
| Data Security | Between Groups | 29.362 | 3 | 9.787 | 3.491 | **.022** |
| | Within Groups | 137.393 | 49 | 2.804 | | |
| | Total | 166.755 | 52 | | | |
| Access Control and Authentication | Between Groups | 115.423 | 3 | 38.474 | 14.277 | **.000** |
| | Within Groups | 132.049 | 49 | 2.695 | | |
| | Total | 247.472 | 52 | | | |
| System Logs and Audit | Between Groups | 137.060 | 3 | 45.687 | 12.316 | **.000** |
| | Within Groups | 181.770 | 49 | 3.710 | | |
| | Total | 318.830 | 52 | | | |
| Backup and Recovery | Between Groups | 209.054 | 3 | 69.685 | 19.425 | **.000** |
| | Within Groups | 175.776 | 49 | 3.587 | | |
| | Total | 384.830 | 52 | | | |

Source: Survey Data

A significant F value indicates that there are differences in the means, but it does not tell you where those differences are and therefore, various methods have been developed for doing multiple comparisons of group means. Multiple comparisons will allow a researcher to compare all the group means with each other providing an in depth understanding of the differences in the mean. From Table 6.4, it was observed that all variables are found to be significant, hence no multiple comparisons were executed with an LSD model.

**Table 6.5: Information Technology risk management across different types of banks**

| | | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Monitoring Systems | Foreign | 15 | 16.800 | 2.6511 |
| | Private | 13 | 16.000 | 3.0000 |
| | Public Sector | 11 | 17.727 | 2.9695 |
| | Cooperative | 14 | 12.429 | 3.4130 |
| | Total | 53 | 15.642 | 3.5631 |
| Software Development and Deployment | Foreign | 15 | 12.267 | 2.5204 |
| | Private | 13 | 13.538 | 1.8081 |
| | Public Sector | 11 | 14.727 | .9045 |
| | Cooperative | 14 | 10.500 | 1.1602 |
| | Total | 53 | 12.623 | 2.3141 |
| Physical Security | Foreign | 15 | 9.933 | .2582 |
| | Private | 13 | 9.923 | .2774 |
| | Public Sector | 11 | 10.000 | .0000 |
| | Cooperative | 14 | 9.286 | .4688 |
| | Total | 53 | 9.774 | .4225 |
| Network Security | Foreign | 15 | 6.267 | 1.7915 |
| | Private | 13 | 6.000 | 2.6141 |
| | Public Sector | 11 | 8.000 | 2.3664 |
| | Cooperative | 14 | 5.571 | 2.2434 |
| | Total | 53 | 6.377 | 2.3552 |

Source: Survey Data

Table 6.5 explains that, monitoring systems were found to be deployed more in public sector banks (17.727) followed by foreign banks (16.800), private banks (16.000) and the lowest was observed among co-operative sector banks (12.429). Software development and deployment

methods were best in public sector banks (14.727) followed by private sector banks (13.538), foreign banks (12.267) and the lowest in cooperative sector banks (10.500).

Physical security measures were found to be the best in public sector banks (10.000) followed by foreign banks (9.933), private banks (9.923) and the lowest in cooperative banks (9.286). Network security controls were found to be best in public sector banks (8.000) followed by foreign banks (6.267), private banks (6.000) and the lowest in cooperative banks (5.571).

**Table 6.6: ANOVA - Information Technology risk management across types of banks**

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Monitoring Systems | Between Groups | 214.178 | 3 | 71.393 | 7.843 | **.000** |
| | Within Groups | 446.010 | 49 | 9.102 | | |
| | Total | 660.189 | 52 | | | |
| Software Development and Deployment | Between Groups | 124.607 | 3 | 41.536 | 13.229 | **.000** |
| | Within Groups | 153.846 | 49 | 3.140 | | |
| | Total | 278.453 | 52 | | | |
| Physical Security | Between Groups | 4.569 | 3 | 1.523 | 15.834 | **.000** |
| | Within Groups | 4.714 | 49 | .096 | | |
| | Total | 9.283 | 52 | | | |
| Network Security | Between Groups | 40.091 | 3 | 13.364 | 2.637 | .060 |
| | Within Groups | 248.362 | 49 | 5.069 | | |
| | Total | 288.453 | 52 | | | |

Source: Survey Data

Table 6.6 details the test result for IT risk management across different type of banks. It was observed that for the first three risk management controls (monitoring systems, software development and deployment, physical security), the test was found to be significant ($p<0.05$) and should conclude that there is sufficient evidence to believe that these controls varies significantly across different bank groups. It was also observed that for network security this test was not found to be significant.

A significant F value indicates that there are differences in the means, but it does not tell you where those differences are and therefore, various methods have been developed for doing multiple comparisons of group means. Multiple comparisons will allow a researcher to compare all the group means with each other providing an in depth understanding of the differences in the mean. From Table 6.6, it was observed that all variables were not found to be significant, hence multiple comparisons were executed with an LSD model.

**Table 6.7: LSD Model - Multiple Comparisons – ITRM across different type of banks**

| Dependent Variable | (I) Bank Type | (J) Bank Type | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| Monitoring Systems | Foreign | Private | .8000 | 1.1432 | .487 |
| | | Public Sector | -.9273 | 1.1976 | .442 |
| | | Cooperative | 4.3714* | 1.1212 | **.000** |
| | Private | Foreign | -.8000 | 1.1432 | .487 |
| | | Public Sector | -1.7273 | 1.2360 | .169 |
| | | Cooperative | 3.5714* | 1.1620 | **.003** |
| | Public Sector | Foreign | .9273 | 1.1976 | .442 |
| | | Private | 1.7273 | 1.2360 | .169 |
| | | Cooperative | 5.2987* | 1.2156 | **.000** |
| | Cooperative | Foreign | -4.3714* | 1.1212 | **.000** |
| | | Private | -3.5714* | 1.1620 | **.003** |
| | | Public Sector | -5.2987* | 1.2156 | **.000** |

| Dependent Variable | (I) Bank Type | (J) Bank Type | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| Software Development and Deployment | Foreign | Private | -1.2718 | .6714 | .064 |
| | | Public Sector | -2.4606* | .7034 | **.001** |
| | | Cooperative | 1.7667* | .6585 | **.010** |
| | Private | Foreign | 1.2718 | .6714 | .064 |
| | | Public Sector | -1.1888 | .7259 | .108 |
| | | Cooperative | 3.0385* | .6825 | **.000** |
| | Public Sector | Foreign | 2.4606* | .7034 | **.001** |
| | | Private | 1.1888 | .7259 | .108 |
| | | Cooperative | 4.2273* | .7139 | **.000** |
| | Cooperative | Foreign | -1.7667* | .6585 | **.010** |
| | | Private | -3.0385* | .6825 | **.000** |
| | | Public Sector | -4.2273* | .7139 | **.000** |
| Physical Security | Foreign | Private | .0103 | .1175 | .931 |
| | | Public Sector | -.0667 | .1231 | .591 |
| | | Cooperative | .6476* | .1153 | **.000** |
| | Private | Foreign | -.0103 | .1175 | .931 |
| | | Public Sector | -.0769 | .1271 | .548 |
| | | Cooperative | .6374* | .1195 | **.000** |
| | Public Sector | Foreign | .0667 | .1231 | .591 |
| | | Private | .0769 | .1271 | .548 |
| | | Cooperative | .7143* | .1250 | **.000** |
| | Cooperative | Foreign | -.6476* | .1153 | **.000** |
| | | Private | -.6374* | .1195 | **.000** |
| | | Public Sector | -.7143* | .1250 | **.000** |
| Network Security | Foreign | Private | .2667 | .8531 | .756 |
| | | Public Sector | -1.7333 | .8937 | .058 |
| | | Cooperative | .6952 | .8366 | .410 |
| | Private | Foreign | -.2667 | .8531 | .756 |
| | | Public Sector | -2.0000* | .9223 | **.035** |
| | | Cooperative | .4286 | .8671 | .623 |
| | Public Sector | Foreign | 1.7333 | .8937 | .058 |
| | | Private | 2.0000* | .9223 | **.035** |
| | | Cooperative | 2.4286* | .9071 | **.010** |
| | Cooperative | Foreign | -.6952 | .8366 | .410 |
| | | Private | -.4286 | .8671 | .623 |
| | | Public Sector | -2.4286* | .9071 | **.010** |
| ** The mean difference is significant at the 0.05 level.* | | | | | |

Source: Survey Data

In the case of monitoring systems, it differed significantly ($p < 0.05$) for the cooperative banks alone when we compared it with the other groups viz private, foreign and public sector banks. Hence we can concluded that the monitoring system in cooperative banks was significantly different from private, foreign and public sector banks.

In the case of software development and deployment practices, it differed significantly for the cooperative banks alone when we compare it with the other groups viz foreign, private and public sector banks. Hence we can conclude that the software development and deployment practices for cooperative banks differed significantly from foreign, private and public sector banks. It was also found that the software development and deployment practices differ significantly between public sector and foreign banks.

In the case of physical security, it differed significantly for the cooperative banks alone when we compare it with the other groups viz private, foreign and public sector banks. Hence we can conclude that the physical security in cooperative banks is significantly different from private, foreign and public sector banks.

Network security was found differing significantly between the public sector banks and cooperative banks and private banks. Hence we can conclude that the physical security mechanism in cooperative banks is significantly different from public sector banks and the physical security mechanisms in private sector banks are also significantly different from public sector banks.

**Table 6.8: IT Risk Management Constructs - Variation Across Different Bank Types**

| No | IT Risk Management Across Bank Types | High | | | Low |
|---|---|---|---|---|---|
| 1 | Policies and procedures | PSB (5.00) | FB (4.73) | PVT (4.54) | COB (2.79) |
| 2 | Data security | FB (8.33) | PSB (8.18) | PVT (7.92) | COB (6.50) |
| 3 | Access control and authentication | PSB (18.47) | PVT (18.85) | FS (18.47) | COB (15.86) |
| 4 | System logs and audit | PSB (19.64) | FB (18.73) | PVT (18.38) | COB (15.36) |
| 5 | Backup and recovery | PSB (14.91) | FB (13.93) | PVT (13.62) | COB (9.71) |
| 6 | Monitoring systems | PSB (17.73) | FB (16.8) | PVT (16.00) | COB (12.43) |
| 7 | Software development & deployment | PSB (14.73) | PVT (13.54) | FB (12.27) | COB (10.50) |
| 8 | Physical security | PSB (10.00) | FB (9.93) | PVT (9.92) | COB (9.29) |
| 9 | Network security | PSB (8.00) | FB (6.27) | PVT (6.00) | COB (5.57) |

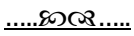
Source: Survey Data

COB – Cooperative Bank, FB – Foreign Bank, PVT – Private Bank, PSB – Public Sector Bank

## 6.3 Conclusion

This chapter six analysed the various IT risk management constructs and how each of it varied with different bank types like public banks, private sector banks, foreign banks and cooperative sector banks. The analysis of each of the IT risk management constructs against each of the different type of banks were explained in detail under the respective sections. The analysis had shown that for the first five risk management controls (policies and procedures, data security, access control and

authentication, system logs and audit, backup and recovery), the test was found to be significant ($p<0.05$) and these controls varied significantly across different bank groups. The risk management controls (monitoring systems, software development and deployment, physical security and network security) in cooperative sector banks, differed significantly when compared with other bank groups. Software development and deployment differed significantly between public sector banks and foreign sector banks. Network security differed significantly between public sector banks and private and cooperative sector banks.



# Chapter 7

# ANALYSIS OF IT RISK IMPACT CONSTRUCTS

Contents



## 7.1 IT Risk Impacts

As explained in chapter 3, extensive literature review resulted in the identification of several IT risk impact factors. The impacts of IT risks on assets are grouped into financial and nonfinancial. The study being focussed in Indian banking organizations, RBI and Basel guide lines were followed in this process and which resulted in the creation of the following two general type of IT risk impacts, namely financial impacts and nonfinancial impacts. The following categories are identified and listed.

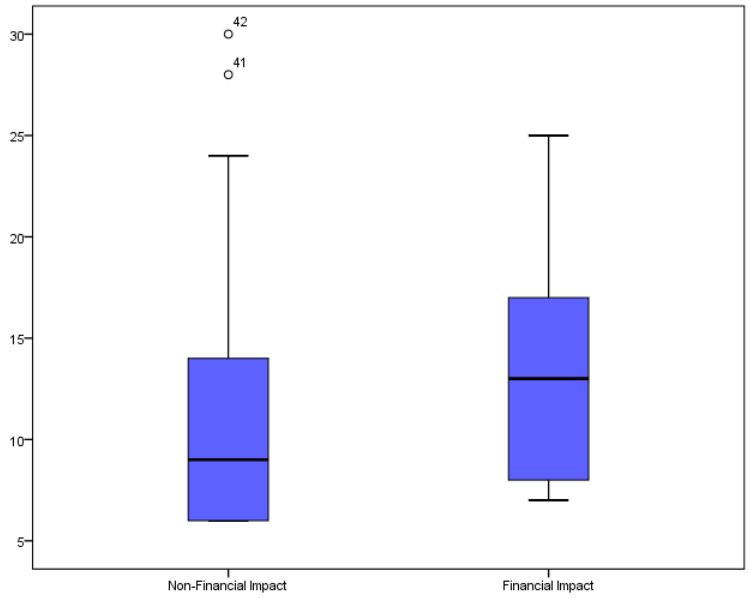
### 7.1.1 Non-Financial Impacts

a) Confidentiality
b) Integrity
c) Availability
d) Reputation
e) Non-compliance
f) Business (customer loss, customer complaints and account closure)

### 7.1.2 Financial Impacts

a) Financial loss (loss of money)

Figure 7.1 shows the box plot for the above listed financial and non-financial impact variables.




Source: Survey Data

**Figure 7.1: Box Plot - IT Risk Impact Variables**

There were actually two sub components in the measurement of Information Technology risk impacts on banks. After the computation of variables, a box plot was generated to check the spread of the data and to find out outliers, if any. Outliers were identified and treated based on the methods explained in section 5.1. Suitable methods were used to adjust the outliers according to the need of the data and merit of the method to arrive in producing the descriptive statistics as shown in Table 7.1

**Table 7.1: Descriptive Statistics – Information Technology risk management**

| | Non-Financial Impact | Financial Impact |
|---|---|---|
| Mean | 10.943 | 13.170 |
| Std. Deviation | 5.7493 | 5.0942 |
| Variance | 33.054 | 25.951 |
| Minimum | 6.0 | 7.0 |
| Maximum | 30.0 | 25.0 |

Source: Survey Data

Table 7.1 explains the descriptive statistics of the two sub components of Information Technology risk impacts and is explained as under.

Financial impacts were reported with a mean of 13.170 with a standard deviation of 5.0942 on a one to thirty five scale. The spread was observed as (18) with a minimum of 7 and maximum of 25. The mean of 13.170 on a thirty point scale indicated that the average financial impacts in banks were below average. The standard deviation of 5.0942 showed that, fairly large number of respondents had indicated that banks may face average or below average financial impacts due to technology risks present in their banks. Thus we can also say that the distribution is moderately diverse.

Non-financial impacts were reported with a mean of 10.943 with a standard deviation of 5.7493 on a one to thirty scale. The spread was observed as (24) with a minimum of 6 and maximum of 30. The mean of 10.943 on a thirty point scale indicates that the average non-financial impacts in banks were below average. The standard deviation of 5.7493 showed that, fairly large number of respondents had indicated that banks may face average or below average impacts due to technology risks present in their banks. Thus we can also say that the distribution is moderately diverse.

**Table 7.2: Summary of IT Risk Impacts**

| No | IMPACTS | MEAN | SCALE | LEVEL |
|---|---|---|---|---|
| **1** | Financial Impacts | 13.170 | 7 – 35 | Low |
| **2** | Non-Financial Impacts | 10.943 | 6 – 30 | Low |

Source: Survey Data

## 7.2 Analysis of IT Risk Impacts across Different Type of Banks

The following sections analyse the IT risk impacts (financial and non-financial) across different type of banks, viz foreign, private, public and cooperative sector banks.

**Table 7.3: Information Technology Risk Impacts across different types of banks**

| | | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Non-Financial Impact | Foreign | 15 | 8.800 | 3.6878 |
| | Private | 13 | 11.692 | 5.2502 |
| | Public Sector | 11 | 7.636 | 1.7477 |
| | Cooperative | 14 | 15.143 | 7.4613 |
| | **Total** | **53** | **10.943** | **5.7493** |
| Financial Impact | Foreign | 15 | 11.933 | 4.4636 |
| | Private | 13 | 14.462 | 5.3012 |
| | Public Sector | 11 | 10.091 | 2.4680 |
| | Cooperative | 14 | 15.714 | 5.7703 |
| | **Total** | **53** | **13.170** | **5.0942** |

Source: Survey Data

Table 7.3 explains that, non-financial impacts were found to be affected more in cooperative sector banks (15.143) followed by private sector banks (11.692), foreign banks (8.800) and the lowest was observed among public sector banks (7.636). Financial impacts were found to be

more cooperative banks (15.714), followed by private banks (14.462), foreign banks (11.933) and then public sector banks (10.091).

**Table 7.4: ANOVA - Information Technology risk impact across types of banks**

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Non-Financial Impact | Between Groups | 443.401 | 3 | 147.800 | 5.678 | **.002** |
| | Within Groups | 1275.429 | 49 | 26.029 | | |
| | **Total** | **1718.830** | **52** | | | |
| Financial Impact | Between Groups | 239.541 | 3 | 79.847 | 3.525 | **.022** |
| | Within Groups | 1109.930 | 49 | 22.652 | | |
| | **Total** | **1349.472** | **52** | | | |

Source: Survey Data

Table 7.4 details the test result for IT risk impacts across different type of banks. It was observed that for both the financial and non-financial impacts, the test was not found to be significant ($p<0.05$) and should conclude that there was sufficient evidence to believe the financial and non-financial impacts varied significantly across different bank groups.

A significant F value indicates that there are differences in the means, but it does not tell you where those differences are and therefore, various methods have been developed for doing multiple comparisons of group means. Multiple comparisons will allow a researcher to compare all the group means with each other providing an in depth understanding of the differences in the mean. From Table 7.4, it is observed that all variables are not found to be significant, hence multiple comparisons were executed with an LSD model.

**Table 7.5: LSD Model – IT risk impacts multiple comparisons**

| Dependent Variable | (I) Bank Type | (J) Bank Type | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| Non-Financial Impact | Foreign | Private | -2.8923 | 1.9333 | .141 |
| | | Public Sector | 1.1636 | 2.0252 | .568 |
| | | Cooperative | -6.3429* | 1.8959 | **.002** |
| | Private | Foreign | 2.8923 | 1.9333 | .141 |
| | | Public Sector | 4.0559 | 2.0901 | .058 |
| | | Cooperative | -3.4505 | 1.9651 | .085 |
| | Public Sector | Foreign | -1.1636 | 2.0252 | .568 |
| | | Private | -4.0559 | 2.0901 | .058 |
| | | Cooperative | -7.5065* | 2.0556 | **.001** |
| | Cooperative | Foreign | 6.3429* | 1.8959 | **.002** |
| | | Private | 3.4505 | 1.9651 | .085 |
| | | Public Sector | 7.5065* | 2.0556 | **.001** |
| Financial Impact | Foreign | Private | -2.5282 | 1.8035 | .167 |
| | | Public Sector | 1.8424 | 1.8893 | .334 |
| | | Cooperative | -3.7810* | 1.7686 | **.038** |
| | Private | Foreign | 2.5282 | 1.8035 | .167 |
| | | Public Sector | 4.3706* | 1.9498 | **.030** |
| | | Cooperative | -1.2527 | 1.8331 | .498 |
| | Public Sector | Foreign | -1.8424 | 1.8893 | .334 |
| | | Private | -4.3706* | 1.9498 | **.030** |
| | | Cooperative | -5.6234* | 1.9176 | **.005** |
| | Cooperative | Foreign | 3.7810* | 1.7686 | **.038** |
| | | Private | 1.2527 | 1.8331 | .498 |
| | | Public Sector | 5.6234* | 1.9176 | **.005** |

**. The mean difference is significant at the 0.05 level.*

Source: Survey Data

In the case of non-financial impacts, it differed significantly ($p < 0.05$) for the cooperative banks alone when we compared it with the

other groups viz foreign and public sector banks. Hence we can conclude that the non-financial impacts in cooperative banks are significantly different from foreign and public sector banks.

In the case of financial impacts, it differed significantly for the cooperative banks when we compared it with the other groups viz foreign and public sector banks. Hence we can conclude that the financial impacts for cooperative banks differed significantly from foreign and public sector banks. It was also found that the financial impacts differ significantly between public sector and private sector banks.

**Table 7.6: IT Risk Impact Constructs – Variations across Different Bank Types**

| No | IMPACTS | High | | | Low |
|---|---|---|---|---|---|
| **1** | Financial Impacts | COB (15.71) | PVT (14.46) | FB (11.93) | PSB (10.09) |
| **2** | Non-Financial Impacts | COB (15.14) | PVT (11.69) | FB (8.80) | PSB (7.64) |

Source: Survey Data

## 7.3 Financial Vs Non-Financial Impacts

IT risks like fraud, identity theft or failure of systems can cause non-financial damages like loss of reputation to the bank, loss of business, or even regulatory actions from the Central Bank and subsequent closure of the Bank itself. These non-financial risks are more damaging, and the risks and impacts in one bank may affect other banks and may even lead to a systemic risk, which can even affect the financial stability of a country. Some of relevant literature review is attached below.

"The report on 'Management of Non-Financial Risks' by Bank for International Settlements (Central Bank Governance Group, 2009) focuses on the opportunities available to central banks to enhance, and thus gain more benefits from, their management of non-financial risks, like operational risks, policy risk, reputational risk, etc. Damage to reputation and/or brand has moved up to No. 4 from No. 6 among the Top 10 risks identified in Aon's 2011 Global Risk Management Risk Ranking. Reputation risk, perhaps it is of greater significance and importance to banks due to the fact that banks deal more with others' (other than owners') money, be it that of depositors, customers, counterparties, investors, among others. This paper (Sumit, 2013) makes an attempt to understand the gamut of reputational risks and understand the challenges, opportunities and possible responses from banks towards this new risk."

"A study of impact of technology (mobile devices) on information security on IT professionals ( Dimensional Research, 2013) revealed that, securing corporation information, including customer information is a challenge and the related security incidents are very expensive. These incidents and the impacts of such greater security risk than reported to be worse than cybercriminals. The costs and consequences of non-compliance too within financial services firms are greater than ever before. Other than monitory fines, organization may fire senior managers, may experience expensive and disruptive operational consequences and customer distrusts (Stacey & Susannah, 2013)"

## 7.4 Conclusion

Chapter seven analysed the financial and non-financial impacts of IT risks and how each of it varies with different bank types like public banks, private sector banks, foreign banks and cooperative sector banks. The analysis of impacts against each of the different types of banks was explained in detail under the respective sections. The analysis has shown that nonfinancial and financial impacts differ significantly for cooperative sector banks when compared with public and foreign banks. Financial impacts differ significantly between private and public sector banks.

Chapter 8

# ANALYSIS & DISCUSSION OF IT RISK, RISK MANAGEMENT & IMPACTS

Contents



## 8.1 Introduction

Chapter 3 has already presented the hypotheses on the anticipated relationship among the variables in the study. This section presents the results of the hypothesis tests.

IT risk, risk management and impacts are metric in nature whereas bank characteristics are categories. ANOVA was used for testing hypothesis H1, H2, H3 and H4 which checked for variation of the metric dependent variable risk, risk management and impacts across categories of the independent variable such as bank characteristics.

## 8.2 Analysis of IT Risk, IT Risk Management and Impacts across Bank Types

Table 8.1 explains that, based on the data analysis, IT risk was found to be more in cooperative sector banks (68.4286) followed by private sector banks (56.2308), foreign banks (54.8667) and the lowest was observed among public sector banks (48.8182). IT risk management was reported to be the best in public sector banks (118.0909), followed by foreign banks (109.4667), private banks (108.7692) and co-operative sector banks (88.00). It was seen than banks with better IT risk management controls reported lower IT risks.

The impacts of IT risk on different bank types were also analysed and the results were as follows. The non-financial impacts were found to be the highest in co-operative sector banks (15.143), followed by private sector banks (11.692), Foreign banks (8.8) and the least in public sector banks (7.636). The financial impacts were found to be the highest in co-operative banks (15.714), followed by private banks (14.462), foreign banks (11.933) and the least in public sector banks (10.091). It was observed that the financial and non-financial impacts were reported to be highest in co-operative sector banks and lowest in public sector banks.

**Table 8.1: Descriptive Statistics - IT Risk, risk management and impact across different types of banks**

| | | N | Mean | Std. Deviation |
|---|---|---|---|---|
| **Information Technology Risk** | Foreign | 15 | 54.8667 | 13.63748 |
| | Private | 13 | 56.2308 | 15.63732 |
| | Public | 11 | 48.8182 | 6.20996 |
| | Cooperative | 14 | 68.4286 | 6.58336 |
| | Total | 53 | 57.5283 | 13.23835 |
| **Information Technology Risk Management** | Foreign | 15 | 109.4667 | 10.10563 |
| | Private | 13 | 108.7692 | 12.74202 |
| | Public | 11 | 118.0909 | 5.64720 |
| | Cooperative | 14 | 88.0000 | 13.28967 |
| | Total | 53 | 105.4151 | 15.44149 |
| **Non-Financial Impact** | Foreign | 15 | 8.800 | 3.6878 |
| | Private | 13 | 11.692 | 5.2502 |
| | Public | 11 | 7.636 | 1.7477 |
| | Cooperative | 14 | 15.143 | 7.4613 |
| | Total | 53 | 10.943 | 5.7493 |
| **Financial Impact** | Foreign | 15 | 11.933 | 4.4636 |
| | Private | 13 | 14.462 | 5.3012 |
| | Public | 11 | 10.091 | 2.4680 |
| | Cooperative | 14 | 15.714 | 5.7703 |
| | Total | 53 | 13.170 | 5.0942 |

Source: Survey Data

**Table 8.2: Summary of IT risk, risk management and impact across different types of banks**

| No | VARIABLE | High | | | Low |
|---|---|---|---|---|---|
| **1** | IT Risk | COB (68.43) | PVT (56.23) | FB (54.87) | PSB (48.82) |
| **2** | IT Risk Management | PSB (118.09) | FS (109.47) | PVT (108.77) | COB (88.00) |
| **3** | FI | COB (15.71) | PVT (14.46) | FB (11.93) | PSB (10.09) |
| **4** | NFI | COB (15.14) | PVT (11.69) | FB (8.80) | PSB (7.64) |

Source: Survey Data

COB – Cooperative Bank, FB – Foreign Bank, PVT – Private Bank, PSB – Public Sector Bank

### 8.2.1 Hypothesis Testing

**H5**: There is significant variation in IT risk, IT risk management and impacts among different type of banks.

**H5a**: There is a significant variation in IT risk across different types of banks.

**H5b**: There is a significant variation in IT risk management across different types of banks

**H5c**: There is a significant variation in IT risk impacts across different types of banks

Table 8.2 details the test result for IT risk, IT risk management and Impacts across different type of banks. It was observed that for IT risk, IT risk management, Impacts (financial and non-financial), the test was found to be significant ($p<0.05$) and should conclude that there was sufficient evidence to believe the IT risk, IT risk management and impacts were significantly different across different bank groups.

A significant F value indicates that there are differences in the means, but it does not tell you where those differences are and therefore, various methods have been developed for doing multiple comparisons of group means. Multiple comparisons will allow a researcher to compare all the group means with each other providing an in depth understanding of the differences in the mean. From Table 8.2, it was observed that all variables were not found to be significant, hence multiple comparisons were executed with an LSD model.

**Table 8.3: ANOVA – IT risk, risk management and impact across different types of banks**

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Information Technology Risk | Between Groups | 2626.102 | 3 | 875.367 | 6.612 | .001 |
| | Within Groups | 6487.106 | 49 | 132.390 | | |
| | Total | 9113.208 | 52 | | | |
| Information Technology Risk Management | Between Groups | 6405.918 | 3 | 2135.306 | 17.459 | .000 |
| | Within Groups | 5992.950 | 49 | 122.305 | | |
| | Total | 12398.868 | 52 | | | |
| Non-Financial Impact | Between Groups | 443.401 | 3 | 147.800 | 5.678 | .002 |
| | Within Groups | 1275.429 | 49 | 26.029 | | |
| | Total | 1718.830 | 52 | | | |
| Financial Impact | Between Groups | 239.541 | 3 | 79.847 | 3.525 | .022 |
| | Within Groups | 1109.930 | 49 | 22.652 | | |
| | Total | 1349.472 | 52 | | | |

Source: Survey Data

**Table 8.4: LSD (Multiple Comparisons) – IT risk, risk management and impact across different types of banks**

| Dependent Variable | (I) Bank Type | (J) Bank Type | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| Information Technology Risk | Foreign | Private | -1.36410 | 4.36003 | .756 |
| | | Public Sector | 6.04848 | 4.56743 | .192 |
| | | Cooperative | -13.56190* | 4.27579 | **.003** |
| | Private | Foreign | 1.36410 | 4.36003 | .756 |
| | | Public Sector | 7.41259 | 4.71373 | .122 |
| | | Cooperative | -12.19780* | 4.43173 | **.008** |
| | Public | Foreign | -6.04848 | 4.56743 | .192 |
| | | Private | -7.41259 | 4.71373 | .122 |
| | | Cooperative | -19.61039* | 4.63593 | **.000** |
| | Cooperative | Foreign | 13.56190* | 4.27579 | **.003** |
| | | Private | 12.19780* | 4.43173 | **.008** |
| | | Public Sector | 19.61039* | 4.63593 | **.000** |
| Information Technology Risk Management | Foreign | Private | .69744 | 4.19068 | .869 |
| | | Public Sector | -8.62424 | 4.39002 | .055 |
| | | Cooperative | 21.46667* | 4.10971 | **.000** |
| | Private | Foreign | -.69744 | 4.19068 | .869 |
| | | Public Sector | -9.32168* | 4.53064 | **.045** |
| | | Cooperative | 20.76923* | 4.25960 | **.000** |
| | Public | Foreign | 8.62424 | 4.39002 | .055 |
| | | Private | 9.32168* | 4.53064 | **.045** |
| | | Cooperative | 30.09091* | 4.45586 | **.000** |
| | Cooperative | Foreign | -21.46667* | 4.10971 | **.000** |
| | | Private | -20.76923* | 4.25960 | **.000** |
| | | Public Sector | -30.09091* | 4.45586 | **.000** |
| Non-Financial Impact | Foreign | Private | -2.8923 | 1.9333 | .141 |
| | | Public Sector | 1.1636 | 2.0252 | .568 |
| | | Cooperative | -6.3429* | 1.8959 | **.002** |
| | Private | Foreign | 2.8923 | 1.9333 | .141 |
| | | Public Sector | 4.0559 | 2.0901 | .058 |
| | | Cooperative | -3.4505 | 1.9651 | .085 |
| | Public | Foreign | -1.1636 | 2.0252 | .568 |
| | | Private | -4.0559 | 2.0901 | .058 |
| | | Cooperative | -7.5065* | 2.0556 | **.001** |
| | Cooperative | Foreign | 6.3429* | 1.8959 | **.002** |
| | | Private | 3.4505 | 1.9651 | .085 |
| | | Public Sector | 7.5065* | 2.0556 | **.001** |

| Dependent Variable | (I) Bank Type | (J) Bank Type | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| Financial Impact | Foreign | Private | -2.5282 | 1.8035 | .167 |
| | | Public Sector | 1.8424 | 1.8893 | .334 |
| | | Cooperative | -3.7810* | 1.7686 | **.038** |
| | Private | Foreign | 2.5282 | 1.8035 | .167 |
| | | Public Sector | 4.3706* | 1.9498 | **.030** |
| | | Cooperative | -1.2527 | 1.8331 | .498 |
| | Public | Foreign | -1.8424 | 1.8893 | .334 |
| | | Private | -4.3706* | 1.9498 | **.030** |
| | | Cooperative | -5.6234* | 1.9176 | **.005** |
| | Cooperative | Foreign | 3.7810* | 1.7686 | **.038** |
| | | Private | 1.2527 | 1.8331 | .498 |
| | | Public Sector | 5.6234* | 1.9176 | **.005** |
| ** The mean difference is significant at the 0.05 level.* | | | | | |

Source: Survey Data

In the case of IT risks and IT Risk Management, it differed significantly ($p < 0.05$) for the cooperative banks alone when we compared it with the other groups viz foreign, private and public sector banks. Hence we concluded that the IT risks and risk management in cooperative banks were significantly different from foreign and public sector banks.

In the case of non-financial impacts, it differed significantly between co-operative banks and public sector and foreign banks. The financial impact differed significantly between co-operative banks and public sector banks. No other significant variations were found between other types of banks. ANOVA & LSD Multiple Comparisons shows that,

a) IT risk, IT risk management, financial impact and nonfinancial impact in cooperative banks was significantly different when compared with other groups

b) IT risk management was significantly different between public and private sector banks

c) Financial impact differed significantly between PSB and PVT

These findings supported the hypothesis (H5a, H5b, H5c) that there was a significant relationship between bank type and IT risk, risk management and its impacts.

## 8.3 Analysis of IT Risk, Risk Management and Impacts Based On Geographical Spread

Table 8.4 explains that, based on the data analysis, IT risk was found to be more in banks operating in a single state (68.4286) followed by banks in multiple countries (54.8667) and the least for banks operating in multiple states (52.8333). IT risk management was found to be more in banks operating in multiple state (113.0417) followed by banks in multiple countries (109.4667) and the least for banks operating in single states (88.0). It was seen that banks with better IT risk management controls, reported lower IT risks irrespective of the geographical spread.

### 8.3.1 Hypothesis Testing

**H5d**: There is a significant variation in IT risk across different geographical spread of the bank

**H5e**: There is a significant variation in IT risk management across different geographical spread of the bank

**H5f**: There is a significant variation in IT risk impacts across different geographical spread of the bank

The risk impacts based on geographical spread were also analysed and the results were as follows. The non-financial impacts were found to be the highest in banks operating in single state (15.143), followed by

banks in multiple states (9.833) and the least in banks operating in multiple countries (8.8). The Financial impacts were found to be the highest in banks operating in single state (15.714), followed by banks in multiple states (12.458) and the least in banks operating in multiple countries (11.933). It was observed that the financial and non-financial impacts were reported to be highest in banks operating in single state and lowest with banks operating in multiple countries.

**Table 8.5: Descriptive statistics – IT risk, Risk management and Impact based on Geographical Spread of banks**

| | | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Information Technology Risk | Multiple Location, Single State | 14 | 68.4286 | 6.58336 |
| | Multiple Location, Multiple State | 24 | 52.8333 | 12.59284 |
| | Multiple Location, Multiple Countries | 15 | 54.8667 | 13.63748 |
| | **Total** | **53** | **57.5283** | **13.23835** |
| Information Technology Risk Management | Multiple Location, Single State | 14 | 88.0000 | 13.28967 |
| | Multiple Location, Multiple State | 24 | 113.0417 | 11.00387 |
| | Multiple Location, Multiple Countries | 15 | 109.4667 | 10.10563 |
| | **Total** | **53** | **105.4151** | **15.44149** |
| Non-Financial Impact | Multiple Location, Single State | 14 | 15.143 | 7.4613 |
| | Multiple Location, Multiple State | 24 | 9.833 | 4.4689 |
| | Multiple Location, Multiple Countries | 15 | 8.800 | 3.6878 |
| | **Total** | **53** | **10.943** | **5.7493** |
| Financial Impact | Multiple Location, Single State | 14 | 15.714 | 5.7703 |
| | Multiple Location, Multiple State | 24 | 12.458 | 4.7180 |
| | Multiple Location, Multiple Countries | 15 | 11.933 | 4.4636 |
| | **Total** | **53** | **13.170** | **5.0942** |

Source: Survey Data

**Table 8.6: Summary of IT risk, Risk management and Impact based on Geographical Spread of banks**

| No | Based on Geographical Spread | High | Medium | Low |
|---|---|---|---|---|
| **1** | ITR | Single State | Multiple Countries | Multiple States |
| **2** | ITRM | Multiple State | Multiple Countries | Single State |
| **3** | FI | Single State | Multiple State | Multiple Countries |
| **4** | NFI | Single State | Multiple State | Multiple Countries |

Source: Survey Data

Table 8.7 details the test result for IT risk, IT risk management and impacts on assets across banks with different geographical spreads. It was observed that for IT risk, IT risk management, impacts (non-financial only), the test was found to be significant ($p<0.05$) and should be concluded that there was sufficient evidence to believe the IT risk, IT risk management and Impacts were significantly different across different bank groups based on geographical spread.

A significant F value indicates that there are differences in the means, but it does not tell you where those differences are and therefore, various methods have been developed for doing multiple comparisons of group means. Multiple comparisons will allow a researcher to compare all the group means with each other providing an in depth understanding of the differences in the mean. From Table 8.7, it was observed that all variables were not found to be significant, hence multiple comparisons were executed with an LSD model.

**Table 8.7: ANOVA – IT risk, risk management and impact based on Geographical Spread of banks**

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| **Information Technology Risk** | Between Groups | 2298.712 | 2 | 1149.356 | 8.433 | **.001** |
| | Within Groups | 6814.495 | 50 | 136.290 | | |
| | **Total** | **9113.208** | **52** | | | |
| **Information Technology Risk Management** | Between Groups | 5888.176 | 2 | 2944.088 | 22.610 | **.000** |
| | Within Groups | 6510.692 | 50 | 130.214 | | |
| | **Total** | **12398.868** | **52** | | | |
| **Non-Financial Impact** | Between Groups | 345.383 | 2 | 172.691 | 6.287 | **.004** |
| | Within Groups | 1373.448 | 50 | 27.469 | | |
| | **Total** | **1718.830** | **52** | | | |
| **Financial Impact** | Between Groups | 125.723 | 2 | 62.861 | 2.568 | .087 |
| | Within Groups | 1223.749 | 50 | 24.475 | | |
| | **Total** | **1349.472** | **52** | | | |

Source: Survey Data

**Table 8.8: LSD (Multiple Comparisons) – IT risk, risk management and impact based on Geographical Spread of banks**

| Dependent Variable | (I) Geographical Spread | (J) Geographical Spread | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| **Information Technology Risk** | Multiple Location, Single State | Multiple Location, Multiple State | 15.59524* | 3.92603 | **.000** |
| | | Multiple Location, Multiple Countries | 13.56190* | 4.33832 | **.003** |
| | Multiple Location, Multiple State | Multiple Location, Single State | -15.59524* | 3.92603 | **.000** |
| | | Multiple Location, Multiple Countries | -2.03333 | 3.84249 | .599 |
| | Multiple Location, Multiple Countries | Multiple Location, Single State | -13.56190* | 4.33832 | **.003** |
| | | Multiple Location, Multiple State | 2.03333 | 3.84249 | .599 |

| Dependent Variable | (I) Geographical Spread | (J) Geographical Spread | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| **Information Technology Risk Management** | Multiple Location, Single State | Multiple Location, Multiple State | -25.04167* | 3.83752 | **.000** |
| | | Multiple Location, Multiple Countries | -21.46667* | 4.24051 | **.000** |
| | Multiple Location, Multiple State | Multiple Location, Single State | 25.04167* | 3.83752 | **.000** |
| | | Multiple Location, Multiple Countries | 3.57500 | 3.75586 | .346 |
| | Multiple Location, Multiple Countries | Multiple Location, Single State | 21.46667* | 4.24051 | **.000** |
| | | Multiple Location, Multiple State | -3.57500 | 3.75586 | .346 |
| **Non-Financial Impact** | Multiple Location, Single State | Multiple Location, Multiple State | 5.3095* | 1.7626 | **.004** |
| | | Multiple Location, Multiple Countries | 6.3429* | 1.9476 | **.002** |
| | Multiple Location, Multiple State | Multiple Location, Single State | -5.3095* | 1.7626 | **.004** |
| | | Multiple Location, Multiple Countries | 1.0333 | 1.7251 | .552 |
| | Multiple Location, Multiple Countries | Multiple Location, Single State | -6.3429* | 1.9476 | **.002** |
| | | Multiple Location, Multiple State | -1.0333 | 1.7251 | .552 |
| **Financial Impact** | Multiple Location, Single State | Multiple Location, Multiple State | 3.2560 | 1.6637 | .056 |
| | | Multiple Location, Multiple Countries | 3.7810* | 1.8384 | **.045** |
| | Multiple Location, Multiple State | Multiple Location, Single State | -3.2560 | 1.6637 | .056 |
| | | Multiple Location, Multiple Countries | .5250 | 1.6283 | .748 |
| | Multiple Location, Multiple Countries | Multiple Location, Single State | -3.7810* | 1.8384 | **.045** |
| | | Multiple Location, Multiple State | -.5250 | 1.6283 | .748 |
| ***The mean difference is significant at the 0.05 level.*** | | | | | |

Source: Survey Data

In the case of IT risks and IT risk management it differed significantly ($p < 0.05$) for the banks in single state when we compared it with the other groups viz banks in multiple states and banks in multiple countries. Hence we can conclude that the IT risks and IT risk management in banks operating in single state was significantly different from banks operating in multiple states and multiple countries. And the data also showed that there was no significant variation in IT risks and IT risk management between banks operating in multiple states and multiple countries.

In the case of impacts (financial and non-financial) it differed significantly between banks operating in single state with that operating in multiple states and multiple countries. There was no significant variation in the impacts between banks operating in multiple states and multiple countries. ANOVA & LSD Multiple Comparisons shows that,

a) IT risk and IT risk management in banks operating in single state was significantly different from banks operating in multiple states and multiple countries.

b) Financial and nonfinancial impacts differed significantly between banks operating in single state with that operating in multiple states and multiple countries.

These findings supported the hypothesis (H5d, H5e, H5f) that there was a significant relationship between geographical spread of the bank and IT risk, risk management and impacts.

## 8.4 Analysis of IT Risk, Risk Management and Impacts Based On Technology Characteristics

The following sections describe the descriptive statistics for IT risk, IT risk management and impacts based on technology characteristics.

### 8.4.1 Software Development Methodology

**Hypothesis Testing**

**H5g**: There is a significant variation in IT risk across different software development methodology used by the bank

**H5h**: There is a significant variation in IT risk management across different software development methodology used by the bank

**H5i**: There is a significant variation in IT risk impacts across different software development methodology used by the bank

Based on the analysis shown in Table 8.9, IT risk was found to be more in banks using software developed by outsourced vendors (58.6154) compared to banks using in-house developed software (51.90). IT risk management was found to be strong in banks using in-house developed software (113.00) compared to banks using outsourced software (103.5897). This showed that, greater risk management controls while using in-house developed software was reducing the IT risks in banks.

Non-financial impacts while using in-house developed and outsourced software were found to be 10.90 and 10.641, showing not much variation. But financial impacts were considerably high (13.564) while using outsourced software compared to in-house developed software (9.3).

**Table 8.9: Descriptive statistics (Group) – IT risk, risk management and impact based on software development methodology used**

| | Software Development Methodology | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Information Technology Risk | Outsourced IS Development | 39 | 58.6154 | 12.71264 |
| | In-house Developed | 10 | 51.9000 | 14.92537 |
| Information Technology Risk Management | Outsourced IS Development | 39 | 103.5897 | 16.07829 |
| | In-house Developed | 10 | 113.0000 | 11.81336 |
| Non-Financial Impact | Outsourced IS Development | 39 | 10.641 | 4.6311 |
| | In-house Developed | 10 | 10.900 | 7.4751 |
| Financial Impact | Outsourced IS Development | 39 | 13.564 | 4.9140 |
| | In-house Developed | 10 | 9.300 | 3.1990 |

Source: Survey Data

From the group statistics table, it was interpreted that IT risk was more for banks having systems with outsourced IS development when compared to that of in house developed. But it was observed that IT risk management was given keen importance, if the software development methodology used is in house. So it was interpreted that in-house developed systems in banks are having more IT risk management controls and consequently lesser risks.

The non-financial impacts were slightly more for information systems developed by outsourcing compared to that in-house developed. From the group statistics it is also seen that financial impacts were considerably more for outsourced systems. In house development team had more domain knowledge, commitment, user interaction which would allow the team to build a system which is very much customized for the bank's needs and characteristics. Responsiveness to failures in any system control

was also immediate. This could reduce the financial impacts considerably. The above observations were tested with an independent sample t test.

**Table 8.10: Independent Samples Test - IT risk, risk management and impacts based on software development method**

| Software Development Methodology | | | |
|---|---|---|---|
| | t-test for Equality of Means | | |
| | t | df | Sig. (2-tailed) |
| Information Technology Risk | 1.439 | 47 | .157 |
| Information Technology Risk Management | -1.729 | 47 | .090 |
| Non-Financial Impact | -.138 | 47 | .891 |
| Financial Impact | 2.595 | 47 | **.013** |

Source: Survey Data

It is interpreted that the means significantly varies for financial impact alone ($t=2.59$, $df = 47$, $p<0.05$). From this we can conclude that, financial impact will be less, if the software development methodology chosen is in house. We did not have enough evidence to prove other observations since the tests were not found to be significant.

These findings supported the hypothesis (H5i) that there was a significant relationship between software development methodology of the bank and IT risk impacts.

### 8.4.2 Level of Automation

**Hypothesis Testing**

**H5j**: There is a significant variation in IT risk across different level of automation used by the Bank

**H5k**: There is a significant variation in IT risk management across different level of automation used by the Bank

**H5l**: There is a significant variation in IT risk impacts across different level of automation used by the Bank

Table 8.11 explains that, based on the data analysis, IT risk was found to be more in banks with low level of automation (74.6000), followed by banks with medium level of automation (66.0714) and it was found to be the least in banks with high level of automation (52.0938). It has been found that high level of automation using system reduces IT risk.

**Table 8.11: Descriptive Statistics - IT risk, risk management and impact based on level of automation**

| | | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Information Technology Risk | High | 32 | 52.0938 | 12.14525 |
| | Medium | 14 | 66.0714 | 6.14522 |
| | Low | 5 | 74.6000 | 5.98331 |
| | Total | 51 | 58.1373 | 13.12405 |
| Information Technology Risk Management | High | 32 | 112.5938 | 9.54737 |
| | Medium | 14 | 97.1429 | 9.67039 |
| | Low | 5 | 74.8000 | 8.61394 |
| | Total | 51 | 104.6471 | 15.23263 |
| Non-Financial Impact | High | 32 | 9.063 | 4.2573 |
| | Medium | 14 | 14.286 | 7.0648 |
| | Low | 5 | 14.800 | 6.0581 |
| | Total | 51 | 11.059 | 5.8324 |
| Financial Impact | High | 32 | 11.500 | 4.2121 |
| | Medium | 14 | 14.714 | 5.9021 |
| | Low | 5 | 19.600 | 2.0736 |
| | Total | 51 | 13.176 | 5.1950 |

Source: Survey Data

IT Risk management controls were found to be more in banks with high level of automation (112.5938), followed by medium level of automation (97.1429) and low level of automation (74.8). It has been found that systems with high level of automation also provided high level of IT risk management.

The non-financial impacts and financial impacts were found to be more (32.0) with banks using high level of automation when compared to banks using medium (14) and low level (5) of automation. It showed that banks with high level of automation when affected by IT risks, the impacts would also be high.

**Table 8.12: Summary of IT risk, risk management and impact based on level of automation**

| No | Level Of Automation | High | Low |
|---|---|---|---|
| **1** | IT Risk | Low Automation | High Automation |
| **2** | IT Risk Management | High Automation | Low Automation |
| **3** | Non-Financial Impact | Low Automation | High Automation |
| **4** | Financial Impact | Low Automation | High Automation |

Source: Survey Data

Table 8.13 details the test result for IT risk, IT risk management and Impacts across banks with different level of automation. It was observed that for IT risk, IT risk management, impacts (financial and non-financial), the test was found to be significant ($p<0.05$) and should conclude that there was sufficient evidence to believe the IT risk, IT risk management and impacts were significantly different across different bank groups based on the level of automation used.

A significant F value indicates that there are differences in the means, but it does not tell you where those differences are and therefore, various methods have been developed for doing multiple comparisons of group means. Multiple comparisons will allow a researcher to compare all the group means with each other providing an in depth understanding of the differences in the mean. From Table 8.13, it was observed that all variables were not found to be significant, hence multiple comparisons were executed with an LSD model.

**Table 8.13: ANOVA – IT risk, risk management and impacts based on level of automation**

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| **Information Technology Risk** | Between Groups | 3405.192 | 2 | 1702.596 | 15.696 | **.000** |
| | Within Groups | 5206.847 | 48 | 108.476 | | |
| | Total | 8612.039 | 50 | | | |
| **Information Technology Risk Management** | Between Groups | 7263.414 | 2 | 3631.707 | 40.183 | **.000** |
| | Within Groups | 4338.233 | 48 | 90.380 | | |
| | Total | 11601.647 | 50 | | | |
| **Non-Financial Impact** | Between Groups | 343.291 | 2 | 171.646 | 6.069 | **.004** |
| | Within Groups | 1357.532 | 48 | 28.282 | | |
| | Total | 1700.824 | 50 | | | |
| **Financial Impact** | Between Groups | 329.355 | 2 | 164.677 | 7.749 | **.001** |
| | Within Groups | 1020.057 | 48 | 21.251 | | |
| | Total | 1349.412 | 50 | | | |

Source: Survey Data

**Table 8.14: LSD (Multiple Comparisons) – IT risk, risk management and impact based on level of automation**

| Dependent Variable | (I) Level of Automation | (J) Level of Automation | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| Information Technology Risk | High | Medium | -13.97768* | 3.33739 | .000 |
| | | Low | -22.50625* | 5.00850 | .000 |
| | Medium | High | 13.97768* | 3.33739 | .000 |
| | | Low | -8.52857 | 5.42618 | .123 |
| | Low | High | 22.50625* | 5.00850 | .000 |
| | | Medium | 8.52857 | 5.42618 | .123 |
| Information Technology Risk Management | High | Medium | 15.45089* | 3.04632 | .000 |
| | | Low | 37.79375* | 4.57169 | .000 |
| | Medium | High | -15.45089* | 3.04632 | .000 |
| | | Low | 22.34286* | 4.95295 | .000 |
| | Low | High | -37.79375* | 4.57169 | .000 |
| | | Medium | -22.34286* | 4.95295 | .000 |
| Non-Financial Impact | High | Medium | -5.2232* | 1.7041 | .004 |
| | | Low | -5.7375* | 2.5574 | .030 |
| | Medium | High | 5.2232* | 1.7041 | .004 |
| | | Low | -.5143 | 2.7707 | .854 |
| | Low | High | 5.7375* | 2.5574 | .030 |
| | | Medium | .5143 | 2.7707 | .854 |
| Financial Impact | High | Medium | -3.2143* | 1.4772 | .035 |
| | | Low | -8.1000* | 2.2168 | .001 |
| | Medium | High | 3.2143* | 1.4772 | .035 |
| | | Low | -4.8857* | 2.4017 | .047 |
| | Low | High | 8.1000* | 2.2168 | .001 |
| | | Medium | 4.8857* | 2.4017 | .047 |

** The mean difference is significant at the 0.05 level.*

Source: Survey Data

In the case of IT risks it differed significantly ($p < 0.05$) for the banks with high level of automation when we compared it with the other groups viz banks with medium and low level of automation. Hence we concluded that the IT risks in banks with high level of automation was significantly different from banks with medium and low level of automation. And the data also showed that there was no significant variation in IT risks between banks with medium and low level of automation.

IT risk management was found to differ significantly with each other (banks with high, medium and low level of automation)

In the case of non-financial impacts, it differed significantly between banks with high level of automation and that with medium and low level of automation. The results showed that there was no significant difference in non-financial impacts between banks with low and medium level of automation. But financial impacts were found to differ significantly between banks with high, medium and low level of automation.

Hence, ANOVA & LSD Multiple Comparisons showed that,

a) IT risks in banks with high level of automation was significantly different from banks with medium and low level of automation

b) IT risk management was found to differ significantly with each other (banks with high, medium and low level of automation)

c) Nonfinancial impacts, differed significantly between banks with high level of automation and that with medium and low level of automation

d) Financial impacts were found to differ significantly between banks with high, medium and low level of automation.

These findings supported the hypothesis (H5j, H5k, H5l) that there was a significant relationship between level of automation in the bank and IT risk, risk management and impacts.

### 8.4.3 Skilled IT Man Power

The data analysis had shown that there were no consistent variations for IT risks based on skilled IT man power availability in Banks. The results were therefore discarded.

### 8.4.4 Training to Employees

**Hypothesis Testing**

**H5m**: There is a significant variation in IT risk across different levels of training provided to the employees by the bank

**H5n**: There is a significant variation in IT risk management across different levels of training provided to the employees by the bank

**H5o**: There is a significant variation in IT risk impacts across different levels of training provided to the employees by the bank

Table 8.15 showed that, based on the data analysis, IT risk was found to be more in banks which provided no regular training to employees (74.6000), compared to those provided regular training to employees. IT risk mean was shown as 58.2353 for banks given training to employees once in a year, 64.4444 for banks given training twice in a year, 37.5 for banks given training three times a year and 47.75 for banks given training more than three times a year for their employees.

**Table 8.15: Descriptive Statistics - IT risk, risk management and impact based on level of training to employees**

| | | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Information Technology Risk | Not Provided | 2 | 69.5000 | 4.94975 |
| | One time an Year | 34 | 58.2353 | 12.93822 |
| | Two Times an Year | 9 | 64.4444 | 8.79078 |
| | Three Times an Year | 2 | 37.5000 | 14.84924 |
| | > than 3 Times | 4 | 47.7500 | 10.40433 |
| | Total | 51 | 58.1373 | 13.12405 |
| Information Technology Risk Management | Not Provided | 2 | 80.5000 | 13.43503 |
| | One time an Year | 34 | 105.5588 | 14.82666 |
| | Two Times an Year | 9 | 98.7778 | 13.09368 |
| | Three Times an Year | 2 | 117.5000 | 9.19239 |
| | > than 3 Times | 4 | 115.7500 | 11.29528 |
| | Total | 51 | 104.6471 | 15.23263 |
| Non-Financial Impact | Not Provided | 2 | 9.500 | 3.5355 |
| | One time an Year | 34 | 11.471 | 6.0814 |
| | Two Times an Year | 9 | 12.444 | 6.4442 |
| | Three Times an Year | 2 | 7.500 | 2.1213 |
| | > than 3 Times | 4 | 7.000 | 2.0000 |
| | Total | 51 | 11.059 | 5.8324 |
| Financial Impact | Not Provided | 2 | 19.500 | 3.5355 |
| | One time an Year | 34 | 12.588 | 4.9855 |
| | Two Times an Year | 9 | 15.333 | 4.2720 |
| | Three Times an Year | 2 | 12.500 | 7.7782 |
| | > than 3 Times | 4 | 10.500 | 7.0000 |
| | Total | 51 | 13.176 | 5.1950 |

Source: Survey Data

IT Risk management was reported to be high in banks which provided training to their employees compared to those not provided training to employees. The IT risk management results for different training frequencies were obtained as follows, 80.50 (no training),

105.5588 (once in a year), 98.7778 (two times in a year), 117.5 (three times a year) and 115.75 (more than 3 times a year).

The nonfinancial impacts were not found to be varying with the level of training provided to employees. But financial impacts were found to be more in banks which did not provide any training to employees (19.5) and found to be comparably less in banks which provided training. The results showed the values of financial impacts based on training frequency as 12.588 (training once in a year), 15.333 (training two times in a year), 12.5 (three times a year) and 10.5 (more than three times a year)

**Table 8.16: Summary of IT risk, risk management and impact based on level of training to employees**

| No | TRAINING | High | Low |
|---|---|---|---|
| **1** | IT Risk | No Training | Training |
| **2** | IT Risk Management | Training | No Training |
| **3** | Non-Financial Impact | Training | No Training |
| **4** | Financial Impact | No Training | Training |

Source: Survey Data

Table 8.17 shows the test result for IT risk, IT risk management and Impacts across banks with different level of training given to their employees. It was observed that for IT risk and IT risk management the test was found to be significant ($p<0.05$) and should conclude that there was sufficient evidence to believe the IT risk and IT risk management were significantly different across different bank groups based on the level of training provided to employees.

A significant F value indicates that there are differences in the means, but it does not tell you where those differences are and therefore, various methods have been developed for doing multiple comparisons of group means. Multiple comparisons will allow a researcher to compare all the group means with each other providing an in depth understanding of the differences in the mean. From Table 8.15, it was observed that all variables were not found to be significant, hence multiple comparisons were executed with an LSD model.

**Table 8. 17: ANOVA - IT risk, risk management and impacts based on level of training to employees**

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Information Technology Risk | Between Groups | 1899.949 | 4 | 474.987 | 3.255 | .020 |
| | Within Groups | 6712.090 | 46 | 145.915 | | |
| | Total | 8612.039 | 50 | | | |
| Information Technology Risk Management | Between Groups | 2327.959 | 4 | 581.990 | 2.887 | .033 |
| | Within Groups | 9273.688 | 46 | 201.602 | | |
| | Total | 11601.647 | 50 | | | |
| Non-Financial Impact | Between Groups | 119.131 | 4 | 29.783 | .866 | .491 |
| | Within Groups | 1581.693 | 46 | 34.385 | | |
| | Total | 1700.824 | 50 | | | |
| Financial Impact | Between Groups | 163.176 | 4 | 40.794 | 1.582 | .195 |
| | Within Groups | 1186.235 | 46 | 25.788 | | |
| | Total | 1349.412 | 50 | | | |

Source: Survey Data

**Table 8.18: LSD (Multiple Comparisons) – IT risk, risk management and impact based on level of training to employees**

| Dependent Variable | (I) Training to Employees | (J) Training to Employees | Mean Difference (I-J) | Std. Error | Sig. |
|---|---|---|---|---|---|
| Information Technology Risk | Not Provided | One time an Year | 11.26471 | 8.78915 | .206 |
| | | Two Times an Year | 5.05556 | 9.44300 | .595 |
| | | Three Times an Year | 32.00000 | 12.07953 | **.011** |
| | | > than 3 Times | 21.75000 | 10.46118 | **.043** |
| | One time an Year | Not Provided | -11.26471 | 8.78915 | .206 |
| | | Two Times an Year | -6.20915 | 4.52818 | .177 |
| | | Three Times an Year | 20.73529 | 8.78915 | **.023** |
| | | > than 3 Times | 10.48529 | 6.38517 | .107 |
| | Two Times an Year | Not Provided | -5.05556 | 9.44300 | .595 |
| | | One time an Year | 6.20915 | 4.52818 | .177 |
| | | Three Times an Year | 26.94444 | 9.44300 | **.006** |
| | | > than 3 Times | 16.69444 | 7.25889 | **.026** |
| | Three Times an Year | Not Provided | -32.00000 | 12.07953 | **.011** |
| | | One time an Year | -20.73529 | 8.78915 | **.023** |
| | | Two Times an Year | -26.94444 | 9.44300 | **.006** |
| | | > than 3 Times | -10.25000 | 10.46118 | .332 |
| | > than 3 Times | Not Provided | -21.75000 | 10.46118 | **.043** |
| | | One time an Year | -10.48529 | 6.38517 | .107 |
| | | Two Times an Year | -16.69444 | 7.25889 | **.026** |
| | | Three Times an Year | 10.25000 | 10.46118 | .332 |
| Information Technology Risk Management | Not Provided | One time an Year | -25.05882 | 10.33104 | **.019** |
| | | Two Times an Year | -18.27778 | 11.09960 | .106 |
| | | Three Times an Year | -37.00000 | 14.19866 | **.012** |
| | | > than 3 Times | -35.25000 | 12.29640 | **.006** |
| | One time an Year | Not Provided | 25.05882 | 10.33104 | **.019** |
| | | Two Times an Year | 6.78105 | 5.32256 | .209 |
| | | Three Times an Year | -11.94118 | 10.33104 | .254 |
| | | > than 3 Times | -10.19118 | 7.50533 | .181 |
| | Two Times an Year | Not Provided | 18.27778 | 11.09960 | .106 |
| | | One time an Year | -6.78105 | 5.32256 | .209 |
| | | Three Times an Year | -18.72222 | 11.09960 | .098 |
| | | > than 3 Times | -16.97222 | 8.53233 | .053 |
| | Three Times an Year | Not Provided | 37.00000 | 14.19866 | **.012** |
| | | One time an Year | 11.94118 | 10.33104 | .254 |
| | | Two Times an Year | 18.72222 | 11.09960 | .098 |
| | | > than 3 Times | 1.75000 | 12.29640 | .887 |
| | > than 3 Times | Not Provided | 35.25000 | 12.29640 | **.006** |
| | | One time an Year | 10.19118 | 7.50533 | .181 |
| | | Two Times an Year | 16.97222 | 8.53233 | .053 |
| | | Three Times an Year | -1.75000 | 12.29640 | .887 |

Source: Survey Data

In the case of IT risks it differed significantly ($p < 0.05$) for the banks did not provided training to employees and those provided training to employees three or more times. IT risks differed significantly for banks that provided training once a year and that provided training thrice a year. The IT risk also differed significantly for banks that provided training to employees two times a year and that provided three or more times a year

IT risk management differed significantly for banks that did not provide training to that provided training one or three times a year. Hence, ANOVA & LSD Multiple Comparisons shows that

a) IT risks differ significantly for banks that provided training once a year and that provided training thrice a year.

b) IT risk management differs significantly for banks that did not provide training to that provided training one or three times a year.

c) Nonfinancial and financial impacts did not show significant variation based on training

These findings supported the hypothesis (H5m, H5n, H5o) that there was a significant relationship between training provided to employees in banks and IT risk, risk management and impacts.

### 8.4.5 Training to Customers

Almost all banks reported a 'No' for training to customers and there were no significant variations in the IT risks based on the training pattern of different banks.

### 8.4.6 Type of Software Used

**Hypothesis Testing**

**H5p**: There is a significant variation in IT risk across different type of software used by the Bank

**H5q**: There is a significant variation in IT risk management across different type of software used by the Bank

**H5r**: There is a significant variation in IT risk impacts across different type of software used by the Bank.

Table 8.19 showed that, based on the data analysis, IT risk were found to be more in banks which used open source technologies (60.7) compared to banks which used Microsoft based technologies (57.8125) and the ones used a combination of both (56.1429). IT risk management was found to be more in banks which used Microsoft based technologies (106.75) compared to banks which used mixed technologies (105.00) and the ones used open sourced technologies (101.85). IT Risk management was reported to be high in banks which used Microsoft based technologies and the IT risks were found to be low.

The non-financial impacts were not found to be more for banks which used Microsoft based technologies (12.125) followed by banks using open source technologies (10.550) and the least for banks using a combination of technologies. Financial impacts where found to be more for open source based technologies (14.15), followed by Microsoft based technologies (13.063) and mixed technologies (12.286). It was observed that mixed technologies reduce the financial and non-financial impacts of IT risks.

**Table 8.19: Descriptive Statistics – IT risk, risk management and impact based on type of software used**

| | | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Information Technology Risk | Open Source | 20 | 60.7000 | 11.61714 |
| | Microsoft Based | 16 | 57.8125 | 13.92944 |
| | Both | 14 | 56.1429 | 14.19565 |
| | Total | 50 | 58.5000 | 12.99647 |
| Information Technology Risk Management | Open Source | 20 | 101.8500 | 14.85819 |
| | Microsoft Based | 16 | 106.7500 | 14.52125 |
| | Both | 14 | 105.0000 | 16.90243 |
| | Total | 50 | 104.3000 | 15.18223 |
| Non-Financial Impact | Open Source | 20 | 10.550 | 3.9931 |
| | Microsoft Based | 16 | 12.125 | 8.0571 |
| | Both | 14 | 10.071 | 5.1060 |
| | Total | 50 | 10.920 | 5.8058 |
| Financial Impact | Open Source | 20 | 14.150 | 4.8153 |
| | Microsoft Based | 16 | 13.063 | 5.6032 |
| | Both | 14 | 12.286 | 5.4126 |
| | Total | 50 | 13.280 | 5.1943 |

Source: Survey Data

**Table 8.20: Summary of IT risk, risk management and impact based on type of software used**

| No | Type of Software Used | High | Medium | Low |
|---|---|---|---|---|
| **1** | IT Risk | Open Source | Microsoft Based | Mixed |
| **2** | IT Risk Management | Microsoft Based | Mixed | Open Source |
| **3** | Non-Financial Impact | Microsoft Based | Open Source | Mixed |
| **4** | Financial Impact | Open Source | Microsoft Based | Mixed |

Source: Survey Data

Table 8.21 shows the test result for IT risk, IT risk management and Impacts across banks based on the technology used. It was observed that for IT risk, IT risk management, non-financial impact and financial impacts were not found to be significant ($p<0.05$) and concluded that there was no sufficient evidence to believe the IT risk, IT risk management and Impacts were significantly different across different bank groups based on the technology used.

**Table 8.21: ANOVA – IT risk, risk management and Impact based on type of software used**

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Information Technology Risk | Between Groups | 182.148 | 2 | 91.074 | .529 | .593 |
| | Within Groups | 8094.352 | 47 | 172.220 | | |
| | Total | 8276.500 | 49 | | | |
| Information Technology Risk Management | Between Groups | 222.950 | 2 | 111.475 | .473 | .626 |
| | Within Groups | 11071.550 | 47 | 235.565 | | |
| | Total | 11294.500 | 49 | | | |
| Non-Financial Impact | Between Groups | 36.051 | 2 | 18.026 | .524 | .595 |
| | Within Groups | 1615.629 | 47 | 34.375 | | |
| | Total | 1651.680 | 49 | | | |
| Financial Impact | Between Groups | 29.735 | 2 | 14.868 | .541 | .586 |
| | Within Groups | 1292.345 | 47 | 27.497 | | |
| | Total | 1322.080 | 49 | | | |

Source: Survey Data

There is no sufficient evidence to believe the IT risk, IT risk management and Impacts were significantly different across different bank groups based on the technology used.

So these findings did not support the hypothesis (H5p, H5q, H5r) that there was a significant relationship between technology used in banks and IT risk, risk management and impacts.

### 8.4.7 Data Center Model Used

**Hypothesis Testing**

**H5s**: There is a significant variation in IT risk across different type of data center model used by the bank

**H5t**: There is a significant variation in IT risk management across different type of data center model used by the bank

**H5u**: There is a significant variation in IT risk impacts across different type of data center model used by the bank

Table 8.22 showed that, based on the data analysis, IT risk were found to be slightly more for banks with a data center hosted with third parties (57.6667) compared to those with own data center arrangements (57.4138). IT risk management was found to be more in banks with third party managed data centers 9107.75) compared to banks with own data centers (103.4828). Non-financial impacts were less for banks with third party hosted data centers (10.542) and more for banks with own data center (11.276) but financial impacts were more for banks with third party hosted data centers (13.833) and less for banks with own data centers (12.621).

**Table 8.22: Descriptive Statistics (Group) - IT risk, risk management and impact based on data center model used**

| | Data Center Model | N | Mean | Std. Deviation |
|---|---|---|---|---|
| Information Technology Risk | Hosted with Third Party | 24 | 57.6667 | 11.94795 |
| | Own Data Center | 29 | 57.4138 | 14.42844 |
| Information Technology Risk Management | Hosted with Third Party | 24 | 107.7500 | 11.30314 |
| | Own Data Center | 29 | 103.4828 | 18.14745 |
| Non-Financial Impact | Hosted with Third Party | 24 | 10.542 | 5.4691 |
| | Own Data Center | 29 | 11.276 | 6.0468 |
| Financial Impact | Hosted with Third Party | 24 | 13.833 | 3.7955 |
| | Own Data Center | 29 | 12.621 | 5.9726 |

Source: Survey Data

**Table 8.23: Summary of IT risk, risk management and impact based on the data center used**

| No | Data Center Model | High | Low |
|---|---|---|---|
| **1** | IT Risk | Third Party | Own |
| **2** | IT Risk Management | Third Party | Own |
| **3** | Non-Financial Impact | Own | Third Party |
| **4** | Financial Impact | Third Party | Own |

Source: Survey Data

From the group statistics table, it was interpreted that IT risk more for banks with information systems on hosted with third party centers compared to that hosted in own data centers. But IT risk management controls were found to be more with hosted data centers. (This could be because hosting centers like amazon cloud, etc use standard and state of the art technologies for IT risk controls and management.)

From the group statistics, it was observed that the non-financial impacts are more with own data center and less with third party hosted centers. Financial impacts on the other hand were found to be more for banks with third party hosted data centers compared to one's having own data centers.

**Table 8.24: Independent Samples Test - IT risk, risk management and impacts based on type of software used**

| Type of Software Used | | | | |
|---|---|---|---|---|
| | | t-test for Equality of Means | | |
| | | t | df | Sig. (2-tailed) |
| Information Technology Risk | | .069 | 51 | .946 |
| Information Technology Risk Management | | 1.045 | 47.655 | .301 |
| Non-Financial Impact | | -.464 | 50.566 | .645 |
| Financial Impact | | .896 | 48.061 | .375 |

Source: Survey Data

It is interpreted that the means does not vary significantly. Since the tests were found to be non-significant ($p>0.05$), we don't have enough evidence to prove the observations that IT risk, risk management or impacts varies significantly across banks with hosted data center and own data center.

From the analysis, The tests were found to be non-significant ($p>0.05$), we did not have enough evidence to prove the observations that IT risk, risk management or impacts varied significantly across banks with hosted and own data center. So, these findings did not supported the hypothesis (H5s, H5t, H5u) that there was a significant relationship between data center model used in banks and IT risk, risk management and impacts.

## 8.5 Conclusion

The analysis of impacts based on bank type showed that financial and nonfinancial impacts are highest in co-operative sector banks and lowest in public sector banks. Banks with better IT risk management were reported to have lower IT risks, irrespective of the geographical spread of the banks. The financial and non-financial impacts were reported to be highest in banks operating in single state and lowest with banks operating in multiple countries. The IT risks in cooperative banks were significantly different from foreign and public sector banks. The FI and NFI differed significantly between co-operative sector banks and public sector banks. IT risk, IT risk management and Impacts were significantly different across different bank groups based on geographical spread. There was no

significant variation in IT risks and IT risk management between banks operating in multiple states and multiple countries.

In the case of impacts (financial and non-financial) it differed significantly between banks operating in single state with that operating in multiple states and multiple countries. There was no significant variation in the impacts between banks operating in multiple states and multiple countries. The study also showed that, in-house developed software reported to be reducing the IT risks in banks.

It has been found that high level of automation using systems reduces IT risks. It has also been found that systems with high level of automation also provided high level of IT risk management. It showed that banks with high level of automation when affected by IT risks, the impacts would also be high. IT risk, IT risk management and impacts were significantly different across different bank groups based on the level of automation used. And the data also showed that there was no significant variation in IT risks between banks with medium and low level of automation.

In the case of non-financial impacts, it differed significantly between banks with high level of automation and that with medium and low level of automation. The results showed that there was no significant difference in non-financial impacts between banks with low and medium level of automation. But financial impacts were found to differ significantly between banks with high, medium and low level of automation.

IT risk was found to be more in banks which provided no regular training to employees, compared to those provided regular training to

employees. IT Risk management was reported to be high in banks which provided training to their employees compared to those not provided training to employees. There was sufficient evidence to believe the IT risk and IT risk are significantly different across different bank groups based on the level of training provided to employees. IT risk management differed significantly for banks that did not provide training to that provided training one or three times a year.

IT Risk management was reported to be high in banks which used Microsoft based technologies and the IT risks were found to be low. It is observed that mixed technologies reduce the financial and non-financial impacts of IT risks. There was no sufficient evidence to believe the IT risk, IT risk management and Impacts are significantly different across different bank groups based on the technology used.

It was interpreted that IT risk more for banks with information systems on hosted with third party centers compared to that hosted in own data centers. The non-financial impacts were more with own data center and less with third party hosted data centers. Financial impacts on the other hand were found to be more for banks with third party hosted data centers compared to one's having own data centers.

Chapter 9

# MODELS LINKING IT RISK, RISK MANAGEMENT & IMPACTS

Contents



## 9.1 Introduction

The advancement of Information Technology has brought about rapid changes to the way businesses and operations are being conducted in the financial industry. IT is no longer a support function within a financial institution but a key enabler for business strategies including reaching out to and meeting customer needs (Monetary Authority of Singapore, 2013). Financial systems and networks supporting FI's business operations have also grown in scope and complexity over the years.

The growing dependence of banking organizations on Information Technology emphasizes one aspect of the need to identify and control this technology related risks. In banking organizations, based on Basel guidelines, Information Technology related risks are treated under

operational risks. Operational risk arises from the potential that inadequate information systems, operational problems, breaches in internal controls, fraud, or unforeseen catastrophes will result in unexpected losses (Federal Reserve , 1995). Although operational risk does not easily lend itself to quantitative measurement, it can result in substantial costs through error, fraud, or other performance problems.

Inadequate IT controls could result in cyber frauds and poor implementation of technology could lead to unsound decision making based on inaccurate information/data. The cyber threat landscape is also changing over the years and needs to be factored in while considering mitigating measures. (RBI, 2011).

Very few studies have been done in past linking IT risk, IT risk management and its financial and non-financial impacts specific to Indian context. The following conceptual framework, which has an integrated and comprehensive view of IT risk, IT risk management and its impacts is tested in this study.

## 9.2 Conceptual Framework

The following conceptual model as shown in Fig. 1.7 is an integrated and comprehensive view of Information Technology risk, risk management and its financial and non-financial impacts. This figure is included below for a quick reference.

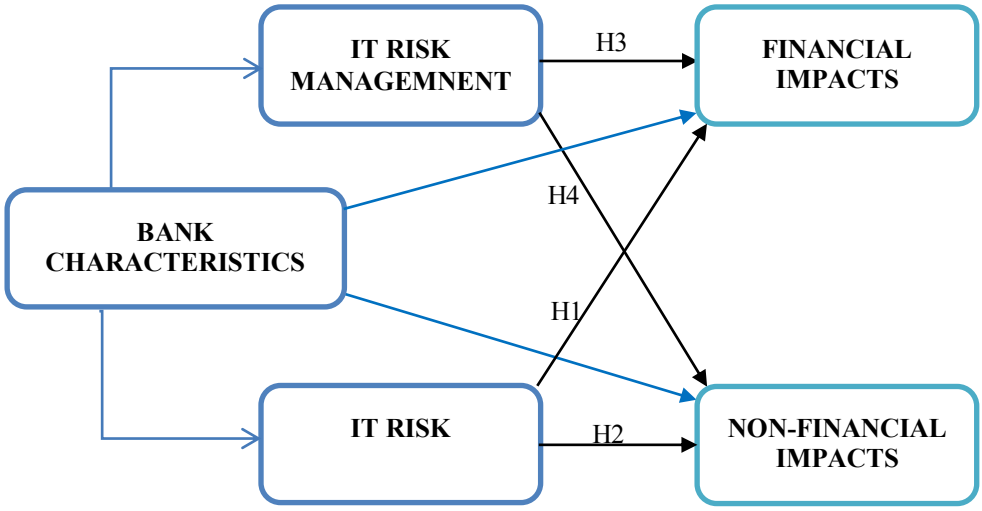



**Figure 9.1: Conceptual Framework linking IT risk, IT risk management and impacts**

Based on literature, the researcher has formulated the following five (alternate) hypotheses on the anticipated relationship among the variables in the study.

**H1**: IT risk has significant positive relationship with financial impacts

**H2**: IT risk has significant positive relationship with nonfinancial impacts

**H3**: IT risk management has significant negative relationship with financial impacts

**H4**: IT risk management has significant negative relationship with nonfinancial impacts

**H5**: There is significant variation in IT risk, IT risk management and impacts across the different organizational characteristics of the bank.

The major variables of this study are,

- Information Technology Risk
- Information Technology Risk Management
- Financial Impacts
- Non-Financial Impacts

Information Technology risks are also analysed based on the characteristics of the bank and the characteristics of the technology used. The following section analyses the possible relationship between these variables.

Since, the concept of risk and risk management are live across the banking scenario in India and are simultaneous in occurrence, the model is attempted in two parts. From the causality aspect, the risk element precedes risk management and should have a positive relationship. That means, more the risk in a banking organisation, more the risk management practices will be. But in the context of this study where the perception regarding both risk and risk management are measured in a context of simultaneous occurrence, it is obvious that risk management will be having a negative relationship with risk because risk management is done in order to reduce risk. Hence this cannot be linked in a single path model starting from risk to risk management and then to the impact since it contradict the causality argument or the measurement concept. It is therefore decided to split the path model into two, where the first one deals with the impact of IT risk on financial impact and nonfinancial impact and later the impact of IT risk management on financial and nonfinancial impacts.

## 9.3 Analysis of IT Risk and its Financial and Non-Financial Impacts

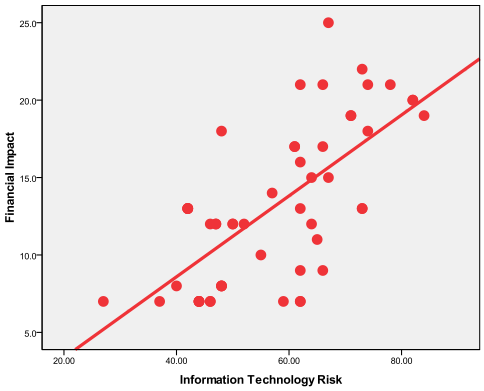
Correlation is a bivariate measure of association (strength) of the relationship between two metric variables. Pearson correlation is the most popular measure of correlation, sometimes called *product moment correlation*. Pearson's r is a measure of association which varies from -1 to +1, with 0 indicating no relationship (random pairing of values) and 1 indicating perfect relationship. A canonical correlation is the correlation of two canonical (latent) variables, one representing a set of independent variables, the other a set of dependent variables. The purpose of canonical correlation is to identify the relation of the two sets of variables, not to model the individual variables.

Correlation between IT risk and its impacts (financial and non-financial) are tested using pearson correlation and x-y scatter graph. In the x-y scatter graph, the two variables being correlated is better described by a straight line than by any curvilinear function

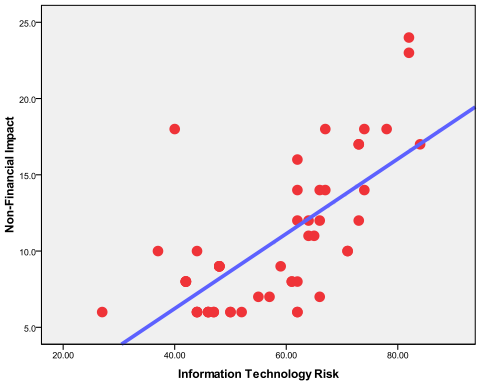
### 9.3.1 Scatter Plot

The first step to proceed with a model is to check the linear relationship between the variables to be related in the model. A scatter plot is a useful tool used to have a summary of a set of bivariate data (two variables), usually drawn before working out a linear correlation coefficient or fitting a regression line. Fig.9.2 explains that Information Technology risk is linearly related to both financial impact and nonfinancial impact as well. From the figure, it is easily identified that there is a positive relationship between IT risk and its impact.

Information Technology Risk and Financial Impact




Information Technology Risk and Nonfinancial Impact




Source: Survey Data

**Figure 9.2: Scatter Plot Information Technology Risk and its Financial & Nonfinancial Impacts**

### 9.3.2 Correlation between IT Risk and Financial and Nonfinancial Impacts

The following table shows the correlations between IT risk and its financial and nonfinancial impacts. The correlation between IT risk and its impacts (financial and non-financial) was found to be significant at the 0.01 level (2 – tailed).

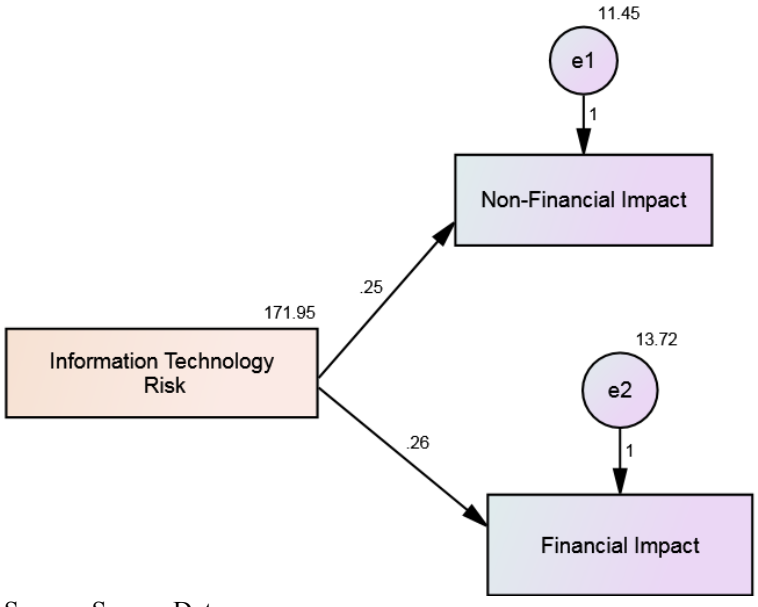
**Table 9.1: Correlations between IT Risk and financial and non-financial impacts**

| CORRELATIONS | | | | |
|---|---|---|---|---|
| | | **Information Technology Risk** | **Non-Financial Impact** | **Financial Impact** |
| **Information Technology Risk** | Pearson Correlation | 1 | .689** | .679** |
| | Sig. (2-tailed) | | .000 | .000 |
| ***** Correlation is significant at the 0.01 level (2-tailed).*** | | | | |

Source: Survey Data

IT risk was positively correlated with both nonfinancial impacts and financial impacts. It was more correlated with nonfinancial impact (.689) when compared with financial impact (.679). Both the correlations were found to be significant ($p<0.05$). The first model was proposed by taking IT risk as the independent variable predicting nonfinancial and financial impacts. The diagram will give the pictorial representation of the same.

Path analysis using SEM (Structured Equation Modelling) was used and here the parameters were estimated by maximum likelihood (ML) methods rather than by ordinary least squares (OLS) methods. OLS methods minimize the squared deviations between values of the criterion variable and those predicted by the model. ML (an iterative procedure) attempts to maximize the likelihood that obtained values of the criterion variable will be correctly predicted.




Source: Survey Data

**Figure 9.3: Model relating IT risk to financial and non-financial impacts**

The fit of the path analysis is ascertained by the following benchmark measures which is explained with respect to the observed values.

**Table 9.2: Threshold values of Measures in Path Analysis**

| Measures | Threshold Values | Observed Values |
|---|---|---|
| **CMIN/DF** | < 3 Ideal. The values are acceptable between 3 and 5 | 0.959 |
| **CFI** | > 0.95 | 1.00 |
| **GFI** | > 0.95 | .988 |
| **AGFI** | > 0.80 | .928 |
| **RMSEA** | < 0.05 good and 0.05 to 0.10 Moderate | .000 |
| **P CLOSE** | > 0.05 | .358 |

Source: Survey Data

CMIN/DF, the relative chi-square, is an index of how much the fit of data to model has been reduced by dropping one or more paths. One rule of thumb is to decide you have dropped too many paths if this index exceeds 5. Here in this case the CMIN/DF is 0.959 which is less than the threshold value. GFI, the goodness of fit index, tells you what proportion of the variance in the sample variance-covariance matrix is accounted for by the model. This should exceed 0.95 for a good model and in this case it is 1.00. The Root Mean Square Error of Approximation (RMSEA) estimates lack of fit compared to the saturated model. RMSEA of 0.05 or less indicates good fit, and 0.08 or less adequate fit. PCLOSE is the p value testing the null that RMSEA is no greater than 0.05. Since all parameters have threshold values within the limits, the path found to have a good fit.

### 9.3.3 Hypothesis Testing

**H1:** IT risk has significant positive relationship with financial impacts

**H2:** IT risk has significant positive relationship with nonfinancial impacts

The next step is to explain the relationship by means of regression weights. The relationship between IT risk to NFI and FI was found to be significant ($p < 0.01$)

**Table 9.3: Regression Weights: Default model**

| | | | Estimate | S.E. | C.R. | P |
|---|---|---|---|---|---|---|
| **Nonfinancial Impact** | <--- | IT risk | .245 | .036 | 6.853 | p<0.01 |
| **Financial Impact** | <--- | IT Risk | .261 | .039 | 6.670 | p<0.01 |

Source: Survey Data

In order to find the impact of independent variable over the dependent variable, standardized coefficients or beta coefficients are used. They are the estimates resulting from an analysis carried out on independent variables that have been standardized so that their variances are 1. Therefore, standardized coefficients refer to how many standard deviations a dependent variable will change, per standard deviation increase in the predictor variable. Standardization of the coefficient is usually done to answer the question of which of the independent variables have greater effects on the dependent variable in a multiple regression analysis, when the variables are measured in different units of measurement. From the Standardized Regression Weights, it was interpreted that IT risk impacts were more on nonfinancial impacts.

**Table 9.4: Standardized Regression Weights**

| | | | Estimate |
|---|---|---|---|
| **Nonfinancial Impact** | <--- | IT Risk | .689 |
| **Financial Impact** | <--- | IT Risk | .679 |

Source: Survey Data

These findings supported the alternate hypothesis that there was a significant positive relationship between IT risk with financial impacts and nonfinancial impacts. So H1 and H2 were accepted.

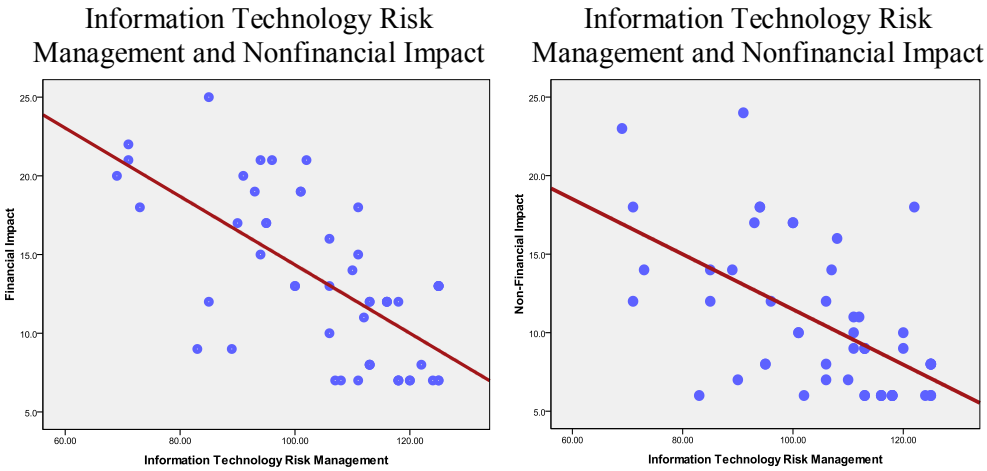
## 9.4 Analysis of IT Risk Management and its Financial and Nonfinancial Impacts

The following sections discuss the correlation between IT risk management and its financial and nonfinancial risks using scatter plots and person correlation.

### 9.4.1 Scatter Plot

The next step was oriented to extract the linear relationship, if any exists between Information Technology risk management and its financial and nonfinancial impacts. Information Technology risk management was linearly related to both financial impact and nonfinancial impact as well. It was important to note that there was a negative relationship between IT risk management and its financial and nonfinancial impact. This gave us a clear direction to proceed with a model linking all the variables pertaining to IT risk management and its impacts.

These findings supported the alternate hypothesis that there was a significant positive relationship between IT risk with financial impacts and nonfinancial impacts. So H1 and H2 were accepted.




Source: Survey Data

**Figure 9.4: Scatter Plot Information Technology Risk Management and its Financial and Nonfinancial Impacts.**

### 9.4.2 Correlation between IT Risk and Financial and Nonfinancial Impacts

The following table shows the correlations between IT risk and its financial and non-financial impacts. The correlation between IT risk and its impacts (financial and non-financial) was found to be significant at 0.01 level (2 – tailed). Correlation tables are reported in Table 9.5. Collinearity problem will not create problems in this particular case because the model considered in this thesis do have a single independent variable

IT risk management was negatively correlated with IT risk, non-financial impacts and financial impacts. Financial and nonfinancial impacts were found to be negatively correlated with IT risk management. All these correlations were found to be significant ($p<0.05$). The second model was proposed by taking IT risk management the independent variable and financial and nonfinancial impacts as dependent variables.

The following diagram (Fig 9.10) will give the pictorial representation of the same.

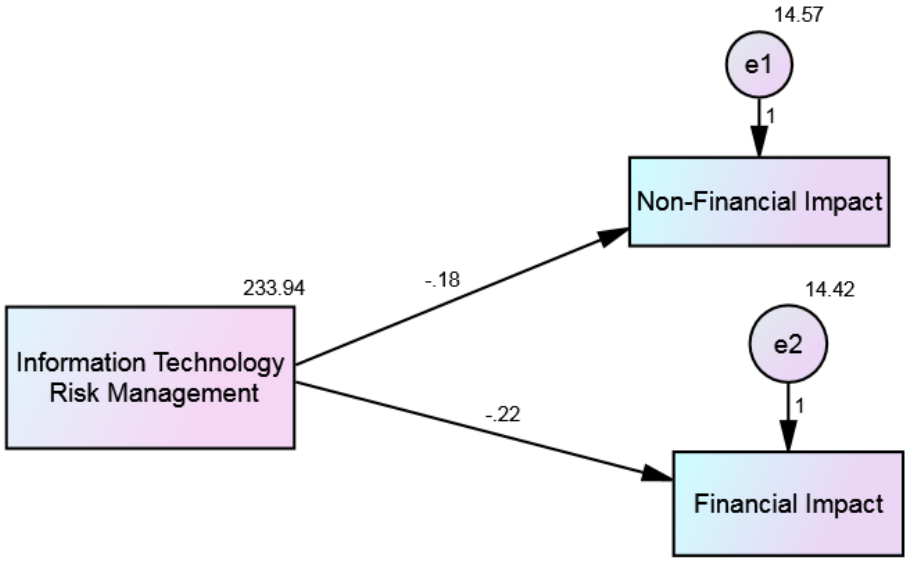
**Table 9.5: Correlation and Modelling of IT Risk Management and Impacts**

| | | Information Technology Risk | Information Technology Risk Management | Financial Impact | Non-Financial Impact |
|---|---|---|---|---|---|
| **Information Technology Risk Management** | Pearson Correlation | -.828** | 1 | -.659** | -.576** |
| | Sig. (2-tailed) | .000 | | .000 | .000 |
| **Financial Impact** | Pearson Correlation | .679** | -.659** | 1 | .396** |
| | Sig. (2-tailed) | .000 | .000 | | .003 |
| **Non-Financial Impact** | Pearson Correlation | .689** | -.576** | .396** | 1 |
| | Sig. (2-tailed) | .000 | .000 | .003 | |
| ****. Correlation is significant at the 0.01 level (2-tailed).*** | | | | | |

Source: Survey Data

Path analysis using SEM (Structured Equation Modelling) was used and here the parameters are estimated by maximum likelihood (ML) methods rather than by ordinary least squares (OLS) methods. OLS methods minimized the squared deviations between values of the criterion variable and those predicted by the model. ML (an iterative procedure) attempts to maximize the likelihood that obtained values of the criterion variable will be correctly predicted.

Figure 9.5 provides a model linking IT risk management and the financial and nonfinancial impacts.




Source: Survey Data

**Figure 9.5: Model relating IT risk management and financial and non-financial impacts**

The fit of the path analysis was ascertained by the following benchmark measures which are explained with respect to the observed values.

**Table 9.6: Threshold values of Measures in Path Analysis**

| Measures | Threshold Values | Observed Values |
|---|---|---|
| **CMIN/DF** | < 3 Ideal. The values are acceptable between 3 and 5 | 3.28 |
| **CFI** | > 0.95 | .963 |
| **GFI** | > 0.95 | .956 |
| **AGFI** | > 0.80 | .820 |
| **RMSEA** | < 0.05 good and 0.05 to 0.10 Moderate | .072 |
| **P CLOSE** | > 0.05 | .057 |

Source: Survey Data

CMIN/DF, the relative chi-square, is an index of how much the fit of data to model has been reduced by dropping one or more paths. One rule of

thumb is to decide you have dropped too many paths if this index exceeds 5. Here in this case the CMIN/DF was 3.28 which was in the acceptable range of values (3 and 5). GFI, the goodness of fit index, tells you what proportion of the variance in the sample variance-covariance matrix is accounted for by the model. This should exceed 0.95 for a good model and in this case it was 0.963 . The Root Mean Square Error of Approximation (RMSEA) estimates lack of fit compared to the saturated model. RMSEA of 0.05 or less indicates good fit, and 0.08 or less adequate fit. PCLOSE is the p value testing the null that RMSEA was no greater than 0.05. Since all parameters had threshold values within the limits, the path found to have a good fit.

### 9.4.3 Hypothesis Testing

**H3:** IT risk management has significant negative relationship with financial impacts

**H4:** IT risk management has significant negative relationship with nonfinancial impacts

The next step is to explain the relationship by means of regression weights. The relationship between IT risk management to NFI and FI was found to be significant ($p < 0.01$)

**Table 9.7: Regression Weights: (Group number 1 - Default model)**

| | | | Estimate | S.E. | C.R. | P | Result |
|---|---|---|---|---|---|---|---|
| **Nonfinancial Impact** | <--- | IT Risk Management | -.176 | .035 | -5.077 | P<0.05 | Supported |
| **Financial Impact** | <--- | IT Risk Management | -.217 | .034 | -6.310 | P<0.05 | Supported |

Source: Survey Data

In order to find the impact of independent variable over the dependent variable, standardized coefficients or beta coefficients were used. They are the estimates resulting from an analysis carried out on independent variables that have been standardized so that their variances are 1. Therefore, standardized coefficients refer to how many standard deviations a dependent variable will change, per standard deviation increase in the predictor variable. Standardization of the coefficient is usually done to answer the question of which of the independent variables have greater effects on the dependent variable in a multiple regression analysis, when the variables are measured in different units of measurement. From the Standardized Regression Weights, it was interpreted that IT risk management impacts more on FI.

**Table 9.8: Standardized Regression Weights: (Group number 1 - Default model)**

| | | | Estimate |
|---|---|---|---|
| **Nonfinancial Impact** | <--- | IT Risk Management | -.576 |
| **Financial Impact** | <--- | IT Risk Management | -.659 |

Source: Survey Data

These findings supported the alternate hypothesis that there was a significant negative relationship between IT risk management and its financial and non-financial impacts. Hence H3 and H4 were accepted.

## 9.5 Conclusion

Correlation analysis showed a strong negative correlation between IT risk dimensions and IT risk management dimensions. The results also showed a negative correlation between IT risk and financial and

nonfinancial impacts. Similarly IT risk were positively correlated with financial and nonfinancial impacts.

Thus it was concluded that there was a relationship among IT risk, IT risk management and financial and nonfinancial impacts. There were some organizational and technology characteristics of the bank which also have an impact on these relationships.

# Chapter 10

# SUMMARY OF FINDINGS AND CONCLUSIONS

Contents



## 10.1 Introduction

Irrespective of the business, organizations are forced to adopt various Information Technology systems for performing their day to day operations, meeting customer expectations, meeting increased market competition and also meeting regulatory requirements. Increased adoption of Information Technology has also increased the risks due to Information Technology. Service failures and financial losses due to IT risks are a common problem across the world and banks are no exception. IT risks and risk management in banks are considered under head 'operation risk' by Basel Committee for banking supervision.

Financial and non-financial losses due to IT risks can be attributed to various IT risk factors present in the technologies, systems and procedures used by the Bank. Experts in the area recommend that IT risk present in Banks must be identified and managed well to reduce these impacts.

Various research studies have looked at the IT risk and risk management, but these studies had many limitations.

Most of the studies were reported from developed countries and hence conclusions cannot be generalized. Comprehensive and validated measures of IT risk and risk management were rarely used in these studies. The results were not validated across different bank characteristics and technology characteristics. Also, linkages among IT risk, IT risk management and its financial and non-financial impacts were generally overlooked. No major research work on this theme was reported from India though India though India has various types of Banks and a large customer base.

Motivation for this research was derived from these limitations. The major objective of this research was to obtain a better understanding of IT risk and IT risk management by identifying the themes that characterize them and link these constructs to the financial impacts and non-financial impacts of the risks. After the analysis of data the researcher could come out with some valuable information with regard to these constructs and their inter-linkages.

## 10.2 Major Findings

The research was initiated with specific objectives such as to study the nature of IT risk and risk management in banks, to explore the link between IT risk and IT risk manage and to develop a model linking IT risk and IT Risk management to its impacts (financial and non-financial). The major findings with respect to these objectives are discussed below.

### 10.2.1 Developing insights and reliable measures for IT risk and risk management

IT risk was seen to be a multidimensional construct. IT risk could not be directly observed but was indirectly measured through a series of indicators. The indicators were picked up from Basel and RBI guidelines for operational and technology risk management recommendations and guidelines. These indicators were divided into a seven factor structure namely internal fraud, external fraud, employment practices and work place safety, clients products and business practices, damage to physical assets, business disruption and system failures and execution, delivery and process management.

The study also developed a validated measure of IT risk in banks in the Indian context. The researcher followed the accepted procedures in instrument development. Scales were developed for each of these risk dimensions. Various validity and reliability tests were conducted to finalize the instrument. Confirmatory Factor Analysis was used on the final data to confirm the risk factor structure that emerged from the exploratory factor analysis on the pilot data. A second order factor model was hypothesized for risk construct which was positively tested using structural equation modelling. This was in line with the findings of Wallace (1999).

The second construct used in the study namely IT risk management also was subjected to rigorous analysis. There were no validated measures readily available for IT risk management constructs. The indicators for IT Risk management were picked up from RBI guidelines on Information Technology risk management in banks, Basel recommendations, NIST

reports, security guidelines, audit manuals, previous research work and from experts in the field. After a series of validity and reliability tests, a nine factor structure emerged for risk management. The factors were policies and procedures, data security, access control and authentication, system logs and audit, backup and recovery, monitoring systems, software development and deployment, physical security and network security. The nine factor structure was confirmed through Confirmatory Factor Analysis.

### 10.2.2 Exploring the link between bank characteristics and IT risk, IT risk management and impacts.

A series of ANOVA tests showed that IT risk scores varied significantly across categories of the bank characteristics, namely: type of the bank, geographical spread, software development methodology, level of automation, training provided to employees and the data center model used. These findings were generally in agreement with literature. Regression models were developed for each IT risk, risk management and impacts linking it to bank characteristics The models defined how each risk and risk management dimension was influenced by bank type, geographical spread and other technology characteristics.

### 10.2.3 Model linking IT risk and IT risk management and impacts

The research explored a model linking IT risk and risk management to each of the impacts namely nonfinancial and financial impacts. The linkages among IT risk, risk management and impacts were explored through testing of various models. The first model was a basic regression model where the financial and nonfinancial measures were linked only to the IT risk dimensions. Financial and nonfinancial variables were taken as

the dependent variable with the IT risk as independent variable. All models were statistically significant.

The second model had IT risk management linked to financial and nonfinancial impacts directly. This model was tested with structural equation modelling. The analysis showed that IT risk management had a direct link (negative correlation) with financial and nonfinancial impacts.

### 10.2.4 Summary of Findings

a) Internal and external frauds were reported as very low compared with other IT risk categories

b) IT risks in public sector banks were found to be low when compared to other bank groups.

c) Cooperative banks reported highest IT risks in almost all categories and the IT risks, IT risk management, financial impacts and nonfinancial impacts for cooperative banks differs significantly when compared with other bank groups

d) Access control and authentication and physical security were found very high among all categories of IT risk management categories

e) Financial impacts differ significantly between different bank groups

f) IT risk, IT risk management, financial impact and nonfinancial impact in banks operating in single state were significantly different from banks operating in multiple states and multiple countries.

g) Financial impact was found to be less, if the software development methodology chosen was in house

h) IT risk, IT risk management, financial impact and nonfinancial impact in banks with high level of automation were significantly different from banks with medium and low level of automation.

i) IT risk and IT risk management differ significantly for banks that provided training once a year and that provided training thrice a year.

j) IT risk management was significantly different between public and private sector banks

k) Financial impact differed significantly between public and private sector banks

l) Findings of this study supported the alternate hypotheses that,

There is a significant positive relationship between IT risk with financial impacts and nonfinancial impacts.

There is a significant negative relationship between IT risk management and its financial and non-financial impacts.

## 10.3 Research Contribution

Based on the gaps identified from the review of literature this study explored the IT risks, IT risk management and its impacts on Indian banks.

The study could fill the gap in the academic literature by contributing information about the IT risk and risk management practices in different types of Indian banks and its impacts.

### 10.3.1 Implications for Practice

Banks across the globe are faced with the IT risks and consequent financial and nonfinancial losses. Risks or failure in on bank can cause failures in other banks as well as the financial system of the country in a systemic risk. Proper identification of technology and operational related risks present in the bank and deploying appropriate risk management strategies can reduce the financial and nonfinancial impacts in any bank.

The study has also provided a detailed list of risk management controls that risk managers can use for controlling and mitigating IT risks in Banks. Current Basel and RBI recommendations only focus on financial losses/impacts of the IT risk. This study has also provided an insight into the nonfinancial impacts of IT risks in banks.

a) Study of the linkages between the IT risks and its financial and nonfinancial impacts can help CIOs to identify and choose the right implementation strategies to achieve the desired outcome (ie. reduced financial or non-financial losses to the bank).

b) Category wise IT risk profiles help banks to identify the areas of concern (IT risks) and to implement proper IT Risk Management controls to reduce those risks and impacts

c) Insights into IT risk levels, variations and linkages based on bank types, areas of operation, etc help regulators (central banks) to formulate IT risk management policies and regulatory guidelines

d) Cooperative banks all over the country are in the early stages of implementing core banking systems and other online banking systems. Significant variations in IT risk, IT risk management and impacts in cooperative banks shows the need for special attention by the cooperative bank management and the RBI

e) The findings of the study could be used by practicing risk managers in banks to implement better risk management

f) The IT risk landscape keep changing over time, so banks and RBI needs to do regular evaluation of IT risks, risk mitigating measures and impacts of banks in India, to prevent and reduce any damage to the financial system in the country

Co-operative banks are in the initial phases of implementing large and complex core banking systems to cater to the customer needs and to achieve a competitive position in the market. The lower technical knowledge of the co-operative sector management, use of smaller and non-competitive outsourced companies for implementing the core banking systems, localized data centers without necessary security and backups, lack of DR sites, lack of customer awareness, lack of employee training and knowledge in using and following the industry standard risk management controls are some of the major reasons or increased risk exposure.

Some of the suggestions for improving the situation are as follows.

- The state can provide a data center facility with all required infrastructure and security matching industry standards.
- Co-operative sector banks can share and use this facility to deploy and maintain their IT systems. Which will also reduce the IT costs.
- Frequent IT risk and Risk Management training for employees to make them aware of the threats. This can be organized by the Co-operative departments
- IT Audits – to ensure proper development, deployment and maintenance of IT systems

## 10.4 Scope for Future Research

This study provided a good review of the existing research work on IT risk and IT risk management strategies. Various models linking IT risk, IT risk management and impacts were also reviewed and compared. This gives a strong theoretical foundation for future academic research.

This study developed and empirically tested two measurement models: one for IT risk and the other for IT risk management. These measures were grounded in both practice and theory. These measurement instruments identified the most prevalent IT risk items in banks and IT risk management techniques which can be used to counter these risks. The existence of validated and reliable measures will enable numerous future researchers to approach these constructs from the same perspective.

The study made extensive use of statistical techniques for developing and testing theories. These statistical techniques were explained in details so as to help new researchers to apply these tools in their research.

The study demonstrated that IT risk varied across different type of banks. But more focused research work needs to be done in modelling IT risk and identifying appropriate IT risk management strategies for each of the categories. This knowledge could further assist banks to tailor their IT risk management strategies more appropriately.

Similar studies could be conducted in banks of other countries and also on other type of organizations which extensively depend on Information Technology for their businesses. Other risk mitigation techniques like insurance, outsourcing etc. and their relationships with IT risk and its impacts can also be studied further.

Research studies are exposed to inherent limitations while exploring, describing or explaining a phenomena, depending upon the nature of the research. More detailed studies can be conducted eliminating these limitations of the present study as shown below.

- Technology, technology related risks and its control mechanisms constantly evolve and change. Hence new researches can be done capturing every possible aspect of these constructs and latest changes in those studies.

- Basel and RBI guidelines were used as the sample frame for this study. Researchers can study possible extension to other financial institutions that does not come under the regulatory controls of RBI.

- A more detailed research can be done using multiple respondents or informants.

## 10.5 Conclusion

IT risks and losses have become the major concern for banks and regulatory authorities all over the world. However, the study on IT risk, risk management and impacts with respect to banks was not easy. Lack of published material in the Indian context was the first challenge. This was overcome by the use of international literature and expert opinion. Data collection posed the next major challenge. The delicacy of revealing IT related information and opinion posed a major hurdle. The senior management of the organization had to be taken into confidence with regard to the confidentiality and the strictly academic nature of the study. The participating banks were promised a consolidated report of the research.

The study has identified major IT risk and IT risk management factors in the Indian context. Models grounded in theory are developed and empirically validated. The findings of the study could be used by practicing risk managers in banks for better risk management. The models developed in this research can be refined and improved further by future researchers. The objectives laid down in the beginning of the research could be finally achieved to a high degree of satisfaction. As in all research, this work too has its limitations mentioned earlier.

This research was a very important learning experience for the researcher. Though the researcher had practical exposure to IT systems and implementation in banks for thirteen years, this research has brought in

new dimensions to his understanding of IT risk and IT risk management. Also, this work has helped the researcher to appreciate the role and application of research methodology in management research.

# References


[1] ACFE, 2012. *Report to the Nation on Occupational Fraud and Abuse,* s.l.: Association of Certified Fraud Examiners.

[2] Ahmad, A. & Abu-Musa, 2004. *Investigating the security controls of CAIS in an emerging economy An empirical study on the Egyptian banking industry,,* s.l.: Department of Accounting and MIS, College of Industrial Management, King Fahd University of Petroleum and Minerals, SA.

[3] Albert, C., 2009. *Computer and Information Security Handbook.* s.l.:Morgan Kaufmann Publications, Elsevier Inc. P. 232.

[4] Anand, S., 2009. *Improving Information Security Risk Management,,* s.l.: The University of Minnesota.

[5] Anass, B., Stephen, F. & Liezel, C., 2013. *Valuing Information Technology (IT) and Operational Risk Management.* s.l., s.n., pp. 20 -23.

[6] Anderson, J. & Gerbing, D., 1979. Structural Equation Modelling in Practice: A Review and Recommended Two –Step Approach. *Psychological Bulletin 103(3),* pp. 411-423.

[7] Anderson, R., 2001. *Security Engineering.* s.l.:Wiley.

[8] Ans, S., 2008. *Managing IT Related Operational Risks,* s.l.: Communications, ICT College, Belgrade.

[9] Arunkumar, R. & Kotreshwar, G., 2006. *Risk Management in Commercial Banks (A Case Study of Public and Private Sector Banks),* s.l.: s.n.

[10] ATIS, 2012. *ATIS Telecom Glossary 2012 - Audit Trail.* s.l.:ATIS Committee PRQC.

[11] Banable Frontier Associates, 2008. *Managing the Risk of Mobile Banking Technologies,* s.l.: s.n.

[12] Barki, H., Rivard, S. & Talbot, J., 1993. Toward an Assessment of Software Development Risk.. *Journal of Management Information Systems 10(2),* pp. 203-225.

[13] Barve, J., 2013. *COBIT Case Study: IT Risk Management in a Bank.* [Online] Available at: http://www.isaca.org/knowledge-center/cobit/pages/cobit-case-study-it-risk-management-in-a-bank.aspx.

[14] Basel Committee, 2001b. *Consultative document: operational risk,* s.l.: The Bank for International Settlements.

[15] Basel Committee, 2002b. *Overview paper for impact study.,* s.l.: Bank for International Settlements.

[16] Basel Committee, 2002c. *About the Bank for International Settlements, Basel,* s.l.: The Bank for International Settlements.

[17] Basel Committee, 2004. *International convergence of capital measurement: A Revised Framework,* s.l.: The Bank for International Settlements.

[18] Basel, 2005. *Compliance and the compliance function in Banks,* s.l.: BCBS.

[19] BCBS, 2001a. *The new Basel Capital Accord: an explanatory note,* s.l.: The Bank for International Settlements.

[20] BCBS, 2001c. *Working paper on the regulatory treatment of operational,* s.l.: The Bank for International Settlements.

[21] BCBS, 2001d. *Sound practices for the management and supervision,* s.l.: The Bank for International Settlements.

[22] BCBS, 2002. *Operational Risk Data Collection Exercise - 2002,* s.l.: Bank for International Settlements.

[23] BCBS, 2002a. *Sound practices for the management and supervision,* s.l.: The Bank for International Settlements.

[24] BCBS, 2003. *Risk Management Principles for Electronic Banking,* s.l.: s.n.

[25] BCBS, 2003a. *Sound practices for the management and supervision,* s.l.: The Bank for International Settlements.

[26] BCBS, 2003b. *The New Basel Capital Accord consultative document.,* s.l.: The Bank for International Settlements.

[27] BCBS, 2005. *Compliance and Compliance Function in Banks,* s.l.: Basel Committe on Banking Supervision.

[28] BCBS, 2011. *Operational Risk – Supervisory Guidelines for Advanced Measurement Approaches,* s.l.: s.n.

[29] BCBS, 2013. *Revised International Framework,* s.l.: Basel (BIS).

[30] Bentler, P. & Bonett, D., 1980. Significance Tests and Goodness of Fit in the Analysis of Covariance Structures.. *Psychological Bulletin 88,* pp. 588 -606..

[31] Bessis, J., 1998 . *Risk Management in Banking.* New York: John Wiley and Sons.

[32] Bohrnstedt, G. W., 1983. *Measurement, Handbook of Survey Research.* San Diego: Academic Press INC.

[33] Boran, S., 2003. *IT Security Cook Book.* s.l.:Boran Consulting.

[34] Boyer, K. & Verma, R., 2000. Multiple raters in survey-based operations management research. *Production and Operations Management 9 (2),* pp. 128-140.

[35] Bruce, L., 2003. *Information Security - Key issues and developments.* [Online] Available at: www.pwcglobal.com/jm/fig/information security risk.pdf

[36] BS OHSAS, 2007. *OHSAS 18001,* s.l.: British Standards, BS OHSAS, 18001.

[37] Carmines, E. & Zeller, R., 1990. *Reliability and Validity Assessment.* s.l.:Sage Publications, USA.

[38] Carmines, E. & Zeller, R., 1990. *Reliability and Validity Assessment.* USA: Sage Publications.

[39] Chakrabarty, D. K. C., 2013. *Financial Fraud.* Delhi, National Conference on Financial Fraud, ASSOCHAM.

[40] Charette, R. N., 1996. *Software Engineering Risk Analysis and Management.* s.l.:McGraw-Hill Software Engineering Series.

[41] Chin, W. & Todd, P., 1995. On the use, Usefulness, and Ease of Use of Structural Equation Modelling in MIS Research: A Note of Caution. *MIS Quarterly 19(2),* p. 237 – 246.

[42] Churchill, 1979. A Paradigm for Developing better measures of Marketing Constructs. *Journal of Marketing Research,* pp. 16, 64 – 73.

[43] CISA, 2006. *Review Manual,* s.l.: Certified Information Systems Auditor.

[44] CISCO, 2012. *What is Network Security.* [Online] Available at: http://www.cisco.com/cisco/web/solutions/small_business/resource z_center/ articles/secure_my_business/what_is_network_security/index.html

[45] CNSS, 2010. *Instruction No 4009,* s.l.: Committee on National Security Systems, USA.

[46] Committe on Computer Audit, RBI, 2001. *Check List for IS Audit,* s.l.: RBI, DBS, CO.

[47] Committee on National Security Systems, 1996. *National Information Assurance Glossary.* s.l.:Committee on National Security Systems.

[48] Computergram Weekly, 2003. SAS Survey Shows Companies Hit by Operational Risk. 10 9, p. No. 4752.

[49] Cronbach, L., 1951. Coefficient Alpha and the Internal Structure of Tests. *Psychometrica 16(3),* p. 297 – 334.

[50] Davis, E., 2009. *Loss Data Collection and Modelling,* s.l.: Operational Risk: Practical Approaches to Implementation, London: Risk Books.

[51] Dedolph F, M., 2003. The Neglected Management Activity: Software Risk Management.. *Bell Labs Technical Journal 8(3),* p. 91–95.

[52] Deephouse, C., Mukhopadhyay, T., Goldenson, D. R. & Kellner, M. I., 2005. Software Processes and Project Performance. *Journal of Management Information Systems (Winter 1995-96) 12(3),* pp. 185-203.

[53] Deloitte, 2013. *A Global Survey,* s.l.: Deloitte Touche Tohmatsu Limited (DTTL).

[54] Dictionary of Computing, 1996. *Disctionary of Computing, Fourth Ed..* s.l.:Oxford University Press.

[55] DLA Piper, 2014. *Data Protection Laws of The World.* s.l.:DLA Piper.

[56] Edin, O. & Sejfudin, Z., 2013. *Perception of Information Security of Management of Banking and Insurance Companies in Countries of Western Balkans,* s.l.: Macro Think Institute.

[57] Ernst & Young, 2010. *The Top 10 Risks for Business,* s.l.: Ernst & Young.

[58] Ernst & Young, 2011. *Insights on IT Risks,* s.l.: Ernst & Young.

[59] Federal Reserve, 1995. *Rating the Adequacy of Risk Management Processes and Internal Controls - ,* Washington DC: Federal Reserve System - SR 95-51 SUP.

[60] FIPS PUBS, 2010. *Federal Information Processing Standards Publications (FIPS PUBS),* http://www.nist.gov/itl/fips.cfm: NIST, US Department of Commerce.

[61] Fleischmann, V. S. a. M., 2011. IT Risk Management in Banking Industry. *ACTA OECONOMICA PRAGENSIA.*

[62] Garcia, M. L., 2007. *Design and Evaluation of Physical Protection Systems.* s.l.:Butterworth-Heinemann pp. 1-11.

[63] Garg, A., Curtis, J. & Halper, H., 2003. *Quantifying the financial impact of IT security breaches,* s.l.: Information Management and Computer Security, Vol. 11, No2, pp 74.

[64] Habib Bank AG Zurich, 2010. *Risk Control Matrix V4.5,* s.l.: HBZ IT.

[65] Hair, J., Anderson, R., Tatham, R. & Black, W., 1998. *Multivariate Data Analysis.* New Jersey, USA: Prentice-Hall International.

[66] Hair, J., Anderson, R., Tatham, R. & Black, W., 1998. *Multivariate Data Analysis.* New Jersey, USA: Prentice-Hall International.

[67] Hansson, S. O., 2012. *The Stanford Encyclopedia of Philosophy.* s.l.:Edward N Zalta (ed).

[68] Hatcher, L., 1994. A Step by Step Approach to Using the SAS System for Factor Analysis and Structural Equation Modelling. *Cary NC: SAS Institute Inc.*.

[69] Hoffer, J. & Straub, D., 1989. *The 9 to 5 undergound: are you policing computer crimes?,* s.l.: Sloan Managmenet Review, Vol 30, No.4, pp.35-43.

[70] Homolya, D., 2011. *Operational risk of banks and firm size,* s.l.: , Institute of Finance and Accounting, Department of Finance, Corvinus University of Budapest, .

[71] Hood, K. & Yang, J.-W., 1998. *Impact of banking information systems security on banking in China: the case of large state-owned banks in Shenzhen economic special zone – an introduction,* s.l.: Journal of Global Information Management, Vol. 6 No. 3, pp. 5-15..

[72] Hussain, A., 2000. *Managing Operational Risk in Financial Markets.* Oxford: Butterworth Heinemann.

[73] IBM, 2013. *Data Security and Privacy.* [Online] Available at: http://www-01.ibm.com/software/data/security-privacy/[Accessed 2013].

[74] Information Security Forum, 2007. *The Standard of Good Practice,* s.l.: Information Security Forum.

[75] Information Security Forum, 2013. *Standard of Good Practice for Information Security,* s.l.: Information Security Forum.

[76] Infosys, 2012. *Needed, A Holistic Approach to Reputation Risk Management in Banks - Thought Paper,* s.l.: Infosys.

[77] Institute of International Finance and EY, 2013. *Fourth Annual Survey on Banking Risk Management,* s.l.: Ernst & Young.

[78] ISACA, 2006. *CISA Review Manual 2006,* s.l.: ISACA p 85.

[79] ISACA, 2007. *CISA Review Manual,* s.l.: ISACA.

[80] ISACA, 2009. *The Risk IT Framework.* s.l.:ISACA.

[81] ISO/IEC 17799, 2005. *Information technology - Security techniques - Code of practice for information security management,* s.l.: National Research Council.

[82] ISO/IEC 27002, 2005. *Information Technology – Security Techniques – Code of practice for information security management,* s.l.: ISO/IEC.

[83] ISO/IEC FIDIS, 2008. *Information Tehnology - Security Techniques - Information Security Risk Management,* s.l.: ISO/IES FIDIS 27005:2008.

[84] ITGI, 2007b. *IT control objectives for Basel II: The importance of governance and risk management for compliance,* s.l.: Rolling Meadows - IT Governance Institute.

[85] J¨oreskog, K. & S¨orbom, D., 1996. Structural equation modeling with the SIMPLIS command language. *Scientific Software International.*

[86] Jochum, C., 2006. *IT risk management in the banking industry,* s.l.: s.n.

[87] Kanchu, T. & Manoj Kumar, M., 2013. *Risk Management In Banking Sector - An Empirical Study,* s.l.: Internatiional Journal of Marketing, Financial Services & Management Research Vol 2.

[88] Kaplan, R. & Scauzzo, D., 1993. *Psychological Testing: Principles, applications and issues.* CA: Pacific Grove.

[89] Kaspersky Lab, 2011. *Global IT Security Risks,* s.l.: s.n.

[90] Kaspersky Lab, 2011. *Gobal IT Security Risks,* s.l.: s.n.

[91] Katsicas, S. K., 2009. *Computer and Information Security Handbook.* s.l.:Morgan Kaufmann Publications. Elsevier Inc. p. 605.

[92] Kim, E. & Muller, R., 1998. IC-Processed Piezoelectric Microphone. *IEEE Electr. Dev. Letters, 8, 467-468.*

[93] Kros, J., Foltz, C. & Metcalf, C., 2004. *Assessing and Quantifying the loss of network intrusion,* s.l.: Journal of computer Information Systems, Vol 45, No.2, pp.36-43.

[94] Laker, J. F., 2006. *The Evolution of Risk and Risk Management – A Regulators Perspective,* s.l.: Chairman's Speech, Australian Prudential Regulatory Authority. September.

[95] Lynda, 2012. *Physical Security Assessment,* s.l.: SAIC.

[96] 'Management of Non-Financial Risks' by Bank for International Settlements (Central Bank Governance Group, 2009)

[97] Marco, M. & Giovanni, M., 2008. *Reputational Effects of Operational Risk Events for Financial Institutions,* s.l.: University of Cagliari, Itali.

[98] Marshall, C., 2001. *Measuring and Managing Operational Risk in Financial Institutions.* Singapore: John Wiley & Sons.

[99] Marshall, J. & Haffes, E., 2003. *Study Faults Bank Risk Management.* s.l.:Financial Executive, Vol 19, No 9.

[100] Martina, H., 2014. *Non Financial Risk,* s.l.: University of Economics.

[101] Mercy, 2011. *A PROJECT REPORT ON REPUTATION RISK MANAGEMENT IN INDIA,* s.l.: Risk-Pro Professionals.

[102] Michael, P. & Blaize, H. R., Spring, 2009. Governing Information Technology Risk University of California. *California Management Review.*

[103] Microsoft, 2006. *Information Security Controls - Security Risk Management Guide,* s.l.: Microsoft.

[104] Microsoft, 2013. *Access Control.* [Online] Available at: http://msdn.microsoft. com/en-us/library/windows/desktop/aa374860%28 v=vs.85%29.aspx [Accessed 2013].

[105] MITS, 2013. *Operational Security Standard: Management of Information Technology Security.* [Online] Available at: http://www.tbs-sct.gc.ca/pol/ doc-eng.aspx?id=12328&section=text [Accessed 2013].

[106] Monetary Authority of Singapore, 2002. *Technology Risk Management Guidelines for Financial Institutions,* s.l.: s.n.

[107] Monetary Authority of Singapore, 2013. *TRM Guidelines,* s.l.: Monetary Authority of Singapore.

[108] Moore, G. C. & Benbasat, I., 1991. Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. *Information Systems Research 2(3),* pp. 192-222.

[109] Moore, J. H., 1979. A Framework for MIS Software Development Projects. *MIS Quarterly 3(1),* p. 29 – 38.

[110] Neale, J. & Liebert, R., 1986. *Science and Behaviour: An Introduction to Methods of Research.*. New Jersey: Prentice – Hall International Inc.

[111] NIATEC, 2014. *NIATEC Glossary Of Terms.* s.l.:National Information Assurance Training and Education Center ( http://niatec.info/Glossary.aspx).

[112] NIST SP 800-26, 2002. *Security Self Assessment Guide for Information Technology Systems,* s.l.: NIST.

[113] NIST SP 800-30, 2002. *Risk Management Guide for Information Technology Systems,* s.l.: National Institute of Standards and Technology, US Department of Commerce.

[114] NSTISSI, 2012. *Security Instruction No 1000,* s.l.: National Security Telecommunications and Infomration Systems Security Instruction.

[115] Nunnally, J., 1978. *Psychometric Theory.* New York: McGraw – Hill.

[116] OGC, 2010. *Management of Risk, Guidance for Practitioners,* s.l.: Office of the Government Commerce.

[117] OMB, 2000. *CIRCULAR NO. A-130 Revised (Management of Federal Information Resources),* http://www.whitehouse.gov/omb/circulars_a130_ a130trans4: Office of the Management and Budget.

[118] Önal, M. Z., 2008. *An Aggregated Information Technology Checklist for Operational Risk Management,* https://www.bddk.org.tr/ WebSitesi/ turkce/Raporlar/BDDK_Dergi/4214Makale-3.pdf: BDDK Bankac›l›k ve Finansal Piyasalar.

[119] Pavel, N. & Simona, F., 2013. *Implications of The Operational Risk Practices Applied In the Banking Sector on the Information Systems Area,* s.l.: The Bucharest University of Economic Studies, Romania.

[120] Pinder, J., Wilkinson, S. J. & Demack, S., 2003. *A Method for Evaluating Workplace Utility. Property Management 21(4), 218 – 229.* s.l.:s.n.

[121] Pinsonneault, A. & Kraemer, K., 1993. The Impact of Information Technology on Middle Managers. *MIS Quarterly 17(3),* pp. 271-292..

[122] Pinsonneault, A. & Kraemer, K., 1993. The Impact of Information Technology on Middle Managers. *MIS Quarterly 17 (3)*, pp. 271-292.

[123] PWC, 2013. *Technology Risk Management,* s.l.: s.n.

[124] Radford, 1978. *The Journal of Operational Research Society Vol 29(7),* pp. 677-682.

[125] Ramanathan, H., 2014. Banking Risk. *Banking Journal,* pp. 23-25.

[126] RBI , 2011. *Report of the Working Group on Electronic Banking,* s.l.: Reserve Bank of India.

[127] RBI , 2013. *RBI Guide Lines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds,* Mumbai: Reserve Bank of India, Department of Banking Supervision.

[128] RBI Guidelines, 2012. *Information Systems Audit Policy for Banking and Financial Sector,* s.l.: Reserve Bank of India.

[129] RBI List of Banks, 2013. *Banks in india.* [Online] Available at: http://www.rbi.org.in/commonman/English/scripts/banksinindia.aspx [Accessed 2013].

[130] RBI, 1998. *Framework for Internal Control Systems in Banking Organisations,* s.l.: RBI.

[131] RBI, 2005. *Guidance on Management of Operational Risk,* Mumbai: RBI.

[132] RBI, 2010. *Guidelines on The Standardised Approach for Calculating Operational Risk Capital Charge,* s.l.: RBI.

[133] RBI, 2011. *Report of the Working Group on Electronic Banking,* http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111_C2.pdf: RBI.

[134] RBI, 2011. *Report of Working Group on Information Security,* s.l.: Reserve Bank of India.

[135] RBI, 2013. *Risk Management Systems in Banks.* [Online] Available at: http://rbidocs.rbi.org.in/rdocs/notification/PDFs/9492.pdf [Accessed 2013].

[136] RBI, 2013. *Security and Risk Mitigation Measures for Electronic Payment Transactions,* s.l.: Reserve Bank of India.

[137] Rechards, H., 2001. *Supervision of IT Risks,* s.l.: Federal Reserve Board.

[138] Reputational Risk in Banking – The Current Approach and A Way Ahead, Sumit K Dev, TCSBNCS, 2013

[139] Romero, A., 2005. *Oracle Database Backup and Recovery Basics,* s.l.: Oracle.

[140] Roopadarshini, S. & Shilpa, S., 2014. *A Study on Impact of Information Technological Innovation in Present Banking Scenario,* s.l.: K.S.School of Engineering and Management, Bangalore.

[141] Rot, A., 2009. Enterprise Information Technology Security. *Risk Management Perspective Proceedings of the World Congress on Engineering and Computer Science, WCECS 2009 , San Francisco, USA,* pp. 20-22.

[142] Sartaj, H., 2013. *Management of Operational Risk In J&K Bank Limited,* s.l.: University of Kashmir.

[143] Semantec, 2007. *IT Risk Management Report,,* s.l.: Semantec, Vol 1.

[144] Simmonds, A., Sandilands, P. & Van Ekert, L., 2004. An Ontology for Network Security Attacks, Lecture Notes in Computer Science. In: s.l.:s.n.

[145] Smith, H., 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly 20(2),* p. 167 – 196.

[146] Solarwinds, 2013. *IT Security Checklist - 9 Key Recommendations,* http://www.solarwinds.com/resources/whitepaper/it-security-checklist-9-key-recommendations.html: Solarwinds.

[147] Straub, D., 1995. Validating Instruments in MIS Research. *MIS Quarterly 13(2),* p. 146 – 169.

[148] Study of Impact of Mobile Devices on Information Security: Dimensional Research Group, June 2013,

[149] Sureshchander, G., Rajendran, C. & Anantharaman, R., 2001. A Holistic Model for Total Quality Service. *International Journal of Service Industry Management 12,* p. 378 – 412.

[150] Swanson, M., 2001. *Security Self Assessment Guide Information Technology Systems,* http://infohost.nmt.edu/~sfs/Regs/sp800-26.pdf: NIST.

[151] Taylor, S. & Todd, P., 1995. Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research 6(2),* p. 144 – 176.

[152] The Govt of Hong Kong, 2009. *Security Risk Assessment and Audit Guidelines,* s.l.: The Govt of Hong Kong.

[153] The Journal of Risk Finance, 1999. *Banks' risk management: a comparison study of UAE national and foreign banks,* s.l.: Emerald.

[154] The rising costs of non-compliance: From the end of a career to the end of a firm. Stacey English & Susannah Hammond, 2013

[155] Unites States Congress, 1987. *Computer Security Law of 1987,* s.l.: US Congress.

[156] US Department of Army, 2001. *Physical Security - Systems Approach ( Fiield Manual ).* s.l.:US Department of Army.

[157] US Department of Army, 2001. *Physical Security Challenges - Field Manual - Chapter 1.* s.l.:United States Department of Army.

[158] US Federal Law, 1974. *Privacy Act of 1974,* s.l.: US Fedaral Law.

[159] Vilhelm, B. & Frida, W., 2004. *A case study of major Swedish banks concerning the concept of information risk management,* s.l.: School of Economics and Commercial Law, Goteborg University.

[160] Vlasta Svatá, M. F., 2011. IT Risk Management in Banking Industry. *Advanced Online Publication (AOP 1 9 ( 3 ), 2 0 11, ISSN 0572-3043),* p. 60.

[161] Wallace, L., 1999. *The development of an instrument to measure software project risk,* s.l.: Thesis.

[162] Wallace, L., Keil, M. & Rai, A., 2004. Understanding Software Project Risk A Cluster Analysis. *Information and Management 42(1),* p. 115 – 125.

[163] Woo, T. Y. C., 1992. Authentication for Distributed Systems. *IEEE Computer, Vol 25.*

[164] Yogieta, S. M., 2011. *Operational Risk Management In Indian Banks : Impact of Ownership and Size on Range of Practices for Implementation of Advanced Measurement Approach,* s.l.: University of Delhi.

.....ൠ.....

# Appendix

**1. Copy of authorization letter -**

(from the department given to the bank/respondent for data collection)

School of Management Studies
Cochin University of Science and Technology

CUSAT P.O., Kochi – 682 022
Phone – 0484 2575310/5096 Fax – 0484 2575492

**To**

Dear Sir/Madam,

**Mr. Anil Kumar P**, **M. Tech**., is a doctoral scholar researching in the area of **Information Technology Risk Management in the Indian Banking Industry**, under the guidance of **Dr. Jagathy Raj M.Tech, MBA, PhD (IIT Kharagpur), Professor, School of Management Studies, CUSAT, Kochi**. This study on '**Information Technology(IT) Risk Management in Indian Banks**', aims at understanding the existing IT Risks and IT Risk Management practices among Indian banks and tries to bring out a framework for effective IT Risk Management in Banks.

I request you to kindly provide your valuable responses in the attached questionnaire and help him to successfully complete the survey. The information provided by you as part of this survey and/or interview, will be **used *ONLY* for academic purpose and will be kept confidential**.

Thanking You,
Yours Faithfully

Date: **Dr. Jagathy Raj V. P.**
CUSAT, KOCHI

**2. Copy of the instrument used for the data collection with a covering letter**

**Anil Kumar P.** M. Tech
Research Scholar
School Of Management Studies E-mail: **anildfs@gmail.com**
CUSAT, Kochi, Kerala, India Mobile: 9645420888, 9946356641

Dear Sir/Madam,

I am a doctoral scholar researching in the area of **Information Technology Risk Management in the Indian Banking Industry**, under the guidance of **Dr. Jagathy Raj M.Tech, MBA, PhD (IIT Kharagpur), Professor, CUSAT, Kochi**. This study on '**Information Technology(IT) Risk Management in Indian Banks**', aims at understanding the existing IT Risks and IT Risk Management practices among Indian banks and brings out a framework for effective IT Risk Management in Banks.

Ten Senior Executives from the banking industry, risk management and information technology domain evaluated the intrusive nature of the questions in the questionnaire. In order to encourage active participation of the respondents, ***ONLY* non-intrusive** questions are asked.

I request you, to kindly go through the following questions and **answer all of them**. The information provided by you will be **used *ONLY* for academic purpose and will be kept confidential**.

If you would like to have a copy of the findings, please provide your name and address or email id in the space provided below.

| |
|---|
| **Name :** |
| **Address :** |
| |
| |
| |
| **EMail :** |

**Thank you.**

**Anil Kumar P**

## SECTION A: BANK CHARACTERISTICS

***Please mark your responses with a* checkmark ("√")**

1. **Which of the following best describes your bank?**
   - ☐ Public Sector
   - ☐ Private Sector - Old Generation
   - ☐ Foreign Bank
   - ☐ Private Sector - New Generation
   - ☐ Others, Please specify _____

2. **Which of the following best describes the geographical spread of your bank?**
   - ☐ Single Location
   - ☐ Multiple location, Single State
   - ☐ Multiple Location, Multiple States
   - ☐ Multiple Location, Multiple Countries
   - ☐ Others, Please Specify _____

3. **What is the approximate number of Branches for your Bank**?
   _____

4. **What is the approximate number of Customers in your Bank?**
   _____

5. **What is the approximate number of Employees in your Bank?**
   _____

6. **Is your bank certified in any of the following standards? (tick whichever is applicable)**
   - ☐ ISO 27001 ☐ BS 7799 ☐ Basel II/III ☐ ISO 9001:2000
   - ☐ Others, please specify _____

## SECTION B: TECHONOLOGY CHARACTERISTICS

7. **Which of the following best suits the development methodology used by your Bank to build the Core Banking System?**
   - ☐ Outsourced IS Development
   - ☐ In house developed information system
   - ☐ Shared (Software as a Service Model)
   - ☐ CBS Shared with sister concerns (Banks)
   - ☐ Others, Please specify_____

8. **If outsourced, Please provide the Vendor' Name** _____

9. **What is the level Automation/Batch Processing/STP (Straight Through Processing) currently used in your Bank (Examples: Inter Branch Reconciliation, Inward Remittance, Outward Remittance, Clearing, etc)**

☐ High ☐ Medium ☐ Low

10. **What is the nature of skilled IT man power in your Bank?**

☐ Bank has an in house IT Development Team
☐ Branch Level IT Support Team
☐ Centralized Technical Support Team
☐ Technical Support is provided by external Vendors
☐ Others, Please specify_____

11. **What is the yearly frequency of IT Training provided to your Bank Employees?**

_____ Times/Year

12. **What is the yearly frequency of IT Training provided to your Bank Customers?**

_____ Times/Year

13. **What is the Type of Software used for building the Core Banking System in your Bank?**

☐ Open Source Based (Linux/Java/etc)
☐ Microsoft Based (Windows/.Net/etc)
☐ Both (Open Source and Microsoft based)
☐ Others, Please Specify _____

14. **What is the data center model used for the Core Banking System**

☐ Hosted with third party Data Center ☐ Own Data Center
☐ Hosted in Cloud ☐ Shared data center facility with sister concerns
☐ Others, Please specially_____

## SECTION C: INFORMATION TECHNOLOGY RISKS

**Information Technology Risks (and likely hood)**

***15***. *Using the following scale, please read through the list of statements that follow and indicate with a checkmark ("√") the extent to which each of the following statements accurately applied to your Bank*

| Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

| | STATMENT | Strongly Disagree | | | | Strongly Agree |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| | **INTERNAL FRAUD** | | | | | |
| 15.1 | In my Bank, there is a good chance for employees to intentionally perform *Unauthorized Activities* using the current System | 1 | 2 | 3 | 4 | 5 |
| 15.2 | There are security lapses in the current Banking Systems that allow *employees to perform Theft and/or Fraud* in the Bank | 1 | 2 | 3 | 4 | 5 |
| | **EXTERNAL FRAUD** | | | | | |
| 15.3 | In my Bank, there is a chance for *Theft and/or Fraud by external people* or agencies due to lack of sufficient security in the Banking Systems. | 1 | 2 | 3 | 4 | 5 |
| 15.4 | The security measures in the current system are not sufficient to prevent *attacks by hackers* and protect confidential information of the Bank | 1 | 2 | 3 | 4 | 5 |
| | **EMPLOYMENT PRACTICES AND WORKPLACE SAFETY** | | | | | |
| 15.5 | My bank does not consider employees as assets and does not follow *sound employment practices and labor policies.* | 1 | 2 | 3 | 4 | 5 |
| 15.6 | My Bank is not much concerned about *environment and work place safety and health* | 1 | 2 | 3 | 4 | 5 |
| 15.7 | As part of an organizational culture and/or policy, there are some *discriminations* existing in my Bank. | 1 | 2 | 3 | 4 | 5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **CLIENTS, PRODUCTS AND BUSINESS PRACTICES** | | | | | |
| 15.8 | My bank does not strictly maintain *confidentiality* of customer information, without any disclosures and/or breach of privacy | 1 | 2 | 3 | 4 | 5 |
| 15.9 | My bank follows or allows *improper business or market practices*, like insider trading, money laundering, or unlicensed activities, at times. | 1 | 2 | 3 | 4 | 5 |
| 15.10 | In the current banking system, some of the banking products/modules do still have some *defects and flaws or bugs* | 1 | 2 | 3 | 4 | 5 |
| 15.11 | In my bank, we, the employees of the Bank, does not maintain very *sound and cordial relationship* with each other. | 1 | 2 | 3 | 4 | 5 |
| 15.12 | In my bank, we do not always perform strict**,** *identity check* for our customers or follow all *KYC* norms | 1 | 2 | 3 | 4 | 5 |
| 15.13 | *Client exposures (limits)* are not always strictly checked and validated by the current system and it allows exceptions at times. | 1 | 2 | 3 | 4 | 5 |
| 15.14 | In my bank there are disputes some times over the performance of *advisory activities***.** | 1 | 2 | 3 | 4 | 5 |
| | **DAMAGE TO PHYSICAL ASSETS** | | | | | |
| 15.15 | My bank has a potential chance of being affected by *natural/human disasters* (flood, fire, terrorism, etc) | 1 | 2 | 3 | 4 | 5 |
| | **BUSINESS DISRUPTION AND SYSTEM FAILURES** | | | | | |
| 15.16 | My bank has experienced down times due to *hardware failures* in the last one year | 1 | 2 | 3 | 4 | 5 |
| 15.17 | My bank has experienced down times due to *software failures* in the last one year | 1 | 2 | 3 | 4 | 5 |
| 15.18 | My bank has experienced down times due to *network failures* in the last one year | 1 | 2 | 3 | 4 | 5 |
| 15.19 | My bank has experienced down time due to *Power failures/disruptions* in the past one year | 1 | 2 | 3 | 4 | 5 |
| | **EXECUTION, DELIVERY AND PROCESS MANAGEMENT** | | | | | |
| 15.20 | The current system has reported *issues/errors on data entry, transaction executions and delivery*, at times | 1 | 2 | 3 | 4 | 5 |
| 15.21 | The bank has failed at times in producing *timely and accurate reports* to authorities due to system problems | 1 | 2 | 3 | 4 | 5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 15.22 | The bank does not always complete all the *customer documentations* and stores it securely before start of making transactions | 1 | 2 | 3 | 4 | 5 |
| 15.23 | In my bank**,** *Access to accounts are not restricted* to privileged employees only (level of information access is not strictly based on their profile) | 1 | 2 | 3 | 4 | 5 |
| 15.24 | My bank has incurred losses due to *incorrect, partial and/or missing documentation* | 1 | 2 | 3 | 4 | 5 |
| 15.25 | My bank has incurred losses due to *counter party mis-performance and disputes.* | 1 | 2 | 3 | 4 | 5 |
| 15.26 | There is considerable risk in *outsourcing* the systems and processes to third party vendors. | 1 | 2 | 3 | 4 | 5 |

## SECTION D: INFORMATION TECHNOLOGY RISK MANAGEMENT

***16***. *Using the following scale, please read through the list of statements that follow and indicate with a checkmark ("√") the extent to which each of the following statements accurately applied to your Bank*

| Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

| | STATEMENT | Strongly Strongly Disagree Agree | | | | |
|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | **5** |
| | **POLICIES AND PROCEDURES** | | | | | |
| 16.1 | My Bank has well documented and well implemented *IT Security Policies and Procedures* | 1 | 2 | 3 | 4 | 5 |
| | **DATA SECURITY** | | | | | |
| 16.2 | My bank has used strong cryptography mechanisms for *encryption* of all critical and confidential data for storage as well as for transmission over the network, to prevent any hacking of confidential information. | 1 | 2 | 3 | 4 | 5 |
| 16.3 | There is proper mechanisms for *disposal* of equipments, storage disks, tapes and paper print outs in my Bank | 1 | 2 | 3 | 4 | 5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **ACCESS CONTROL & AUTHENTICATION** | | | | | |
| 16.4 | My bank uses strong *authentication* mechanisms for accessing the systems | 1 | 2 | 3 | 4 | 5 |
| 16.5 | The system uses *two factor authentication* for all important transactions using online channels | 1 | 2 | 3 | 4 | 5 |
| 16.6 | The core banking system in my bank uses *a multi-stage entry and authorize* for all transaction processing | 1 | 2 | 3 | 4 | 5 |
| 16.7 | There is a *clear segregation of duties* to each staff and the staff can only access the data/information permitted to their user profile? | 1 | 2 | 3 | 4 | 5 |
| | **SYSTEM LOGS and AUDIT** | | | | | |
| 16.8 | The current system in the Bank maintains all necessary *logs for any required digital evidence* of successful or unsuccessful transactions | 1 | 2 | 3 | 4 | 5 |
| 16.9 | The current banking system maintains necessary *audit entries* for any system or legal audits | 1 | 2 | 3 | 4 | 5 |
| 16.10 | My bank performs *reconciliation* regularly of all interbank transactions | 1 | 2 | 3 | 4 | 5 |
| 16.11 | My bank performs regular *internal audits* of all their systems, departments and activities | 1 | 2 | 3 | 4 | 5 |
| | **BACKUP and RECOVERY** | | | | | |
| 16.12 | My bank has got sufficient *redundancy and backup* for all hardware, software and network to provide 24/7 system availability | 1 | 2 | 3 | 4 | 5 |
| 16.13 | My bank has got a fully functional and tested *Disaster Recovery* (DR) center and *Business Continuity*(BC) plans implemented | 1 | 2 | 3 | 4 | 5 |
| 16.14 | My bank has well defined *incident response and management* process | 1 | 2 | 3 | 4 | 5 |
| | **MONITORING SYSTEMS** | | | | | |
| 16.15 | My bank has implemented *Transaction Monitoring* systems integrated to the Core Banking System to detect high value or suspicious transactions. | 1 | 2 | 3 | 4 | 5 |
| 16.16 | My Bank has deployed *Intrusion Detection and Prevention* Systems | 1 | 2 | 3 | 4 | 5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 16.17 | My Bank has implemented *protection*(virus scanners and firewalls) *against malicious software*, across the bank | 1 | 2 | 3 | 4 | 5 |
| 16.18 | The bank performs regular *monitoring and review of all system logs* and access logs, and also takes necessary actions on any breaches found. | 1 | 2 | 3 | 4 | 5 |
| | **SOFTWARE DEVELOPMENT & DEPLOYMENT** | | | | | |
| 16.19 | The bank follows the standard principles of *software development and deployment* for all changes and/or new product/service addition to the bank | 1 | 2 | 3 | 4 | 5 |
| 16.20 | My bank maintains the *software source code* in safe custody of the bank or in ESCRO arrangements, if it is outsourced | 1 | 2 | 3 | 4 | 5 |
| 16.21 | In my bank many core banking operations are *centralized* (Example: Account Opening, Loan Approval, etc) | 1 | 2 | 3 | 4 | 5 |
| | **PHYSICAL SECURITY** | | | | | |
| 16.22 | In my bank, the datacenter, branches and ATMs are provided with multiple levels of *physical security* mechanisms (like access controls, human security, camera, etc) | 1 | 2 | 3 | 4 | 5 |
| 16.23 | The datacenter and branches of my bank are equipped with *fire and other environmental controls* like A/C, Power Backup, etc | 1 | 2 | 3 | 4 | 5 |
| | **NETWORK SECURITY** | | | | | |
| 16.24 | My bank network is not connected to any *public network*(internet) from within the branch or data center. (ie Users cannot access internet from their work stations, and send any information/mail to external entities) | 1 | 2 | 3 | 4 | 5 |
| 16.25 | In my bank users are not allowed to bring in their laptops, storage devices, etc to the bank or connect them to the *bank network*. | 1 | 2 | 3 | 4 | 5 |

## SECTION E: NON-FINANCIAL IMPACT OF INFORMATION TECHNOLOGY RISKS

**Non-Financial Impact of Information Technology Risks**

***17.*** *Using the following scale, please read through the list of statements that follow and indicate with a checkmark ("√") the extent to which each of the following statements accurately applied to your Bank*

| Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

| | Statement | Strongly Disagree | | | | Strongly Agree |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 17.1 | In my Bank, the current information system cannot maintain 100% "**Confidentiality**" of all information stored in the Bank Database | 1 | 2 | 3 | 4 | 5 |
| 17.2 | In my Bank, the current information system cannot maintain 100% "**Integrity**" of all information stored in the Bank Database | 1 | 2 | 3 | 4 | 5 |
| 17.3 | In my Bank, the current information system cannot assure 100% "**Availability**" of the system | 1 | 2 | 3 | 4 | 5 |
| 17.4 | I believe that the IT risks prevailing in the current system can affect the **Reputation** of the Bank | 1 | 2 | 3 | 4 | 5 |
| 17.5 | I believe that the IT Risks existing in the current Banking System can cause **non-compliance** which can lead to regulatory Inquiry or Penalty | 1 | 2 | 3 | 4 | 5 |
| 17.6 | The IT Risks existing in the current information system can lead to **Customer Complaints, Account Closure and Customer Loss** | 1 | 2 | 3 | 4 | 5 |

## SECTION F: FINANCIAL IMPACT OF INFORMATION TECHNOLOGY RISKS

**Financial Impact of Information Technology Risks**

***18.*** *Using the following scale, please read through the list of statements that follow and indicate with a checkmark ("√") the extent to which each of the following statements accurately applied to your Bank*

| Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

| | Statement | Strongly Disagree | | | | Strongly Agree |
|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | **5** |
| 18.1 | In the current IT systems used in the Bank, there is chances for financial losses due to *Internal Fraud* | 1 | 2 | 3 | 4 | 5 |
| 18.2 | In the current IT systems used in the Bank, there is good chances for financial losses due to *External Fraud* | 1 | 2 | 3 | 4 | 5 |
| 18.3 | In the current IT systems used in the Bank, there is chances for financial losses due to *Employment Practices and Workplace Safety* | 1 | 2 | 3 | 4 | 5 |
| 18.4 | In the current IT systems used in the Bank, there is chances for financial losses due to *Clients, Products and Business Practices* | 1 | 2 | 3 | 4 | 5 |
| 18.5 | In the current IT systems used in the Bank, there is chances for financial losses due to *Damage to Physical Assets* | 1 | 2 | 3 | 4 | 5 |
| 18.6 | In the current IT systems used in the Bank, there is chances for financial losses due to *Business Disruption and System Failures* | 1 | 2 | 3 | 4 | 5 |
| 18.7 | In the current IT systems used in the Bank, there is chances for financial losses due to *Execution, Delivery and Process Management* | 1 | 2 | 3 | 4 | 5 |

**SECTION G: BACKGROUND INFORMATION OF THE RESPONDENT**

**Background information of the respondent**

19. **How many years of professional experience you have?** _____Years

20. **How long have you been with the present bank?** _____Years

21. **How long have you been in the IT department in your present bank?** _____Years

22. **What is your designation in the present bank?** _____

23. **Do you have any of the following certifications?**

☐ CISA ☐ CISSP ☐ Ce.ISB ☐ DSA (ICAI)

☐ Others, Pls. specify_____

24. **Please use the following space, if you wish to make any comments with respect to the formulation, application or effectiveness of IT Risk Management within your organization**

.

**Anil Kumar P**

.....ꕥ.....

# List of Publication

**[1] STP & Operational Risk Management in Banking Systems**

*International Conference on Information Security in Banking, 20-21st March 2006, Alberain Institute of Management, Kochi.*

**[2] Information Security and Privacy Controls in Banking Systems**

*International Conference on Recent – Trends in Computational Science (ICRTCS-2008)*

*11th-13th Jan 2008, TocH Institute of Science and Technology, Kochi*

**[3] Study of STP and Technology Risk Management in Banking**

*21st Kerala Sciene Congress 2009, 28-31th Jan 2009, Kollam*